Lucent Technologies
Bell Labs Innovations

4ESS™ Switch
Common Channel Signaling Systems
Common Network Interface (CNI)

System Description Manual

234-100-120
Issue 9
March 1998

Notice

Every effort is made to ensure that the document information is complete and accurate at the time of printing. However, information is subject to change.

Trademarks

1A ESS is a trademark of AT&T

4ESS is a trademark of Lucent Technologies

5ESS is a registered trademark of Lucent Technologies

Acculink is a registered trademark of AT&T

CLLI COMMON LANGUAGE is a registered trademark and CLEI, CLLI, CLCI, and CLFI are trademarks of Bell Communications Research, Inc.

DATATEL is a registered trademark of DATATEL Inc.

Star Server is a registered trademark of AT&T

UNIX is a registered trademark of Novell, Inc.

Ordering Information

To order this document and all associated documentation, use one of the following methods:

a. **Lucent Technologies Employees:** Mail or fax Form IND 1-80.80, available from the Lucent Technologies Customer Information Center, by using the following address or fax number.

Note: Lucent Technologies Business Unit/Division and all required billing information must be provided.

Lucent Technologies Customer Information Center
Attention: Order Entry Department
2855 North Franklin Road
P.O. Box 19901
Indianapolis, Indiana 46219-1999
or
Call: 1-888-LUCENT-8 Fax: 1-800-566-9568

b. **AT&T:** Submit orders by calling 1-800-432-6600 or fax orders to 1-800-566-9568.

c. **Local Exchange Carriers (LEC):** Process orders through your Technical Information Resource Management (TIRM) coordinator. If you are unsure of the identity your TIRM coordinator, call 1-888-LUCENT-8.

d. **Federal Government:** Orders must be faxed to the Lucent Technologies Customer Information Center using the following number:

Call: 1-800-566-9568

e. **All Others:** Call: 1-888-LUCENT-8

Developed by:

Lucent Technologies Network Systems Operations/Switching and Access Systems Group.
Lucent Technologies is the successor to the business and assets of AT&T Network Systems business unit.

Contents

Contents

Contents

Figures

1 High Level Description

2 Hardware Description and Functions

3 Signaling Links

Figures

4 Message Flow

5 Measurements, Reports, and Critical Events

Figures

6 Maintenance Guidelines

Tables

Tables

5 Measurements, Reports, and Critical Events

6 Maintenance Guidelines

Tables

Overview

Contents

Overview

General

This document contains the system description and operational information describing Common Network Interface (CNI) equipment as applicable to the 4ESS™ Switch. Thus, CNI features, equipment, and/or applications that pertain to other switching systems are not covered in this manual. Additional information for CNI equipped 4ESS Switch offices is provided in the following documents:

- 234-351-120 — *Common Network Interface Trouble Clearing and Routine Maintenance*
- 234-153-055 — *Common Network Interface Growth*
- AT&T IM-4A001-01 — *4ESS Switch/APS Input Message Manual*
- AT&T OM-4A001-01 — *4ESS Switch/APS Output Message Manual*
- AT&T *4ESS Switch Translation Guide (TG4) Division 12 - CNI Data Management System (DMS).*

Reason for Reissue

This document is reissued to support CNI equipment operating with CNI Software Release 13.4 for the 4ESS™ Switch with the 4E23R1 (4AP16) Generic Program.

Scope

The following briefly describes the content of each Section in this document:

Overview — Provides a description of what is covered in the CNI system description document.

1 **High-Level Description** — Provides a high-level overview and description of the CNI system.

2 **Hardware Description and Functions** — Provides a physical and functional description of the CNI system hardware.

3 **Signaling Links** — Provides a description of Common Channel Signaling No. 7 (CCS7) and D-Channel (DCHN) signaling links.

4 **Message Flow** — Provides a description of how different types of signaling messages are routed by the CNI system application.

5 **Measurements, Reports, and Critical Events** — Lists and defines all measurements, critical events, and fixed format reports provided in the CNI application.

6 **Maintenance Guidelines** — Provides maintenance guidelines and other maintenance related descriptive information.

Notes — Provided for the document user to conveniently make notes.

Glossary — Provides definitions of terms used in this document.

Acronyms and Abbreviations — Provides a list of acronyms and abbreviations used in the text of this document and their definitions.

Index — Provides listings and page numbers of all subjects in this document.

High Level Description

1

Contents

High Level Description

1

General

This section provides a high-level description of the Common Network Interface (CNI) System as equipped for and applicable to the 4ESS™ Switch. The Common Network Interface system abilities and features, system overview, software architecture, system description, system operation, and reliability features are subjects in this section.

Capabilities and Features

The CNI System has the following capabilities and features:

a. High message-handling capacity

b. Terminations for different link types and speeds:

- Unencrypted 56-kb/s links (SS7 only)

c. Reliable system operation software:

- *Fault Recovery* — Automatically attempts system recovery following a hardware fault.
- *Diagnostics* — Analyzes and resolves most faults while identifying suspect circuit packs within a cabinet.
- *System Integrity* — Ensures a working system in the presence of errors and overload conditions.
- *Human Interfaces* — Provides surveillance, control, and maintenance.

d. Measurements: The CNI system is able to collect and report performance measurements and critical event data to facilitate office maintenance, engineering, and administration. Reports can be generated locally and transmitted to remote collection centers. The CNI system provides various reports:
   - Scheduled and demanded reports
   - Total office and link specific reports
   - Generic-defined fixed format and user-defined flexible format reports
   - Real-time notification of CCS network critical events.

e. Software and Hardware Integrity Audits:
   - System Audits
   - Internal data audits on a per-link basis and total office basis
   - Neighbor node hardware audits.

f. Disk and Tape Backup Ability: All file systems, operating software, and data bases can be backed up via disk and/or tape.

g. Initialization: Should faults occur that require reinitialization, the CNI system provides several levels. The first levels do not interrupt normal system operation, but as reinitialization attempts progress, service is interrupted.

h. Incore Function Replacement: Allows the CNI system SLMK and CNIINIT kernel processes to implement the UNIX* System RTR field update mechanism known as "Incore Function Replacement." *Field update* is the method used to install selected software changes at field sites. *Incore function replacement* is a type of field update performed on a running process where the unit of change is a function or specific bytes of data. *Function replacement* modifies a feature and/or data without having to kill and restart the process. This eliminates rebooting the system and creating the process from disk.

i. Maintenance and Fault Recovery: In addition to the reliability features, previously described, the CNI system has tools and facilities for fault detection, isolation, and recovery:
   - Automatic Ring Recovery (ARR) program
   - Ability to isolate faulty sections of the ring and to quarantine single nodes that require maintenance
   - Diagnostics for nodes and links (automatic and demand)
   - Quick ring reinitialization—even in the presence of failures
   - Overload and congestion controls for the ring, nodes, links, and central processor.

* UNIX is a registered trademark of Novell, Inc.

Common Network Interface System Overview

The CNI system is a stored program controlled (SPC) subsystem designed to provide a 4ESS Switch interface, as shown in Figure 1-2, to the Common Channel Signaling (CCS) network. This interface allows the 4ESS Switch to route CCS messages to and receive CCS messages from other switching offices, data bases, and signal transfer points (STPs) within the CCS switching network. The CNI system also allows direct digital connections from customer premise equipment (PBXs, etc.) to the 4ESS Switch.

The CNI system provides the hardware (control nodes, user nodes, etc.) and software (control programs, user node protocols, protocol handling programs, etc.) required to implement the communication functions that are common to all users. The CNI system uses the AT&T 3B Computer as a central processing unit. The central processor interfaces with a community of peripheral processors known as nodes. Nodes are defined as access points on the ring where digital information either enters, exits, or is further processed. The nodes are serially connected in a "ring-type" network by the dual ring. One ring propagates data in the opposite direction of the other ring, which permits ring reconfiguration as part of automatic fault recovery. This redundancy in the ring design is partly responsible for the system's high level of availability.

The following subsystem components are included in the divisions of the CNI system software.

a. 3B Computer UNIX RTR operating system

b. Common Network Interface (CNI) subsystem

c. Interprocess Message Switch (IMS) subsystem

d. Application support subsystem.

All software subsystems are designed to work together so that each subsystem builds upon the lower level. Each subsystem performs some share of the functions necessary to keep the system operational. Lower level software modules provide the basic services necessary for the functions of the higher level software to be perform. Each subsystem is independently partitioned software and possesses characteristics (for example, protocol, maintenance, measurements) unique to a particular system function.

Common Network Interface Software Architecture

UNIX® Real-Time Reliable Operating System

The CNI system 3B Computer central processing unit performs its functions using the UNIX RTR operating system. This system enables applications to meet the high availability demands of real-time processing in telecommunication systems. In addition, the UNIX RTR operating system provides a multi-execution environment for other software subsystems used by the common network interface. This multi-execution environment permits layered CNI and IMS software functions to co-exist as background tasks.

The 3B Computer is primarily responsible for performing processing functions as defined by the 4ESS Switch Attached Processor application software. The CNI/IMS subsystem software is embedded in the Attached Processor application software. This creates an operating environment where the CNI/IMS subsystem software provides the instructions necessary for the 3B Computer to function as the CNI ring central processor while the application software is fulfilling its primary responsibilities as an Attached Processor System (APS).

In addition to CNI/IMS subsystem software being embedded in the Attached Processor application software, the Attached Processor application software must be enhanced to handle administrative, maintenance, and operational functions for the CNI ring. Some 4AP generic CNI ring enhancements include the following:

a. CNI initialization

b. DLN configuration management

c. 3B Computer CNI system display pages

d. CNI recent change interface (Data Management System).

Common Network Interface (CNI) Subsystem

The CNI subsystem software allows 3B Computer equipped switching offices, data bases, and other CNI equipped offices to be connected to the common channel signaling (CCS) switching network. The CNI subsystem contains the software needed to implement the communication protocol functions that are common to all users interfacing with the CCS switching network.

The CNI subsystem utilizes the Signaling System 7 protocols. The SS7 protocol is used to control the destination routing of signaling messages between SS7 nodes within the CCS network. In addition, the CNI subsystem incorporates another common subsystem known as the interprocess message switch (IMS) subsystem.

Interprocess Message Switch (IMS) Subsystem

The IMS subsystem is a high-capacity packet switching software package that allows data messages to be routed between application functions in the community of peripheral processors. This multiprocessing of data messages is performed in a reliable environment with a minimal amount of delay.

The IMS subsystem performs its functions using a hardware configuration consisting of a 3B Computer central processor, an interconnecting "ring-type" dual bus, and application nodes as illustrated in Figure 1-1. Nodes provide ring access for both the central processor and the application. Software to provide application and central processor message distribution, interprocess communication strategies, craft interface, hardware maintenance, system initialization, audits, and measurements are all contained in the IMS subsystem. The community of peripheral processors utilize an internal communication protocol and is independent of all signaling network protocols.

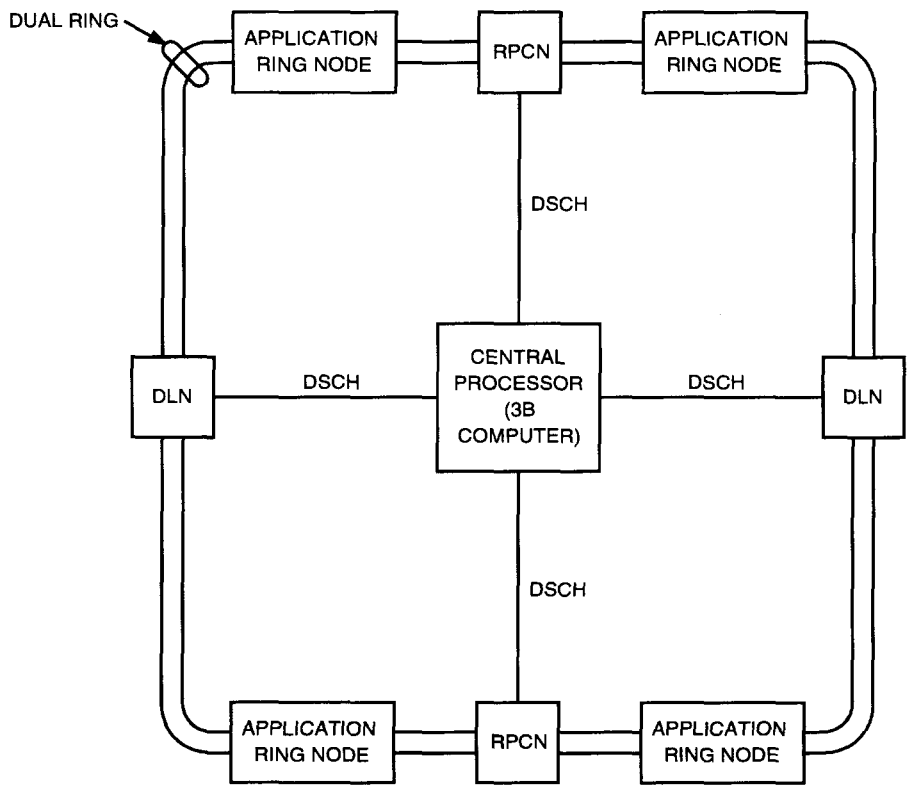
The IMS subsystem makes use of distributed processing. Distributed processing is controlled by the community of peripheral processors working through an interconnection with a central processor, along with the software necessary to support high-capacity packet communications. The community of peripheral processors are interconnected in a "ring-type" busing arrangement via direct memory access (DMA) hardware. The message-distributing software allows messages to be moved from one microprocessor to another and also permits messages to be sent from one process to another process. The IMS software is embedded in the CNI software and the CNI software is embedded in the UNIX Real Time Reliable (RTR) operating system.

Software Subsystem Functions

A breakdown of the functions performed by each software subsystem in the central processor and node processor are shown in Tables 1-A and 1-B. The RPCN and LN functions are performed independently from, but in cooperation with, the central processor functions.

The processors used with CNI software include the 3B Computer central processor, the node processor (NP) circuitry of all nodes, and the attached processor (AP) circuitry of DLNs. Each software subsystem has a set of processes operating under the control of central processor software in main memory. These software subsystems and associated functions are identified in

Table 1-A. The operating system schedules the various processes involved is scheduled so that its particular functions are performed in coordination with all other processes. Processes in the central processor often communicate with node processes in order to perform their functions. The CNI/IMS system can relay messages between cooperating processes in different processors. These messages are referred to as maintenance messages.



Legend:

RPCN - Ring Peripheral Controller Node
DSCH - Dual Serial Channel
DLN - Direct Link Node

Figure 1-1. Interprocess Message Switch Configuration

Table 1-A. Central Processor Functions

Subsystem	Functions
UNIX RTR System	• User PDS command execution and display page access • Audit control • Execution environment for all CNI software • ECD maintenance
CNI	• Initialization • Measurement and critical event generation • Measurement data cumulation, history file maintenance, and report generation • CNILOG file maintenance and message outputting • Data base updating (point code routing data, link data, and MOCT data) • Link management and link status auditing • Overload and insanity detection • SS7 routing and load sharing (MTP and SCCP routing)
IMS	• System initialization and downloading of nodes • Measurement generation and collection • Error detection, error message analysis, and ring recovery • Maintenance of ring and nodes, and ring reconfiguration • Diagnostics administration • Real-time overload control and insanity detection • Display pages • Ring node control auditing • Software trace reporting control • Message switching

In DLNs, the attached processor (AP) circuitry performs application-specific functions. These functions include translations for trunk signaling, network management interface for direct signaling, an interface to the common network interface (CNI) system, and the ability to interface the 4ESS Switch Attached Processor Interface (API) via direct memory access (DMA).

Many of the subsystem functions performed by the RPCNs or the LNs are under control of software in the respective node processor's memory. As in the central processor, each subsystem has a set of processes in each node's node processor memory. The node processor contains instructions that schedules these various processes. Node processor memory is smaller than central processor memory because nodes are responsible for fewer functions. Note that there are only IMS functions in an RPCN because its only role in the interprocess message switch is moving messages between the central processor and the ring.

Table 1-B. Node Processor Functions

Subsystem	Functions
IMS in RPCN	• Measurement generation • Error detection • Ring hardware state data administration • Maintenance and stand-alone ring and NP diagnostics • Message flow control to central processor • Local audit control (for example, neighbor node audits) • Signaling message and interprocess message transporting between ring and central processor
CNI in LN	• Measurement generation • Link interface diagnostics • Overload and congestion controls • Discrimination and distribution of messages from the ring and network • Alternate routing for banded messages • Link and signaling route management • Signaling link protocol execution
IMS in LN	• Measurement generation • Error detection • Ring hardware state data administration • Maintenance and stand-alone ring and NP diagnostics • Internal overload and overflow control • Local audit control (for example, neighbor node audits) • Signaling message and interprocess message transporting between ring and link • Execution environment for the CNI application software

Common Network Interface System Description

The CNI system consists of a dual serial bus that connects nodes to form a ring (Figure 1-2). All nodes contain the following circuitry and software:

- Node processor (NP) circuitry
- Ring Interface (RI) circuitry
- Special-purpose circuitry (3BI circuit, DLN-Attached Processor circuit, etc.) for Ring Peripheral Controller Node (RPCN) and Direct Link Node (DLN) applications only
- Applicable network facility link interface circuitry
- Software to support ring interface
- Software to determine node function

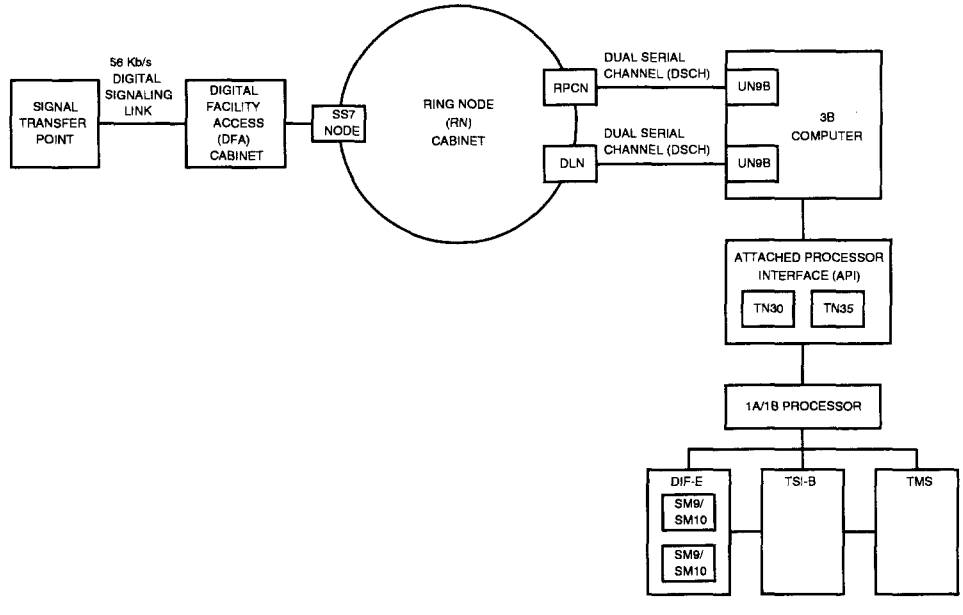


Figure 1-2. Common Network Interface Ring — 4ESS™ Switch Application

The node processor circuitry enables the node to perform specific autonomous functions. The ring interface circuitry controls the inserting of messages onto the ring and removing messages from the ring. Due to there being two separate rings and the fact that messages on ring 0 flow in ascending address order and messages on ring 1 flow in descending address order, circuitry for RI0 is different from the circuitry for RI1. Special-purpose circuitry is designed to perform very specific functions that are only applicable to the ring peripheral controller nodes (RPCNs) and direct link nodes (DLNs). Link interface circuitry enables the nodes to be connected to the appropriate network facilities. Software provides the instructions to perform all processes involved to operate the CNI system.

Nodes designed to interface with the CNI system for specific applications (SS7, etc.) are commonly referred to as application link nodes. Nodes that provide access to the central processor are referred to as ring peripheral controller nodes (RPCNs) and nodes that aid in performing signal processing normally performed by the central processor (3B Computer) are referred to as direct link nodes (DLNs). An example of one DLN function is the sending and receiving of CCS information to and from the Attached Processor Interface (API) via the 3B Computer direct memory access (DMA) buffers. All nodes are interconnected by a dual ring bus which provides access between all nodes for internode communication. This system of interconnected processors uses an internal packet communication protocol which is independent of any application network protocol. Furthermore, the ring does not determine the destination of the data given to it. That determination is made by the nodes.

In the physical sense, nodes consist of a group of circuit packs that are mounted in units housed in cabinets. The ring is actually a high-speed data bus between the nodes. The nodes interfacing with the central processor (3B Computer) connect to direct memory access (DMA) controllers in the central processing unit via high-speed dual serial channels (DSCHs).

The following is a typical example of the node switching function.

1. A message arrives at the node.
2. The node determines if the message is to be routed directly to an outgoing node or routed to the central processor (3B Computer) for additional processing.
3. Messages destined to an outgoing node are passed around the ring until the desired outgoing node is reached, removed from the ring, and appropriately processed for final disposition.
4. Messages destined to the central processor (3B Computer) for additional processing is routed to the central processor, additional processing performed, and retained in the central processor for final disposition or returned to the ring with an identified outgoing node designation. Messages returned to the ring with an identified outgoing node destination are passed around the ring until the desired outgoing node is reached, removed from the ring, and appropriately processed for final disposition.

The CNI system function of moving messages around the ring is basically accomplished using the node circuitry described in the preceding paragraph. However, to transfer messages between the node processor of specific node applications and the appropriate network facility requires link interface (LI) circuitry. The link interface circuitry converts node processor messages to a compatible format that interfaces with the appropriate facility access circuits.

Since many CNI system functions require considerable processing power and are often centralized functions, the ring and nodes themselves are not sufficient to establish a complete CNI system. Therefore, a centralized computer or central processor is required to complete the system. This central processor is the 4ESS Switch Attached Processor System (APS) 3B Computer. Special nodes have been designed to interface the ring to the 3B Computer. These nodes are identified as the ring peripheral controller node (RPCN) and direct link node (DLN).

As with other nodes, the RPCN contains node processor and ring interface circuitry as previously described. In addition, the RPCN contains 3B interface (3BI) circuitry that allows the RPCN to communicate with the 3B Computer duplex dual serial bus selector (DDSBS) circuitry. This communication consists of 3B Computer DDSBS control signals and RPCN 3BI control signals. Communication between the 3B Computer and RPCN is via a DSCH that bidirectionally transfers data in a serial format.

As with the RPCN, the DLN contains node processor, ring interface and 3B interface circuitry as previously described. The DLN also uses a dual-serial channel as its communication medium to and from the 3B Computer. In addition to this circuitry, the DLN uses direct link node-attached processor (DLN-AP) circuitry that allows the DLN to perform specific signaling message processing. The DLN-AP circuitry contains dual-port random access memory (DPRAM) that is used to store application specific software. This circuitry along with the DLN's ability to interface with the 3B Computer gives the DLN its message processing capabilities.

Interframe buffer (IFB) circuitry is also a part of the ring. The IFB circuitry is basically designed to overcome certain physical limitations of the ring hardware. Other than to effectively increase the ring's length, the IFB circuitry does not affect the function of the ring. However, placement of interframe buffers is important when configuring a ring.

The SS7 node is designed to route signaling messages between nodes within the domestic common channel signaling (CCS) switching network. The SS7 node is supported by the SS7 protocol. The SS7 protocol meets all requirements as defined by the North American Standard and International Telegraph and Telephone Consultative Committee (CCITT) specifications. Each domestic SS7 node is associated with a single 56 kb/s signaling link via a digital facility access (DFA) circuit.

Common Network Interface System Operation

The operation of the ring is intended to be transparent to users; that is, the messages need only specify their destination, and the ring then handles the "how to get them there." Because the ring operates autonomously, no user software action is normally required to keep the ring operational. Manual maintenance actions require craft/machine interfaces via input/output messages.

Nodes are connected serially by a data bus to form the ring. Rings 0 and 1 are independent of each other while one is designated as ACTIVE and the other as STANDBY. The ACTIVE ring is used for traffic and message handling. The STANDBY ring is used to carry internal maintenance messages. The rings propagate data in opposite directions. Nodes are designed so that faulty equipment may be temporarily removed from service. A node may be either isolated, not part of the active ring segment, or quarantined, part of the active ring segment, but not operational. The node processor (NP) circuitry of a quarantined node is electrically separated from the ring. The ring may, at any point in time, contain both an active segment and an isolated segment. Only internal maintenance messages can be transmitted on the isolated ring segment.

The hardware that interfaces a node's node processor (NP) circuitry to the ring is the ring interface (RI) circuitry. There are two RI circuit packs (RI0 and RI1). The NP and the RIs combined are referred to as a node. As shown in Figure 1-3, each RI consists of a pair of independent ring access circuits (RACs) and data selectors (DSs). Each RAC operates functionally as a buffer and allows messages to be inserted onto, removed from, or passed along a specific ring. The node processor circuitry communicates with each of its RACs via direct memory access buses. The DSs are used to redirect data from one ring to another in order to form an isolated segment; that is, rings 0 and 1 looped back on each other as shown in Figure 1-4).

While a message is in the RAC, it is examined by the RAC controller to determine its disposition. If the message is destined for that particular node, the node processor (NP) direct memory access (DMA) controller is instructed to read the message into NP memory. Each node has a set of buffers in NP memory used by the RAC controller when sending messages between the ring and a node. If the message is not destined for that particular node, the message is forwarded to the next node on the ring.

A special message called the token message travels around each ring and allows other messages to be placed on the ring without causing congestion. A node waits until the token message is detected in the RAC of the upstream node, holds the token there, sends any pending messages onto the ring, and then lets the token continue. Data on the ring is passed from one RAC to the next in an asynchronous fashion. Some RACs have a token track flip flop (TTFF) that is used to locate token errors.

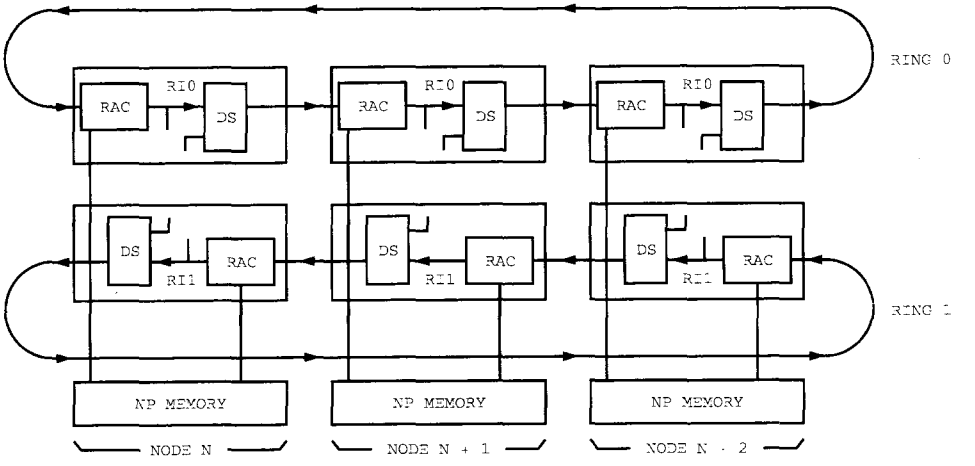


Figure 1-3. Dual Ring Structure — Normal

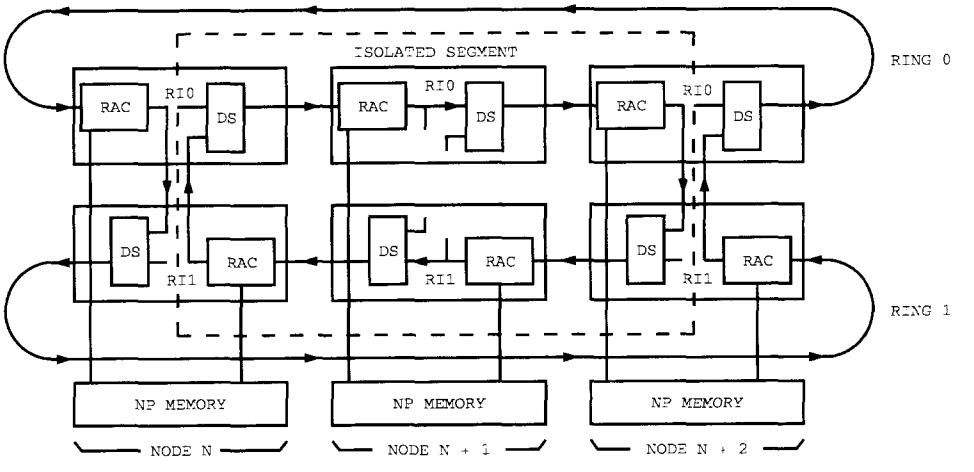


Figure 1-4. Dual Ring Structure — Isolated

Messages can be written in blocks (packets) containing either a single message or multiple messages. These packets are delivered to their destination node using the hardware physical address and the address specified in the message. In addition to the address, a destination channel may also be specified in the message. The destination channel is used to indicate which software function receives the message. Senders and receivers (i.e., software) know which channels they are concerned with and insert the appropriate data (destination channel) into a message before transmitting it.

The following are the normal sequences for writing to and reading from the ring. These sequences are used by both a normal ring and a ring with isolated or quarantined nodes.

a. **To write a packet onto the ring:**
   1. Messages are queued in the node processor (NP) buffer until the token is detected by the ring access circuit (RAC) at the upstream node (that is, node N+1 writes to the ring while the token is held in the RAC of node N).
   2. The token is held in the upstream ring access circuit (RAC) and the direct memory access (DMA) controller sends all waiting messages onto the ring. However, if the total size of the write exceeds the maximum size of one message, the waiting messages are broken up into blocks no larger than the maximum size message. In this case, it may take multiple token visits to write all waiting messages onto the ring.
   3. The sender is notified of direct memory access (DMA) completion, and the token is allowed to continue.

b. **To read a packet from the ring:**
   1. The ring access circuit (RAC) detects its node address in the messages and activates the direct memory access (DMA).
   2. The DMA controller sends the message to the node processor (NP) buffer.
   3. The message is queued onto the appropriate channel. If there are multiple messages that are back-to-back on the ring and they are all destined for the same node, the messages are all transferred into the NP memory before the software distributes them to the appropriate channels.

Nodes are peripheral processors through which digital information enters the ring, exits the ring, or is processed further. To a degree, each node is dependent on the proper operation of other nodes. All nodes must recognize and report internal failures or ring failures to the central processor for analysis and corrective action. In some cases, special purpose nodes (RPCNs, DLNs, etc.) autonomously attempt to recover from a failure. However, severe failures require the aid of the central processor. The CNI hardware and software contains logic for detecting faulty equipment. The central processor can remove equipment from service and, if necessary, reconfigure the ring around the faulty equipment. Software identifies a beginning and ending node for the isolated

segment and instructs these nodes (BISO and EISO) to redirect rings 0 and 1 to isolate the faulty nodes. It is important to note that the BISO and EISO nodes are not part of the isolated segment but are its neighbors. The isolated nodes can then be diagnosed and/or repaired. If no faults are found, the ring can be reconfigured again and the nodes restored to service. Equipment failures associated with the ring are grouped into the following major classes:

a. **Ring Down**—The ring is totally unusable. Some cases include hardware faults where there is no communication between the ring components; the 3B Computer may not be responding to the RPCNs; no ring traffic when the 3B Computer is operating normally, and/or both the ring and the central processor are down.

b. **Multiple Node Isolation**—There may be faulty and nonfaulty nodes in the isolated segment. The affected nodes are in the out-of-service (OOS) isolated state and are not part of the active ring. This is usually due to hardware problems in two or more ring nodes that make normal operation in the ring impossible. Nonfaulty nodes in the segment are innocent victims.

c. **Single Node Isolation**—The faulty node is out-of-service (OOS) and is not part of the active ring. This state is differentiated from the previous state because only one node is in the isolated segment.

d. **Node OOS-Quarantined**—This state is the normal out-of-service (OOS) state when the node is not isolated; there may also be an isolated segment elsewhere on the ring. In this state, other nodes in the active ring may send messages through the ring interface (RI) of the faulty node. The faulty node itself may not communicate with the ring.

e. **Unexplained Loss of Token**—This is an obscure error condition and the cause is unknown. A software token-tracking procedure is called each time this error occurs.

Common Network Interface System Reliability Features

The CNI system reliability features aid in eliminating unplanned downtime. The following list contains some of the CNI system reliability features.

- Node Initialization
- Full Process Initialization
- Critical Node Restore
- Protected Application Segment.

Node Initialization

Prior to the node initialization feature, all node restorations required that the node be pumped with text and data. The node initialization feature increases system availability by allowing nodes to be restored without being pumped.

Originally, when a node experienced a hard panic, the node was placed in the quarantine state and processes returned to boot monitor. The 3B Computer detected an out-of-service (OOS) node and issued a restore node request. A reset message was sent to the node causing it to start the "boot read-only memory" initialization process.

With the node initialization feature, most hard panics are converted to panic types. If a node experiences a firm panic, the node is placed in the quarantine state. The 3B Computer detects the out-of-service (OOS) node and the CNI system is informed that the node is no longer active. The IMS software starts a checksum audit of the nodes text and data. If the audit is successful, the node is reinitialized. If the audit is unsuccessful, the node is returned to boot monitor processes and is reinitialized with a complete pump of text and data.

Full Process Initialization

The full process initialization (FPI) feature provides a faster and more reliable initialization response than the abort and boot initialization. The difference is in determinism, disk access, resource handling, and dependence on low level processes.

The current boot scheme is as follows:

a. All CNI and IMS processes are terminated.

b. The CNI USER creates CNIINIT.

c. CNIINIT creates and sequences the CNIINIT critical child processes.

d. "imsdrv.p" creates and sequences "imsdrv.p" critical child processes and initializes the ring.

e. The CNI USER along with the CNI SLMK process, starts ring traffic.

f. Non-critical CNI and IMS processes (measurements, pages, etc.) are created and sequenced.

The full process initialization simulates a CNI level 2 initialization so that no disk access is required for the initialization to successfully complete. In addition, all CNI and IMS processes are involved in the initialization.

The full process initialization proceeds as follows:

a. The CNI USER grants CNIINIT permission to begin the initialization.

b. All processes that use IMS channels must cease using them or be prevented from using them.

c. CNIINIT "syncs" with and sequence CNIINIT critical children.

d. "imsdrv.p" initializes the ring.

e. The CNI USER along with the CNI SLMK process starts ring traffic.

f. Non-critical processes (measurements, pages, etc.) are recovered.

Critical Node Monitor

Out-of-service nodes are restored by the IMS Automatic Ring Recovery (ARR) feature, which uses a priority list to determine which out-of-service nodes to restore first. If all nodes are out-of-service, the ring has no communications with the outside world and a high priority straggly must be assigned for restoring the nodes. The ARR priority list reserves the priority four indicator to identify "user critical" nodes. Using this priority, CNI software can nominate nodes required to restore contact between the ring and the outside world. This nomination is performed by a module called the *critical node monitor.*

If all DLN's are out of service, the critical node monitor sends a message nominating a DLN to be put in priority four on the ARR priority list. Every 5 seconds the critical node monitor checks to see if the node was restored. If it is determined that the node cannot be restored, then the critical node monitor nominates another DLN until one is restored. The same procedure is performed if all nodes are out-of-service. The critical node monitor stops nominating when at least one DLN and one node has been restored.

Protected Application Segment

The CNI data that rarely changes is referred to as *static data* and is kept in the protected application segment (PAS) of the 3B Computer memory. The PAS is a sanctuary in the 3B Computer memory which is preserved over all UNIX system RTR initializations except for a level 54 initialization. The CNI system re-uses its static data from PAS during CNI init level 2, to save time that would be wasted downloading the data from disk.

To make PAS data safe to use, it must be protected from processes that might accidentally write in it. For this purpose, CNI incorporates the "PAS Write Access Limitation" feature which limits the processes that can write in PAS. In addition, CNI upgrades this area to be "write protected" which limits not only which processes can write, but also when these processes can write.

Hardware Description and Functions

2

Contents

Contents

Hardware Description and Functions

2

General

This section includes a physical and functional description of the Common Network Interface (CNI) system hardware as equipped for and applicable to the 4ESS™ Switch; CNI system equipment features and requirements, equipment descriptions, and equipment addressing and assignments are also included.

The CNI system uses the 3B Computer as its central processing unit. The central processor interfaces with a community of peripheral processors known as nodes arranged in a ring-type local network. The nodes that interface with the central processor connect to direct memory access (DMA) controllers in the central processing unit via high-speed dual serial channels (DSCHs). *Nodes* are defined as access points on the ring where digital information either enters onto the ring, exits the ring, or is processed further. Digital information is transferred to and from the central processor for processing via special nodes known as ring peripheral controller nodes (RPCNs). Digital information enters from and exits to transmission facilities via other nodes known as application link nodes. All nodes are serially connected by the dual rings which propagate data in opposite directions and permit ring reconfiguration as part of automatic fault recovery. This redundancy in the ring design is partly responsible for the system's high level of availability.

In the physical sense, nodes consist of a group of circuit packs mounted in units that are housed in cabinets. The ring is actually a high-speed data bus between these nodes. Interconnection to a facility from the nodes is made through facility access circuits. Facility access cabinets contain the facility access circuits, data sets, and other circuits that permit access to signaling links (SLKs). Distribution frames provide terminations to make transmission facility assignments to specific signaling links. In addition, distribution frames permit a convenient method to reassign terminations.

Signaling links are the medium by which messages are transferred to and from CNI systems in the domestic Common Channel Signaling (CCS) network and special access customer premise equipment. Signaling link transmission rates vary according to the application for which they support. Both digital and analog signaling links may exist in a CNI system.

Equipment Features and Requirements

Physical Design Features

A modular approach to the physical design of the CNI system hardware has been emphasized in order to achieve the flexibility necessary to configure a specific system to its end requirements. Except for some miscellaneous circuits, all interunit and intercabinet wiring is connectorized. This permits system growth and changes to be made with a minimum of cabling difficulties. The equipment is bolted together and secured to the building in individual cabinet line-ups. The equipment has been designed to meet the *New Equipment Building Standards* (NEBS) and restructions of Underwriters Laboratories (UL).

Cabinets

The basic support structure for all related equipment is a steel cabinet enclosure. All units, backplanes, and circuit pack assemblies must be matched to the application cabinet. The steel cabinet enclosures are equipped with doors on the front and back. The rear doors are ventilated. Cabinets are 6 feet 4 inches high, 2 feet 2 inches wide, and 2 feet 6 inches deep. Each cabinet is equipped with casters and leveling feet that are insulating, nylon-type, and adjustable. A skirt is provided to conceal the feet and enclose the space at the bottom of the cabinets. Cabinets are bolted together, side-by-side, to form a single cabinet lineup. Cabling between cabinets is routed via overhead cabling racks or through holes provided in the side of the cabinets.

In the small Scale Integrated (SSI) ring-node cabinet, the cabinets are designated 00 and 32. In the high-density (HD) ring-node cabinet, the cabinets are designated 06 and 38.

Within the cabinets, the individual unit assemblies are supported by mounting plates. Mounting plates span the area between the cabinet uprights and the height is determined by the units they support. The units, backplanes, and circuit packs described below are all housed in cabinets.

Units

Shelf units, formed from various parts such as apparatus mountings, card guides, circuit packs, connectors, and interconnecting wiring, form the basic building block for cabinets. Circuit packs and other equipment are housed in apparatus mountings that are attached to the mounting plate. Within the apparatus mountings are guides that align the circuit packs with the connector pin field on the backplane, which is also attached to the mounting plate.

Backplanes

The backplane assembly provides intercabinet and intracabinet connections via the printed wiring board connectors and backplane pin fields. The backplane assembly also supports mechanical alignment of the apparatus mountings and circuit packs. The mounting plate provides the structural support for both the apparatus mountings and the backplane assembly. The apparatus mountings, circuit pack organizers, are attached to one side of the mounting plate, and the backplane assembly is attached to the other side.

Circuit pack connectors plug onto a field of square pins (25-mil) placed on 0.125 inch centers. The pins are press-fitted into an epoxy-glass backplane. The backplane may be unplated and serve only as a holder for the pins which can be wire-wrapped on the opposite side. However, in most cases a double-sided or multilayer-printed wiring board is used. The backplane terminals are finished with a hard gold plate and are inserted from the equipment side of the backplane. They extend 0.700 inch from either side of the backplane. Before assembly, a cover coat is applied over the backplane to prevent short circuits caused by possible solder smears or foreign matter. After assembly, the pins are straightened to ensure proper alignment.

Circuit Packs

Circuit packs are housed in apparatus mountings. Within the apparatus mountings are guides to align the circuit packs with the connector pin field at the back of the shelf assembly. All circuit packs are keyed to prevent the insertion of a wrong circuit pack in a slot. The circuit packs within a unit are horizontally spaced across the cabinet with sufficient space between the boards to provide air flow for cooling.

Environmental Requirements

Heat Dissipation

In general, the CNI system can be characterized as a high heat system. The heat dissipation of equipment cabinets vary up to a maximum of 1740 watts with a maximum of 25 watts per circuit pack. The integrated circuits used in circuit pack designs require that the operating circuit board temperature does not exceed 70 degrees Celsius—158 degrees Fahrenheit. This temperature restriction aids in ensuring reliable circuitry operation.

Where necessary, cabinets are equipped with DC powered fans to ensure that maximum operating temperatures are not exceeded even under the worst case of office ambient temperature conditions. The fan units are designed to draw ambient office air into the bottom of the cabinet and move it vertically through circuit pack mountings above the fan unit. Covers are provided on the front of units to prevent air leaks. To further prevent air leakage, there is virtually zero clearance between units as they are successively stacked in a cabinet. To

maintain cooling efficiency, the air intake at the fan unit and the air outlet at the top of the stack must be kept free of physical obstructions. The fan unit is equipped with a filter that must be periodically replaced to keep the filter from becoming dirty or clogged. Maximum cooling performance requires strict adherence to specified filter maintenance routines.

Temperature, Humidity, and Altitude

The CNI system equipment is designed to remain operational in central offices located from 200 feet below sea level to 10,000 feet above sea level. Room ambient temperature and humidity limits are identified in Table 2-A.

Table 2-A. Environmental Limits

Description	Limit
Operating temperature	+40° F to +100° F
Short-term temperature (less than 72 consecutive hours and not more than 15 days per year)	+35° F to +120° F
Nominal (or wide band) temperature	+65° F to +80° F
Maximum rate of temperature change	15° F per hour
Operating relative humidity*	20% to 55%
Short-term relative humidity*	20% to 80%

* Relative humidity considerably less than 80% occurs for ambient temperatures above 95° F. During a short-term emergency condition of 120° F, the relative humidity should be below 20%.

Electromagnetic Compatibility

The CNI system equipment has been designed for electromagnetic compatibility (EMC) with existing switching office equipment. The equipment operates properly in an environment where ambient Radio-frequency (RF) fields are equal to or less than 10 volts per meter. In addition, the CNI system equipment has been designed to minimize electromagnetic interference (EMI). Electrostatic discharges damage CNI equipment. Therefore, a grounded anti-static wrist strap must be worn when handling equipment. The wrist strap should be connected to a ground that is common to the equipment ground. When an appropriate wrist strap is not available, always touch grounded metal before handling equipment. Never pass an unprotected piece of equipment to a person that is not grounded.

Power Distribution

A -48 volt power supply is required to supply all load units associated with the CNI system. Each cabinet load unit is powered by "ORed" power. 495FA power converters are used to supply power to nodes. Power converters are configured to minimize the number of nodes that fail due to a single converter failure. Each ring peripheral controller node (RPCN) is powered by a single converter. The power distribution for direct link nodes (DLNs) is the same as power distribution for application link nodes. Power distribution in the analog facility access (AFA) cabinet and digital facility access (DFA) cabinet is diversified in such a way that in the case of a fuse or power failure, only one-half of the associated units are affected.

The 4ESS Switch office provides a backup power supply for both the 3B Computer and CNI system. The backup power supply allows the equipment to function without a capacity loss during adverse primary-power failures.

Equipment Descriptions

Ring Node Cabinet

General

The ring node cabinet (RNC) (Figure 2-1) provides ring bus connections between the nodes, access to the application, and access to the 3B Computer. Each ring node cabinet contains application link nodes, ring peripheral controller nodes (RPCNs), and direct link nodes (DLNs). The number of cabinets required is determined by the traffic forecast for each office. However, a minimum of two ring node cabinets is required for the 4ESS Switch application. The ring bus within the cabinet consists of short backplane wiring between the nodes within the cabinet. The ring bus between the cabinets consists of a balanced cable pair.

Each ring node cabinet must contain at least two interframe buffer (IFB) circuit packs to allow proper data transmission over the intercabinet cabling. The IFB circuitry is provided to make an electrical transition between the ring bus (balanced cable pair) and TTL-type signals associated with a node's ring interface circuitry. Therefore, an IFB circuit pack is required where the ring bus enters, before first node, and exits, after last node, the ring node cabinet.

The ring node cabinet equipment is housed in 132B apparatus mountings commonly referred to as:

a. Line Node (LN) units

b. 3B Interface (3BI) units

c. Integrated Ring Node (IRN) Unit.

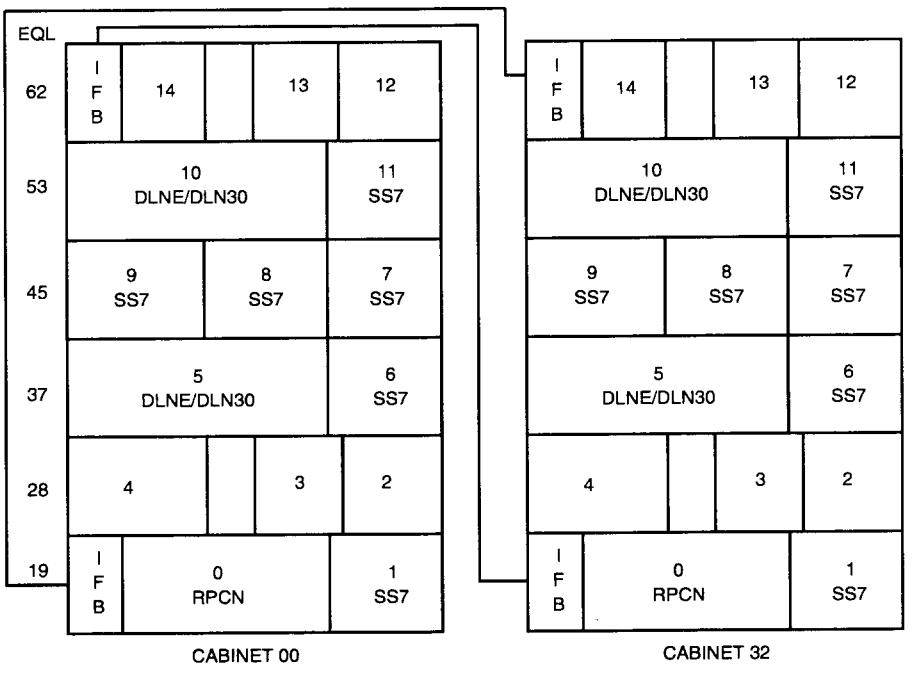
The apparatus mounting units are designed to accept required DC-to-DC converters and circuit packs in addition to providing the necessary backplane wiring to construct the following:

a. Special purpose nodes (RPCNs and DLNs)

b. Application link nodes (SS7)

c. Other applicable circuitry (IFBs, T1FAs, etc.).

The ring node cabinet also contains a fuse and control panel and fan unit assemblies.



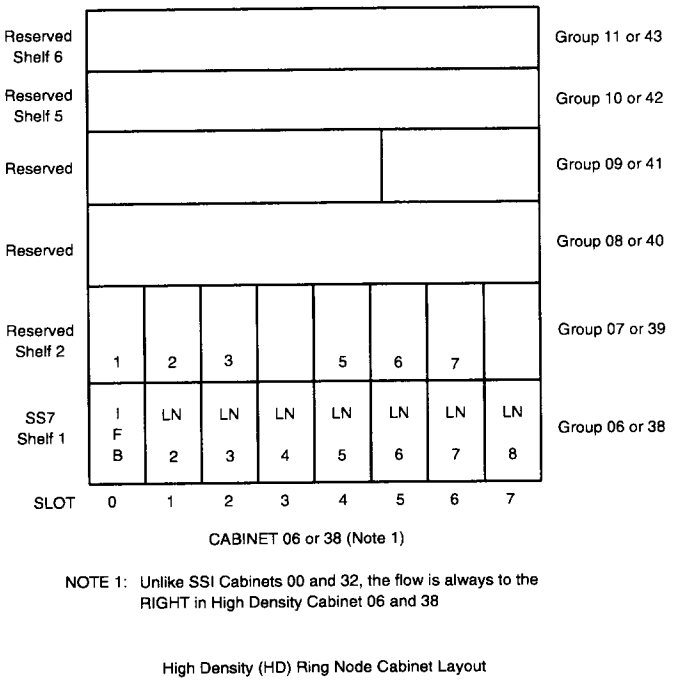
Small Scale Integrated (SSI) Ring Node Cabinet Layout

Figure 2-1. Typical Ring Node Cabinet Layout (Sheet 1 of 2)

Link Node Units

Link node (LN) units (Figure 2-2) can be equipped to support three application link nodes of the same type (SS7) or a mixture of three application link nodes (SS7 or IUN). Link node units are identified as type "A" and type "B" units. Type "A" units are equipped with nodes that are addressed in ascending order from left to right. Type "B" units are equipped with nodes that are addressed in descending order from right to left. These address sequences are determined by the backplane wiring of the units; thus, making type "A" and type "B" units not interchangeable. Type "A" and type "B" units are equipped in the ring node cabinet in an alternate fashion, starting initially with a type "A" unit. ***When ordering link node units, the equipment engineer must be particularly careful to specify the proper unit type.*** The J-specifications and schematic diagrams (SDs) for type "A" and type "B" link node units as applicable to the 4ESS Switch are as follows:

- Link Node Unit A (J-3F011AB-1/SD-3F009-01)
- Link Node Unit B (J-3F011AC-1/SD-3F010-01).



High Density (HD) Ring Node Cabinet Layout

Figure 2-1. Typical Ring Node Cabinet Layout (Sheet 2 of 2)

3B Interface (3BI) Unit

The 3BI unit (Figure 2-3) can be equipped to support either a ring peripheral controller node (RPCN) or a direct link node (DLN) in addition to one application link node (SS7 or IUN). The nodes are addressed in ascending order from left to right. As with link node units and DS1 units, the address sequence is determined by backplane wiring. The J-specification and schematic diagram (SD) for the 3BI unit as applicable to the 4ESS Switch are J-3F011AA-1 and SD-3F048-01.

Integrated Ring Node (IRN) Unit

The IRN unit (Figure 2-4) can be equipped to support eight node positions. The node positions are identified as 0 through 7. All node positions (0 through 7) can be equipped with SS7 nodes. However, all equipped nodes in an IRN unit must

be of the same type with the exception of an IUN. When necessary, node positions 0 and 7 can be equipped with an interframe buffer (IFB), and node position 3 can be equipped with a T1 facility access (T1FA) interface. The nodes are addressed in ascending order from left to right and, as with all other units, the address sequence is determined by backplane wiring. Ring node cabinets equipped with IRN units containing SS7 nodes in the 4ESS Switch environment are identified as high density backplane (HDB) cabinets as illustrated in Figure 2-4. The SD and J-specification for the IRN (UN303B)/IRN2 (UN304B) unit as applicable to the 4ESS Switch are J-3F011DC-1 and SD-3F037-1 (for the SSI cabinet); J3F011GB-1 and SD-3F050-1 (for the HD cabinet).

The 5-node IRN unit is shown in Figure 2-4, Sheet 2 of 2, and is arranged for 5 node positions labeled 0 - 4. The applicable J-specification is J-3F011GD-1.

Ring Peripheral Controller Node Circuit Packs

The RPCN provides access to the CNI system central processor (3B Computer). This access is used to transfer information between the ring and 3B Computer for maintenance, administrative, and message processing functions. The RPCNs are located on the ring in a manner so that the number of application link nodes between the RPCNs are approximately equal. This minimizes the possibility that more than one RPCN will be included in a multiple application link node isolation. Every node on the ring is associated with a RPCN through software. This association allows all nodes to determine the appropriate destination for 3B Computer bound messages. Software balances the load between RPCNs to prevent one RPCN from becoming overloaded. Two RPCNs are required in a CNI system designed for the 4ESS Switch application.

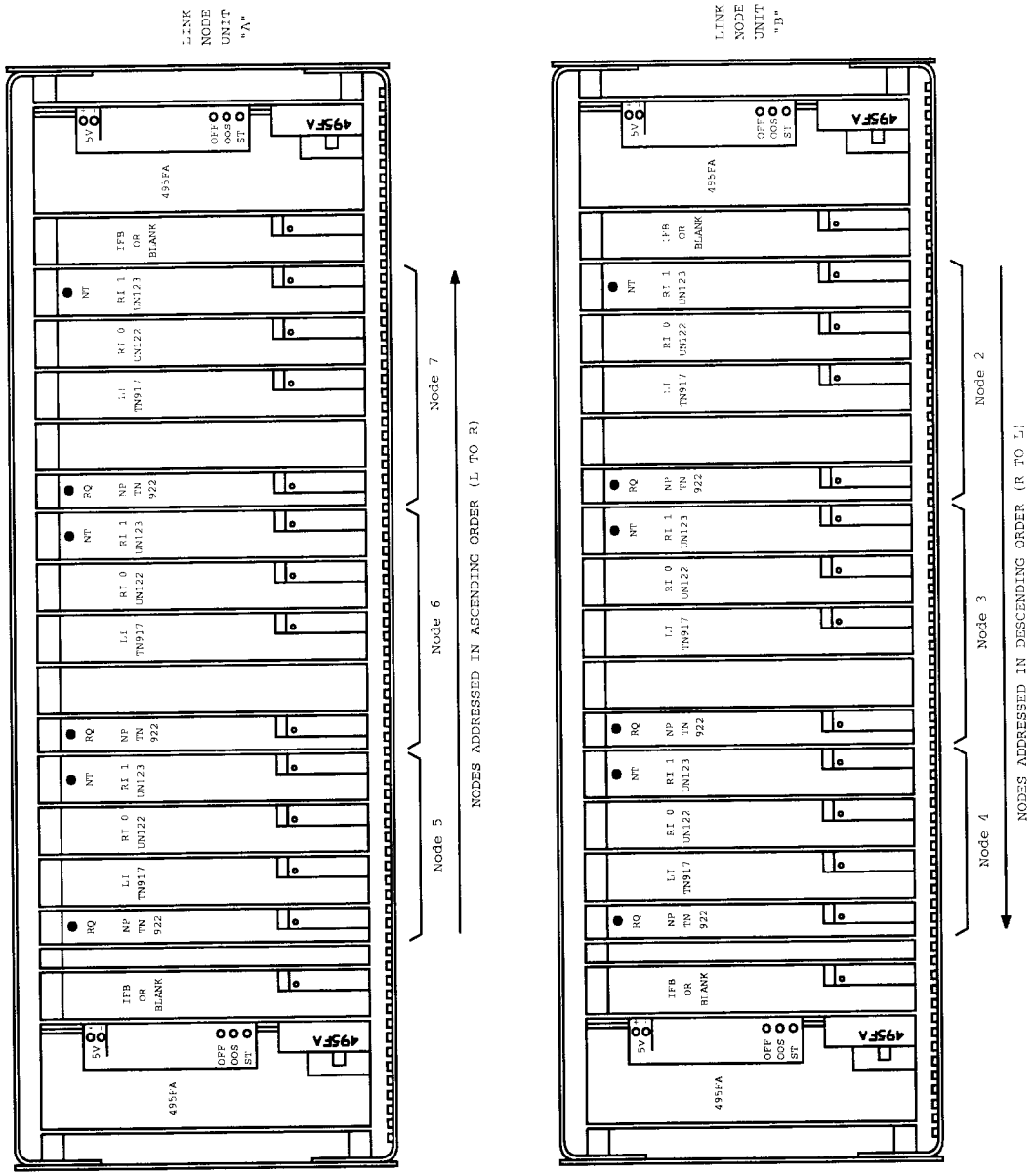


Figure 2-2. Link Node Units (Type A and B)

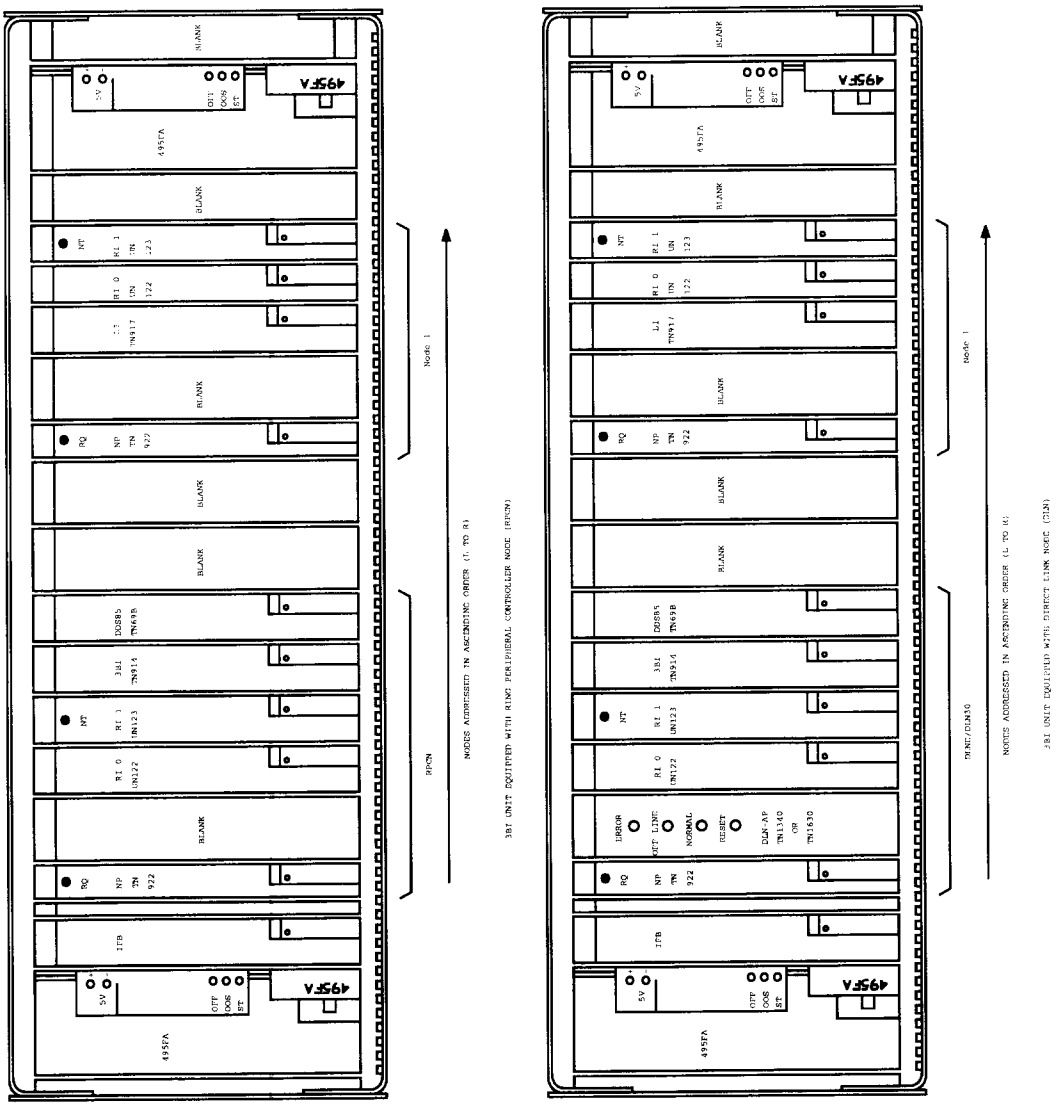


Figure 2-3. 3BI Units Equipped With RPCN and DLNE/DLN30

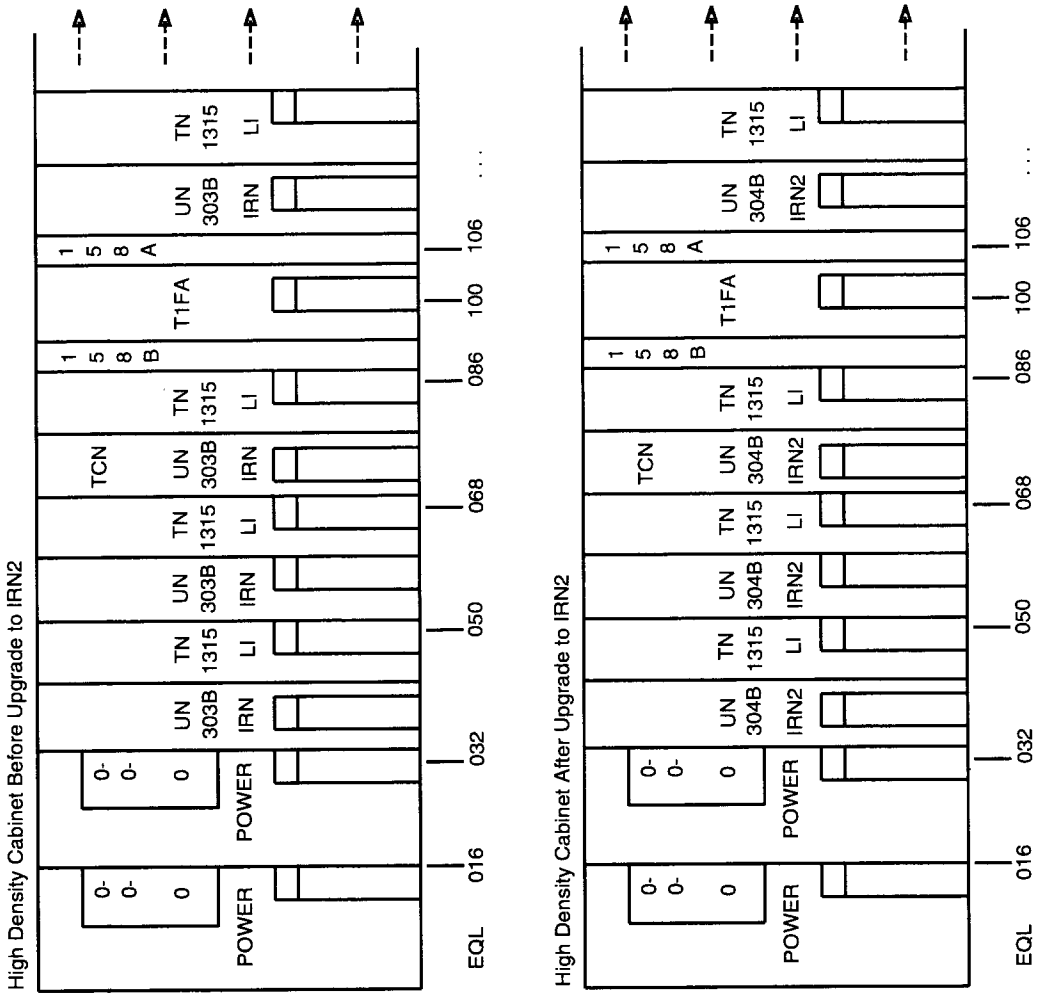


Figure 2-4. Integrated Ring Node (IRN) Unit (Sheet 1 of 2)

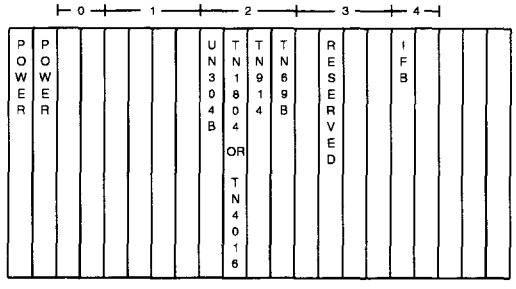


Figure 2-4. Integrated Ring Node (IRN) Unit (Sheet 2 of 2)

The RPCN consists of the following circuit packs:

a. *Ring Interface (RI)*—Ring interface circuitry provides access to the dual ring. There are two distinct ring interface circuits:

- Ring Interface 0 (RI0)—UN122/UN122B/UN122C
- Ring Interface 1 (RI1)—UN123/UN123B.

Ring interface 0 circuitry interfaces with ring 0 while ring interface 1 circuitry interfaces with ring 1. Two ring interface circuits are required due to the flow of messages on the rings. Messages flow in ascending address order on ring 0 and in descending address order on ring 1. The ring interface circuitry (RI0 and RI1) provides the circuits necessary to insert messages onto the rings, extract messages from the rings, pass messages along the rings, and perform message error checks in addition to other ring interface maintenance functions.

The ring interface circuitry also controls ring reconfiguration, thus permitting faulty nodes to be isolated. Many functions are duplicated in both ring interface circuits. However, some functions are performed for both rings by one ring interface circuit.

b. *Node Processor (NP)*—The node processor (TN922) provides the circuits necessary to control node operations. Most node processor responsibilities are performed by intelligent circuitry that utilizes on-board memory containing stored processing data.

The node processor is essentially a self-contained microcomputer composed of a central processing unit (CPU), memory, interrupt logic, input/output ports, and direct memory access (DMA) circuitry for ring communication. Node processor software is downloaded from the 3B Computer into NP memory during CNI system initialization. Node processor software varies depending on the type of node—application link node, DLN, or RPCN. Software processes that perform node processor operations are scheduled and executed by the CPU on a priority basis.

Primary responsibilities of the node processor for all node applications include:

- Relay messages between the ring and signaling link
- Provide temporary storage/buffer for messages
- Process maintenance messages in addition to data messages
- Control DMA circuitry used to perform ring read and write operations
- Identify problems and notify the control processor of such problems
- Control messages between the ring and the 3B Computer when associated with a RPCN application
- Control messages between the ring interface circuitry and the attached processor; and between the 3B interface circuitry and the attached processor when associated with a DLN application.

c. *3B Interface (3BI)*—The 3B interface (TN914) circuitry provides an interface between the node processor and the duplex dual serial bus selector (DDSBS). When viewed from the DDSBS circuitry, the 3B interface circuitry can be described as a writable control port and readable status port. By controlling the direct memory access (DMA) operations to the node processor and DDSBS, the 3BI circuitry allows the node processor and central processor (3B Computer) to send and receive data when it is ready. This operation is accomplished with a data buffer that is accessible by both the node processor and the DDSBS. The various control and status registers along with interrupt circuitry allow concurrent operation of the node processor, 3B interface, and DDSBS circuitry. The 3B interface also provides data conversion between the 16-bit data bus in the node processor and the 36-bit data bus in the DDSBS.

   The 3B interface communications are either via a direct memory access (DMA) or a programmed input/output (I/O) utility provided by the 3B Computer operating system. The DMA is generally used to transfer blocks of messages and involves queuing the data at the transmitting end for subsequent transfer by the receiving end. During each message switch cycle, software in the node processor or 3B Computer determines the status of any pending request before queuing more data. The programmed I/O utility is initiated and used by the central processor to issue urgent commands or synchronize data transfers.

d. *Duplex Dual Serial Bus Selector (DDSBS)*—The DDSBS (TN69/TN69B) circuitry serves as a termination for the dual serial channels (DSCHs) between the central processor (3B Computer) and applicable node's (RPCNs and DLNs) 3B interface (3BI) circuitry. Each control unit in

the central processor contains a number of DSCHs used for data transmission. At the applicable node (RPCN or DLN) the multiple DSCHs terminate at the DDSBS circuitry. The DDSBS circuitry selects the appropriate channels upon request. In addition, the DDSBS circuitry bidirectionally converts data between the parallel format of the 3B interface circuitry and the serial format of the DSCHs.

Direct Link Node Circuit Packs (DLN)

The direct link node (DLN) relieves the CNI system central processor (3B Computer) of performing specific functions when interfacing with the 4ESS Switch 1A/1B Processor. These functions include processing messages between the 1A/1B Processor and the ring, providing ring related translations, and reformatting messages. The following are the two existing versions of the DLN:

a. DLN-Enhanced (DLNE)

b. IRN2 DLN (DLN30)

The DLN-enhanced (DLNE) consists of the following circuit packs:

a. *Integrated Ring Node (IRN):* The IRN (UN303B) circuit pack has been designed using very large scale integrated (VLSI) circuitry. This design allows the IRN circuitry to perform all operations previously performed by the small scale integrated (SSI) ring interface 0 (UN122/UN122B/UN122C), ring interface 1 (UN123/UN123B), and node processor (TN922) circuit packs previously described. The IRN is functionally, physically, and electrically compatible to the three SSI circuit packs.

b. *Attached Processor (AP30):* The attached processor (AP30) circuitry (TN1630B) is utilized by the DLNE. The attached processor AP30 circuitry has been designed to support an increased message capacity. The attached processor AP30 circuitry communicates with the IRN circuitry (UN303B) to perform all operations.

c. *3B Interface (3BI):* The 3B interface circuitry (TN914) performs the same functions for the DLNE and the RPCN.

d. *Duplex Dual Serial Bus Selector (DDSBS):* The DDSBS circuitry (TN69B) performs the same functions for the DLNE and the RPCN.

The IRN2 direct link node (DLN30), available in the 4E22R1 generic program, consists of the following circuit packs:

a. *Integrated Ring Node (IRN2):* The IRN2 (UN304B) circuit pack has been designed using very large scale integrated (VLSI) circuitry. This design allows the IRN2 circuitry to perform all operations previously performed by the small scale integrated (SSI) ring interface 0 (UN122/UN122B/UN122C), ring interface 1 (UN123/UN123B), and node processor (TN922) circuit packs previously described. The IRN2

is functionally, physically, and electrically compatible to the three SSI circuit packs.

b. *Attached Processor (AP30):* The attached processor (AP30) circuitry (TN1630B) is utilized by the DLN30. The attached processor AP30 circuitry has been designed to support an increased message capacity. The attached processor AP30 circuitry communicates with the IRN2 circuitry (UN304B) to perform all operations.

c. *3B Interface (3BI):* The 3B interface circuitry (TN914) performs the same functions for the DLN30 and the RPCN.

d. *Duplex Dual Serial Bus Selector (DDSBS):* The DDSBS circuitry (TN69B) performs the same functions for the DLN30 and the RPCN.

Table 2-B shows the DLN capacity figures for the 4ESS Switch generics.

Table 2-B. DLN Capacity Figures 4E19/22 Generics

APS Generic	4ESS™ Switch Generic	DLN Memory [terms supported]	1-Way DLN Message Capacity [msg/sec/DLN]	2-Way DLN Message Capacity [msg/sec/DLN]
4AP12	4E19	107,520K	1425	1200
4AP13/14	4E20/21	107,520K	1550	1317
4AP15*	4E22	107,520K	1850	1800

* Assumes IRN2 ring node processor upgrade.

Application Link Nodes (SS7) Circuit Packs

Application link nodes provide CNI system ring entry and exit points that permit analog and digital signaling links of specific applications to send and receive messages via the ring. Various link nodes designed for specific applications are available to interface with the ring. Application link nodes are defined by their signaling link data rate, signaling protocol, and data security requirements. In addition, link nodes control message flow and provide link protocol control, ring operations, and many other functions associated with the message switching environment. Application link nodes consist of the following circuit packs:

a. *Ring Interface (RI)*: The ring interface circuitry (UN122/UN122B/UN122C for RI0 and UN123/UN123B for RI1) performs the same functions for the application link nodes as for the RPCN.

b. *Node Processor (NP)*: The node processor circuitry (TN922) performs the same functions for the application link nodes as it provides for the RPCN.

c. *Integrated Ring Node (IRN):* The integrated ring node (IRN) (UN303B/UN304B) circuit pack has been designed using very large scale integrated (VLSI) circuitry. This design allows the IRN circuitry to perform all operations previously performed by the small scale integrated (SSI) ring interface 0 (UN122/UN122B/UN122C), ring interface 1 (UN123/UN123B), and node processor (TN922) circuit packs previously described. The IRN is functionally, physically, and electrically compatible to the three SSI circuit packs. Application link nodes (CCS7 and IUN) utilizing the IRN (UN303B) circuit pack or application link node (DCHN) utilizing IRN2 (UN304B) circuit packs in the 4ESS Switch environment are commonly referred to as high density backplane (HDB) application link nodes.

d. *Link Interface (LI)*: The link interface (LI) circuitry performs the function of transferring data between the signaling link (SLK) and the node processor. The link interface circuitry is controlled by Common Network Interface (CNI) software and primarily provides the proper protocol for bidirectionally interfacing the signaling link with the ring. Signaling link load-sharing and data security functions are other responsibilities of the link interface circuitry. Due to the unique functions performed by the link interface circuitry for application-specific signaling links (SLKs), this circuitry is different for all link node applications.

Signaling System No. 7 (SS7) Node

Link interface circuitry for the SS7 node is identified as "LI" (TN916). The "LI" circuitry bidirectionally converts the node processor TTL-type signaling to a signaling type that is compatible with the digital facility access (DFA) frame circuits. The DFA frame circuits require a RS423 signaling format. The TN916 link may be updated with the improved Processor Outage (IMPROCOT) feature for the link. (This is done using a PROM kit.) The TN916 link interface is used when data encryption is not a criteria. A maximum of one "LI" (TN916) link interface can be equipped per CCS7 node. Therefore, a fully equipped CCS7 node can accommodate one signaling link.

Interframe Buffer (IFB) Circuit Packs

The ring interface circuitry of a node drives each bus on the dual ring with a TTL-type signal. The distance this signal can be transmitted without decay is limited to a few inches of cable. Therefore, when the ring cabling extends from a node in one ring node cabinet to a node in another ring node cabinet, some compensation is necessary. The interframe buffer (IFB) provides this compensation with balanced drivers and receivers. The balanced drivers and receivers of the IFB solve the electrical problems caused by connections made using longer cable lengths. An identical pair of IFBs must be installed on the ring at any point where the cable length between nodes exceeds 25 inches.

In addition to providing a balanced transmission media between nodes, the IFBs also provide first-in first-out (FIFO) buffers to pad the message storage capacity of the ring. There are two types of interframe buffers:

1. Padded IFBs (TN915/TN1506/TN1509, TN1803)
2. Unpadded IFBs (TN918/TN1508).

Unpadded IFBs (TN918/TN1508) provide 16 bytes of storage; while padded IFBs (TN915 and TN1506/TN1509) provide 512 bytes and 4K bytes of storage, respectively. This is an important IFB characteristic since the data storage capacity of the ring must be equal to or greater than two times the length of the longest message (508 bytes x 2) plus the length of the token (8 bytes). This requirement must be met in order to avoid a message propagation on the ring. Both the TN915 and TN918 operate at a 4 Mb/s data transfer rate; whereas, the TN1506/TN1508/TN1509 is capable of operating at a rate up to 8 Mb/s.

NOTE:
If the ring contains 80% or more IRN/IRN2 nodes and all RPCNs are IRN/IRN2, any TN918 circuit packs should be upgraded to TN1508 circuit packs.

A minimum of four padded IFBs (TN915 or equivalent) must be installed on the ring. This provides a padded IFB at the entry node and exit node in each ring node cabinet. If additional IFBs are required between the entry and exit nodes to meet cabling specifications, pairs of unpadded IFBs (TN918 or equivalent) should be installed.

Fuse and Control Panel

The fuse and control panel (Figure 2-5) provide the ring node cabinet with fuse blocks to fuse units within the cabinet, a portable data terminal jack, an office telephone jack, a 660-type telephone circuit jack, and power/alarm circuitry controls. The power/alarm circuitry controls include the following:

- Alarm Cutoff key
- Lamp Test key
- Power Alarm Reset key.

The ALARM CUTOFF key closes SCAN circuits that request the processor to silence the present audible alarm. However, subsequent alarms are not inhibited by this action. The LAMP TEST key activates the FA lamp on the fuse panel and the PWR ALM lamp on the control panel. The PWR ALM RESET key is used to release all activated alarm relays after power troubles have been cleared. However, if the power alarm is due to a problem with the cabinet fan units, the problem must be corrected and the fan unit alarm ON/RESET key operated prior to operating the PWR ALM RESET key on the fuse and control panel. The J-specifications and SD for the fuse and control panel, as applicable to the 4ESS Switch, are J-3F011AD/AF and SD-3F022-01, respectively.

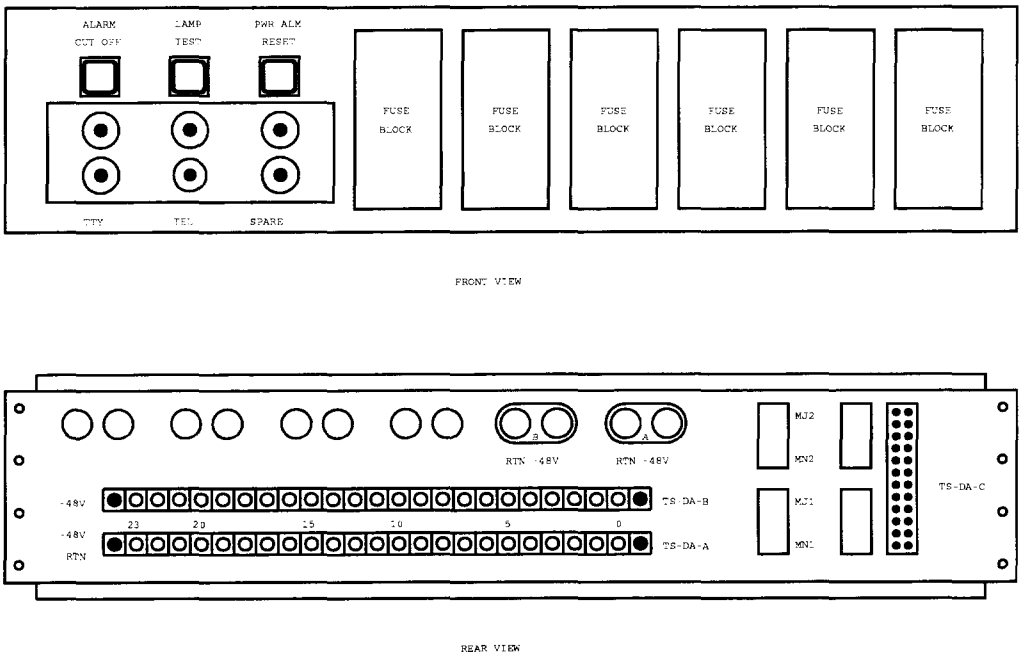


Figure 2-5. Fuse and Control Panel Mounting

Fan Units

The ring node cabinet contains two fan unit assemblies (Figure 2-6). Each fan unit assembly consists of two fans, a filter, and control panel. The fans provide cooling for the circuit packs. The filter is washable and should be serviced on a routine basis. The control panel consists of two status LEDs (FAN A and FAN B), an OFF pushbutton, and an ON/RESET pushbutton. The status LEDs light when power is removed from the associated fan unit. The OFF pushbutton removes power from both fans. The ON/RESET pushbutton restores power to both fans and/or resets alarm circuitry within the unit. The J-specification and schematic diagram (SD) for the fan unit assembly as applicable to the 4ESS Switch are J-3F011AE and SD-3F022-01.

Digital Facility Access Cabinet

General

The digital facility access (DFA) cabinet (Figure 2-7) contains circuits that provide an interface between digital SLKs and nodes. This interface is known as a DFA circuit. A digital facility access circuit is required for each node connected to a digital SLK. Therefore, each DFA circuit in the DFA cabinet serves one digital

SLK. A fully equipped DFA cabinet can provide ten DFA circuits, thus providing the interface equipment necessary to connect ten nodes to ten digital SLKs.

The primary functions of the DFA circuit is to convert the RS449 digital signal format to a bandpass bipolar signal usable by the 56 kb/s digital SLK and provide loopback circuitry to enable signaling link tests to be performed. The following three basic units make up the DFA circuit hardware:

1. Digital Service Unit (DSU)
2. Channel Service Unit (CSU)
3. Digital Service Adapter (DSA).

Digital Service Unit

The DSU (Figure 2-8) in conjunction with the DSA and possibly a CSU is used to provide access from the node to the network's synchronous transmission system.

The primary function of the DSU is to convert the RS232/V.35 signaling format to an acceptable signal that can be transmitted on the 56kb/s digital data service transmission facility. Several versions of the unit is available for use with the DFA circuits:

a. AT&T 500B Digital Service Unit
b. AT&T 2556A Digital Service Unit
c. DCP3189 Digital Service Unit.

AT&T 500B Digital Service Unit

Data access circuits utilizing the AT&T 500B digital service unit (DSU) are completed using the digital service adapter (DSA) and the channel service unit (CSU). The DSU receives serial, unipolar data and transmits a baseband, bipolar signal whose frequency corresponds to the transmitted data rate. The data and clock signals between the node side of the DSA and the DSU conform to the requirements of a balanced interface per V.35 CCITT recommendations, while the control signals conform to the Electronic Industries Association (EIA) RS-232C standard. The signals between the CSU side of the DSA and the DSU are loopback and data signals. In essence, for a transmitted signal, the DSU receives signals from the node through the DSA to the CSU. A received signal from the facility follows the same path in reverse. Connections between the DSU and the DSA are made via connectorized cable. Leads from the line side of the DSU and to the CSU are data transmission pairs (T, R, T1, and R1). In the case of a collocated office, the transmission leads bypass the CSU and connect to facility equipment.

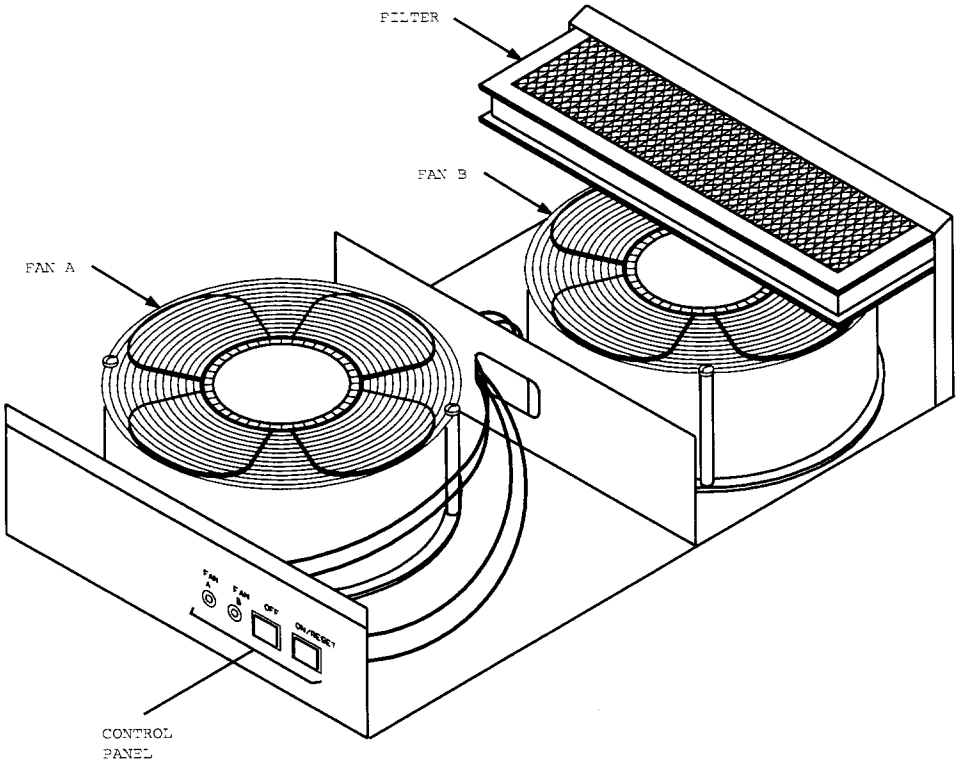


Figure 2-6. Ring Node Cabinet Fan Unit Assembly

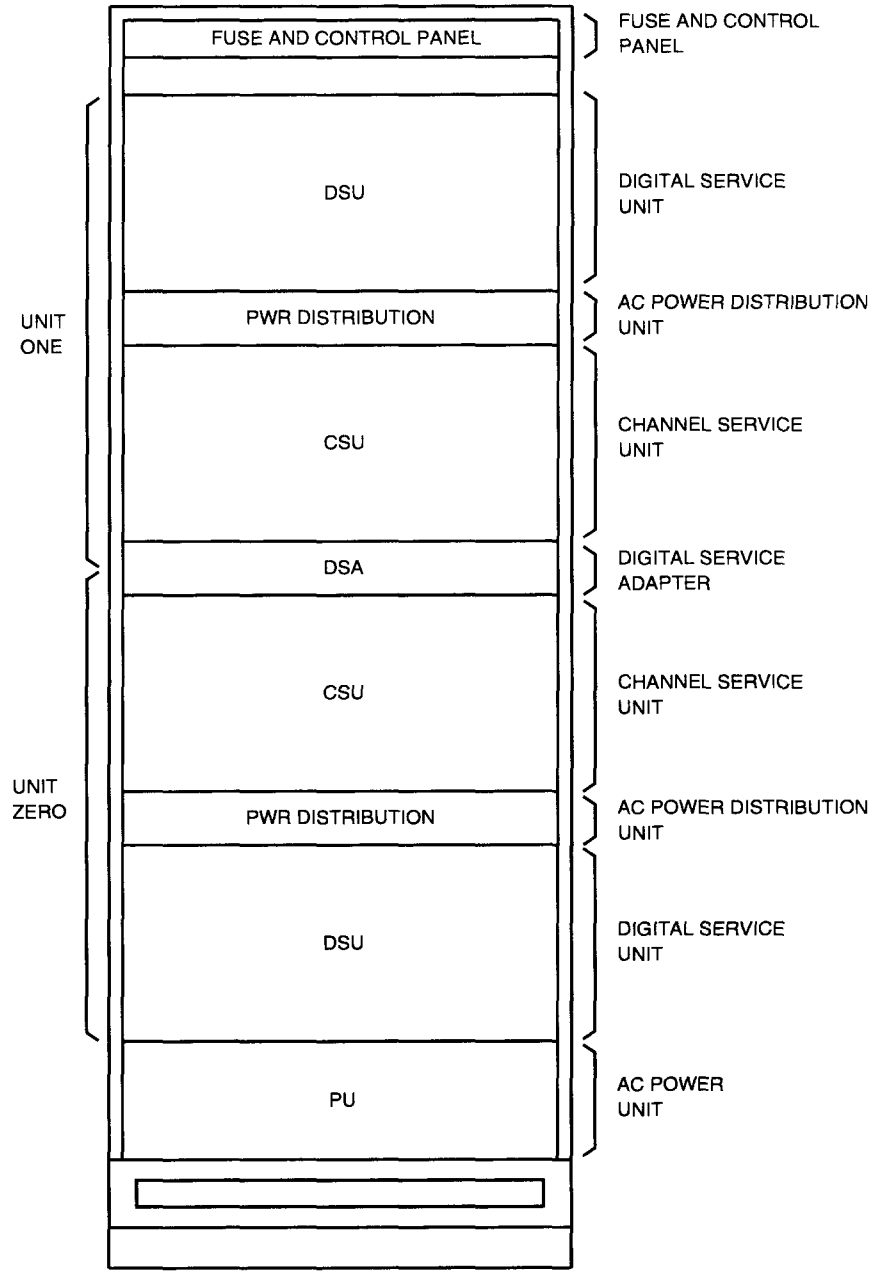


Figure 2-7. Digital Facility Access (DFA) Cabinet Layout

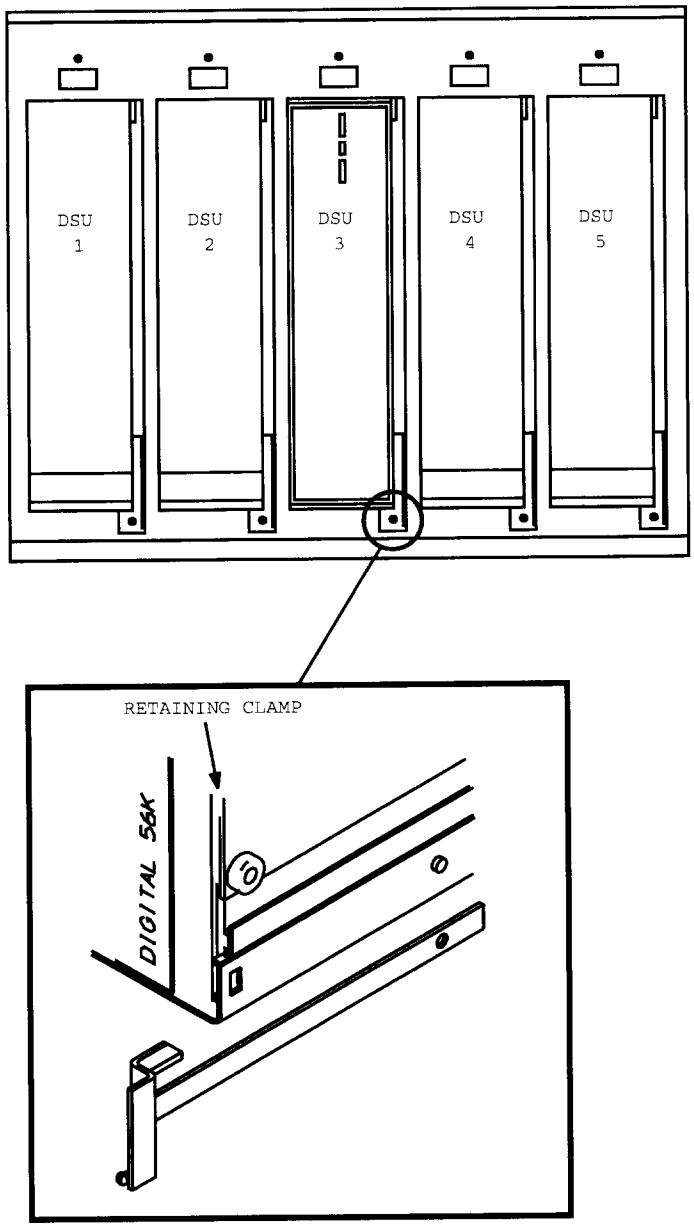


Figure 2-8. Digital Service Unit (DSU) Mounting

To enhance error detection on unencrypted links, the DSU detects bipolar violations and informs the link interface circuitry. This causes the link interface circuitry to detect a link error and enter the octet counting mode. In this mode, the link interface circuitry is searching for the next flag.

There are different versions of the AT&T 500B DSU for different signaling speeds. When a 56-kb/s signaling speed is used, the DSU version used is a AT&T 500B-L1/5. The DSU consists of a transmitter, receiver, control logic, and customer interface circuits which are mounted on two circuit packs and interconnected by a flexible cable harness.

A slide switch and four LEDs are provided on the DSU. Normally, the switch is in the center position for data mode operation. The other two positions of the switch provide loopback control for testing toward the line side or drop side on the transmit-receive leads. The LEDs indicate the power and signal present status of the DSU and the type of loopback control being used.

When the AT&T 500B DSU is used for accessing synchronous transmission facilities (long haul), only the addition of a retaining clamp is required at the mounting unit. However, if the AT&T 500B DSU is used to access a nonsynchronous transmission facility (short-haul metallic), a 112A circuit module is added internally to the DSU to control synchronization. When the AT&T 500B DSU contains the 112A circuit module, it is designated a AT&T 502B DSU. The 112A circuit module is added to the AT&T 502B DSU when the link serves a collocated office. The signaling link length from a collocated office is short enough to not require the CSU.

AT&T 2556A Digital Service Unit

The AT&T 2556A digital service unit (DSU) is currently used with the digital service adapter (DSA) to provide a digital facility access circuit. All functions performed by both the DSU and the CSU are performed by this unit. Access from the node to the synchronous 56 kb/s digital data service transmission facility is provided by the DSU via the DSA. The access is intended for full-duplex operation in a 4-wire application. Normally, this type of access involves long-haul synchronous transmission facilities. When the AT&T 2556A DSU is used for accessing these type facilities, only the addition of a retaining clamp is required at the mounting unit. However, if the AT&T 2556A DSU is used to access a nonsynchronous transmission facility (short-haul metallic), an internal switch option controlling DSU timing must be activated to control synchronization. ***This timing option must only be activated at one end of the link, the master location.***

The AT&T 2556A DSU receives serial data in a V.35 signaling format and transmits a baseband, bipolar signal whose frequency corresponds to the transmitted data rate. The data and clock signals between the DSA and the DSU conform to the requirements of a balanced interface V.35 per CCITT recommendation, while the control signals from the DSA conform to the Electronic Industries Association (EIA) RS-232C standards. In addition, a local

loopback lead allows the DSA to command the DSU to assume a loopback configuration. This configuration provides software control of the loopback mode. On the line side of the DSU, connectorized cable containing two pairs of transmit and receive leads connect with the facility. Essentially, the DSU consists of a transmitter, receiver, control logic, and customer interface circuits.

To enhance error detection on unencrypted links, the DSU detects bipolar violations and informs the link interface circuitry. This causes the link interface circuitry to detect a link error and enter the octet counting mode. In this mode, the link interface circuitry is searching for the next flag.

DCP3189 Digital Service Unit

The DCP3189 digital service unit (DSU) is functionally the same as the AT&T 2556A DSU. Essentially, the DSU consists of transmitter, receiver, control logic, and customer interface circuits, which are contained on a single circuit pack. The DSU is equipped with ten front panel LEDs that display data, control signals, and diagnostics. The LEDs indicate the power and signal present status of the DSU and the type of loopback control being used when it is initiated. AC power is provided to the DSU via a mounting that contains two power circuit packs. These circuit packs operate in an active/standby mode such that each circuit pack can provide power to all DSUs in the nest. Each DSU is individually fused.

There are three front panel loopback controls: local digital, local analog, and remote digital. Under normal conditions, a software-controlled loopback is used rather than the front loopback panel controls. Circuit board mounted switches control programming, diagnostics, and loopback enabling. These switches select the data speed required in the office. Also, when the signaling link connects to a collocated office, these switches are used to select the internal clock option.

Channel Service Unit

The channel service unit (CSU) (Figure 2-9) is used only with the 56kb/s digital data service transmission facility and is primarily intended for full-duplex operation in a four-wire application. No channel service unit is required for short-haul signaling links to a collocated office. The channel service unit provides access to the synchronous 56kb/s digital data service transmission facility while providing maintenance testing abilities, equalization, wave shaping, and loop loss. Data is transmitted via the channel service unit in a modified bipolar format.

Physically, the channel service unit consists of a housing, a power unit, and two circuit packs interconnected by a flexible cable harness. The circuit packs consist of a transmitter and receiver. They are of the HR-type and are coded according to the signaling speed being used. Digital signaling links operating with a 56 Kb/s signaling speed use the AT&T 550A-L1/5 CSU.

The receiver circuit pack provides a fixed-line build-out network and an automatic-line build-out network. The two networks compensate for variations in the gauge and length of cable. The transmitter circuit pack is equipped with a

relay that can be operated by a remote test center to set up a loopback circuit. The relay contacts bridge the leads toward the facility and open the leads toward the digital service adapter. A pair of transmit leads and a pair of receive leads connect the channel service unit with the digital service adapter. A status indicator lead connects the channel service unit with the associated node. The node is informed, via the status indicator lead, when a loopback has been set up so that an attempt is not made to use the channel

A PWR and TST LED is provided on the channel service unit. The PWR LED is lighted when AC power is supplied to the channel service unit and 8.2V DC is available from the power unit. The TST LED is lighted when a remote test center has a loopback established for testing purposes.

Digital Service Adapter

Each digital service adapter (DSA) (Figure 2-10) is associated with a digital service unit (DSU) and possibly a channel service unit (CSU). A CSU may not be required when the signaling link is used in a collocated arrangement. All signals transmitted to or received from a digital signaling link (SLK) pass through a digital service adapter.

The digital service adapter provides signal level translations between the RS442/RS423 link interface signaling format and the RS232/V.35 digital service unit signaling format. Control lead signals conform to the unbalanced RS232 format standards; while the data and clock leads conform to the balanced V.35 CCITT format standards. The digital service adapter also provides an external loopback on the line side of the digital service unit. The loopback is controlled by the central processor (3B Computer) and is established by the operation of a relay in the digital service adapter. The relay contacts bridge the transmission leads in the local direction. When the relay is in the normal or non-operated state, the leads are cut through to the signaling link.

The digital service adapter is equipped with the circuitry to select the signaling speed at which the digital facility access circuit operates. Two miniature-ganged switches are set to different positions to obtain the correct signaling speed. All digital facility access circuits used by the common channel signaling (CCS) signaling speed. However, signaling speeds of 2.4, 4.8, and 9.6 Kb/s can be provided for other digital signaling link applications.

The following are the two existing versions of the digital service adapter (DSA):

- TF5 Digital Service Adapter
- TF9 Digital Service Adapter.

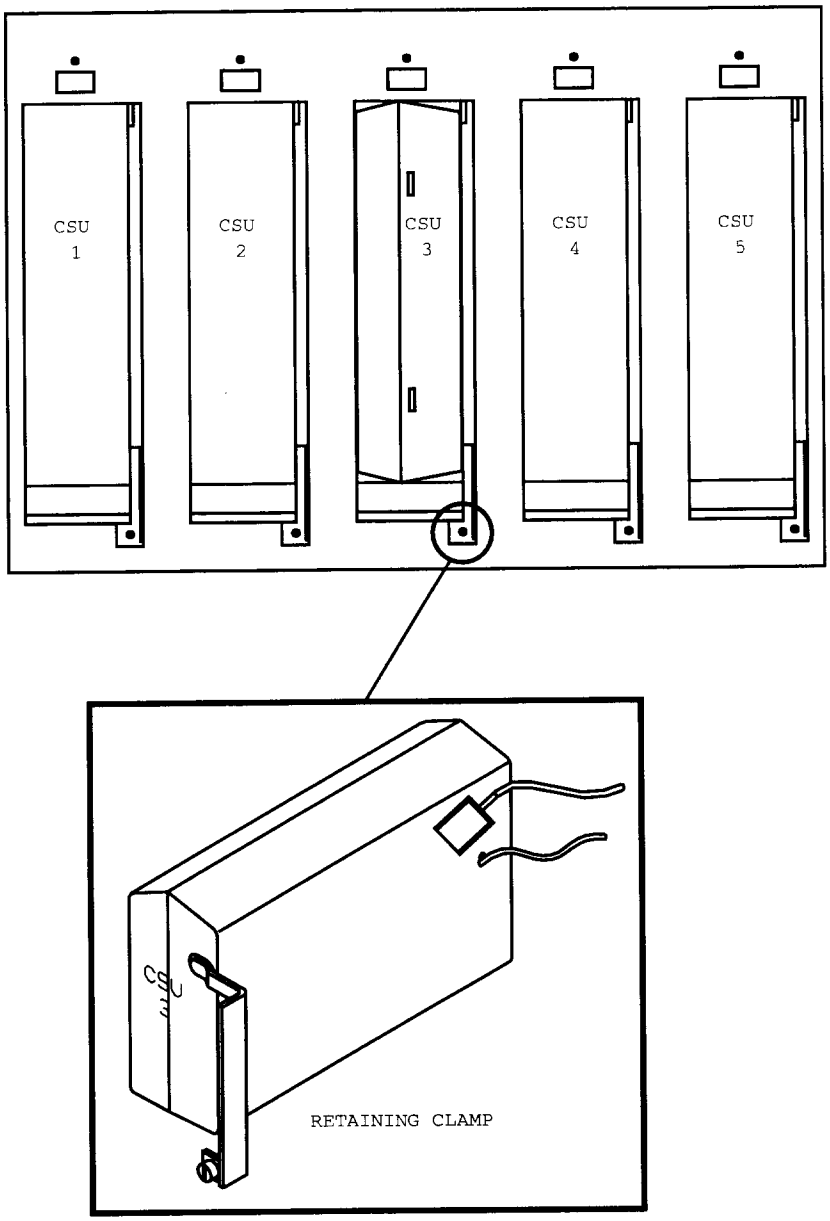


Figure 2-9. Channel Service Unit (CSU) Mounting

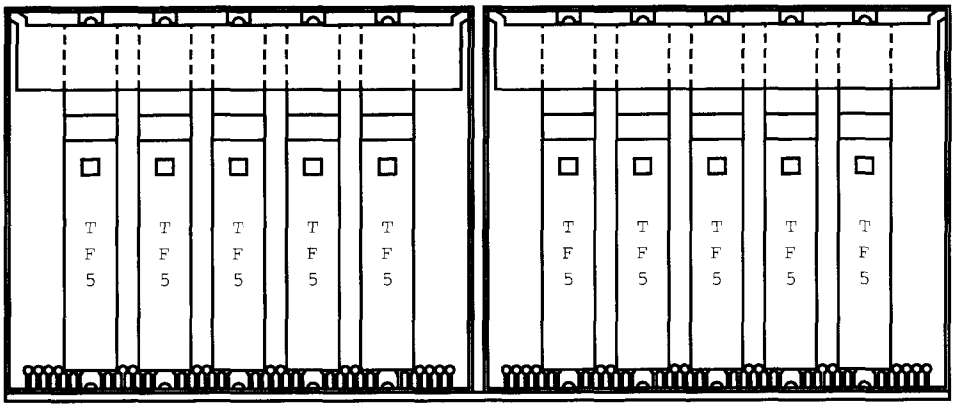


Figure 2-10. Digital Service Adapter (DSA) Mounting

Both versions of the digital service adapter perform the same functions with the exception that the TF9 DSA does not connect to the line side of the data selector unit. The reason for two versions of the digital service adapter is the digital service unit used with each. The TF5 digital service adapter is used when a AT&T 500B data service unit or an unmodified AT&T 2556 data service unit/channel service unit (DSU/CSU) combination is used. The TF9 digital service adapter is used when a Datatel digital service unit or a modified AT&T 2556 (2556 L-1A/2) data service unit/channel service unit (DSU/CSU) is used.

Both the TF5 and TF9 digital service adapter operate using -48V DC and include DC-to-DC converters to convert the -48V DC to various voltage levels required for on-board integrated circuits. All input/output wiring is made using connectorized cables and backplane connector fields.

AC Power Unit

The AC power unit (Figure 2-11) houses two -48V DC to 120V AC inverters that consists of a 393A and a 495H1 power module. These inverters (A and B) supply power to the AC power distribution units. Each AC power distribution unit (Figure 2-12) is equipped with five duplex receptacles that are accessed from the rear of the unit. In addition, the distribution units contain five 70G fuses associated with the receptacles. The AC power distribution unit receptacles provide power for the DSUs and CSUs.

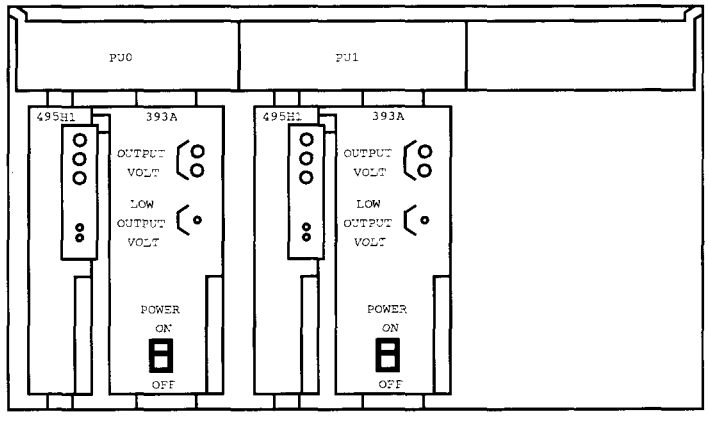


Figure 2-11. AC Power Unit Mounting

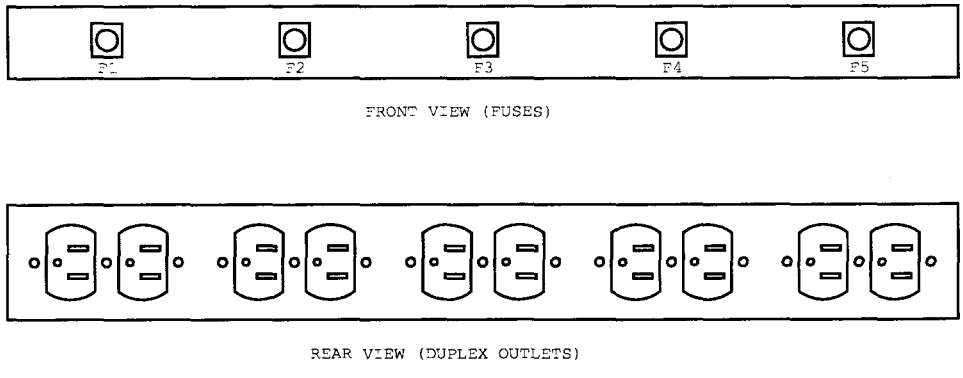


Figure 2-12. AC Power Distribution Unit Mounting

Fuse and Control Panel

The fuse and control panel (Figure 2-13) provides the digital facility access (DFA) cabinet with fuse blocks to fuse units within the cabinet, a portable data terminal jack, an office telephone jack, a 660-type telephone circuit jack, and power/alarm circuitry controls. The power/alarm circuitry controls include the following:

- Alarm Cutoff Key
- Lamp Test Key
- Power Alarm Reset Key.

The ALARM CUTOFF key closes SCAN circuits that request the processor to silence the present alarm. However, subsequent alarms are not inhibited by this action. The LAMP TEST key activates the FA lamp on the fuse panel and the PWR ALM lamp on the control panel. The PWR ALM RESET key is used to release all activated alarm relays after power troubles have been cleared. However, if the power alarm is due to a problem with the cabinet fan units, the problem must be corrected and the fan unit alarm reset key (ON/RESET) operated prior to operating the PWR ALM RESET key on the fuse and control panel.

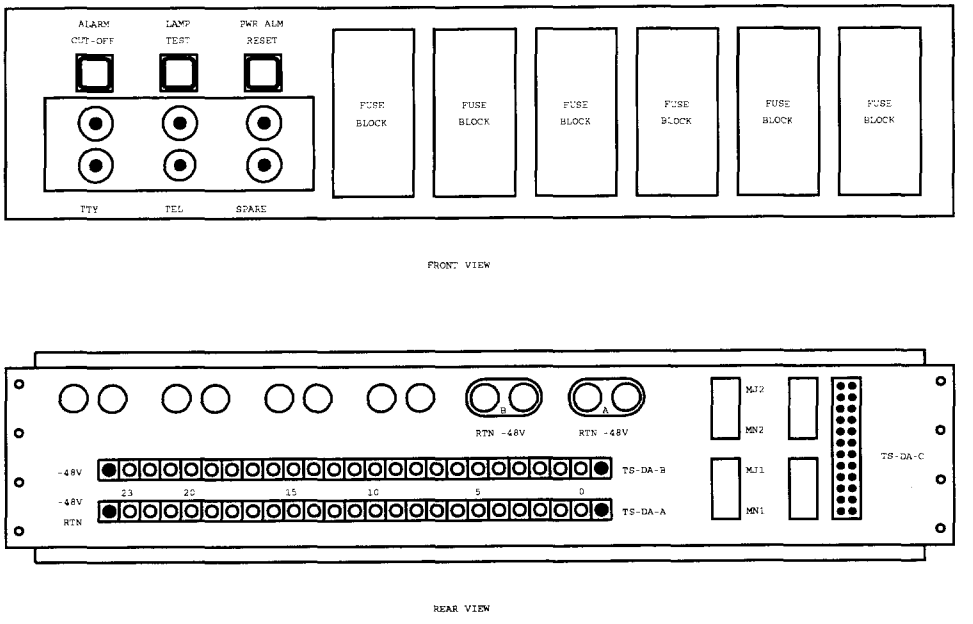


Figure 2-13. Fuse and Control Panel Mounting

Equipment Addressing and Assignments

Node Addressing

Each node (LN, RPCN, DLN, etc.) on the ring has a physical and machine address assigned to it. The physical address is assigned using strapped wiring on the backplane of each unit. Each address is unique to the cabinet, group number, and the position, member number, in the cabinet. Therefore, units are not interchangeable without modifying the address strapping and ensuring that shelf units are correctly numbered left to right or right to left. The machine address is based on the physical address, which is determined by group and member number. There are 64 (0 through 63) groups and 16 (0 through 15) members in each group. The formula to compute the machine address is illustrated by the following example:

Machine address = $(16)(x) + y$

x = Group number (0 through 63)
y = Member number (0 through 15).

Using the above formula:

A LN in position 15 of group 32 has machine address $(16)(32) + 15 = 527$.

A RPCN in position 0 of group 32 has machine address $(16)(32) + 0 = 512$.

Node Assignments

It is recommended that node assignments be made in a manner so that, in the event of a ring failure, paired nodes would not both be isolated by most multiple ring fault configurations. Diversity can be provided by using an intricate node assignment and power distribution scheme.

To provide maximum reliability in the event of a ring reconfiguration, it is recommended that the RPCNs be spaced with an approximately equal number of nodes between RPCNs. This number is determined by dividing the number of nodes by the number of required RPCNs. The DLNs should also be spaced apart from each other on different shelves and away from RPCNs.

Facility Assignments

The equipment engineer and the administration/engineering support organization should work together in making facility assignments. In general, assignments should take paired links and links from the same location and separate them according to power diversity within the cabinets.

Signaling Links

3

Contents

Signaling Links

3

General

The CNI ring application link nodes interface with the SS7 network or customer premise equipment (CPE) via signaling links. Signaling links associated with the 4ESS Switch CNI ring are categorized as SS7 signaling links.

Each in-service link of a link set is associated with one or more signaling link selection (SLS) codes. The Balancing Load Selection On-Link Selection (BLSLS) feature, available with 4E21R1 (4AP14) generic program, ensures that SLS codes are evenly distributed among the in-service links.

Signaling System No. 7 Signaling Links

General

The SS7 signaling links (SLKs) operate at 56 kb/s and, as shown in Figure 3-1, is comprised of a digital service adapter (DSA) and a digital service unit (DSU) which may be used in conjunction with a channel service unit (CSU). The digital service adapter may be either a TF5 or TF9 circuit pack. The digital service unit may be one of the following:

- AT&T 500B DSU
- AT&T 500B DSU/AT&T 550A CSU combination
- **DATATEL*** DSU/CSU combination
- AT&T 2556 DSU/CSU combination.

The TF5 digital service adapter is used with a AT&T 500B DSU, an AT&T 500B DSU/550A CSU combination, or an unmodified AT&T 2556 DSU/CSU combination. The TF9 digital service adapter is used with a **DATATEL** DSU/CSU combination or a modified AT&T 2556 (2556 L-1A/2) DSU/CSU combination.

NOTE:
The modified AT&T 2556 (2556 L-1A/2) DSU/CSU combination provides loopback abilities. Presently, the AT&T 2556 L-1A/2 is not available. Upon availability, more information will be provided.

The SLK length determines whether or not a channel service unit (CSU) and/or transmission facility is required for digital transmissions. When a transmission facility is not required, internal timing must be provided by modifying the control office digital service unit (DSU). This is accomplished by adding a transmit clock (112A circuit module, J3F010, List 6) to the AT&T 500B DSU. The AT&T 500B DSU with an added 112A circuit module is designated as an AT&T 502B DSU.

The SLK length determines the configuration of DSUs, CSUs, and transmission facilities used with digital signaling links. Signaling link lengths can be classified as follows:

- 1000 feet or less
- Greater than 1000 feet but less than or equal to 9 miles
- Greater than 9 miles.

* Registered trademark of DATATEL Inc.

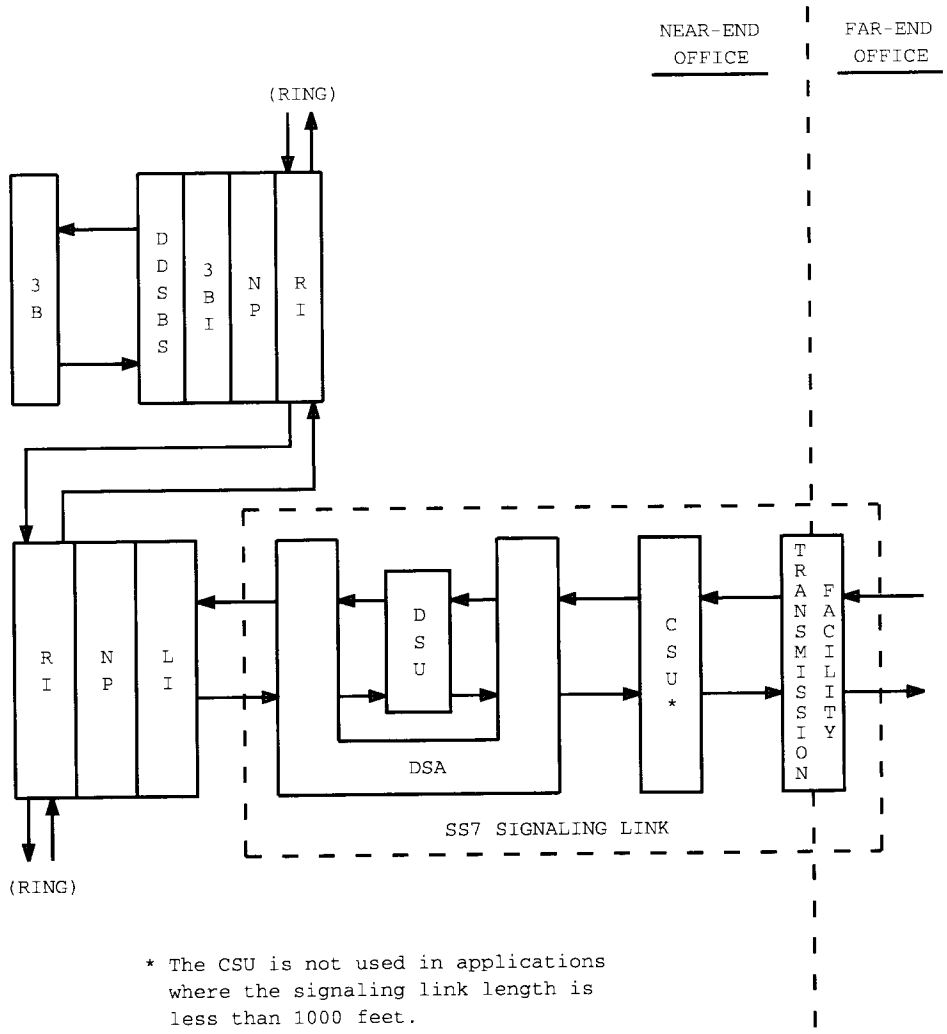


Figure 3-1. Signaling System No. 7 Signaling Link

Cases A, B, C, and D (Figure 3-2) use block diagrams to illustrate the configuration of DSUs, CSUs, and transmission facilities used with the different signaling link length classifications.

Case A (Figure 3-2) illustrates a signaling link with a length of 1000 feet or less. Under this condition, only a DSU is required at each end of the signaling link. At the designated control office, an AT&T 502B DSU (AT&T 500B DSU with 112A circuit module modification) must be used to provide internal timing. The other office uses a AT&T 500B DSU. Neither a CSU nor a transmission facility is required with this signaling link.

Case B (Figure 3-2) illustrates a signaling link with a length greater than 1000 feet but less than or equal to 9 miles. Under this condition, a DSU and CSU are required at both ends of the signaling link. At the 4ESS Switch office, an AT&T 502B DSU (AT&T 500B DSU with 112A circuit module modification) must be used to provide internal timing. The other office uses an AT&T 500B DSU. No transmission facility is required with this signaling link. However, repeaters are required for distances greater than 3 miles. A maximum of two repeaters may be installed per signaling link.

Case C (Figure 3-2) illustrates a signaling link with a length greater than 9 miles. Under this condition, a DSU and CSU is required at both ends. A transmission facility is also required with this signaling link. Timing is provided by the transmission facility; so, an AT&T 500B DSU is used at both ends of this arrangement.

Case D (Figure 3-2) illustrates a signaling link that uses the **DATATEL** DSU/CSU combination or AT&T 2556 DSU/CSU combination. A transmission facility may or may not be used with this signaling link. A transmission facility is not required for collocated offices. If a transmission facility is not required, the DATATEL or AT&T 2556 DSU/CSU combination must be set up via options provided to operate as an AT&T 502B DSU. For the **DATATEL** DSU/CSU combination, Switch 1-Position 5 must be enabled (ON) to provide this feature. For the AT&T 2556 DSU/CSU combination, Switch Position 6 must be enabled (ON) to provide the same feature.

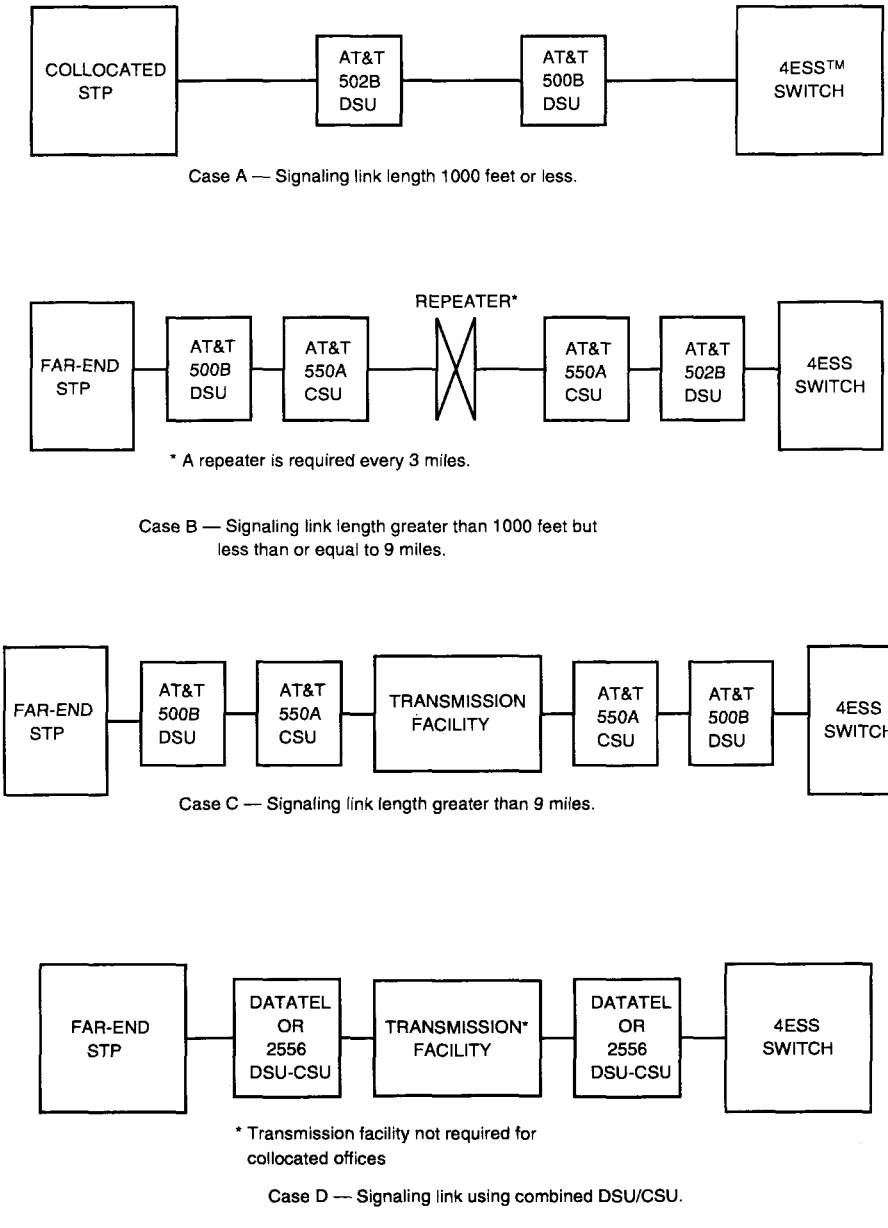


Figure 3-2. Signaling System No. 7 Signaling Link Lengths

SS7 Signaling Link States

Three *major SS7 signaling link states* exist: **UNEQUIPPED, UNAVAILABLE**, and **AVAILABLE**. To change from one major state to another, a recent change (RC) function must be used. The major states are considered static states because they can only be changed by performing a recent change, and their status resides in both main memory and on the disk. In a system boot, the major states of the signaling links are restored from the disk.

In addition to the major states, there are related *minor signaling link states*. The minor states are under control of program documentation standard (PDS) commands found in the Input Message Manual and Output Message Manual. The minor states are considered dynamic states because they can easily be changed via PDS input commands, and their status is stored in main memory only. In a system boot, the minor states are set to either **Grow** or **OOS**.

The following paragraphs describe some basic characteristics about each signaling link state:

a. ***UNEQUIPPED:*** The signaling link has no link configuration data in main memory or on the disk. Diagnostics can be run while in this state.

b. ***UNAVAILABLE:*** The signaling link must be in this state for the user to change link configuration data.

   Two minor states, **Grow** and **Test**, are associated with this major state. While in the **UNAVAILABLE-Grow** state, no link usage information (for example, cyclic redundancy check [crc] errors, etc.) is provided to the user. The signaling links that have passed their installation acceptance tests and are not ready for preservice testing should be left in the **UNAVAILABLE-Grow** state.

   When the signaling link is ready for preservice testing, it should be moved to the **UNAVAILABLE-Test** state. While in this state, the signaling link provides the user with link usage information (crc errors detected on the link, number of unsolicited frames received on the link, etc.), but does not start the link protocol. A low cycle redundancy check (crc) error count indicates that the link is properly terminated to another protocol entity. Unlike some other signaling links, the protocol on the link cannot execute while in the self-looped mode. Attempting to do this causes protocol exception measurement counts but has no other adverse effect.

c. ***AVAILABLE:*** Three minor states, **In-Service, Out-of-Service,** and **Manual Out-of-Service**, are associated with this major state. When a signaling link is moved from the **UNAVAILABLE** state to the **AVAILABLE** state, the signaling link is first moved to the **AVAILABLE-OOS** state while the protocol attempts to be established. If the signaling link protocol is successfully established, the signaling

link is moved to the **AVAILABLE-IS** state. Once in this state, the signaling link is in service, and signaling traffic can commence. In general, all signaling links should be moved to the **AVAILABLE-IS** state by the service-order due date.

A signaling link in the **AVAILABLE-IS** state is automatically moved to the **AVAILABLE-OOS** state, when an extended error condition occurs—greater than 90 seconds of link outage. The system automatically attempts to recover signaling links in this state; that is, return them to the **AVAILABLE-IS** state. This activity continues indefinitely; unless, the node is removed manually for diagnostics; or the link is moved to the **AVAILABLE-MOOS** state.

If it is necessary to work on a signaling link in the **AVAILABLE-IS** state, such as running diagnostics or replacing hardware, the link must manually be removed from service. When the link is moved to the **AVAILABLE-MOOS** state, the protocol on the link is disconnected. However, the link is still monitored for valid and invalid frames.

Table 3-A shows the transitions that can be made from one signaling link state to another. A signaling link in one state can be changed to another state via either a recent change or PDS command.

Table 3-A. Signaling System No. 7 Signaling Link State Transitions

From	To			
UNEQP	UNAVL GROW	UNAVL TEST	-	-
UNAVL GROW	UNEQP	UNAVL TEST	-	-
UNAVL TEST	UNAVL GROW	AVL MOOS	-	-
AVL MOOS	AVL OOS	AVL IS	-	-
AVL OOS	UNAVL GROW *	UNAVL TEST *	AVL MOOS *	AVL IS
AVL IS	UNAVL GROW	UNAVL TEST	AVL MOOS	AVL OOS

* Transient state that is automatically accessed when signaling link is moved to the AVL-IS state.

SS7 Signaling Link Hardware Indicators

The SS7 signaling link DSU is responsible for providing link node access to the synchronous digital data system (DDS) through the digital service adapter (DSA) and the CSU. The AT&T 2556 and DATATEL DCP3189/DCP3189-B DSUs combine the DSU and CSU circuitry into one unit. All DSUs receive serial, unipolar data and transmit a baseband, bipolar signal with a frequency corresponding to the transmission data rate. Data and clock signals passed from the link node to the DSA and DSU meet CCITT V.35 recommendations for a balanced interface while control signals conform to the Electronic Industries Association (EIA) RS-232C requirements. Generally, transmitted signals flow from the link node to the DSU via the DSA and CSU, while signals received from the facility follows the same route in reverse.

All DSUs are capable of communicating with each other, but different DSU types offer unique functions. The most effective testing involves end-to-end testing using the same DSU types. However, testing between unlike DSUs can still offer valuable maintenance information. One attendant end-to-end tests cannot be performed between unlike DSU types, but tests can be performed if both offices have voice communication. It is also possible for testing to be performed from remote test centers.

The following is a description of loopback mode switches and lamps pertaining to end-to-end testing for the AT&T 500B DSU/AT&T 550A CSU combination, AT&T 2556 DSU, and DATATEL DCP3189/DCP3189-B DSU.

a. *AT&T 500B DSU/550A CSU Combination:*

Loopback Mode Switches

LL - Operation of the **LL** switch provides local bidirectional loopback at the DSU line interface.

RT - Operation of the **RT** switch provides unidirectional loopback at the V.35 interface toward the facility.

Loopback Lamp Indicators

LL - The **LL** lamp when illuminated indicates when the LL switch is operated or when a CHANNEL LOOPBACK command is received from the network.

b. *AT&T 2556 DSU*

Loopback Mode Switches

LL - Operation of the **LL** switch provides local loopback at the DSU line interface. There is a 5-second pause after operation.

DL - Operation of the **DL** switch provides digital loopback at the DSU line interface.

c. *DATATEL DCP3189/DCP3189-B DSU*

Loopback Mode Switches

LAL - Operation of the **LAL** switch provides local loopback at the DSU line interface.

LDL - Operation of the **LDL** switch provides digital loopback at the DSU line interface.

Loopback Lamp Indicators

TST - The **TST** lamp when illuminated indicates when the DSU is in the test mode.

CMP - The **CMP** lamp when illuminated indicates successful reception of test pattern.

Signaling System No. 7 Signaling Link Hardware Options

The SS7 signaling link digital service unit (DSU), channel service unit (CSU), and digital service adapter (DSA) hardware have options that can be set for specific applications. These options for specific hardware types are identified in Tables 3-C *through* 3-F.

Signaling System No. 7 Signaling Link Routing

The SS7 signaling link routing activity can include the addition of SS7 signaling links, the deletion of SS7 signaling links, and changing SS7 link configuration data. Signaling link routing is performed via a combination of input/output messages and recent change/verify functions using the maintenance CRT.

Table 3-B. TF5 Digital Service Adapter Options

Option Switch	Option Setting
S1A	ON
S1B	OFF

Table 3-C. AT&T 500B Digital Service Unit Options

Option Designation	Option Name	Option Setting
XL	System status removed	H1 header position 8 shunted
XN	Switch LED assembly installed	-
XO	LL spring clip installed	-
YK or YL	Signal ground connected (YK) or disconnected (YL) from frame ground	S1 switch either IN or OUT depending on what provides the best SLK performance.
YR	Circuit assurance removed	H1 header position 5 shunted
YS	Continuous request to send	H1 header position 2 shunted

Table 3-D. Channel Service Unit Options

Option Designation	Option Name	Option Setting
WV	Fixed line build-out network installed	H1 header position 3, 5, and 9 shunted
YK or YL*	Signal ground either connected (YK) or disconnected (YL) from frame ground	S1 switch either IN or OUT depending on what provides the best SLK performance

Table 3-E. DATATEL* Digital Service Unit Options

Option Switch Designation	Option Switch Position	Option Setting (Note)
S1	1	OFF
	2	OFF
	3	ON
	4	ON
	5	OFF*
	6	OFF
	7	ON
	8	ON
S2	1	OFF
	2	ON
	3	OFF
	4	ON
	5	ON
	6	ON
	7	ON
	8	ON

Note: Do not change the setting on the **DATATEL** DSU while the power is ON.

* This switch should be ON when the DSU is modified to be a AT&T 502B DSU.

* DATATEL is a registered trademark of DATATEL Inc.

Table 3-F. AT&T 2556 Digital Service Unit Options

Option Switch Position	Option Setting	Option Switch Position	Option Setting
1	Enable	7	*
2	Disable	8	Disable
3	Enable	9	Enable
4	Disable	10	Enable
5	Disable	11	Enable
6	*	12	Not used

*This switch should be enabled when the DSU is modified to be an AT&T 502B DSU.

Message Flow

4

Contents

Message Flow

4

General

This section provides an understanding of the "message flow" processes from both the common channel signaling (CCS) network and CNI ring perspective.

Common Channel Signaling Network Overview

The purpose of implementing the common network interface (CNI) ring into the 4ESS™ Switch environment is to gain access to the common channel signaling (CCS) network. The CCS network is utilized by the 4ESS Switch to communicate with other switching offices regarding call setup, calls in-progress, call disconnects, specialized data bases, etc. The communication exchanged is referred to as signaling. The CCS network allows signaling data to be exchanged over paths that are separate from voice paths.

A simplified illustration of a CCS network is shown in Figure 4-1. The network is comprised of signal transfer points (STPs), network control points (NCPs), and switching systems (4ESS Switches, 5ESS® Switches, 1A ESS™ Switches, etc). All interconnected via signaling links (SLKs). Each stored program-controlled system (STP, Service Control Point (SCP), Switching System, etc.) must be equipped with a CNI ring.

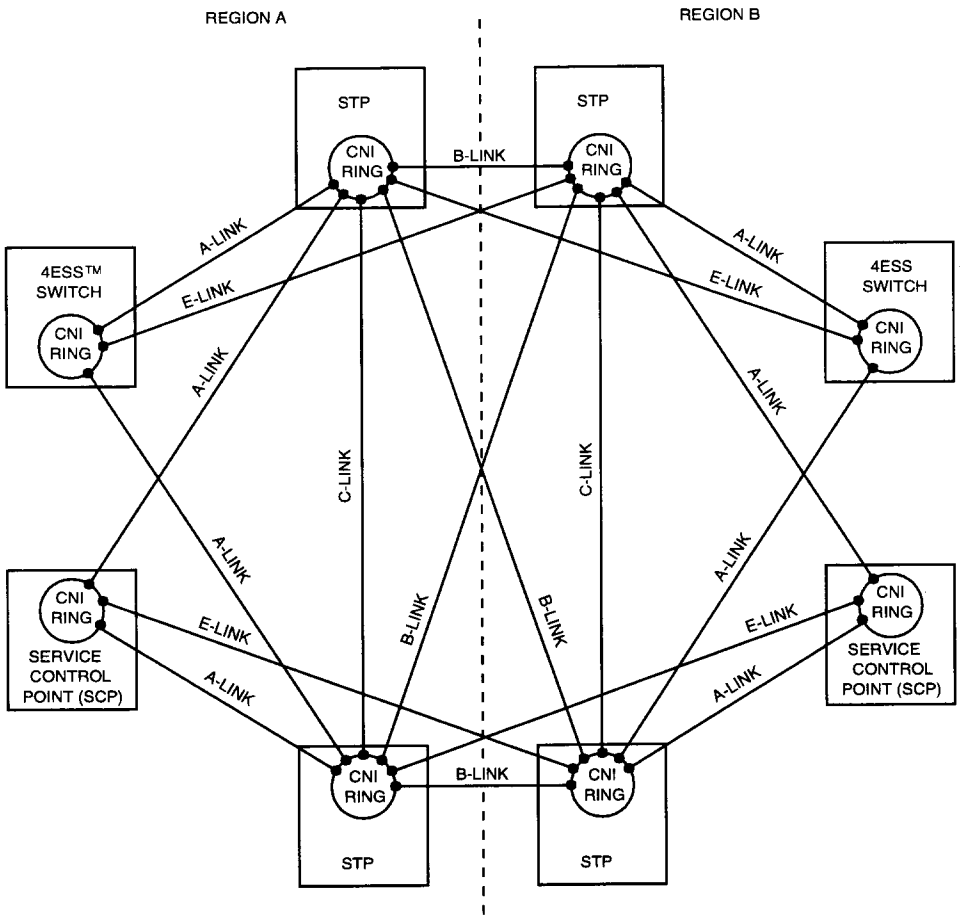


Figure 4-1. Simplified Common Channel Signaling (CCS) Network

A brief description of the functions performed by each CCS network component is as follows:

- ***Signal Transfer Point (STP)*** routes data from one connecting office to another while also administrating the CCS network.
- ***Network Control points (NCPs)*** contain data that provides a variety of custom routing, billing, and calling services to CCS network users.
- ***Switching Systems*** communicate to each other by exchanging signaling data over the CCS network. The signaling data is used to setup voice paths, make data base queries, obtain switching system status, etc.
- ***Signaling Links (SLKs)*** are used to transfer data between users of the CCS network. The four types of signaling links used in the CCS network are as follows:

    1. *Access (A) links* are used to connect all switching offices and network control points (NCPs) in the same region to a mated pair of STPs. All A-links are equipped in pairs with one signaling link to each local STP within a region.
    2. *Bridge (B) links* are used to connect a mated pair of STPs in one region to a mated pair of STPs in another region.
    3. *Cross (C) links* are used to connect a STP to its mate STP in the same region.
    4. *Extended Access (E) links* access is the connection of signaling links between SEPs and non-home STPs. At the switch E-links provide alternate routing to traffic that is carried by A-links. The E-link feature gives CNI the ability to specify up to three routes (either A-link or E-link sets) to any signaling point.

As previously stated, each system connected to the CCS network must be equipped with a CNI ring. The CNI ring provides the signaling link ring access nodes, ring bus structure, control nodes and 3B Computer (Figure 4-2). All users of the CCS network are connected together using specific signaling links (A, B, or C links) and CNI ring access nodes (SS7 nodes). The exchange of information between SS7 nodes over digital signal links within the CCS network is governed by the SS7 signaling protocol. The SS7 protocol is based on a modified structure of the open systems interconnection (OSI) model.

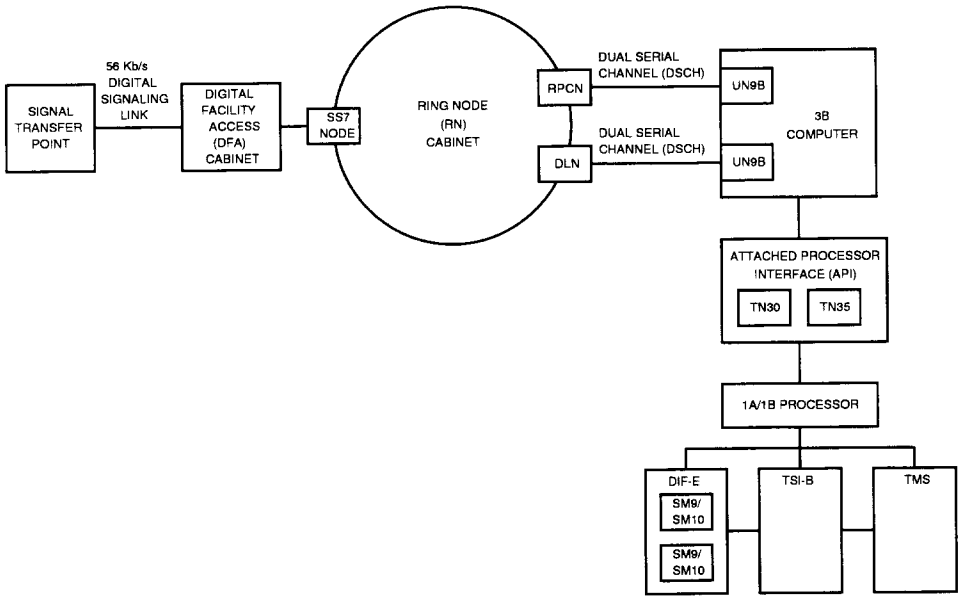


Figure 4-2. Common Network Interface Ring—4ESS™ Switch Application

Open Systems Interconnection Protocol Model

The open systems interconnections (OSI) protocol model consists of seven layers defined by the International Telegraph and Telephone Consultative Committee (CCITT) to standardize the interconnection and exchange of signaling information between common channel signaling (CCS) system users. At the time of development, the OSI mode identified the common communication functions found in all systems, precisely defined the functions, placed the functions into a specific hierarchy, and grouped the functions into seven distinct layers. Interfaces between the seven layers were defined to allow specific layers to work with other layers within the model. Each layer performs a specific function and is dependent on the layers below it to accomplish a task.

The seven layers (TABLE 4-A) can be categorized into two basic groups consisting of three layers each and a layer serving as a bridge between the two groups. Layers 1 through 3 are network specific and define the characteristics of the network data link and addressing scheme. Layers 5 through 7 are end-user specific and define the method users can communicate with each other in addition to describing service characteristics between the end-user layers (5 through 7) and network layers (1 through 3).

Table 4-A. Open Systems Interconnection (OSI) Model Layer Identification

Layer	Identification	Use
7	Application	End-User Specific
6	Presentation	
5	Session	
4	Transport	Bridge
3	Network	Network Specific
2	Data Link	
1	Physical	

The following list identifies each of the seven OSI model layers and defines associated functions performed.

Physical Layer — Defines the physical, electrical, and functional characteristics of a signaling data link. In addition, the Physical Layer controls the data circuits and the transfer of bits to and from the network elements.

Data Link Layer — Determines signaling link to transmit messages on and controls the network connections. The network layer will setup, maintain, and terminate connections between the individual network elements that provide the hardware or software for the transport layer.

Transport Layer — Controls the transfer of data between end users, thereby relieving users of concerns reguarding transfer details.

Session Layer — Establishes, maintains, and terminates the communication session between users. The session layer determines which user has the right to transmit information at a given time and synchronizes activities of other uses.

Presentation Layer — Responsible for preserving the information transferred between the end user applications and resolving any syntax differences that occur during transmission.

Application Layer — Serves the end user by providing information required by the software application. These applications could be data for airline reservations, credit card checking, or other meaningful communication to the end users.

Common Channel Signaling Network Routing

Data is exchanged throughout the CCS network over digital signaling links. The signaling links connect to SS7 nodes on the CNI ring. Arrangements are made throughout the CCS network to ensure the reliable exchange of data during the presence of signaling link transmission disturbances or network failures.

All A-links in a CNI equipped office are duplicated. One signaling link is assigned to each of the two signal transfer points (STPs) in a region. Each signaling link is designed to operate normally at 40 percent capacity and function in a load-sharing manner. If the volume of data increases to over 40 percent, an addition pair of signaling links must be added to handle the load. In the event of a signaling link failure, the mate signaling link supports the total load until the failing link can be restored.

In addition to signaling links being duplicated, mated STPs contain identical routing data. This duplication of routing data further expands the reliability of signaling link selection. Information being exchanged from 4ESS Switch office A to 4ESS switch office B is normally transmitted via signaling link A1, processed through STP 0, and retransmitted via signaling link A3. In the event that signaling link A3 fails, the information is transmitted to STP 1 via cross (C) link C1, processed through STP 1, and retransmitted via signaling, link A4. The CCS network signal link (A, B, and C links) and STP configurations provide a multiple combination of paths that information may use to reach its final destination. However, if all signaling links to an office (A1 and A2 or A3 and A4) fail, the office becomes isolated and cannot perform CCS network functions. Under this condition, the local STPs broadcast a message over the network indicating that the office is isolated and no traffic should be sent to the office.

E-link access (shown in Figure 4-3) is the connection of signaling links between the signaling end points (SEPs) and the non-home STPs.

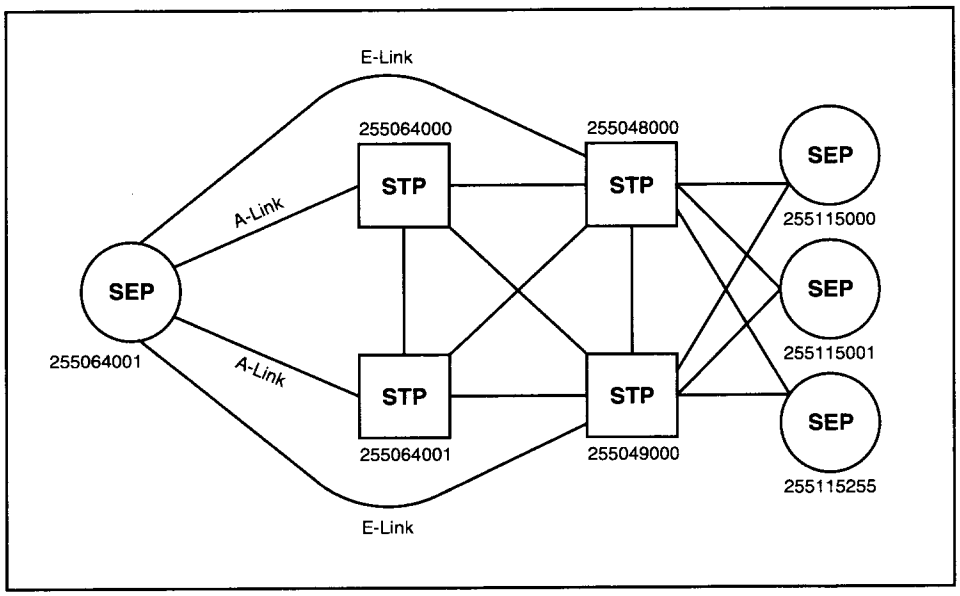


Figure 4-3. Typical E-Link and A-Link Set Routing

Some of the functional characteristics of E-links include the following:

- All Signaling System Number 7 (SS7) data link interfaces that support A-links also support E-links.
- SEP supports E-links to at least two OTHER STP pairs.
- Each SEP supports a maximum total of 16 combined link sets.
- E-links simultaneously support direct routing and back-up routing of traffic to different DPCs.
- The total number of routes to be supported per DPC is three (one primary and two alternates).
- A-link or E-link sets can be provisioned as primary or altrnate per destination.
- The primary link set for a given point code can be the alternate link set for other point codes.
- The number of intranetwork populated and unpopulated clusters supported is 160 (128 populated and 32 unpopulated).

Alternate routing to available back-up link sets is done when signaling points are unavailable over higher priority routes. Alternate routing can occur under the following conditions:

- When primary link set(s) fail
- When the STP mated pair connected to the primary route fails
- When one link set fails and the STP not connected to the failed link set also fails
- Under route unavailability or traffic diversion conditions indicated by Transfer Prohibited (TFP) or Transfer Cluster Prohibited (TCP) Signaling Route Management (SRM) messages.

Signaling End Points does not reroute traffic to alternate routes under congestion, partial link set failures, or any other condition indicated by Transfer Restricted (TFR) or Transfer Cluster Restricted (TCR) SRM messages. Traffic is diverted back to the previously unavailable, higher, priority link set when at least one link of the link set becomes available and in service, or under any condition indicated by TFR, TCR, Transfer Allowed (TFA), or Transfer Cluster Allowed (TCA) SRM messages for the affected destination point.

Integrated Services Digital Network User Part (ISUP) SS7 Call Processing

The ISDN-UP of the SS7 protocol is used for SS7 connection-oriented messages. Figure 4-4 shows a layout of the equipment involved in processing a call for SS7 trunks.

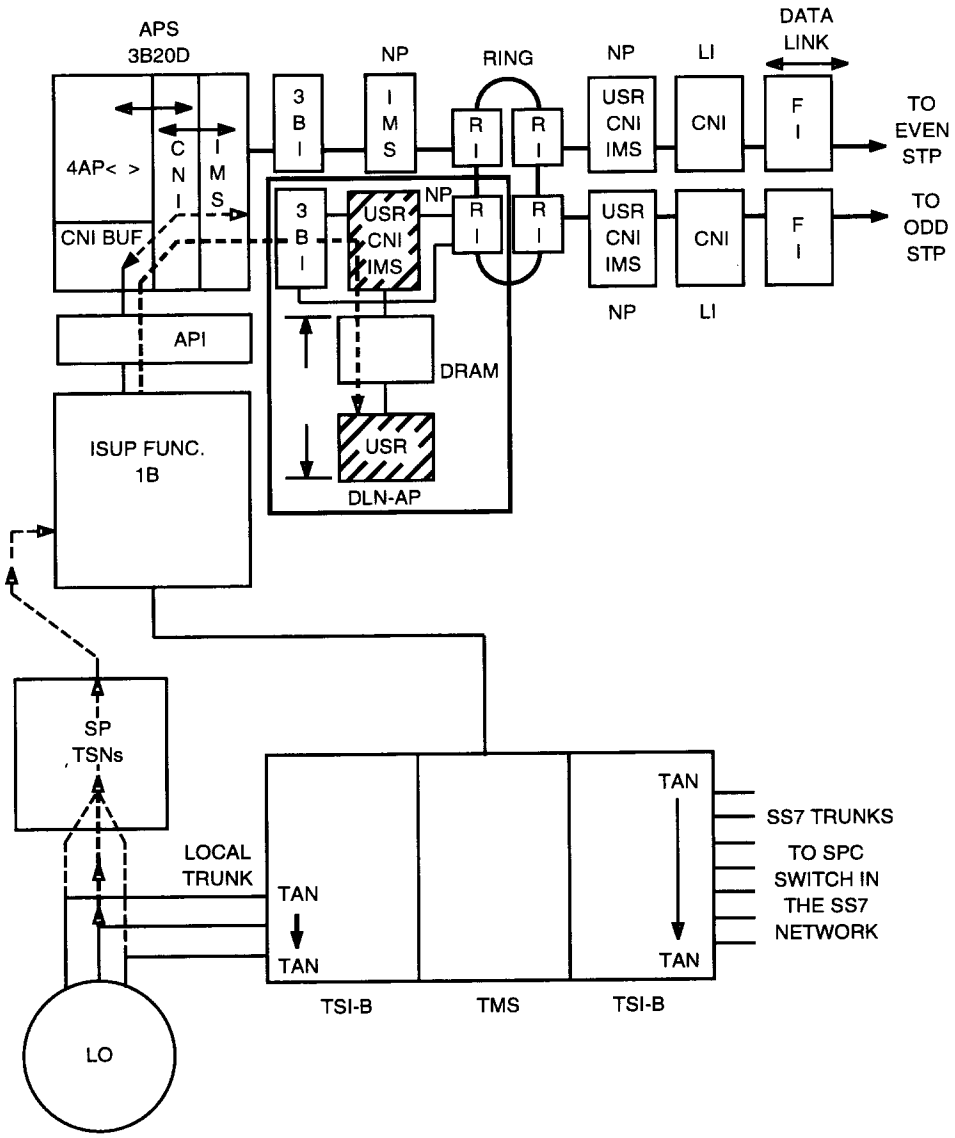


Figure 4-4. ISUP Signaling System No. 7 Call Processing Diagram

The following is a description for a call originating from an LO (local) switching office and terminating over a SS7 trunk to another SPC switching office in the SS7 network.

1. Assume that an incoming call is recognized at the 4ESS switch over a local trunk. The associated SP collects the digits received over the local using the TSN assigned to the trunk. When all the digits are collected, the SP sends the dialed digits to the 1B processor for translation.
2. For this example, assume that the 1B translation identifies the outgoing trunk group as SS7 trunks. Since the outgoing trunk is a SS7 type, the 1B processor ISUP formats the message and sends it to the DLN via the API and CNIBUF.
3. The ISUP - IAM (initial address message) received by the DLN contains the TSN of the associated outgoing TAN and the dialed telephone company BCD digits. The message also contains the ISUP message type, nature of connection, and other information as shown in Figure 4-5.

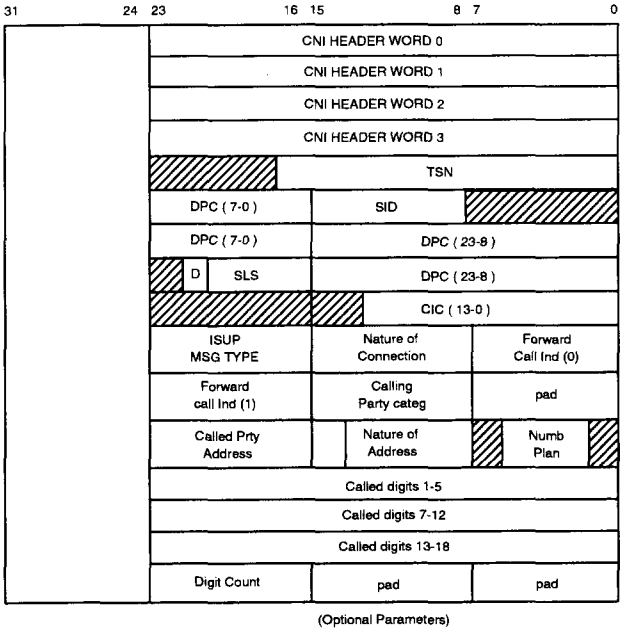


Figure 4-5. ISUP 1B Format — IAM

The DLN-AP translates the TSN into a destination point code for routing the message over the CCS network and a CIC (circuit identification code) to identify the trunk at the far-end switching office. Note that the ISUP 1B format uses a 24-bit word (0 through 23) and has bits 24 through 31 added as a pad for messages from the 1B to the 3B computer. (Refer to Figure 4-6.

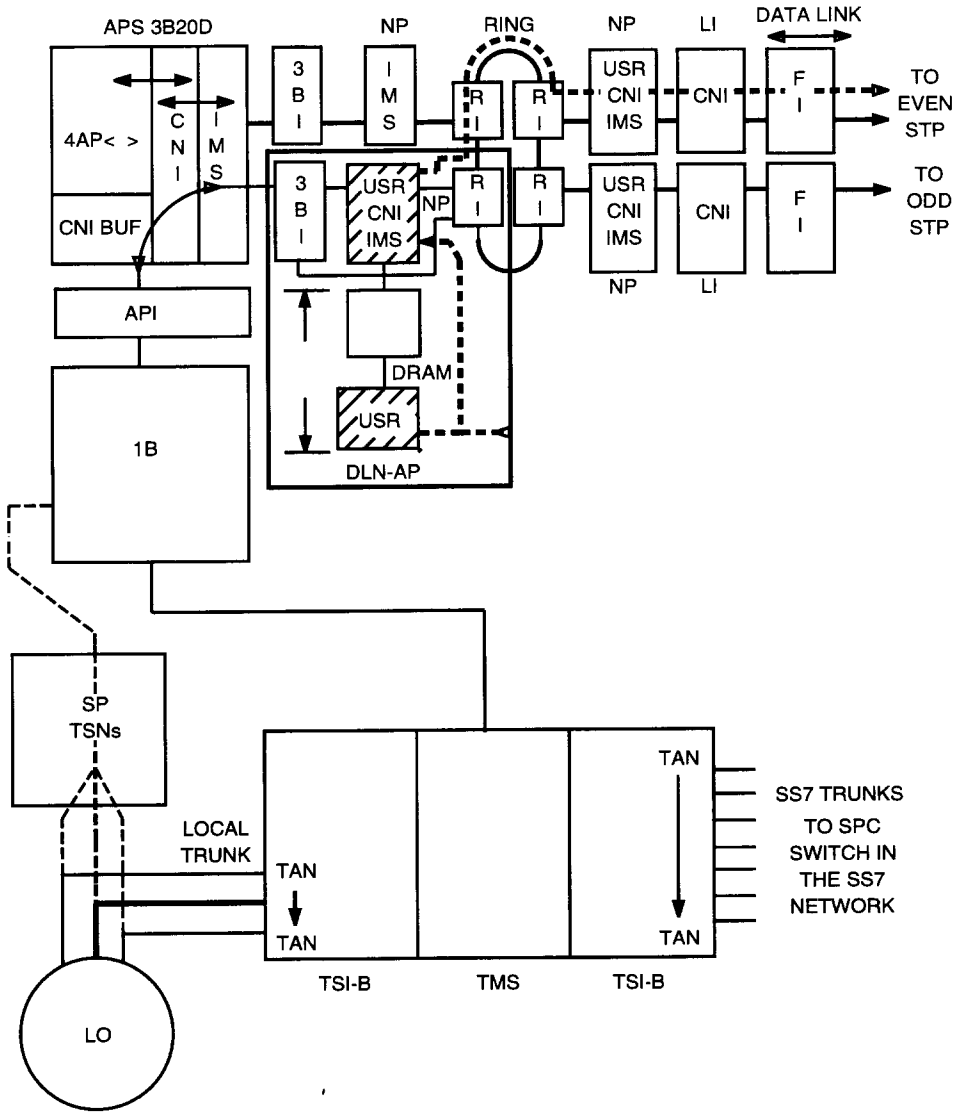


Figure 4-6. DLN-AP Translation of TSN for SS7 Call Processing

4. After the DLN-AP translates the TSN into a DPC and a CIC, DLN-AP then reformats the SS7 message into a 32-bit word format as shown in Figure 4-7.

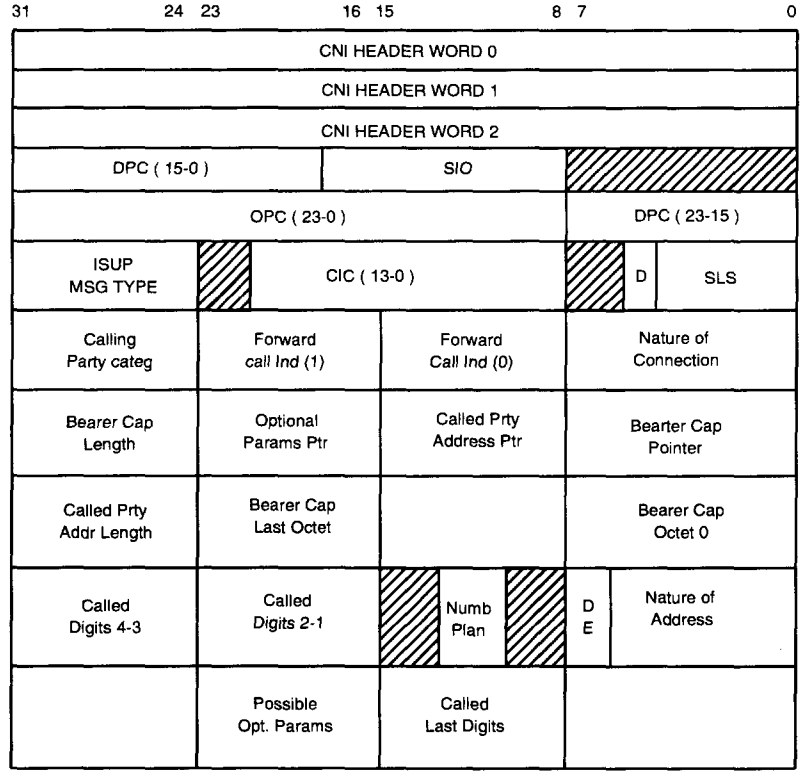


Figure 4-7. ISUP — Initial Address Message for SS7 Routing

The DLN also uses the signaling link selection (SLS) field to specify the outgoing SS7 link for transmission. The MTP function of the CNI software in the DLN uses the SLS field to perform load balancing over the available SS7 links.

5. Once the outgoing SS7 link is determined, the CNI software writes the RNA address of the outgoing link. The IMS software transports the message around the ring from the DLN to the designated SS7 node. The CNI software transmits the message over the signaling link to the STP.

   Various messages are required during a ISUP call setup. The ISUP MSG TYPE field is used to identify one of the following types:

   - ISUP - IAM (initial address message)
   - ISUP - CRO (continuity recheck outgoing)
   - ISUP - CRI (continuity recheck incoming)
   - ISUP - REL (release message)
   - ISUP - ANS (answer message)

   The preceding ISUP message types are routed in the same manner as described for the IAM call process. However, different functions are performed by the 1B processor for each message type (for example, continuity tests, etc.).

6. When subsequent ISUP messages are received from the far-end switch via the STP, the SS7 node routes the message to the DLN. The DLN translates the originating point code (OPC) and CIC into a TSN related to the IAM message for the particular call setup. Since the IAM contains the DPC and OPC, the terminating switch uses the OPC as a DPC for routing the subsequent messages back to the originating office. Therefore, the DLN can relate all subsequent messages to the initial IAM message transmitted. (Refer to Figure 4-8.)

7. When the TSN has been translated by the DLN, a 24-bit word ISUP message is formatted and sent to the 1B for processing. During an ISUP call setup, the originating office puts up the trunk connection to perform the continuity test, if required. If the test is successful and the ANS message is received from the terminating office, the TAN-to-TAN trunk connection is made at both ends. (Refer to Figure 4-8.)

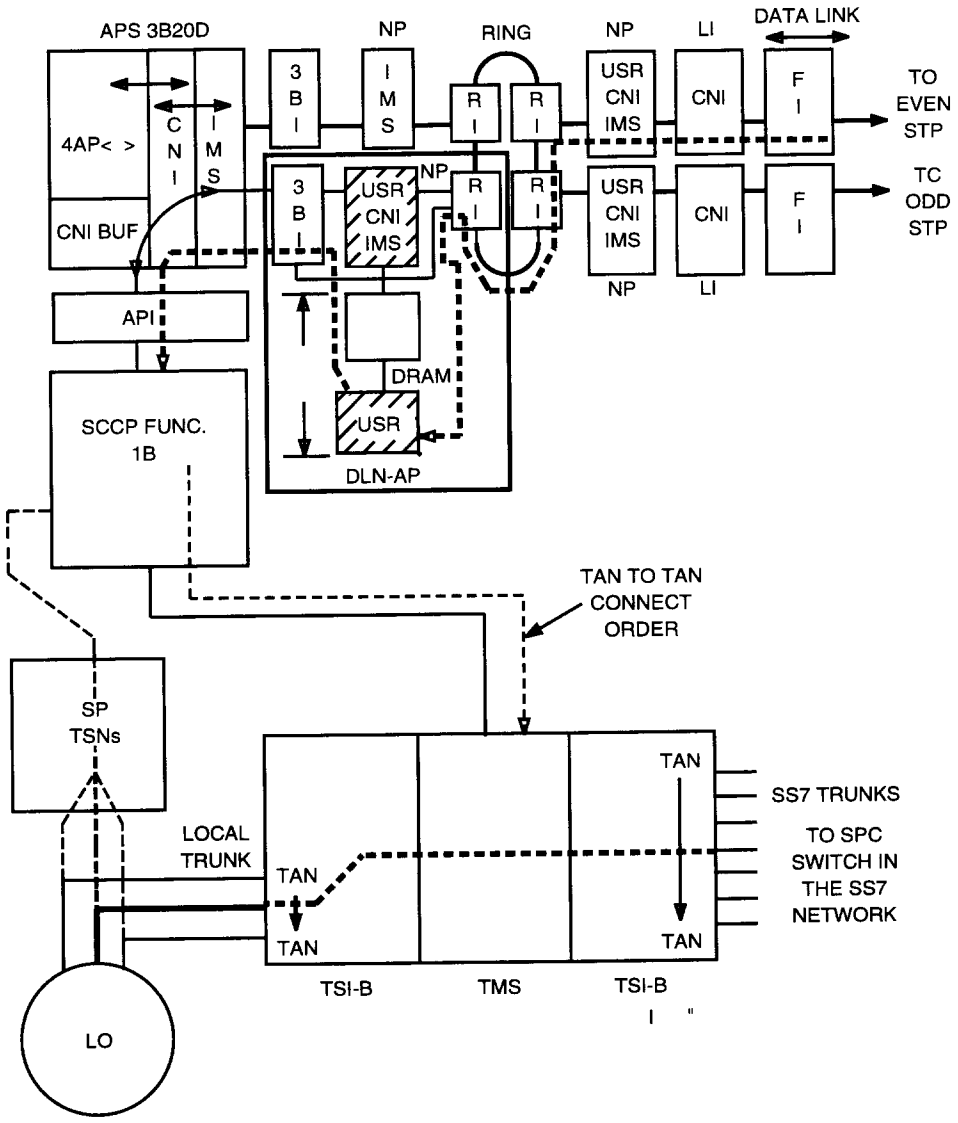


Figure 4-8. OPC and CIC Translated to TSN During SS7 Call Processing

Measurements, Reports, and Critical Events

5

Contents

Contents

Measurements, Reports, and Critical Events

5

General

This section describes the meaning and use of measurement data and critical event messages generated in a CNI-equipped office. This section can be broken down into four parts:

a. ***Description of Measurements:*** The measurements taken, the occurrences that those measurements record, and the internal mechanisms involved in collecting the measurement data are discussed.

b. ***Description of Reports:*** The scheduled and demand reports available to users are listed and explained.

c. ***Description of Critical Events:*** The CCS network critical-event messages and the occurrences they report are described.

d. ***Measurement Output Control Table:*** The format and administration of the five tables composing the measurement output control table (MOCT) are described. This data base is responsible for controlling the output of all measurement reports and critical event messages.

A measurement data plan is intended to provide maintenance and support personnel (users) with data at several different levels. The data is output to users at the level of detail and time intervals required. This is done by taking one common set of measurements in memory, extracting and compiling desired information, and sending the resulting messages and reports to the specified users either automatically or on demand.

NOTE:
Report items not described are not applicable in LEC environment.

Description of Measurements

Introduction

This part discusses the sources of measurements, the generation of measurement data, and measurement descriptions.

A *measurement* can be defined as a "register" that represents the cumulative total of or duration of some occurrence. There are approximately 400 measurements made in a CNI-equipped office. A measurement represents something that happens within the office. This could be an action that occurred within the office as a response to some occurrence outside the office. Therefore, some measurements pertain to the office itself, while others are significant to the entire signaling network. A measurement can be a count of the number of times something happened. For example, it could represent the number of times a new state is entered. Also, it could be the length of time the state lasted. Measurement timers are generally stored in units of milliseconds—exceptions are noted in the measurement descriptions. Most measurements represent occurrences that register in the node processor (NP) or link interface (LI) circuits. Some measurements represent occurrences declared by the central processor.

The measurement data is organized within main memory and on disk files. These files are generated from the measurements collected in the NPs, the LIs, and the central processor. Accessing the data requires that the measurements be identified by some naming conventions. The conventions for naming a measurement are as follows:

a. The mnemonic represents, as closely as possible, the occurrence being measured. The mnemonic is derived from a set of abbreviations representing typical occurrences in a CNI-equipped office. These abbreviations are combined to describe the occurrence.

b. The suffix ***T*** signifies a measurement of an interval, not the number of occurrences.

c. The suffix ***TE*** signifies a threshold has been exceeded.

d. Names include only letters and digits—no special characters.

e. Names are unique and contain no more than 12 characters.

The names given to measurements are used by the MOCT. The *MOCT* controls measurement output to accommodate current operation, administration, and maintenance needs.

Sources of Measurements

The following are two sources of measurements in an office:

- ***Plant Measurements***: originate in the *UNIX** RTR 21.17 Operating System. Refer to the *UNIX* RTR Operating System, Output Message Manual, 3B20D and 3B21D Computers*, 303-081 for plant measurement descriptions.
- ***CNI Measurements***: an occurrence recognized by the CNI-equipped office.

The CNI measurements can be classified into several groups. These measurements are referred to as ring node oriented, link oriented, and total office oriented. This distinction is useful from a maintenance standpoint; faults generally fall into one of these categories. Identifying the source of the error as either a link, a ring node, or the office in general makes troubleshooting easier. Furthermore, the software architecture roughly follows the previously mentioned categories. However, it is not necessary to know which software subsystem generates each measurement.

The measurement data is collected, stored, and output to various destinations within and outside the office. Specifically, UNIX RTR Operating System reports and CNI reports both appear on the maintenance terminal and printer. Support organizations can also request plant or CNI measurement data. An understanding of the source data for particular measurements is very important when designing a customized report.

As previously stated, CNI measurements are classified into the following three categories:

- Ring node oriented measurements
- Link oriented messages
- Total office measurements.

Ring Node Oriented Measurements

Ring node oriented measurements include ring blockages, node isolations, ring read/write errors, etc. Ring node measurements are mostly concerned with counts and transmission errors relating to internal messages—such as messages between the central processor and the ring. Software in the node either pegs these counts or notifies the central processor. The counts are maintained in buffers in the node processors and possibly the central processor. Occasionally, an error notification is sent to the central processor to report error conditions in the ring. In addition to responding to the reported error, software in the central processor often updates the corresponding per-office counts and/or per-node counts. This report to the central processor occurs in real time, independently from the periodic data collection. The measurements maintained

* UNIX is a trademark of UNIX System Laboratories, Inc.

in the central processor are collected for history file generation at the same time the node counts are collected.

The node is also responsible for collecting the link counts maintained by the link interface. The LI counts are read by the NP and placed in NP buffers for subsequent reporting to the central processor.

The IMS measurement descriptions identify the following three types of ring node oriented measurements:

- RPC—Per node measurement originated in a ring peripheral controller (RPC)
- IUN—Per node measurement originated in some ring node other than a ring peripheral controller
- NP—Per node measurement originated in any node processor.

Link Oriented Measurements

Link oriented measurements cover traffic volume counts and error conditions related to CCS messages. Some examples are signaling errors, link failures, link congestions, and buffer overloads. The traffic counts reflect the operating load of the system. This data is most useful in engineering the office and the entire CCS network. This category of measurements also includes those showing network abnormalities such as processor outages and emergency restarts.

Link oriented measurements are maintained in buffers in the link interface circuits and the node processors, and possibly, the central processor when notified by the node. The link interface circuit allows messages, carried between signal points, to enter and exit the CNI system. Since the LI is basically a buffer circuit between the node and the data link, the counts pegged by the LI are very specific traffic related counts. The measurements are usually taken from a circuit standpoint rather than on a message basis.

Other link-related counts are pegged by software in the node and are based on the message discrimination performed by the node. Furthermore, the node software has a view of the node's function and can therefore recognize larger events than the link interface. These counts are maintained in the node.

The SS7 CNI measurement descriptions identify SS7 link oriented measurements. The SS7 protocol is a new internationally accepted standard that allows more efficient and flexible use of the CCS network.

Total Office Measurements

Total office measurements provide an office view of various occurrences. Some, such as the office EMR counts, indicate the impact of corresponding, per-link and per-node, occurrences on the entire office. Others are not specific to any link or node, and are therefore inherently total office counts. The office

measurements include processor outages, initializations, ring failures, link failures, and various counts related to message processing in general—not specific to any link or node. These counts are maintained solely in the central processor. The measurements are pegged in the central processor and are either recognized by the central processor, as initializations or ringdown, or are reported to the central processor by the nodes when they occur.

The IMS measurement descriptions identify the following two types of total office measurements:

- **Office:** Total office measurement.
- **CHN:** Originated for a particular channel—possibly in a ring node or the central processor. When a message is to be read from or written to the ring, an association is made between an open channel and the buffer containing the message. This is via a queue that is dedicated to the channel. A channel can be thought of as a "mailbox" that messages can be sent to and from. The central processor manages the 256 possible channel—each intended for a specific type of message—that can carry messages.

Measurement Process Phases

The measurement history files are disk based files used to store the transient data associated with measurements. The data is considered transient since no cumulative day-to-day record is automatically generated. The generation of measurement history data involves three phases:

1. Data generation: Recognizes and pegs the counts in software
2. Data collection: Accumulation of raw measurements from all nodes periodically
3. Data processing: Creates history files via the MOCT.

These phases take the raw measurement values from buffers in the various processors—node processors and the central processor—cumulate them, and organize them into user accessible data files on disk. The following is a discussion of this process. Understanding the data generation process requires a basic knowledge of the hardware architecture and the UNIX RTR Operating System file structure.

To be measured, an occurrence must first be recognized by the application. This takes place in the various processors in real time. The link interface maintains counts of CCS level 2 protocol measurements for its associated links; the counts represent link related measurements. The cumulative counts are copied to buffers in the node processor of each ring node at data collection time. Likewise, the node processor maintains counts of various occurrences related to messages and the ring. These too are stored in buffers in the node processor. Every 5 minutes the central processor broadcasts a message to all ring nodes

requesting the measurement data in the ring node buffers. As each ring node receives this message, the data in the buffers is sent to the central processor to be stored in main memory.

Note: If IMS measurements are not inhibited, all nodes respond to the message. If IMS measurements are inhibited, only the ring peripheral controller nodes (RPCNs) respond. The counts in central processor measurement buffers, except inhibited measurements, are then combined with the counts from the ring nodes to form a complete set of measurement data.

The central processor, ring node, and link interface buffers are cleared and begin cumulating data for the next 5-minute period. The collected data now resides in main memory as the last 5-minute measurements. The last period measurement (LPM) is a shared data library and is available for use in reports.

Therefore, every 5 minutes the central processor receives all measurement data collected over the preceding 5-minute period. This data consists of IMS, CNI, and application measurement counts. It represents the smallest collection period available to the MOCT and the user. All subsequent data processing builds on this data set. If IMS measurements are inhibited, some of the IMS counts collected by the central processor have not accumulated further. However, the LPM data is still available to the user. The CNI and application counts and all available IMS counts are accumulated as described later. From this description, three limitations are apparent and must be kept in mind when analyzing measurement data:

1. Although the measurements register in real time, the report generation software becomes aware of them only at 5-minute intervals at best. For reporting purposes, a piece of measurement data can be up to 5 minutes old.
2. If just one ring node is faulty or out of communication with the ring (for example, the node processor fails), the measurement data for any affected 5-minute interval is incomplete. That ring node is not reporting any measurements. Data from all ring nodes must be combined in main memory when building the LPM. This problem is relieved by flagging invalid or incomplete data on output reports.
3. If IMS measurements are inhibited, some reports may display IMS counts as zero. Flexible format reports with IMS measurements either ignore these counts or they are not output at all. Also, the **DUMP:SMEAS** command refuses requests to display certain IMS counts. Counts that are unavailable when IMS measurements are inhibited include:

- All IMS counts collected from IMS user nodes (IUNs)
- All IMS channel measurements
- All IUN counts other than IMNPDIF, OOSCFG, OOSCFGT, OOSAU, OOSAUT, OOSMN, and OOSMNT.

The final phase in generating the data files is the processing of the LPM data residing in main memory. This processing is intended to generate files of measurement data that cover longer periods of time and are thus useful in producing reports. The basic data file used is the last 15-minute file (L15M). To get this file, the LPM (5 minutes of measurements data) is cumulated in main memory for 15 minutes. Every 15 minutes the cumulated data is written to disk as an L15M file. The L15M file is one of the "past" measurement files mentioned below. The focal point of the data base processing is the history file descriptor table (HFDT). The HFDT is one of the measurement output control tables. Every 15 minutes, the HFDT is scanned for the purpose of processing measurement data. Any processing that needs to be done is specified in the HFDT. This allows users to specify measurement collection periods that fit their needs. Upon completion of a history file, the report schedule table is scanned to generate any reports necessary. Here it should be noted that the LPM data is available for use in reports, but it is not available for generating history files via the HFDT.

The data files used in the HFDT consist of "current" measurements and "past" measurements. These files are collectively referred to as history files. The current measurement data files contain the cumulative totals for the current collection period. This data is copied into the corresponding past measurement data file at the end of the current collection period. Thus, the past measurement files contain the measurement data for the entire preceding collection period, while the current measurement files at any given time may not contain data for the full collection period. Any history data files created are stored on disk and are available for reports. However, each history file is associated with a particular collection period such as '15 min,' '1 hr,' or '1 day.' They are not associated with a particular day or time of day. In other words, the files are reused at the end of their respective collection periods. These disk files are not automatically backed up. Only certain past measurement files are used in fixed format reports.

Table 5-A provides an alphabetical index of the measurement description tables (Tables 5-B and 5-C). When looking for a particular measurement description, refer to the Alphabetical Index of Measurements (Table 5-A). In Table 5-A, locate the desired measurement name and identify the associated table (Table 5-B or 5-C). Refer to the associated table and locate the desired measurement name for a description.

Tables 5-B and 5-C list the measurement descriptions by subsystems (IMS, SS7 CNI). The tables provide the measurement name, type, and description. The measurement type indicates the measurement is specific to some protocol, some particular unit, or the whole office. The measurement names and descriptions

are presented alphabetically. They are intended to aid the reader in understanding the source, meaning, and use of each measurement. Most importantly, the descriptions help users to develop their own views of the measurement data. These views can then be scheduled for output as reports using the MOCT.

In addition, the measurement descriptions reference to other applicable measurements. These references may provide additional information. They are also intended to eliminate duplicate descriptions of similar measurements. Transmit and receive measurements are usually similar. However, when applicable differences are noted, unless otherwise indicated, transmit and receive measurements count the same things only in opposite directions. For example, the signal units received measurement includes the same types of signal units as the signal units transmitted measurement. This similarity also applies to the measurements of events related to one of the dual rings. Ring 0 format errors mean the same thing for ring 0 as ring 1 format errors mean for ring 1.

Table 5-A. Alphabetical Index of Measurements (IMS, CNI, and CNCE)

Measurement Name	Associated Table	Measurement Name	Associated Table
ABOFL	C	COS7UNERNA	D
ABOFS	C	CRCERTE	D
ARRATT	C	CRCER	D
ARREXR	C	CUTOCUMSG	C
ARRFLR	C	CUTOCUWDS	C
BESERR	C	CUTORMSG	C
BLK0	C	CUTORWDS	C
BLK1	C	DCFLABNT	D
BLKG0	C	DCFLHWPT	D
BLKG1	C	DCFLSWPT	D
BUFSW	C	DCFLXDAT	D
BXMITN3B	C	DCFLXDCT	D
BYMSUR	D	DCFLXERT	D
BYMSUX	D	DLN10800	C
BYRXTE	D	DLN10FAIL	C
BYRX	D	DLN10NETBLK	C
BYR	D	DLN10SDN	C
BYSR	D	DLN10SSP	C
BYSX	D	DLN6800	C
BYX	D	DLN6FAIL	C
CLFAT	D	DLN6NETBLK	C
CLFA	D	DLN6SDN	C
CLFSPT	D	DLN6SSP	C
CLFSP	D	DLNATPDROP	C
CLFT	D	DLNBASE	C
CLF	D	DLNBIBC	C
CNTMOOS	C	DLNBIMC	C
CNTOOS	C	DLNBOBC	C
CONFGT	C	DLNBOMC	C
CONFG	C	DLNBUSY	C
COS7CRFSRCM	D	DLNCFNIN	C
COS7DCHNOOS	D	DLNCFNOUT	C
COS7DSDSRCM	D	DLNCSOUT	C
COS7ERRSRCM	D	DLNGIBC	C
COS7LCDINV	D	DLNGIMC	C
COS7RLCSRCM	D	DLNGOBC	C

Table 5-A. Alphabetical Index of Measurements [(IMS, CNI, and CNCE) Contd]

Measurement Name	Associated Table	Measurement Name	Associated Table
DLNGOMC	C	INIT1B	C
DLNSIN	C	INIT2T	C
DLNTBSY	C	INIT2	C
DLNUUIDROP	C	INIT3T	C
DMAFLT	C	INIT3	C
DMAMISS	C	INIT4T	C
DRP7MSG1	D	INIT4	C
DRP7MSG2	D	INITBTT	C
DRP7MSG3	D	INITBT	C
DRPEMSG1	D	IPFMTER0	C
DRPEMSG2	D	IPFMTER1	C
DRPEMSG3	D	IPSM0	C
DRTMOOS	C	IPSM1	C
DRTOOS	C	IUNOVLD0	C
DSCHWDSREC	C	IUNOVLD1	C
DSCHWDSSNT	C	IUNOVLD2	C
ERSECTE	D	L6MGRV_	D
ERSEC	D	L6MGXV_	D
FORRXBY	D	L6SUPRV_	D
FORRX	D	L6SUPXV_	D
GTTPERFD	D	L7ACOFE	D
GTTUNBC	D	L7ACONE	D
GTTUNBT	D	L7ACOTE	D
GTTUNNT	D	L7ACO	D
IDLE	C	L7AFLT	D
IFBPTER1	C	L7BADRTG	D
IFBTER0	C	L7BOFRT	D
ILLEGAL	C	L7BOFR	D
IMNPDIF	C	L7BOLRT	D
IMOFFDIF	C	L7BOLR	D
INBOF	C	L7BYTO3B	D
INIT0T	C	L7DIF	D
INIT0	C	L7EMRPOT	D
INIT1AT	C	L7EMRPO	D
INIT1A	C	L7EMRT	D
INIT1BT	C	L7EMR	D

Table 5-A. Alphabetical Index of Measurements [(IMS, CNI, and CNCE) Contd]

Measurement Name	Associated Table	Measurement Name	Associated Table
L7FLALIGN	D	LINKDLAY	D
L7FLDT	D	LOT_N	C
L7FLD	D	LOT_R	C
L7LCDIS1XT	D	MGANSRV_	D
L7LCDIS1X	D	MGANSXV_	D
L7LCDIS2XT	D	MGIAMRV_	D
L7LCDIS2X	D	MGIAMXV_	D
L7LCDIS3XT	D	MGMSUR	D
L7LCDIS3X	D	MGMSUX	D
L7LCON1XT	D	MINTRA	C
L7LCON1X	D	MRBADRTG	D
L7LCON2XT	D	MRINTCH	C
L7LCON2X	D	MRNIAUT	C
L7LCON3XT	D	MRNIAU	C
L7LCON3X	D	MRNRING	C
L7LNKACTT	D	MRRGQ0	C
L7MCOFE	D	MRRGQ1	C
L7MCONE	D	MRRING	C
L7MFLT	D	MRSBCO7	D
L7MGSR	D	MRSNTO7	D
L7MGSX	D	MSG7LOOP	D
L7MRPBC	D	MSGREC	C
L7MRPNT	D	MSGSNT	C
L7MSINVSIO	D	MSINVSIO	D
L7PORT	D	MSUDISC_	D
L7POR	D	MSUSAMPL	D
L7POXT	D	MXRG0	C
L7POX	D	MXRG1	C
L7RBFOC	D	NACRETE	D
L7RTGAUD	D	NACR	D
L7THRSWMSU	D	NOCMGT	D
L7TRMDMSUS	D	NOCMG	D
L7TRMSUOCT	D	NPPTER	C
L7TSMSUOCT	D	OCCUPMSU	D
L7XBFLOOK	D	OOSAUT	C
L7XBFOC	D	OOSAU	C

Table 5-A. Alphabetical Index of Measurements [(IMS, CNI, and CNCE) Contd]

Measurement Name	Associated Table	Measurement Name	Associated Table
OOSCFGT	C	RRBOVFLW3	C
OOSCFG	C	RSTTRMT	C
OOSMNT	C	RTESETUNT	D
OOSMN	C	RTESETUN	D
PANICS	C	RTGAUDFL	D
PIOFLT	C	RTMSGSRC	C
PRTOERR	C	RTOCUMSG	C
PTERTE	C	RTOCUWDS	C
RABTER	D	SC7RERPRO	D
RABT	D	SC7RERUATY	D
RACER0	C	SC7RERUA	D
RACER1	C	SC7RERUNE	D
RBOFBLK	C	SC7RGTR	D
RBOF	C	SC7RLNN	D
RCOPTER0	C	SC7RLSS	D
RCOPTER1	C	SC7RNATL	D
RDFMTER0	C	SC7R	D
RDFMTER1	C	SC7UDSX	D
RDINHER0	C	SCRERPRO	D
RDINHER1	C	SCRERUATY	D
RDWNT	C	SCRERUA	D
RDWN	C	SCRERUNE	D
RGCNFGT	C	SCRGTR	D
RGCNFG	C	SCRLNN	D
RINTCH	C	SCRLSS	D
RIPTER0	C	SCRNATL	D
RIPTER1	C	SCR	D
RNIMNT	C	SCSILNKRTY	C
RNIMN	C	SCSRTR	D
RPCBOF	C	SCSRTX	D
RRBOVFLW0	C	SCSSTR	D
RRBOVFLW1T	C	SCSSTX	D
RRBOVFLW1	C	SCUDSX	D
RRBOVFLW2T	C	SEVERSEC	D
RRBOVFLW2	C	SEVERSEC	D
RRBOVFLW3T	C	SFPTER0	C

Table 5-A. Alphabetical Index of Measurements [(IMS, CNI, and CNCE) Contd]

Measurement Name	Associated Table	Measurement Name	Associated Table
SFPTER1	C	WDSREC	C
SPIAPOT	D	WDSSNT	C
SPIAPO	D	WRRGQ0	C
SPIAT	D	WRRGQ1	C
SPIA	D	WSMER0	C
SPIPOT	D	WSMER1	C
SPIPO	D	WTFMTER0	C
SPISPPOT	D	WTFMTER1	C
SPISPPO	D	WXRG0	C
SPISPT	D	WXRG1	C
SPISP	D	ZPEAKOCC	D
SPIT	D		
SPI	D		
SQL	D		
SRNIAUT	C		
SRNIAU	C		
SRSCTRAN	D		
SRSTTRAN	D		
SSATRAN	D		
SSPTRAN	D		
SSTTRAN	D		
TDPRCNG0	C		
TDPRCNG1	C		
TDPRCNG2	C		
THRSWMSU	D		
TLNKACTV	D		
TPROCOTG	D		
TRMDMSUS	D		
TRMSUOCT	D		
TSMSUOCT	D		
UNRCMSGREC	C		
UNVL	D		
UNVL	D		
WBOFNL	C		
WBOFN	C		
WBOFO	C		

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions

Name (Type)	Description
ABOFL (Office)	Long message type application buffer overflow. This count is for the long type single message read buffers referred to in the ABOFS description. It is pegged when there are no more buffers of this type available.
ABOFS (Office)	Short message type application buffer overflow. Messages delivered to IMS channels in the single message read mode are copied into buffers allocated from a common pool—each buffer holds one message. A pointer to the buffer is placed in the read list for the channel (refer to the RBOF description). For memory efficiency, there are two buffer sizes, short and long. This count is pegged whenever an attempt is made to allocate a short-type, single-message, read buffer when the buffer pool is empty. If possible, the message is returned to its origination; otherwise, it is discarded.
ARRATT (NP)	Automatic Ring Recovery (ARR) restoral attempts. The ARR program attempts to diagnose and restore nodes to a working state when a node fails. If a node is alleged to be faulty, ARR diagnoses the node by attempting a conditional restore. An isolated segment may contain nodes with no faults associated with them—innocent victims due to multiple failures on the ring. They are restored unconditionally when they become reachable by ARR one of the faulty nodes in the segment must be restored first. This count is pegged each time ARR attempts to restore a node.
ARREXR (NP)	Automatic Ring Recovery restoral failure is due to excessive restore rate. Each time ARR restores a node, it increments a counter in the ECD in addition to the ARRATT measurement. If that counter exceeds a certain threshold within a given time, the node has a recurring fault. This count is then pegged, and the node is marked for manual intervention.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
ARRFLR (NP)	Automatic Ring Recovery restoral failures. If ARR is unsuccessful at restoring a node, this count is pegged. If the failure to restore is due to a legitimate diagnostic failure, the node is marked for manual intervention. If the diagnostic is aborted due to other reasons, it is retried later. Refer to the ARRATT description.
BLK0 (Office)	Ring 0 blockage. This count is pegged once if a blockage is reported on ring 0 by one or more nodes during a particular listen interval (refer to the BLKG0 description). It is the cumulative count of incidents on ring 0 that result in blockages and a corresponding ring reconfiguration. Each incident may involve multiple blockage reports from many nodes.
BLK1 (Office)	Ring 1 blockage. Refer to the BLK0 description.
BLKG0 (NP)	Ring 0 blockage. Each node contains a ring interface circuit used to access the dual rings. This circuit contains a buffer called a ring access circuit (RAC). Blockages are detected when a RAC has been unable to propagate data to its downstream neighbor for a predetermined period of time. If too much time elapses without any data being transferred, a blockage is reported to the central processor, and this count pegs for the reporting node. The node then dequeues some data to reset the blockage timers of upstream nodes. This is sometimes ineffective, resulting in multinode blockage reports.
BLKG1 (NP)	Ring 1 blockage. Refer to the BLKG0 description.
BUFSW (NP)	Ring receive buffer switch. When the node reads messages from the ring, the data is DMAed to buffers in the node processor memory. Each buffer has a fixed length. If the DMA requires another buffer, it is interrupted, a new buffer is allocated, this count is pegged, and the DMA continues.
BUSERR (NP)	The number of SCSI bus errors that are logged by the SIN node.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
BXMITN3B (NP)	This is the number of bytes transmitted from the node to the 3B. This count is increased by the size in the bytes for each message sent to the 3B.
CNTMOOS (NP)	The count of times a SCSI link went manually out of service (OOS) for a SIN node.
CNTOOS (NP)	The count of times a SCSI link went out of service (OOS) for a SIN node.
CONFG (NP)	Begin/end point of isolation segment. This count is incremented whenever the specified node is either a BISO or EISO node. Whenever a node adjacent to this node is isolated, this node may become the begin-end point depending on how the ring is reconfigured (refer to the SRNIAU or MRNIAU description). The begin-end node is not isolated. Rather, the ring interface circuits in the node cause rings 0 and 1 to loop on each other.
CONFGT (NP)	Duration of begin/end point of isolation segment. The length of time a node is either a BISO or EISO node.
CUTOCUMSG (Office)	3B computer to 3B computer IMS messages. This is a cumulative count of all messages delivered between two channels in the central processor.
CUTOCUWDS Office)	3B computer to 3B computer IMS message words. This is a cumulative count of all words delivered between two channels in the central processor. It is incremented by the size of a message when the message is queued for the destination channel.
CUTORMSG (RPC)	3B computer to ring peripheral controller IMS messages. This is a cumulative count of all messages transmitted to a specific ring peripheral controller. The RPC may or may not be the final destination of the message. The messages could be sent to other nodes on the ring. Messages queued in write buffers are delivered to the ring at each invocation of the message switch.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
CUTORWDS (RPC)	3B computer to ring peripheral controller IMS message words. This is the cumulative count of the sizes of all the messages transmitted to a specific RPC. The count is in 3B computer words; each word is 4 bytes. Also see the CUTORMSG description.
DLNATPDROP (AP)	Number of ISUP ATP parameters that the DLN dropped because the message exceeded the Max. Length.
DLNBASE (AP)	Base cycle counter 10ms/base cycle.
DLNBIBC (AP)	Counter for bad Ring to 1A DMA message blocks in the DLN.
DLNBIMC (AP)	Counter for bad inbound signaling messages in the DLN. Message size invalid, fail translations or contain a bad length field.
DLNBOBC (AP)	Counter for bad 1A to Ring DMA message blocks in the DLN.
DLNBOMC (AP)	Counter for bad outbound signaling messages in the DLN. Message size invalid, fail translations or contain a bad length field.
DLNBUSY (AP)	Peg count of 125us idle in 5 minutes.
DLNCFNIN (AP)	Number of confusion messages that the DLN received from the network and is sending to the 1A.
DLNCFNOUT (AP)	Number of confusion messages that the DLN received from the 1A and is sending to the network.
DLNSIN (AP)	Number of incoming SIN messages in the DLN.
DLNCSOUT (AP)	Number of outgoing SIN messages in the DLN.
DLNGIBC (AP)	Counter for good Ring to 1A DMA message blocks in the DLN.
DLNGIMC (AP)	Counter for good input signaling messages in the DLN from the network that have been reformatted to the 1A.
DLNGOBC (AP)	Counter for good 1A to Ring DMA message blocks in the DLN.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
DLNGOMC (AP)	Counter for good output DLN signaling messages that get sent from the 1A out to the signaling network.
DLNTBSY (AP)	Count of too busy cycles in the DLN when less than .5 ms segments of routine background tasks were not able to run in the last base cycle.
DLNUUIDROP (AP)	Number of ISUP UUI parameters that the DLN dropped because the message exceeded the maximum length.
DLN6FAIL (AP)	Total of DLN SCCP 6 digit GTT messages that were not sent because of translation failures.
DLN6NETBLK (AP)	Total of DLN SCCP 6 digit GTT messages that were not sent out to the network because of routing failure or congestion.
DLN6SDN (AP)	Total DLN SCCP 6 digit GTT messages processed for TT=252.
DLN6SSP (AP)	Total of DLN SCCP 6 digit GTT messages that were not sent out to the signaling network because the subsystem is prohibited.
DLN6800 (AP)	Total DLN SCCP 6 digit GTT messages processed for TT=253.
DLN10FAIL (AP)	Total of DLN SCCP 10 digit GTT messages that were not sent because of translation failures.
DLN10NETBLK (AP)	Total of DLN SCCP 10 digit GTT messages that were not sent out to the network because of routing failure or congestion.
DLN10SDN (AP)	Total DLN SCCP 10 digit GTT messages processed for TT=252.
DLN10SSP (AP)	Total of DLN SCCP 10 digit GTT messages that were not sent out to the signaling network because the subsystem is prohibited.
DLN10800 (AP)	Total DLN SCCP 10 digit GTT messages processed for TT=253.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
DMAFLT (RPC/DLN)	Direct memory access fault. The central processor communicates with the node via both DMA and program I/O requests (the PIOFLT count indicates faults detected during the latter). The DMA is used when a large amount of data needs to be sent to or from the ring and it is not necessary for the sending process to wait for a completion. Hardware (such as the DMA controller, the DDSBS, or 3B computer interface) detects the fault (for example, an incorrect address) while Direct Memory Accessing data. When a fault is detected, the DMA is interrupted; this error is reported to the central processor, and the count pegs.
DMAMISS (RPC)	Direct memory access missed. When the message switch wants to send messages to an RPC or DLN (once each invocation), it first checks to see if the RPC or DLN is ready to accept more messages (that is, it has finished the DMA for the last message switch cycle). If the DMA is complete, the message switch can use the RPC or DLN to send messages to the ring. If the DMA has not finished, the RPC or DLN cannot be used and this count pegs.
DRTMOOS (NP)	The time duration for all the MOOS SCSI links on a SIN node.
DRTOOS (NP)	The time duration for all the OOS SCSI links on a SIN node.
DSCHWDSREC (NP)	The number of words received over the Dual Serial Channel on the SIN node from the 3B.
DSCHWDSSNT (NP)	The number of words sent over the Sual Serial Channel from the SIN node from the 3B.
IDLE (NP)	A relative measure of node processor idle time. Tasks in a node, both message processing and maintenance processing, are scheduled by preemptive priority. When all other tasks have completed, the node processor executes the idle routine; this routine is assigned the lowest possible priority. This count is incremented by the idle routine in an amount proportional to the time spent idle.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
IDLE (NP) (Contd)	This idle routine also sets the idle flag indicating there is no work. The idle flag is checked and cleared every 10 ms by the overload monitor.
IFBPTER0 (NP)	Interframe buffer (IFB) parity error on ring 0. The IFB is considered to be part of the input circuitry of the downstream node. Parity errors detected in the IFB are reported by that node. This error can be considered equivalent to a hard parity error, but occurring in the associated IFB (refer to the RIPTER0 description).
IFBPTER1 (NP)	Interframe buffer parity error on ring 1. Refer to the IFBPTER0 description.
ILLEGAL (NP)	Number of messages processed by the illegal message handler. This includes such messages as source match, destination channel closed, or returned messages. Refer to RTMSGSRC, MRINTCH, and MRRING descriptions.
IMNPDIF (NP)	Node processor data integrity flag. If this count is zero, the data collected is good. If the count is nonzero, it indicates the data collected by the central processor is incomplete. The following describes the meanings of the bits (the IMOFFDIF measurement describes how these bits are derived). The measurement value is as follows: 00000000*abcd0efg*000000000000000h in binary: Where: a = Data collection period skipped b = Data collection period aborted c = Node did not respond (no measurements received) d = Periodic data collection initialized e = Data collection process faulted during data f = Node removed g = Node grown h = Node initialized (this value is collected in the node).

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
IMOFFDIF (Office)	Per office data integrity flag. If this count is zero, the data collected is good. If the count is nonzero, it indicates the data collected by the central processor is incomplete. The data integrity flag is used to determine if an event has occurred in the period of interest which causes the data collected for that period to be suspect. The data integrity flag is actually a decimal representation of one 32-bit word describing the error condition. To determine the meaning of the count, it must be converted from decimal to binary and the bits analyzed. In the following, the measurement value is represented as 00000000ab0c0d000000000000000000 in binary. Each bit in the word that is set (more than one can be set) indicates a particular error: Where: a = Data collection period skipped b = Data collection period aborted c = Periodic data collection initialized d = Data collection process sustained a fault.
INBOF (NP)	Failure to obtain a new ring receive buffer. Messages are read into buffers in node memory as described under the BUFSW measurement. If there are no more buffers available when a buffer switch is attempted, this count is pegged. Any messages not read are then Direct Memory Accessed into the "throwaway" portion of NP memory (effectively discarding them). This count should always be the same as the RRBOVFLW3 count.
INIT0 (Office)	Number of level 0 IMS initializations that started. Level 0 is the audit level. When invoked either automatically or manually by an input message, selected audits start. Should a critical audit fail, then the initialization may escalate to level 1B. At level 0, the message switch is running. Note that the IMS initialization levels are basically the same as the corresponding application and operating system levels.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
INIT0T (Office)	Duration of level 0 IMS initialization. Since the initialization sequences for levels 0, 1A, and 1B do not recreate any IMS processes, these durations are exclusive of the boot prologue and the boot level initializations.
INIT1A (Office)	Number of level 1A IMS initializations that started. This is the recovery level and may be triggered by internal problems. Tables are rebuilt from information in the central processor and ring nodes. A level one system initialization triggers either an IMS level 1A or 1B. During level 1A, IMS is capable of switching messages but messages may be lost due to audits and reinitialization of communications between the central processor and ring. It may escalate to level 1B.
INIT1AT (Office)	Duration of level 1A IMS initialization. Refer to the INIT0T description.
INIT1B (Office)	Number of level 1B IMS initializations that started. During level 1B, IMS is not capable of switching messages (messages are lost).
INIT1BT (Office)	Duration of level 1B IMS initialization. Refer to the INIT0T description.
INIT2 (Office)	Number of level 2 IMS initializations that started. This level immediately escalates to a level 3.
INIT2T (Office)	Duration of level 2 IMS initialization. Refer to the INIT3T description.
INIT3 (Office)	Number of level 3 IMS initializations that started. This is the lowest boot level. If the boot is unsuccessful, CNI and IMS abort. If possible, the previously existing ring configuration is maintained; if necessary, a quick reconfiguration is attempted. Selected nodes may be downloaded.
INIT3T (Office)	Duration of level 3 IMS initialization. The boot level initialization durations do not include the time spent aborting IMS, the time spent recreating the driver, nor the time spent in the boot prologue.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
INIT4 (Office)	Number of level 4 IMS initializations that started. This is the highest boot level. If the boot is unsuccessful due to a software problem, CNI and IMS abort. If the boot is unsuccessful due to a hardware problem, IMS is still capable of performing diagnostics. If the boot is successful, all ring nodes are downloaded. It allows the system to operate even if no usable ring configuration is established. Also, automatic recovery can be inhibited.
INIT4T (Office)	Duration of level 4 IMS initializations. Refer to the INIT2T description.
INITBT (Office)	Number of IMS boot prologues that start. This counts how many times IMS is booted (recreated), whereas the initialization levels 2, 3, and 4 counts indicate how many times the boot leads to those particular sequences. If an initialization fails, it may be retried automatically. Also, since level 2 invokes level 3, the sum of INIT2, INIT3, and INIT4 could exceed this count.
INITBTT (Office)	Duration of IMS boot prologue. This measurement begins when the IMS driver is created. It is exclusive of the boot level initialization durations.
IPFMTER0 (NP)	Ring input format error on ring 0. This error is detected at the input to the RAC. It occurs whenever a message passing through the RAC buffer has format problems; that is, the message is too short to contain a valid header or is longer than the header indicates. This condition is checked even if the message is not read by the node. Furthermore, the format error is also pegged by the RDFMTER0 count when the message is read.
IPFMTER1 (NP)	Ring input format error on ring 1. Refer to the IPFMTER0 description.
IPSM0 (NP)	Ring 0 input source match. Whenever a message on the ring is not dequeued by the node to which it is destined, the message continues to traverse the ring to the sending node. The sender then detects the message, removes and discards it, and notifies the central processor. Then this count pegs for the destination node.
IPSM1 (NP)	Ring 1 input source match. Refer to the IPSM0 description.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
IUNOVLD0 (IUN)	Number of times the IMS user node entered overload level 0 (the normal state). The IUNOVLD_ measurements indicate the number of times the node is in a state in which all available CPU time is consumed (refer to the IDLE description). Entering this state indicates the processor is idle (it pegs when the NP returns to level 0 from level 1 or 2).
IUNOVLD1 (IUN)	Number of times the IMS user node entered overload level 1. The node processor has not been idle for some time. Messages from the user apparatus are processed on a "clocked" schedule to reduce NP load.
IUNOVLD2 (IUN)	Number of times the IMS user node entered overload level 2. The node processor has not been idle for a longer period of time. Messages from the ring and the user apparatus are processed on a "clocked" schedule to further reduce NP load.
LOT_N (OFF)	Unexplained loss of token on a normal two-ring system. This count increments once when an unexplained loss of the token message occurs on ring 0, ring 1 or on both rings simultaneously.
LOT_R (OFF)	Unexplained loss of token on a reconfigured single-ring system. This count increments once when an unexplained loss of the token message occurs on a reconfigured ring. The sum of LOT_N and LOT_R equals the total count of unexplained loss of token events.
MINTRA (RPC)	For a particular ring peripheral controller (RPC) node, this count increments when the following occurs: ■ An intra node IMS message is generated within that RPC. ■ A message is generated by that RPC and specifically addressed to the 3B as its final destination. ■ A message is generated by the 3B and specifically addressed to that RPC as its final destination. This count is not tied to any other count. A very small count is not unusual.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
MRINTCH (NP)	Message returned to the ring due to destination channel being closed. When a message is sent to a closed channel in a node, the message must be returned (refer to the RINTCH description). **Note:** This count is a cumulative total for all channels in the node, while RINTCH is counted per channel in the central processor.
MRNIAU (Office)	Automatic multiple ring node isolation. When a node is isolated, the ring is reconfigured to group all isolated nodes into one isolated segment. The nodes involved may have been isolated automatically, manually, or as innocent victims of the ring reconfiguration. If the segment has more than one node and the most recently isolated node is isolated by automatic action, the entire segment is considered to be isolated automatically. This count is pegged when the ring is successfully reconfigured automatically and the node is isolated.
MRNIAUT (Office)	Duration of automatic multiple ring node isolation. This is the cumulative time in which an automatically generated ring configuration exists with more than one node isolated.
MRNRING (NP)	Message returned from ring. When the node receives a message that is not accepted by the destination, the returned message control code is detected; the message is discarded, and this count is pegged. See the MRRING, RINTCH, and MRINTCH descriptions for reasons why messages are returned.
MRRGQ0 (NP)	Message received from ring 0 queued. In the node processor, messages received from the ring (via DMA reads) are placed in one of the ring receive buffers in memory. A separate list of pointers (queue) to the messages in the buffers is maintained for each channel—except in-place channels. This count is the cumulative total of all messages from ring 0 queued for any of these channels. At a ring peripheral controller, this count is the number of blocks given to the active ring channel. A block may contain several messages.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
MRRGQ0 (NP) (Contd)	In the case of in-place channels, messages are processed in the buffers. After processing, these messages may be queued to be read by some other channel.
MRRGQ1 (NP)	Message received from ring 1 queued. Refer to the MRRGQ0 description.
MRRING (Office)	Message returned to ring with "returned message" control code (destination did not accept message). This count is the number of times messages are returned to the ring because the destination channel is not open; the destination's read queue is full; or there is no buffer space for the message. If the message is not already a returned message, this count is pegged. Then, the "returned message" control code is added to the message; source and destination addresses are swapped; and the message is sent to the ring. If the message is already a returned message, it is discarded and this count is unaffected.
MSGREC (NP)	The number of messages received via the SCSI link from the CDRP to the SIN node.
MSGSNT (NP)	The number of messages sent via the SCSI link from the SIN node to the CDRP.
MXRG0 (NP)	Message transmitted to ring 0. When a message is to be transmitted to the ring, a pointer to the buffer in NP memory containing the message is placed on a queue. The queue represents a block of messages to be Direct Memory Accessed to the ring. This count is incremented at each DMA by the number of messages in the block to be sent to ring 0.
MXRG1 (NP)	Message transmitted to ring 1. Refer to the MXRG0 description.
NPPTER (NP)	Node processor parity error. This count is pegged when the node reports an internal memory parity error. This error currently results in the node processor putting itself in a quarantine state and is not reported to the central processor. Therefore, this count is presently ineffective and should always be zero.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
OOSAU (NP)	Automatic out of service. This count is the number of times the node has entered either the out-of-service state or standby state from some other state due to automatic action. This could be due to failing diagnostics or some automatically detected fault. The node maintenance state may later change to manual; but until the major state changes, it is considered to be "automatic out of service." This count does not peg if the node is an innocent victim of a ring reconfiguration (see the OOSCFG description).
OOSAUT (NP)	Duration of "automatic out of service." This is the cumulative total of the time the node is in this state.
OOSCFG (NP)	Out of service due to ring reconfiguration. This count is the number of times the node has entered either the out-of-service state or standby state from some other state due to automatic action and because it is an innocent victim of a ring reconfiguration. When this state is first entered, the node is isolated. The node maintenance state may later change to manual, but until the major state changes, it is considered to be "automatic out of service." This count also includes those situations where the node is removed from service due to the entire ring down or a ring reconfiguration in progress.
OOSCFGT (NP)	Duration out of service due to ring reconfiguration. This is the cumulative total of time the node is in this state.
OOSMN (NP)	Manual out of service. This count is the number of times the node has entered either the out-of-service state or standby state from some other state due to manual action. The node maintenance state may later change to automatic; but until the major state changes, it is considered to be "manual out of service."
OOSMNT (NP)	Duration of "manual out of service." This is the cumulative total of time the node is in this state.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
PANICS (NP)	Number of recoverable errors. There are conditions which force the node processor to restart. If the condition does not prevent processing from continuing, it is called a soft error and this count pegs. If the processor must be rebooted, it is called a hard error, and it does not effect this count; it does not peg because error logging is not possible.
PIOFLT (RPC/DLN)	Fault received after a program I/O request is issued to a ring peripheral controller. The program I/O is used by the central processor mostly for sending commands to a RPC and for receiving status information from a RPC. There are two types of requests used: (1) *hardware* which causes some hardware action or (2) *software* which sends a command to some process. In both cases, the sending process waits for the program I/O request to complete. If hardware (such as the DMA controller, the DDSBS, or 3B computer interface) detects a fault during the I/O, this error is reported to the central processor and the count pegs.
PRTOERR (NP)	The number of SCSI protocol errors that are logged by the SIN node.
PTERTE (NP)	Number of times soft parity error exceeded a threshold. A "leaky bucket" cumulative count of both SFPTER0 and SFPTER1 is kept by the central processor. When that count exceeds a threshold, this count is pegged, and a ring reconfiguration is triggered to isolate the offending node.
RACER0 (NP)	Ring access controller (RAC) problem on ring 0. The RAC has a set of condition bits in its status ports that indicate troubles in the RAC. When the node processor observes problems in the RAC for ring 0 (indicated by the condition bits), it attempts to clear the problem for a maximum of 10 retries. If unsuccessful, this error report is issued to the central processor and the count pegs.
RACER1 (NP)	Ring access controller problem on ring 1. Refer to the RACER0 description.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
RBOF (CHN)	Single message read list buffer overflow. Each central processor channel using single-message read mode, is allocated a single message read list. This list contains pointers to the messages destined for this channel. The message is actually contained in a buffer from a pool of buffers shared among all single message read list users. The message switch tries to deliver a message to this channel by placing a pointer in the read list. If all pointer slots in the read list contain pointers to messages waiting to be read by the channel owner, this count pegs. This is an indication that messages are being queued faster than the owner of the channel can read them. Block message read list buffer overflow. This count is the block mode equivalent of the RBOF count. A central processor channel using block read mode is allocated a block read list (or buffer).
RBOFBLK (CHN)	This structure is actually just buffer space to hold messages destined for this channel, in contrast to the single message read list. The buffer is allocated from a common pool. The actual message is copied into the channel's private buffer space. If there is not room in the buffer to hold a new message for this channel—the read list is full—the message switch pegs this count. Block read buffers are circular; if there is room, messages are put after the last message delivered and before the oldest message that is still being used.
RCOPTER0 (NP)	Ring access controller output parity error on ring 0. This parity error is generated in the node processor when a message from the RAC for ring 0 is read into the node processor memory. Since the parity is good when the data is transferred into the RAC, the problem is internal to the RAC.
RCOPTER1 (NP)	Ring access controller output parity error on ring 1. Refer to the RCOPTER0 description.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
RDFMTER0 (NP)	Ring read format error on ring 0. Read format errors are detected in the RAC buffer during the reading of the message into NP memory and are usually due to partial or truncated messages received by the node. The size specified in the header is greater than the actual message size as received. Unless the node is an RPC, read format errors are not generated when a broadcast message is involved.
RDFMTER1 (NP)	Ring read format error on ring 1. Refer to the RDFMTER0 description.
RDINHER0 (NP)	Read inhibit error on ring 0. Data in the RAC is read into the NP by direct memory access. The node contains a timer that allows a specific time for the read operation. If after the timer expires no data has been transferred, the node reports this error to the central processor and the count is pegged.
RDINHER1 (NP)	Read inhibit error on ring 1. Refer to the RDINHER0 description.
RDWN (Office)	Entire ringdown. This count is pegged whenever the ring maintenance state is changed to indicate the entire ring is down (it is unusable). All nodes peg either the OOSAU, OOSCFG, or OOSMN count when this occurs, depending on their maintenance states.
RDWNT (Office)	Duration of entire ringdown. This is the cumulative total of the time the ring maintenance state is ringdown.
RGCNFG (Office)	Ring containing an isolated segment. This count pegs when an isolated segment is successfully established—a node is isolated by manual or automatic action. This count is the sum of the SRNIAU, MRNIAU, and RNIMN counts.
RGCNFGT (Office)	Duration of ring containing an isolated segment. This is the cumulative time during which the ring had at least one node isolated—the sum of the SRNIAUT, MRNIAUT, and RNIMNT counts.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
RINTCH (CHN)	Message returned to the ring due to closed destination channel. When a message is sent to a channel in the central processor that is closed, it must be returned. If the message is already a returned message, it is discarded and this count is not pegged. Otherwise, the "returned message" control code is added to the message; source and destination addresses are swapped; the message is sent to the ring; and this count is pegged.
RIPTER0 (NP)	Ring interface (hard) parity error or orphan byte condition on ring 0. This count is pegged if the parity error exists after retry (refer to the SFPTER0 count). The node does not accept the data. This usually results in a corresponding blockage report from the upstream node.
RIPTER1 (NP)	Ring interface (hard) parity error or orphan byte condition on ring 1. Refer to the RIPTER0 description.
RNIMN (Office)	Zero or more ring nodes isolated manually. This count is similar to the MRNIAU count except it is caused by manual action. If the most recently isolated node is isolated by manual action, the entire isolated segment is considered to be isolated manually. An isolated segment with zero nodes is possible when growing nodes. Unequipped nodes are isolated by placing the BISO and EISO nodes around the unequipped nodes. After the nodes are grown and diagnosed, ARR restores them to service and the isolated segment disappears. This count is pegged when the ring is successfully reconfigured manually, and the segment is isolated.
RNIMNT (Office)	Duration of zero or more ring nodes isolated manually. See the RNIMN description for an explanation of zero nodes isolated. This is the cumulative time that a manually generated ring configuration exists with an isolated segment.
RPCBOF (RPC)	Ring peripheral controller (RPC) buffer overflow. The message switch sends and receives messages to the ring by direct memory access channels to the RPCs.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
RPCBOF (RPC) (Contd)	During each message switch cycle, the RPC sends messages in its buffer to the central processor. Also, the central processor sends messages to the RPC buffer. This count pegs when the message switch tries to add a message to the buffer when it is full.
RRBOVFLW0 (NP)	Number of times the ring node has transitioned to overflow state 0 (the normal, no discard state). Messages in the ring receive buffers are being processed at least as fast as they are being received. If the node is an RPC, all IMS user nodes associated with it are notified of the overflow state of the node —this is true for all overflow states.
RRBOVFLW1 (NP)	Number of times the ring node has transitioned to overflow state 1. Messages are being received faster than they can be processed, and buffer occupancy has exceeded the threshold for overflow—all overflow states are associated with some threshold. In state 1, a warning of imminent overflow is sent.
RRBOVFLW1T (NP)	Duration of ring receive buffer overflow state 1.
RRBOVFLW2 (NP)	Number of times the ring node has transitioned to overflow state 2. In state 2, non-IMS messages are discarded in the IUNs only (all IUNs are notified of their home RPC's overflow state). When the home RPC is in state 2 or 3, the IMS does not allow non-IMS messages to be written to the home RPC. When an IUN is in state 2, any non-IMS messages read from the ring are discarded.
RRBOVFLW2T (NP)	Duration of ring receive buffer overflow state 2.
RRBOVFLW3 (NP)	Number of times the ring node has transitioned to overflow state 3. In state 3, the node is in the "throw away" mode. In this state, both the IUNs and RPCs DMA messages read from the ring into a throwaway area of memory (effectively discarded).

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
RRBOVFLW3T (NP)	Duration of ring receive buffer overflow state 3.
RSTTRMT (NP)	Successful restarts without reload. This count is presently ineffective and should always be zero.
RTMSGSRC (IUN)	Message received with a source address match. If a message sent by this node has traversed the entire ring without being taken, the RI hardware detects a match of the source address. When the match occurs, the message is removed from the ring. If the message is not a broadcast message, this count is pegged, and a report is sent to the central processor (see the IPSM_ description).
RTOCUMSG (RPC)	Ring peripheral controller to 3B computer IMS messages. This measurement is a cumulative count of messages received by the central processor from a specific RPC. It is similar to the CUTORMSG count.
RTOCUWDS (RPC)	Ring peripheral controller to 3B computer IMS message words. Each message read from or written to the ring is composed of a number of 3B computer words. The number varies with message type and the particular data the message contains. It is similar to the CUTORWDS count.
SCSILNKRTY (NP)	The number of retries to send a message over the SCSI link from the SIN node to the CDRP.
SFPTER0 (NP)	Soft (transient) parity error on ring 0. This parity error is generated in the RAC while receiving data. After detecting this error, the node requests the RAC to retry the parity error check. If the parity condition is gone, this count is pegged, and the error is considered transient. If the parity condition still exists, the node considers it to be a hard parity (refer to the RIPTER0 description).
SFPTER1 (NP)	Soft (transient) parity error on ring 1. Refer to the SFPTER0 description.
SRNIAU (Office)	Automatic single ring node isolation. This count is similar to the MRNIAU count. If an isolated segment has only one node that is isolated by automatic action, the segment is considered to be isolated automatically. This count is pegged whenever the ring is successfully reconfigured and the node is isolated.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
SRNIAUT (Office)	Duration of automatic single ring node isolation. This is the cumulative time in which an automatically generated ring configuration exists with a single node isolated.
TDPRCNG0 (NP)	This is the time, in milliseconds, the node spent in the normal no-overload state.
TDPRCNG1 (NP)	This is the time, in milliseconds, the node spent in the first level of overload. USER1 interrupt (link data available) operates in a clocked schedule mode for small scale integration (SSI) IUNs. The clocked schedule has the effect of reducing overhead (thus freeing real time) at the expense of increased delays. In this mode, the interrupt remains turned off except when enabled by the overload monitor control mechanism.
TDPRCNG2 (NP)	This is the time, in milliseconds, the node spent in the second level of overload. Both USER1 and End-of-Message interrupts operate in a clocked schedule mode for SSI IUNs.
UNRCMSGREC (NP)	The number of unrecognized messages that the SIN node application received.
WBOFN (CHN)	New write list buffer overflow. Each IMS central processor channel that originates messages is allocated a buffer—this is the new write list—for building messages. When a message is to be built, a request is made for space in this buffer.
WBOFN (CHN)	If the request exceeds the available space in the buffer—the write list overflows—this count is pegged. This is an indication that the destination RPC has not finished a previous DMA. Normally, the message switch empties the write buffer each cycle. Long new write list buffer overflow. This is the long buffer equivalent of the WBOFN count. The buffers used for the long write lists are separate from those used for the short write lists. This count is pegged if a request for space in a long buffer exceeds the available space. This is an indication that the destination RPC has not finished a previous DMA. Normally, the message switch empties the write buffer each cycle.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
WBOFO (CHN)	Old write list buffer overflow. The buffers used to write old messages are the same buffers used to read messages. The messages are read, processed in place, and then written. Each channel is allocated a list of pointers to the buffers containing the messages, the old write list. When too many messages are waiting—the write list is full—this overflow count pegs. This is an indication that the destination RPC has not finished a previous DMA. Normally, the message switch empties the write buffer each cycle.
WDSREC (NP)	The number of words received via the SCSI link from the CDRP to the SIN node.
WDSSNT (NP)	The number of words sent via the SCSI link from the SIN to the CDRP node.
WRRGQ0 (NP)	3B computer words received from ring 0 queued. This count is the cumulative total of the number of words in all messages from ring 0 queued for any channel. Refer to the MRRGQ0 description.
WRRGQ1 (NP)	3B computer words received from ring 1 queued. This count is the cumulative total of the number of words in all messages from ring 1 queued for any channel. Refer to the MRRGQ1 description.
WSMER0 (NP)	Write source match error on ring 0. The source address in a message being written to the ring does not match the node's address as specified in the RI hardware. Since the WSMER condition is counted against the WTFMTER count, this count should always be 0.
WSMER1 (NP)	Write source match error on ring 1. Refer to the WSMER0 description.
WTFMTER0 (NP)	Ring write format error on ring 0. When the token is detected in the RAC, the node begins transmitting any messages that have queued. This error is detected while attempting to write to the ring.

Table 5-B. Interprocess Message Switch (IMS) Measurement Descriptions (Contd)

Name (Type)	Description
WTFMTER0 (NP) (Contd)	If the source address in a message being written does not match the node's address as specified in the RI hardware or the message is too short to contain a valid header, it is reported to the central processor; this count is pegged, and the write is inhibited. The buffer that is being sent to the ring is discarded.
WTFMTER1 (NP)	Ring write format error on ring 1. Refer to the WTFMTER0 description.
WXRG0 (NP)	3B computer words transmitted to ring 0. This count is incremented by the number of words Direct Memory Accessed to ring 0 as described under the MXRG0 count.
WXRG1 (NP)	3B computer words transmitted to ring 1. This count is incremented by the number of words Direct Memory Accessed to ring 1 as described under the MXRG1 count.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions

Name (Type)	Description
BYMSUR (SS7)	Message signal unit bytes received. This count, along with the BYMSUX, MGMSUR, and MGMSUX counts, provides a good measure of traffic flow on the link. A message signal unit contains CCS message data (refer to the MGMSUR count for the types of signal units). When a message signal unit is received, regardless of the message type, this count is incremented in the link interface by the length of the signal unit in bytes, not including flags between signal units.
BYMSUX (SS7)	Message signal unit bytes transmitted. Refer to the BYMSUR description.
BYR (SS7)	Total bytes received excluding flags. Data is transmitted over SS7 links using signal units. All signal units have one flag byte or possibly more at the end to delimit between signal units. Also, all signal units contain a header and check bits. When any level 2- or 3-type signal unit is received, these flag bytes are removed and this count is incremented in the link interface by the length of the signal unit in bytes, including header and check bits. The BYMSUR measurement is included in this measurement. Furthermore, this count includes bytes from all types of signal units (message, link status, or fill-in). Therefore, it is usually a very large value. This count does not include bytes received in error.
BYRX (SS7)	Retransmitted bytes excluding flags. Signal units are composed of varying numbers of bytes, depending on the type of signal unit and the information it contains. Only message signal units (level 3 type) are retransmitted. Should the node determine that a signal unit must be retransmitted, described under the NACR count, this count is incremented in the link interface by the number of bytes sent. This would be the number of bytes in the erroneous signal unit and any subsequent signal units not positively acknowledged, including headers and check bits.
BYRXTE (SS7)	Threshold exceeded for BYRX. When the BYRX count has exceeded a certain value, this count pegs. It indicates too many signal units are being retransmitted. This could be due to a synchronization problem (refer to the L7FLALIGN count) or due to the far end receiving signal units in error.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
BYSR (SS7)	Non-ECIS bytes received excluding flags. Messages are transmitted over SS7 links in message signal units. These signal units are composed of varying numbers of bytes, depending on the type of signal unit and the information it contains. Each signal unit includes a header, check bits, and at least one flag, removed by the link interface. When the node receives a message signal unit containing message data other than ECIS6, this count is incremented by the length of the signal unit in bytes. This measurement is usually a very large value.
BYSX (SS7)	Non-ECIS bytes transmitted. Refer to the BYSR description.
BYX (SS7)	Total bytes transmitted excluding flags. This includes any bytes due to retransmitted messages. Note that since the BYR count does not include bytes due to signal units received in error, this count may very likely differ from the BYR count at the far end. Refer to the BYR description for more detail.
CLF (link set)	Link set failure. When the last available link in the set fails, this count pegs and the appropriate TFx and TCx messages are sent. This count indicates how many times the link set failed. Refer to the CLFA, CLFB, and CLFC descriptions for more details on specific link set failure scenarios. Note that failure of a link set may result in a signaling point isolation (if the combined link set has failed).
CLFA (Office)	A-link set failure. This is a cumulative total of the CLF count for all A-link sets in the office.
CLFAT (Office)	Duration of A-link set failure.
CLFSP (Office)	Link set failure. This is a cumulative count of all link set failures in the office. See the CLF description.
CLFSPT (Office)	Duration of link set failure. This count is a cumulative duration of all link set failures in the office. See the CLFT description.
CLFT (link set)	Duration of link set failure. This time period begins when the last link in the link set fails. The time period ends when any link in the set restores. This count indicates the total time the link set is failed.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
COS7CRFSRCM (SS7)	Number of times a "CREF" message is sent due to a source match.
COS7DCHNOOS (SS7)	Number of times an incoming CO-SCCP message is discarded due to the destination D-channel being OOS.
COS7DSDSRCM (SS7)	Number of times a CO-SCCP message is discarded due to source match.
COS7ERRSRCM (SS7)	Number of times an "ERROR" message is sent due to a source match.
COS7LCDINV (SS7)	Number of times an incoming CO-SCCP message is discarded due to an invalid or unequipped LACID.
COS7RLCSRCM (SS7)	Number of times an "RLC" message is sent due to a source match.
COS7UNERNA (SS7)	Number of times an incoming CO-SCCP message is discarded due to an unequipped ring node.
CRCER (SS7)	Cyclic redundancy check errors (CRCER). The link interface checks for data errors in received signal units using the check bits that are part of the received signal unit. If the CRC check fails, the signal unit is discarded, this count is pegged, and a negative acknowledgment is sent. Otherwise, the signal unit is accepted and a positive acknowledgment is sent. When the rate of these errors exceeds a predetermined value, the node is notified and the link is marked as failed.
CRCERTE (SS7)	Threshold exceeded for CRCER. When the CRCER count exceeds a certain value, this count pegs. It is an indication that the data link carrier failed.
DCFLABNT (SS7)	Cumulative duration of signaling link declared failures due to abnormal FIBR/BNSR. This count pegs in the central processor.
DCFLHWPT (SS7)	Cumulative duration of signaling link declared failures due to general hardware problems. This count pegs in the central processor.
DCFLSWPT (SS7)	Cumulative duration of signaling link declared failures due to general software problems. This count pegs in the central processor.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
DCFLXDAT (SS7)	Cumulative duration of signaling link declared failures due to excessive delay of acknowledgment. This count pegs in the central processor.
DCFLXDCT (SS7)	Cumulative duration of signaling link declared failures due to excessive duration of congestion. This count pegs in the central processor.
DCFLXERT (SS7)	Cumulative duration of signaling link declared failures due to excessive error rate. This count pegs in the central processor.
DRP7MSG1 (SS7)	Number of priority level 1 messages dropped due to RPC congestion. The node examines the service information octet field in the message to determine its priority before sending it on the ring. Except for ECIS6 messages (see the DRPEMSG_ descriptions) this count is the cumulative total of all messages discarded due to level 1 RPC congestion. The DRP6MSG1 description explains the discard strategy.
DRP7MSG2 (SS7)	Number of priority level 2 messages dropped due to RPC congestion. This count is similar to the DRP7MSG1 count (refer to that description) and is the cumulative total of all messages discarded due to level 2 RPC congestion.
DRP7MSG3 (SS7)	Number of priority level 3 messages dropped due to RPC congestion. This count is similar to the DRP7MSG1 count (refer to that description) and is the cumulative total of all messages discarded due to level 3 RPC congestion.
DRPEMSG1 (SS7)	Number of priority level 1 ECIS6 messages dropped due to RPC congestion. This count pegs for any ECIS6 message discarded due to level 1 RPC congestion; the mechanism is similar to that for the DRP7MSG1 count. Note that the DRPEMSG_ counts are not included in the DRP7MSG_ counts.
DRPEMSG2 (SS7)	Number of priority level 2 ECIS6 messages dropped due to RPC congestion. This count is similar to the DRPEMSG1 count (refer to that description) and is the cumulative total of all messages discarded due to level 2 RPC congestion.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
DRPEMSG3 (SS7)	Number of priority level 3 ECIS6 messages dropped due to RPC congestion. This count is similar to the DRPEMSG1 count (refer to that description) and is the cumulative total of all messages discarded due to level 3 RPC congestion.
ERSEC (SS7)	Number of 1-second intervals with at least one error. Each second, the link interface determines if any signal units have been received in error (counted by the CRCER measurement). If there have been signal unit errors, this count pegs. It is not a count of the number of errors that occurred. This measurement is an indicator of long-term performance of the link.
ERSECTE (SS7)	Threshold exceeded for ERSEC. When the ERSEC count has exceeded a certain value, this count pegs. The error is an indication of facility performance degradation.
FORRX (SS7)	The link experienced a forced retransmit cycle. When the far end indicated received errors, the affected messages are retransmitted and this count pegs in the link interface (LI). A large number of forced retransmit cycles could cause transmit buffer congestion and discarding of messages. This count indicates there are high queuing delays which could cause a reduction in throughput.
FORRXBY (SS7)	Bytes retransmitted during forced retransmit mode. This count is pegged in the link interface (LI) and is the cumulative total of bytes transmitted during forced retransmit cycles.
GTTPERFD (Office)	Total number of SS7 global title translations performed by the SCCP in the central processor.
GTTUNBC (Office)	Global title translation could not be performed due to congestion.
GTTUNBT (OFF)	Unable to perform Global Title Translation on message received from the local network due to no translation for address of such nature. This is also referred to as GTT failure diagnostic 0. This is the total number of GTTs for the local NID that failed due to no translation table being assigned for the specified global title (GT) type. The sum of this count and the GTTUNTT count is the total number of such failures for the office.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
GTTUNNT (Office)	Global title translation could not be performed due to congestion.
LINKDLAY (LN7)	This is the average link output delay, measured in milliseconds, for sampled MSUs. This is calculated during report generation with the following algorithm. **LINKDLAY = N*W*** (byte emission time) Where: **N** is a multiplication factor to adjust the header bytes on the link in comparison with the header bytes waiting in the link transmission buffer. **N = (average message length + 7) / (average message length +5)** **W** is the average number of message bytes waiting in the link transmit buffer determined by the following: **W = cumbyt / MSUSAMPL** Byte emission time is 0.143 milliseconds, the time required to transmit all bits of a byte on a 56 kbps link.
L6MGRV_ (SS7)	ECIS6 messages received on virtual link. Since ECIS messages are the only banded messages received on a SS7 link, this is the total count of all banded messages received for the indicated virtual link. These messages are not included in the total SS7 messages received (the L7MGSR count). This count includes initial address (MGIAMRV_) and answer (MGANSRV_) messages. Refer to the L6MGR count also.
L6MGXV_ (SS7)	ECIS6 messages transmitted on virtual link. Since ECIS messages are the only banded messages transmitted on a SS7 link, this count is the total of all banded messages transmitted for the indicated virtual link. It includes the MGIAMX_ and the MGANSX_ counts. See also the L6MGX description.
L6SUPRV_ (SS7)	Telephone message signal units received on virtual link. Since ECIS messages are the only banded messages received on a SS7 link, this is the total count of all signal units involved in banded messages received for the indicated virtual link. This count does not include SYNC, ACU, or PRO signal units.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L6SUPXV_ (SS7)	Telephone message signal units transmitted on virtual link. Since ECIS messages are the only banded messages transmitted on a SS7 link, this is the total count of all signal units involved in banded messages transmitted for the indicated virtual link. This count does not include SYNC, ACU, or PRO signal units.
L7ACO (SS7)	Automatic changeover. This is the sum of near-end (L7ACONE) and far-end (L7ACOFE) changeovers.
L7ACOTE (SS7)	Automatic changeover threshold exceeded. When the L7ACO count has exceeded a certain value, this count pegs. The link is experiencing excessive errors causing repeated changeovers to another link.
L7ACOFE (SS7)	Automatic changeover (COV) initiated by the far end (changeover order has been received). A COV involves transferring signaling messages from the unavailable link to other links (any links in the combined link set or C-links). A C-link COV causes messages to be load balanced between any other available C-links. Both the changeover order and acknowledgment are sent on another link in the specified link's set. When the order is received from the far end, this count pegs and either a COV or emergency COV is initiated. The latter is used when the node is OOS, or the far end indicates out of sequence messages. The following is the COV sequence: (1) The link is removed from service and no new messages are given to the node—message handling pauses. (2) Messages remaining in the transmit/retransmit buffers are retrieved and sent in sequence on other links. An emergency COV does not attempt to retrieve messages from the retransmit buffer.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7ACOFE (SS7) (Contd)	(2) (Contd) Furthermore, if the link node is OOS, the link failed due to near-end PRO, or the far end is blocked by the failure, no messages are retrieved. (3) Message handling resumes with new messages sent to the other links and only synchronization signal units sent on this link. If the COV is automatic, the link changes back when synchronism is restored. If the link cannot sync and change back within 3 minutes, 10 minutes if a long key exchange is involved, it is declared failed (the L7FLD count pegs).
L7ACONE (SS7)	Automatic changeovers initiated at the near end. This occurs usually due to excessive errors on the link. If all links in the combined link set are OOS or the C-links are unable to handle the additional load, an EMR occurs and changeover is denied. If allowed, this count pegs and either a changeover or emergency changeover is initiated. The sequence is described under the L7ACOFE measurement. The sequence indicated is followed; except, a changeover order is sent to the far end rather than being received. Furthermore, all acknowledgments must be received before starting the changeover.
L7AFLT (SS7)	Duration of automatic link out of service including duration of declared failure. Refer to the L6AFLT description.
L7BADRTG (SS7)	Message signal units (MSUs) discarded due to bad or no routing data. If the translation for a received DCIS6 message (that is, an SCCP class 0 message) fails due to no translation data, it is discarded in the incoming node; count is pegged; and a UDS message is returned to the originator. If a received non-DCIS6 message has a destination point code related to an outgoing CCIS 6 pool, it is discarded in the incoming node; count is pegged. Refer to the MRSNTO7 count for the total number of DCIS6 messages discarded in the central processor due to translation failure.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7BOFR (SS7)	The receive buffer in a SS7 link node overflows. Refer to the L6BOFR description.
L7BOFRT (SS7)	Duration of the receive buffer overflow. This timer pegs in the link interface. Refer to the L6BOFRT description.
L7BOLR (SS7)	The receive buffer in a SS7 link node overloads. Refer to the L6BOLR count for a description of buffer overload. No messages are discarded in the overload state. When overload occurs, the link interface stops transmitting positive acknowledgments to the far end until the congestion abates. The far end responds by limiting traffic to the near end.
L7BOLRT (SS7)	Duration of the receive buffer overload. This timer pegs in the link interface. Refer to the L6BOLRT description.
L7BYTO3B (SS7)	The SS7 message bytes sent to 3B computer. This count is incremented by the size of the message when it is sent to the central processor. See the L6BYTO3B description.
L7DIF (SS7)	CNI SS7 data integrity flag. Refer to the L6DIF description.
L7EMR (SS7)	Emergency restart due to local failure. This count pegs only if there are virtual links assigned to the indicated SS7 link. Refer to the EMR description.
L7EMRPO (SS7)	Emergency restart due to far-end processor outage. This count pegs only if there are virtual links assigned to the indicated SS7 link. Refer to the EMRPO description.
L7EMRPOT (SS7)	Duration of emergency restart due to far-end processor outage.
L7EMRT (SS7)	Duration of emergency restart due to local failure.
L7FLALIGN (SS7)	Alignment failure. This count indicates the number of signal units received in error during the initial alignment procedure. This procedure is the first part of the level 2 protocol and is done once whenever a link is restored. When a link is out of alignment (a flag is detected within an signal unit where it is not expected), the link is sending only status signal units indicating that fact. Once alignment is achieved, the link begins a prove-in period.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7FLALIGN (SS7) (Contd)	During the prove-in, the error rate monitor counts signal units received in error. Once prove-in is complete, the link is ready and traffic may start. The link interface now reports the error rate, and the value is accumulated into this count.
L7FLD (SS7)	Declared link failure. A declared failure could be due to a 1-minute continuous buffer overload, a sanity check failure, a 30-second far-end processor congestion, or a changeover lasting more than 3 minutes (10 minutes if a long key exchange is involved). The changeover could be due to far-end request or because errors exceeded the threshold for changeover. This count pegs and the appropriate TFx or TCx messages are broadcast. The link is diagnosed (if the failure is due to a far-end PRO, diagnostics wait until the outage ends). This failure could also cause the combined link set to fail; refer to the CLF measurement in this case. Some of the actions leading to declared failure are described in the L7BOLR, L7ACOFE, L7PCR, and CRCER descriptions.
L7FLDT (SS7)	Duration of declared link failure. Refer to the L6FLDT description.
L7LCDIS1X (SS7)	Level 1 transmit buffer congestion discard. This count is the number of times the transmit buffer occupancy reached the indicated threshold for message discard. Selected messages are being discarded according to the strategy described under the MSURMV measurement. Note that since the corresponding onset level has been reached, far-end signaling points are also discarding messages according to that strategy due to receipt of transfer controlled messages. This count does not peg again at least until occupancy drops below the corresponding abatement threshold.
L7LCDIS1XT (SS7)	Duration of level 1 congestion discard, end at abatement.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7LCDIS2X (SS7)	Level 2 transmit buffer congestion discard. This is the next higher discard level from discard level 1. Refer to the L7LCDIS1X measurement for a description of actions taken.
L7LCDIS2XT (SS7)	Duration of level 2 congestion discard, end at abatement.
L7LCDIS3X (SS7)	Level 3 transmit buffer congestion discard. This is the next higher discard level from discard level 2 and is currently the highest discard level possible. Refer to the L7LCDIS1X measurement for a description of actions taken.
L7LCDIS3XT (SS7)	Duration of level 3 congestion discard, end at abatement.
L7LCON1X (SS7)	Level 1 transmit buffer congestion onset. This count is the number of times the transmit buffer occupancy reached the indicated threshold for congestion. The congestion level is higher than the corresponding abatement level but lower than the corresponding discard level. At each onset level, the node reports the congestion state to the central processor. Network management messages (transfer controlled) are then broadcast to adjacent signaling points to limit messages to the affected node. To avoid further congestion of the transmit buffer, the far end initiates the discard strategy used by nodes at the discard level. See the MSURMV measurement.
L7LCON1XT (SS7)	Duration of level 1 congestion onset, end at abatement. This time period includes levels 2 and 3 also. If the node remains in the same congestion level (1, 2, or 3) for 60 seconds, it is taken OOS and diagnosed. However, since the duration timers for each level are cumulative, they may exceed this 60-second limit.
L7LCON2X (SS7)	Level 2 transmit buffer congestion onset. Messages are being discarded according to the level 1 strategy. The node reports the level 2 congestion state to the central processor. Actions are taken as described under the L7LCON1X measurement.
L7LCON2XT (SS7)	Duration of level 2 congestion onset, end at abatement. This time period includes level 3 also.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7LCON3X (SS7)	Level 3 transmit buffer congestion onset. Messages are being discarded according to the level 2 strategy. The node reports the level 3 congestion state to the central processor. Actions are taken as described under the L7LCON1X measurement.
L7LCON3XT (SS7)	Duration of level 3 congestion onset, end at abatement.
L7LNKACTT (LN7)	Signaling link active time. This time starts when the link restores to service and stops when the link fails or is moved to the MOOS state. This count pegs in the central processor.
L7MCOFE (SS7)	Far-end manual changeover request has been received, usually due to a need for link changes or maintenance. The far end has requested and permission has been granted to initiate a changeover. Either a changeover or emergency changeover is initiated. The sequence is described under the L7ACOFE description.
L7MCONE (SS7)	Near-end manual changeover due to local maintenance action. The changeover could be denied if removing the link from service would cause the far end to become inaccessible. This end requests permission from the far end to initiate a changeover (the far end pegs the L7MCOFE count). If the far end grants permission, either a changeover or emergency changeover is initiated. The sequence is described under the L7ACOFE description. The sequence indicated is followed; except, a changeover request is sent to the far end rather than being received. Furthermore, all acknowledgments must be received before starting the changeover.
L7MFLT (SS7)	Duration of manual link out of service. Refer to the L6MFLT description.
L7MGSR (SS7)	Non-ECIS6 messages received. This count includes only SCCP and network management messages ECIS6 messages are pegged by the L6MGRV_ counts. The count pegs in the node when the message is received from the link interface.
L7MGSX (SS7)	Non-ECIS6 messages transmitted. Refer to the L7MGSR description.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7MRPBC (SS7)	ECIS6 message rejected due to congestion. Banded messages are transmitted on SS7 links using ECIS6. This count is a cumulative total for all virtual links assigned to the indicated link. Refer to the L6MRPBC description.
L7MRPNT (SS7)	ECIS6 message rejected due to no translation data. Banded messages are transmitted on SS7 links using ECIS6. This count is a cumulative total for all virtual links assigned to the indicated link. Refer to the L6MRPNT description.
L7MSINVSIO (LN7)	Message signal units (MSUs) discarded due to invalid Service Indicator Octet (SIO). This measurement is also counted per office as the sum of this measurement for all SS7 links.
L7POR (SS7)	Far-end processor outage occurred. This count is not the number of PRO signal units received but a count of the number of processor outage events recognized by the specified link. When the far-end office sends the message, it indicates that office is undergoing initialization or is overloaded. The far-end link interface is in the processor outage send mode (see the L7POX description). The problem is treated as a link failure. Only fill-in signal units are transmitted and a changeover is initiated. This count pegs once when the first PRO is received and not again at least until the PROs stop.
L7PORT (SS7)	Duration of far-end processor outage.
L7POX (SS7)	Link interface in processor outage send mode. This is similar to the PRO send mode for a CCIS 6 link (see the L6POX measurement); except, a continuous stream of link status signal units are sent instead of PRO signal units. These link status signal units indicate the processor outage condition.
L7POXT (SS7)	Duration of processor outage in effect. This timer pegs in the link interface.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7RBFOC (SS7)	Average receive buffer length in bytes (usually is very small). This is the average occupancy of the buffer. This measurement is obtained by periodically checking buffer length, cumulating the number of bytes used, and then dividing by the number of times the length is checked. Since this is a measure of how long messages are staying in the buffer, it is a relative measure of the load on the link. The count pegs in the link interface.
L7RTGAUD (SS7)	Routing audit failure. This is an automatic audit that checks consistency of the pool to point code table. The data for two pools is checked every 10 seconds. The active 3B computer data is checked first. If errors are found, an output message is generated and the errors corrected. Next, the data is checked in all SS7 nodes. When the pool to point code audit finds errors in the node, they are corrected and this count pegs.
L7THRSWMSU (LN7)	Through-switched message-signal units (MSUs). This is the number of MSUs received by the node in which the destination address does not specify this signaling point. This is the case for most non-global title routed messages and should be very close to the MGMSUR count. The sum of this count and the L7TRMDMSUS count should equal the MGMSUR count.
L7TRMDMSUS (LN7)	Terminated message signal units (MSUs). This is the number of MSUs received by the node in which the destination addr3ess specifies this signaling point. One example of this type of message would be a global title message requiring global title translation. This count normally has a very small value.
L7TRMSUOCT (LN7)	Terminated MSU octets (refer to the L7TRMDMSUS count for more details). This count is incremented by the length of the MSU in bytes (including header and check bits). It should be noted that the headers on messages counted by this measurement are 8 bytes longer than the headers on messages counted in the LI.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
L7TSMSUOCT (LN7)	Through-switched MSU octets (refer to the L7THRSWMSU count for more details). This count is incremented by the length of the MSU in bytes (including header and check bits). It should be noted that the headers on messages counted by this measurement are 8 bytes longer than the headers on messages counted in the LI.
L7XBFLOOK (SS7)	Number of transmit buffer visits by the link interface. This is the number of times the link interface checked buffer occupancy in order to calculate the L7XBFOC and L7RBFOC counts. This count pegs in the link interface.
L7XBFOC (SS7)	Average transmit buffer length in bytes (usually is zero). Refer to the L6XBFOC description.
MGANSRV_ (SS7)	Answer messages received on virtual link. This is the total count of all answer messages received for the indicated virtual link. Refer to the MGANSR description.
MGANSXV_ (SS7)	Answer messages transmitted on virtual link. This is the total count of all answer messages transmitted for the indicated virtual link. Refer to the MGANSX description.
MGIAMRV_ (SS7)	Initial address messages received on virtual link. This is the total count of all IAM messages received for the indicated virtual link. Refer to the MGIAMR description.
MGIAMXV_ (SS7)	Initial address messages transmitted on virtual link. This is the total count of all IAM messages transmitted for the indicated virtual link. Refer to the MGIAMX description.
MGMSUR (SS7)	Message signal units received. Data is transmitted over SS7 links using three types of signal units: Level 3 - Message signal units containing CCS message information; these are passed to/from the node. Level 2 - Link status signal units (indicating such things as alignment status, out of service, or PRO send mode) Level 2 - Fill-in signal units (used for alignment control during link recovery).

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
MGMSUR (SS7) (Contd)	This count is pegged in the link interface when a level 3 type signal unit is received. It is essentially a count of all SS7 CCS traffic messages. It includes ECIS6 messages, SCCP messages, and network management messages. This count, along with MGMSUX, BYMSUR, and BYMSUX provides a good measure of traffic flow on the link.
MGMSUX (SS7)	Message signal units transmitted. When a message signal unit is transmitted, this count is pegged in the link interface. Refer to the MGMSUR description.
MRBADRTG (office)	Message signal units (MSUs) discarded due to routing data error (no routing data). This count is a cumulative total for all SS7 MSUs handled by the SCCP in the central processor.
MRSBCO7 (Office)	The Destination routed CCIS6 (DCIS6) message rejected due to congestion. Direct signaling (DS) messages are transmitted on SS7 links using DCIS6. If the transmit buffer of the outgoing link is congested or the far end of that link is sending processor congestion messages, the DS message is discarded; this count is pegged in the central processor; and a UDS message is returned to the originator (see MRSBCO6).
MRSNTO7 (Office)	The DCIS6 message rejected due to no translation data. Direct signaling messages are transmitted on SS7 links using DCIS6. If the translation for a DCIS6 message fails, it is blocked. The message is discarded, this count is pegged in the central processor, and a UDS message is returned to the originator.
MSG7LOOP (SS7)	The SS7 messages "looped" in the network. Before a SS7 message is transmitted, a check is made for a looping message. Looping usually occurs when: (1) The message is blocked at some other node (see the MRSBCO7 and MRSNTO7 counts) and must be returned to this node to be sent to the origination. (2) The normal outgoing route is blocked and the message must be rerouted. If the outgoing link set for the message, is a direct or combined link set containing the incoming link and the message is a UDS type, it is looping.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
MSG7LOOP (SS7) (Contd)	This count is pegged, and the message is not sent. Furthermore, if the incoming link is a C-link, a TFP or TCP response is returned on the incoming link.
MSINVSIO (SS7 or Office)	Message signal units (MSUs) discarded due to invalid Service Indicator Octet (SIO). This measurement is also counted per office as the sum of this measurement for all SS7 links.
MSUDISC_ (SS7)	Messages removed due to link congestion. The SS7 discard strategy (for level 1, 2, or 3) is as described below: The node first checks the priority of a message before transmitting it. The priority is contained in the service information octet field and is compared with the congestion state of the transmit buffer. Refer to the L7LCDIS_X measurement description. If the priority is less than the congestion level, the message is removed; the corresponding count pegs, and a return message may be sent. Priority 0 messages peg MSUDISCO, priority 1 messages peg MSUDISC1, and priority 2 messages peg MSUDISC2. The return message is sent only if the received message is not a UDS type. If the message to be transmitted is a unit data type SCCP message, a UDS message is created and returned to the originator. If the priority of the message is equal to or greater than the congestion level, it is transmitted and this count is not pegged.
MSUSAMPL (LN)	This is the number of message signal units (MSUs) sampled for link output delay. Link output delay is the interval beginning when the message has been placed in the outgoing signaling link transmission buffer and ending when the last bit of the message has been transmitted on the outgoing signaling link. During each 10-second time interval, every SS7 link node samples the first outgoing MSU at the time it is placed in the link interface (LI) transmit buffer. If an MSU is not transmitted during the interval, no action is taken. A 10-second interval, where no sample is taken is counted as 0; otherwise, the interval is counted as 1. The collected 5-minute value is always 30 or less.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
NACR (SS7)	Negative acknowledgment (ACU) "event" occurred. Upon receiving a negative ACU, this count is pegged once for the first signal unit that must be queued for retransmission and not again until the event ends. If subsequent signal units must be queued for retransmission—for example, due to a sequence error—this count is not pegged. Once sequencing is correct, the event has ended. The basic error correction method in SS7 involves both positive and negative acknowledgments. Each signal unit has a forward sequence number and indicator and a backward sequence number and indicator in its header. The backward sequence number and indicator in a received signal unit is compared with the forward sequence number and indicator in a previously transmitted signal unit to determine whether a positive or negative ACU is being indicated by the far end. Each received signal unit normally, positively acknowledges the previously transmitted signal unit; this occurs at both ends of a link. Any signal units not positively acknowledged are queued for retransmission. A positive ACU, received for any transmitted signal unit, positively acknowledges all previously transmitted signal units. Conversely, a negatively-acknowledged signal unit is retransmitted along with any previously transmitted signal units not yet positively acknowledged.
NACRTE (LN7)	Number of hourly thresholds exceeded for negative acknowledgements received. This count pegs in the central processor.
NOCMG (Office)	The number of times the system entered a state in which it could not process CCS messages. The basis of this measurement is an internal timer which records the current time once each second, as long as messages are being processed. When an inability to process messages is detected, the timer stops and a flag is set indicating the "no message processing state."

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions

Name (Type)	Description
NOCMG (Office) (Contd)	When the problem clears, the timer starts and the elapsed time is calculated. The flag is reset and this count is incremented.
NOCMGT (Office)	The accumulated time (in seconds) during which no messages could be processed. See the NOCMG measurement for a description.
OCCUPMSU (LN7)	This is the link transmission buffer average occupancy based on 10-second scans. Occupancy is defined as the buffer contents measured in MSUs immediately before a sample MSU is placed in the buffer for transmission on the link. At the time of sampling, the LI transmit buffer content (cotb) is measured in bytes and added to the cumulative byte total (cumbyt) to be reset every 5 minutes. The average occupancy, measured in MSUs, is obtained by dividing the cumulative byte total by the number of MSUs sampled (MSUSAMPL) and by the average message length. The average message length is calculated by dividing the bytes transmitted (BYMSUX) by the MSUs transmitted (MGMSUX) during a standard measurement interval. The reported average occupancy is rounded off to the nearest larger integer. **OCCUPMSU = cumbyt / MSUSAMPL *** (average message length) Where: **Average message length = BYMSUX / MGMSUX**
RABT (SS7)	Number of abort events received on the link. When an abort event, also called an octet counting event, is indicated by receiving more than seven consecutive "1" bits, this count is pegged in the link interface (LI). This condition is caused by either hardware and/or software problems or T1 digital facility resynchronization.
RABTER (SS7)	Number of octets received in error during abort events. Errors detected during abort events are included in the signal unit error rate monitor. This count is the cumulative total of these errors and is pegged in the link interface. The average burst size of facility failures is this count divided by the received abort (RABT) count.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
RTESETUN (Cluster)	Route set unavailable. The application uses a specific set of routes to send messages to a specific cluster of destinations. Availability of the route set is determined by the availability of the link sets along the path to the cluster. Failure of any link set could result in one or more members becoming inaccessible to this office. This count is pegged whenever a member of the indicated cluster becomes inaccessible due to route set unavailability. This count is the total number of times a member became inaccessible, but does not indicate current accessibility.
RTESETUNT (Cluster)	Duration of route set unavailable. This is not the cumulative duration of each member's inaccessibility. Rather it is the total time during which any member in the indicated cluster is inaccessible; individual events could overlap.
RTGAUDFL (Office)	Routing audit failure. This is the total number of times the routing audit failed for any node in the office See the L7RTGAUD description.
SC7R (SS7)	Signaling connection control part (SCCP) message received. This is the total number of messages received by the SCCP in the node. These messages may be global title routed or point code routed and some may be sent to the central processor for handling. This count includes messages destined for this point code (the SC7RLNN count) or destined for some other point code, not counted presently. It is pegged in the node when the message is received from the network.
SC7RERPRO (SS7)	SCCP message destined for a prohibited subsystem. The prohibited subsystem may be either local or distant. This is the total number of messages received by SCCP in the node destined for a prohibited subsystem. The count is pegged in the node when the message is received from the network.
SC7RERUA (SS7)	SCCP message destined for an unknown address or global title. SCCP global title routed messages are destined for the central processor for global title translation.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SC7RERUA (SS7) (Contd)	This is the total number of messages received by SCCP in the node destined for an unknown address. The count is pegged in the node when the message is received from the network. See the SCRERUA description.
SC7RERUATY (SS7)	SCCP message destined for an unknown address or global title type. SCCP global title routed messages are destined for the central processor for global title translation. This is the total number of messages received by SCCP in the node destined for an unknown address type. The count is pegged in the node when the message is received from the network. See the SCRERUATY description.
SC7RERUNE (SS7)	SCCP message destined for an unequipped subsystem. This is the total number of messages received by SCCP in the node destined for an unequipped subsystem. The count is pegged in the node when the message is received from the network.
SC7RGTR (SS7)	SCCP message destined for global title routing. This is the total number of messages received by SCCP in the node using global title routing (for example, DCIS6 messages). A global title is either a function number or an NPA-NXX. The count is pegged in the node when the message is received from the network.
SC7RLNN (SS7)	SCCP message destined for the local network node. This is the total number of messages received by SCCP in the node destined for this point code. The count is pegged in the node when the message is received from the network.
SC7RLSS (SS7)	SCCP messages destined for an equipped local subsystem. This is the total number of messages received by SCCP in the node destined for an equipped local subsystem. The destination PC is a subsystem at this node. It is pegged in the node when the message is received from the network.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SC7RNATL (SS7)	Messages discarded due to a blocked point code. When any message destined for an inaccessible signaling point is received, it is discarded and this count is pegged in the incoming node. This count is cumulative for all point codes.
SC7UDSX (SS7)	Unit data service (UDS) message transmitted in response to a unit data message type failure. When a unit data message is received by SCCP in the node, a UDS may be sent to the originator. If SCCP cannot deliver a message to its destination for one of the defined UDS reasons and the message indicates a UDS message should be returned, the UDS is formatted and returned to the originator. This count is pegged in the node when the UDS is sent.
SCR (Office)	Signaling connection control part (SCCP) message received. This is the total number of messages received by SCCP in the central processor. These messages may be global title routed or point code routed. This count includes messages destined for this point code, the SCRLNN count, or destined for some other point code, presently no count. It is pegged when the message is received by the central processor.
SCRERPRO (Office)	The SCCP message destined for a prohibited subsystem. The prohibited subsystem may be either a local or a distant subsystem. This is the total number of locally originated SCCP messages received by message handling in the central processor destined for a prohibited subsystem. The count is pegged when the message is received by message handling in the central processor.
SCRERUA (Office)	The SCCP message destined for an unknown address. A locally originated SCCP global title routed message can be translated to a DPC (called global title translation). Should the application be unable to translate the global title in the received message (that is, the address is unknown), this count is pegged and a UDS message may be returned. This count is not to be confused with the SCRERUATY measurement.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SCRERUA (Office) (Contd)	While this count indicates the number of messages that failed global title translation due to no translation data, the latter is a count of messages received for translation of a global title type that is not provided.
SCRERUATY (Office)	The SCCP message destined for an unknown address type. Should the application not provide the capability to translate the global title type in the received message, the message handler pegs this count. This count is the total number of locally originated SCCP messages received by message handling in the central processor that are destined for global title translation of an unknown or, more specifically, a nonprovided address type. See the SCRERUA description.
SCRERUNE (Office)	The SCCP message destined for an unequipped subsystem. This is the total number of locally originated SCCP messages received by message handling in the central processor which are destined for a subsystem that is currently unequipped. The count is pegged when the message is received by message handling in the central processor.
SCRGTR (Office)	The SCCP message destined for global title routing. This is the total number of messages received by the SCCP in the central processor using global title routing (for example, DCIS6 messages). A global title is either a function number or an NPA-NXX. The count is pegged when the message is received by message handling in the central processor.
SCRLNN (Office)	The SCCP message destined for the local network node. This is the total number of messages received by the SCCP in the central processor destined for this point code. The count is pegged when the message is received by message handling.
SCRLSS (Office)	The SCCP message destined for an equipped local subsystem. This is the total number of locally originated SCCP messages received by message handling in the central processor which are destined for a local subsystem that is equipped. The count is pegged when the message is distributed by message handling in the central processor.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SCRNATL (Office)	This count is currently ineffective—it is always zero.
SCSRTR (Office)	Subsystem routing test message received. This is the total number of such messages received by the SCCP. When the message is received by the central processor, this count is pegged.
SCSRTX (Office)	Subsystem routing test message transmitted. This is the total number of such messages transmitted by the SCCP. When the message is sent by the central processor, this count is pegged.
SCSSTR (Office)	Subsystem status test message received. This is the total number of such messages received by the SCCP. When the message is received by the central processor, this count is pegged.
SCSSTX (Office)	Subsystem status test message transmitted. This is the total number of such messages transmitted by the SCCP. When the message is sent by the central processor, this count is pegged.
SCUDSX (Office)	A Unit data service (UDS) message is transmitted in response to a unit data message type failure. When a locally originated unit data message is received by message handling in the central processor, a UDS message may be sent to the originator. If the SCCP cannot deliver the message to its destination for one of the defined UDS reasons and the message indicates a UDS message should be returned, the UDS is formatted and returned to the originator. This count is pegged when the UDS message is sent by message handling in the central processor.
SEVERSEC (SS7)	Severe error seconds. This count is the total number of seconds during which the link had more than 64 errors (indicating a bit error rate ratio greater than 1 in 1000). It is pegged in the link interface (LI) and can be used to monitor and characterize T1 facility failures.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SPI (SS7)	Adjacent signaling point isolation due to local failure or received TFx. A link set along a path to the indicated destination failed causing a complete failure of all signaling paths to the destination. Failure of any signaling path is caused by either a local link set failing or the receipt of a TFx message indicating some link set along the path to the destination failed. Refer to the SPIA, SPIB, and SPIC descriptions.
SPIA (Office)	Adjacent signaling point isolation due to local failure on A-link. This condition occurs when all C-links are unavailable, and the last available A-link to the indicated destination fails or receives a TFx message indicating some link set along a path to the destination failed. This is a cumulative total of the SPI count for all A-links in the office. The appropriate per-link count is also pegged in this situation (SPI or SPIPO).
SPIAPO (Office)	Adjacent signaling point isolation due to far-end processor outage on A-link. At present, this count is ineffective—it is always zero. See the SPIA count.
SPIAPOT (Office)	Duration of the above. At present, this count is ineffective—it is always zero. See the SPIAT description.
SPIAT (Office)	Duration of the above. See the SPIA description.
SPIPO (SS7)	Adjacent signaling point isolation due to far-end processor outage. A link failed due to receiving PROs from the far end causing a complete failure of all signaling paths to the indicated destination from this office. The effect is the same as the SPI due to local failure or received TFx. See the SPI description.
SPIPOT (SS7)	Duration of the SPIPO. This time period begins when the local link fails due to receiving PROs. It ends when any link set along a path to the destination restores. The count is the total time the far end is isolated from this office.

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SPISP (Office)	Adjacent signaling point isolation due to local failure. This is a cumulative count of all SPIs for all links in the office. Refer to the SPI description.
SPISPPO (Office)	Adjacent signaling point isolation due to far-end processor outage. At present, this count is ineffective—it is always zero. See the SPISP count.
SPISPPOT (Office)	Duration of the above. At present, this count is ineffective—it is always zero).
SPISPT (Office)	Duration of the above. This count is the cumulative duration of all SPIs for all links in the office.
SPIT (SS7)	Duration of the above. This time period begins when a link set along a path to the indicated destination fails causing it to be isolated. It ends when any link set along a path to the destination restores. The count is the total time the far end is isolated from this office.
SQL (SS7)	Link quality. A relative measure indicating the percentage of time the link has operated without errors (0 - 100 percent). This measurement is derived from the ERSEC count.
SRSCTRAN (LNKSET)	Signaling-route-set-congestion-test messages transmitted. Although this measurement is pegged in the central processor, it is not reported, collected, nor accumulated by CNI.
SRSTTRAN (LNKSET)	Signaling-route-set-test messages transmitted. Although this measurement is pegged in the central processor, it is not reported, collected nor accumulated by CNI.
SSATRAN (LNKSET)	Subsystem-allowed transmitted. Although this measurement is pegged in the central processor, it is not reported, collected, nor accumulated by CNI. This measurement counts the subsystem-allowed messages when the following are transmitted: (1) A local signaling connection control part (SCCP) subsystem goes in-service (2) A response is made to an incoming subsystem status test (SST) concerning an in-service subsystem

Table 5-C. SS7 Common Network Interface (CNI) Measurement Descriptions (Contd)

Name (Type)	Description
SSATRAN (LNKSET) (Contd)	(3) A signal transfer point (STP) performs a broadcast upon receipt of a subsystem-allowed message.
SSPTRAN (LNKSET)	Subsystem-prohibited transmitted. Although this measurement is pegged in the central processor and Signaling System No. 7 (SS7) node, it is not reported, collected, nor accumulated by CNI. This measurement counts the subsystem-prohibited messages when the following are transmitted: (1) A local SCCP subsystem goes out-of-service (2) A response is made to receipt of a message destined for a local out-of-service subsystem (3) An STP performs a broadcast upon receipt of a subsystem-prohibited message.
SSTTRAN (LNKSET)	Subsystem-status-test transmitted. Although this measurement is pegged in the central processor, it is not reported, collected, nor accumulated by CNI. This measurement counts all subsystem-status-test messages which are sent to verify the status of SCCP subsystems in the network for which this office marked out-of-service.
TPROCOTG (LN7)	This is the cumulative duration of node processor outage (processor outage refers to an out-of-service node processor). This count, measured in milliseconds, is a CNI accumulation of IMS measurements OOSAUT, OOSCFGT, and OOSNT.
UNVL (SS7)	Link unavailable. A relative measure indicating the percentage of time the link is out of service (0 - 100 percent).
ZPEAKOCC (LN7)	This is the link transmission buffer peak occupancy, measured in MSUs, based on 10-second scans. This is obtained by dividing the largest value of cotb (maxcotb) by the average message length. A maxcotb is determined for each desired time interval. **ZPEAKOCC = maxcotb / average message length**

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions

Name (Data)	Description
C7ACB (gg-mm)	Changeback from a failure that is not a declared failure. This is an automatic changeback to a link that previously did an automatic changeover and then restored. The changeback must normally occur within 3 minutes of the changeover. If the link interface reports a long key exchange is taking place, this time period is extended to 10 minutes. This event occurs for all automatic changebacks exclusive of the C7ACBFLD event. Refer to the L7ACO_ measurements for a description of the changeover/changeback sequence. This event is usually preceded by a C7ACO_ event.
C7ACBFLD (gg-mm)	Automatic changeback from declared failure. This event indicates the link is declared failed, has recovered, and traffic has been routed back to the link. This event is preceded by one of the C7FLD_ events (see these descriptions for more information on declared failure). Note that if a link is in the MOOS state and an emergency condition automatically forces the link back into service (called preemption), the C7MCB event occurs rather than this event.
C7ACOCOV (gg-mm)	Automatic changeover initiated by the far end. A changeover involves transferring signaling messages from the unavailable link to other links. These could be any links in the combined link set or C-links. In the case of a C-link failing, the changeover results in messages being load balanced over the other available C-links. The changeover message and the acknowledgment are both sent on some other link in the specified link's set. When the changeover order is received from the far-end, this event occurs and either an automatic changeover or emergency changeover is initiated. An ***emergency changeover*** is done when the far-end indicates messages were received out of sequence or when the link node is out of service. The following is the changeover sequence: 1. The link is removed from service and new messages are not given to the link node (message handling pauses).

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7ACOCOV (gg-mm) (Contd)	2. A changeover acknowledgment is sent to the far end on some other link in the set. 3. Messages remaining in the transmit and retransmit buffers are retrieved and are transmitted in sequence on other links. An ***emergency changeover*** does not attempt the retrieval from the retransmit buffer. If the link node is out of service or the link failed due to a near-end PRO, no retrieval is done. 4. Message handling resumes with new messages to the other links. 5. Only synchronization messages are sent on this link. In the case of an automatic changeover, the link changes back when sync is regained. Then, it is "proven in" (from 3 to 15 seconds required) and restored. The CCS messages are routed back to the restored link. If the link cannot sync and change back within 3 minutes, 10 minutes if a long key exchange is involved, it is declared failed.
C7ACOER (gg-mm)	Automatic changeover error threshold has been exceeded. The error rate monitor in the link interface has reported excessive signal unit errors. The monitor is described in more detail under the C6ACOER event. Similar actions to those described for the C7ACOCOV event are taken.
C7ALCIF (gg-mm)	Automatic link check (ACF) failure for international links only. When a link is declared failed (a C7FLD_ event), the ALC is initiated. If the ALC is not successful within 15 seconds from the link failure, this event occurs.
C7ALTR (Linkset)	Reports when an alternate or lower priority route is invoked for signaling traffic previously routed over a primary or higher priority route, as a result of either re-routing or changeover procedure.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7ALTRE (Linkset)	Reports when a priority or higher priority route is invoked for signaling traffic previously routed over an alternate or lower priority route as a result of either a re-routing or changeover procedure.
C7FLDCOL (gg-mm)	Declared link failure due to a 1-minute continuous receive buffer overload. This event is followed by a changeover, assuming it is not denied due to a blocked path. The link is removed from service and is diagnosed.
C7FLDCOV (gg-mm)	Declared link failure due to an automatic changeover initiated by the far-end. The changeover lasted more than 3 minutes, 10 minutes if a long key exchange is involved. Actions are taken as described under the C7FLDCOL event except no diagnostics are attempted and the changeover (the C7ACOCOV event) precedes this event.
C7FLDER (gg-mm)	Declared link failure due to error threshold exceeded. This is caused by an excessive number of received signal units in error. Actions are taken as described under the C7FLDCOV event except the changeover (the C7ACOER event) precedes this event.
C7FLDSNT (gg-mm)	Declared link failure due to a sanity check failure. This failure is due to either software or hardware problems causing abnormal node operation. Automatic diagnostics attempt to determine the problem. Actions are taken as described under the C7FLDCOL event.
C7LCABM1X (gg-mm)	Transmit buffer level 1 congestion ends. Buffer occupancy has dropped below the threshold for level 1 abatement after transmit buffer congestion. Messages are not being discarded.
C7LCABM2X (gg-mm)	Transmit buffer level 2 congestion ends. Buffer occupancy has dropped below the threshold for level 2 abatement after transmit buffer congestion. The node reverts to level 1 discard.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7LCABM3X (gg-mm)	Transmit buffer level 3 congestion ends. Buffer occupancy has dropped below the threshold for level 3 abatement after transmit buffer congestion. The node reverts to level 2 discard.
C7LCDIS1X (gg-mm)	Transmit buffer level 1 congestion discard begins. Buffer occupancy has reached the threshold for level 1 discard to be initiated. The SS7 discard strategy (for level 1, 2, or 3) is as described below: The node first checks the priority of a message before transmitting it. The priority is contained in the service information octet field and is compared with the congestion state of the transmit buffer. If the priority is less than the congestion level, the message is removed and a return message may be sent. The return message is sent only if the return indicator in the received message is set. If the message to be transmitted is a unit data type SCCP message, a UDS message is created and returned to the originator. If the priority of the message is equal to or greater than the congestion level, it is transmitted. This event does not occur again, at least until buffer occupancy drops below the level 1 abatement threshold (signaled by the C7LCABM1X event).
C7LCDIS2X (gg-mm)	Transmit buffer level 2 congestion discard begins. Buffer occupancy has reached the threshold for level 2 discard to be initiated. The C7LCDIS1X event describes the discard strategy.
C7LCDIS3X (gg-mm)	Transmit buffer level 3 congestion discard begins. Buffer occupancy has reached the threshold for level 3 discard to be initiated. At this point, all messages are being discarded. The C7LCDIS1X event describes the discard strategy.
C7LCON1X (gg-mm)	Transmit buffer level 1 congestion onset begins. The congestion onset thresholds (level 1, 2, or 3) are higher than the corresponding abatement levels but lower than the corresponding discard levels.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7LCON1X (gg-mm) (Contd)	At each onset level, the node reports the congestion state to the central processor. Network management messages (transfer controlled) are then broadcast to adjacent signaling points to limit messages to the affected node. To avoid further congestion of the transmit buffer, the far end initiates the discard strategy used by nodes at the discard level, described under the C7LCDIS1X event. If the node remains in the same congestion level (1, 2, or 3) for 60 seconds, it is taken OOS and diagnosed.
C7LCON2X (gg-mm)	Transmit buffer level 2 congestion onset begins. Messages are being discarded according to the level 1 strategy. The node reports the level 2 congestion state to the central processor. Actions are taken as described under the C7LCON1X event.
C7LCON3X (gg-mm)	Transmit buffer level 3 congestion onset begins. Messages are being discarded according to the level 2 strategy. The node reports the level 3 congestion state to the central processor. Actions are taken as described under the C7LCON1X event.
C7LSF (Linkset)	Link set failure begins. When the last available link in the set fails, this event occurs. If the failure of the link set results in failure of the associated combined link set, another C7LSF CNCE message is output with the combined link set identification. The end of this event is signaled by the C7LSFE event. The CLF_ measurements describe the various link set failure scenarios. If this failure causes some destination to become isolated from this office (e.g., the combined link set has failed), this event is accompanied by a C7SPI event.
C7LSFE (Linkset)	Link set failure ends. When any link in the set restores, this count pegs.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7MCB (gg-mm)	Manual changeback from manual changeover. This event occurs either due to manually restoring the link, at the near-end or far-end, or due to preemption of the MOOS state by an emergency condition. When the link regains sync, a changeback declaration is sent to the far end. The link state is changed to OOS and new messages are diverted back to the link. Until all acknowledgments are received, these messages are not transmitted; these messages are diverted to other links, if the link fails to return to service. Note that this event occurs before the link is made available.
C7MCOF (gg-mm)	Far-end manual changeover request has been received, usually due to a need for link changes or maintenance. The far end has requested and permission has been granted to initiate a changeover. Either a changeover or emergency changeover is initiated. The sequence is described under the C7ACOCOV event.
C7MCON (gg-mm)	Near-end manual changeover due to local maintenance action. The changeover could be denied if removing the link from service would cause the far-end to become inaccessible. This end requests permission from the far-end to initiate a changeover; the far end recognizes a C7MCOF event. If the far-end grants permission, either a changeover or emergency changeover is initiated. The sequence is described under the C7ACOCOV event.
C7POR (gg-mm)	Adjacent processor outage event begins; the end of this event is signaled by the C7PORE event. Refer to the C6POR description.
C7PORE (gg-mm)	Adjacent processor outage event ends. Refer to the C6PORE description.
CTRTERR (Point Code)	Reports that the MTP received an outgoing signaling message with a distinction point code that does not have any routing data.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
C7SPI (Point Code)	An adjacent signaling point isolation begins due to local failure. A link failed causing a complete failure of all signaling paths to the indicated destination from this office. This condition is usually accompanied by a C7LSF event. The end is indicated by the C7SPIE event. See the SPI_ measurements for more detail.
C7SPIE (Point Code)	Adjacent signaling point isolation ends. Some failed path to the indicated destination has restored due to a local link set recovery. This event indicates the destination is no longer isolated from this office.
C7SPIPO (Point Code)	An adjacent signaling point isolation begins due to a far-end processor outage. A link failed due to receiving PROs from the far end causing a complete failure of all signaling paths to the indicated destination from this office. The end of this condition is indicated by the C7SPIE event. See the C7SPI description.
C7SSAF (Subsystem)	Received a subsystem allowed message. Receiving an SSA message indicates the subsystem, either local or nonlocal, has become allowed. The SSA messages sent by the far end are in response to subsystem status test messages, and the SSP messages sent by the far end are in response to signaling messages destined for a prohibited subsystem. This event and the following C7SSPF event occur only if the following conditions are met: 1. The indicated subsystem is in the same region 2. It is simplex or duplex with the mate subsystem prohibited.
C7SSPF (Subsystem)	Received a subsystem prohibited message. Receiving an SSP message indicates the subsystem, either local or nonlocal, has become prohibited causing it to be blocked. However, an SSP concerning a subsystem at an inaccessible point code is ignored and does not cause this event, any SSP broadcast, or any routing update. Refer to the C7SSAF description for more detail.

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
CPALCIF (PBX Only)	Automatic link check (ALC) failure on the specified link. When a link is declared failed, the CPFLD or CPFLDNS event, the ALC is initiated. If the ALC is not successful within 15 seconds from the link failure, this event occurs.
CPARSFLD (PBX Link)	Automatic return to service from a declared failure.
CPDIS (PBX Link)	A duplex D-channel link has transitioned from the temporary out-of-service (OOS) state to the in-service (IS) state.
CPDOOS (PBX Link)	A duplex D-channel link has transitioned to the temporary OOS state.
CPDSERVF (PBX Link)	A SERV message exchange has failed on the specified D-channel link. The SERV message is sent several times and, if no acknowledgment is received (T321 timer expires), this event occurs. This indicated either a Layer 3 protocol problem, a provisioning problem, or a hardware failure other than facility failure. This event occurs when a link attempts to transition to the in-service (IS) state. Note that since the SERV message exchange is not done for standby links, a standby link could have latent Layer 3 problems.
CPDSTBY (PBX Link)	A duplex D-channel link has transitioned to the standby (STBY) state. If the link was in declared failure, this event indicates it has recovered.
CPDUMOOS (PBX Link)	The mate D-channel link fails while the indicated link is in the manual out-of-service (MOOS) state. No switch over occurs until manual action removes the MOOS state. If the link remains in the MOOS state, the system attempts to recover the mate link normally. This event is a warning of possible service outage.
CPFLD (PBX Link)	Declared link failure (this only applies to PBX links with diagnostic). The link state is changed to OOS, and the central processor is informed. For a D-channel link failure, this event indicates a signaling path failure; therefore, any associated B-channels are removed from service. There are various reasons for the failure, including the following:

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
CPFLD (PBX Link) (Contd)	Layer 1 protocol down (probably failure of DS0 or DS1, no explicit indication of L1 failure) Layer 2 protocol down (protocol exceptions and inability to establish link within 90 sec.) DDS code received Disconnect message received from far end Level 2 error threshold exceeded (usually facility problems).
CPFLDNS (PBX Link)	Non-signaling declared link failure of a mated link. The signaling path is still available on the backup link. The link state is changed to OOS. For the reasons for this event, see the CPFLD description.
CPMOOSE (PBX Link)	Manual out of service ends.
CTREDAL (PBX Node)	Red alarm declared (near-end DS1 facility failure). This is the second most severe trouble condition for a PBX node (see the CT1FAFL description). This event obstructs sensing of the yellow alarm condition. Note that this means there may be no explicit clearing of any yellow alarm in progress (normally indicated by the CTYELALC event).
CTREDALC (PBX Node)	Red alarm cleared. Any yellow alarm in progress is also cleared.
CT1FAFL (PBX Node)	T1 facility access (T1FA) hardware/firmware failure begins. The most severe type of trouble reported by the T1FA control node. This event means a T1FA unit has failed and any associated links are affected. Expect subsequent CPFLD critical event messages as those links are removed from service. This event obstructs sensing of the red and yellow alarm conditions (refer to the CTREDAL description). Note that this means there may be no explicit clearing of any red or yellow alarm in progress (normally indicated by the CTREDALC or CTYELALC event, respectively).

Table 5-D. Common Channel Signaling (CCS) Network Critical Event (CNCE) Descriptions (Contd)

Name (Data)	Description
CT1FARCVRY (PBX Node)	T1FA hardware/firmware failure ends.
CTYELAL (PBX Node)	Yellow alarm declared.
CTYELALC (PBX Node)	Yellow alarm declared.

Description of Reports

Introduction

A *measurement report* is a presentation of measurement data in either a fixed or a flexible format. Thus, there are basically two ways to "view" the measurement data. A report holds a specific view of the common measurement data and some reports make this view user definable via the measurement output control table (MOCT). Automatic reports are output as **REPT SMR** messages; while demand reports are output as **OP SMR** messages. Report forms are available in the following two formats:

- Fixed format reports — Certain measurement data is provided in a fixed layout. This data is output automatically and on demand.
- Flexible format reports — Allows users to have any specified set of measurement data output in one of four ways. These can be scheduled or demanded.

The following paragraphs provide a general overview of the various report types followed by a more detailed look at the report formats. Figures 5-1 through 5-7 illustrate the various scheduled reports.

Report Data

The data in a report is derived from the measurements found in the history files or the LPM. Data in the report is used to evaluate the performance of the CNI-equipped office and the network. Reports provide a measure of equipment performance and signaling performance. The reports also provide the detail needed to identify problems and troubleshoot faults. Different reports contain different measurements. The measurement data on any particular report type is defined by the specific column and row headings shown.

All report types contain a common header section. At the top of each report is a header that provides identifying information for the:

- Reporting office (such as software generic and CLLI* code)
- Particular report being output (such as the report name, time, report coverage, and whether or not it is being automatically generated).

Since some of the measurements in the history files are on a per-link or per-node basis, it is sometimes necessary to accumulate the measurements to derive a useful value for outputting to users. This process takes place when generating

* Registered trademark of Bell Communications Research, Inc.

the report. How the data is accumulated determines what information the final value provides. As an example, ring node out-of-service counts could be cumulated on the basis of link protocol (CCIS 6 or SS7) or on the basis of the type of node they serve—IMS user or ring peripheral controller. The same measurement data is used in both cases but is aggregated differently for different uses. Furthermore, some of the counts are on a per-office basis. The per-office counts may measure the same occurrences that similar, per-link or per-node, counts measure. Therefore, each piece of data is known by a different name. The scope of a particular piece of measurement data is referred to as "granularity." The granularity of the count determines the report in which the data is useful.

To provide information in a more usable form, some data values shown in reports are derived from measurements by algorithms; for example, a value may represent the sum of several measurements. In the figures at the end of this part, the basic measurement used to derive the value is shown. Where the value is not obtained from the history files, no name is given. Where possible, a figure shows the measurement name(s) used for each value in the report. The names shown are not strict definitions of each value nor do the names appear in the actual report. The names are intended to help the reader understand the source of the data and allow the reader to cross-reference to the table of measurement descriptions in the previous part.

Measurements take three forms:

1. Peg Counts - Indicated by a PC in the report
2. Time Durations - In hours, minutes, or seconds
3. Thresholds - Indicated by a TE in the report.

Most reports contain more than one of these three forms (for example, a peg count and its corresponding duration on one report line). When this is the case, the figures in this section, which illustrate report layouts, show the measurement name just once with an "_" in place of the suffix.

In unusual circumstances, the data shown in a report may be incomplete. This is possible if a node is out of service or a fault occurs during measurement collection (refer to a description of the measurement process phases in the previous part). Some reports flag invalid data, while certain reports indicate when their data is questionable. In reports containing specific link data (for example, the SNPR2 and 30MPR reports), an "*" appears in the link type field if there is no data available for the link.

Reports and Measurement Data Output

The users of the measurement data are on-site and at various support system centers. They are involved in the daily maintenance and operations of the CNI-equipped office. The support system users provide administration, maintenance, and operational support. All measurement data gathered is available to any of these users via the output control features of the MOCT. Note that when IMS measurement collection is inhibited, some measurements are not available. To determine whether or not IMS measurements are inhibited, enter **INH:IMSMEAS STATUS!**.

In addition to the scheduled printing of fixed format reports, they can be demanded at any time with the **OP:SMR** input message. The **OP:SMR** message causes the system to search the MOCT schedule table for the report specified. When the entry is found, the report is generated and printed using the current data found in the appropriate history file. Most scheduled and demand reports appear on the maintenance printer but not the maintenance CRT.

The MOCT provides for a delay of up to 5 minutes in printing scheduled reports. Thus, the report may not be output precisely at the scheduled time. Note that this tends to prevent pages of different reports scheduled to print at the same time from being intermingled. Furthermore, some reports, especially those to support systems, may be specified as *polled* reports. This means the report is not output, but is generated and stored for later retrieval.

NOTE:
The system is usually busiest at 15-minute intervals updating history files and printing scheduled reports. Therefore, the user should normally not demand a report at these times; but wait 5 to 10 minutes after this period to request these reports.

In addition to reporting measurements, measurement data can be demanded on an individual measurement basis at any time. Individual measurement messages provide more current real-time data than reports. Therefore, they are most useful to office personnel when troubleshooting. Specific measurement data can be requested by office personnel using the **DUMP:SMEAS** message. This message can output specific measurements for specified links, nodes, etc. It also has the option of printing data on all links, nodes, etc. The data is retrieved from the history files described earlier and output according to measurement type. The data is sent to the indicated destination in the form of an output message. On-site users may use the message to obtain more detailed measurements of conditions identified by a scheduled report. This message is not available to support system users. For information on requesting measurement data, refer to AT&T IM-4A001 — ***4ESS*** *Switch/APS Input Message Manual* or AT&T OM-4A001-01 — ***4ESS*** *Switch/APS Output Message Manual.*

Support system users, on the other hand, receive measurement data from the CNI-equipped office via BX.25 data links. These support systems use the BX.25 data links for reception of reports and messages. Reports and PDS messages are sent to the support system via different BX.25 data links.

Reports designated as "polled" in the MOCT are saved in specific files in a standard system directory. Support system users and on-site users may request data from these files using the **DUMP:SFILE** message. This command searches the directory for the specified file and outputs the file to the requesting user.

Report Formats

The CNI application provides both ***fixed format*** and ***flexible format*** reports are administered by the MOCT. The report names found in the MOCT are indicative of not only the format, but also the frequency of output, the source history files, and the scheduled/demand aspect of the indicated report. The report names are specified by a centralized administrative organization. Refer to the MOCT or office records for this information.

Fixed Format

A fixed format report contains a fixed set of measurements; the contents of the report cannot be changed. The "view" in the MOCT associated with a fixed format report should not be changed. Fixed format reports cannot be tailored to user requirements. The data is presented with labels arranged in a fixed layout.

The format names are generic forms of the actual names used to specify a particular report—input message. All reports, on-site and support system reports or fixed and flexible format reports, basically fall into one of the following three categories.

Total Office	Total office reports provide a general view of the office. The data in the reports is a summary of office performance. There are two total office fixed format reports: 1. Signaling Network Performance Report, Part 1 (SNPR1) 2. Machine Performance Report (MPR). The SNPR1 and the MPR are scheduled to be output daily and hourly. Therefore, they should be output on-site every hour.
Detailed Performance	The detailed performance reports provide a closer look at the individual links and nodes. There are separate measurements for each link in the office. Thus, the reports provide information helpful in isolating problems to a particular link or node. They are necessary for compiling

monthly performance reports. There are two detailed performance reports:

1. Signaling Network Performance Report, Part 2 (SNPR2)
2. Signaling Equipment Performance Reports (SEPR).

The SNPR2 and the SEPR are quite lengthy. Therefore, they are scheduled to be output only once each day and only on-site.

Exception

Exception reports are used to single out those measurements that are significant when they exceed some predetermined value. Any measurement in an exception report that does not exceed this predetermined value is not output in the report.

Furthermore, if there are no measurements that exceed their respective thresholds, the report itself may not be output. The report indicates specific pieces of equipment that have experienced higher than normal errors or excessive loading. There are two fixed format exception reports:

1. Thirty-Minute Marginal Performance Report (30MRP)
2. Ring Peripheral Controller Overflow Report (RINGEX).

Both reports are output on-site indicating problems with either signaling links or RPCs, respectively.

Flexible Format

Flexible format reports are user-defined. The CNI allows users to create customized reports containing data pertaining to their needs via the MOCT. These reports require a view in the MOCT to specify what measurements should be printed. The view in the MOCT is used to extract measurements from the measurement data base, LPM and disk history files.

Often, users in support centers need reports for a specific purpose. If the desired information is not available in a fixed format report or a fixed format report is not scheduled to be sent to the user, a new report can be created to fit that need. Using the MOCT, the user specifies the name, content, frequency, and format of the report. In addition, the user specifies if the report is to be output automatically or only on demand. The format is specified by using the appropriate flexible format report "generator." The creation of such reports is fully described later.

Flexible format reports can be either regular reports or exception reports. The regular format shows a value for all measurements specified in the view (for all links, nodes, etc., equipped) regardless of the value. The exception format shows a value for all measurements specified if any one of those measurements has exceeded its threshold. The output for such reports consists of a report header and up to six additional parts. The report header information and additional report parts are as follows:

a. Report header information
   - Report name
   - Day of year (1-366)
   - Number of 5-minute intervals at measurement start time.

b. Addition report parts per:
   - Office measurements
   - Link measurements
   - Node measurements
   - Channel measurements
   - Cluster measurements
   - Link set measurements.

Each report part appears as follows:

---

aaa = Number of measurements in this part

List of measurement names

bbb = Identification of link, node, channel, cluster, or link set

Corresponding values

ccc = Identification of next link, node, channel, cluster or link set

Corresponding values

NOTE:
If a report is scheduled near midnight and is output the following day, the header may show the past day; the report reflects when the data was created rather than when the report is output.

Normally, flexible format reports are sent to users at support centers. As shown, the report generated is little more than a list of measurement values to be sent to the support system over dedicated data links. The user at the support center then formats the data further.

Signaling Network Performance Report, Part 1

General

The Signaling Network Performance Report, Part 1 (SNPR1) is a total office report that is output automatically for each hour (the data coverage should be 12/12) and once for the entire day (data coverage 288/288). Make particular note of the time of the report. The purpose of the report is to provide an overall view of signaling performance for the office.

The report does not provide detailed measurements for each link. In fact, the data on this report cannot be directly used to determine the condition of any specific piece of hardware. Rather, it shows cumulative counts for the entire office. This report can be used to determine general performance of the office in the areas of signaling-load handled, signaling-link failures experienced, signal-unit errors detected, and the number of message-transfer failures that occurred.

This report should be checked daily for counts indicating poor link performance. The hourly reports from any period should be compared for trends and abnormalities. Keep in mind that a high count on one report is not necessarily an indication of problems. Also, the same count(s) occurring at the same time each day may point to externally induced problems.

If problems are indicated, the user should then refer to the Signaling Network Performance Report, Part 2 (SNPR2) or the Thirty-Minute Marginal Performance Report (30MPR) for detailed measurements of specific links. The following are counts of particular concern:

- Emergency Restarts (EMR)
- Signal Unit Errors (SUER_TE)
- Retransmission Requests (SURX_TE)
- Repeated and Skipped ACUs (AURSTE).

The basic layout of the SNPR1 report is shown in Figure 5-1. There are three sections to this report:

1. Header information
2. CCS7 link data
3. PBX link data.

Each link data section contains signaling load measurements and signaling performance measurements.

```
xx REPT SMR SNPR1 STARTED
   SIGNALING NETWORK PERFORMANCE REPORT - PART 1

   REPORTING OFFICE: local CLLI code REPORT INTERVAL: hourly or daily
   CURRENT GENERIC: gen_id          AUTOMATIC REPORT
   DATE: mm/dd/yy,  TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

   SIGNALING LOAD ---          RECEIVED     TRANSMITTED
    CCIS6 SIGNAL UNITS:           SUR             SUX
    CCIS6 ROUTED MESSAGES:      L6MGR           L6MGX
    CCIS6 DIRECT SIG MSGS:      L6MGSR          L6MGSX

   SIGNALING PERFORMANCE ---                                  PEG        TIME
                                                             COUNT      (SEC)
                                                            ------     ------
    CCIS6 PERFORMANCE ---
       EMERGENCY RESTART                                     EMRSP      EMRSPT
       TRANSMIT BUFFER OVERLOAD                              L6BOLX     L6BOLXT
       DECLARED LINK FAILURES                                L6FLD      L6FLDT
       AUTOMATIC SIG LINK CHANGEOVERS                        L6ACO_
       RECEIVE BUFFER OVERFLOW                               L6BOFR
       RECEIVE BUFFER OVERLOAD                               L6BOLR     L6BOLRT
       EXCEPTION REPORTS (THRESHOLDS EXCEEDED) ---
          SIGNAL UNIT ERRORS                                 SUER_TE
          RETRANSMISSION REQUESTS                            SURX_TE
          REPEATED AND SKIPPED ACU'S                         AURSTE
          AUTOMATIC CHANGEOVERS                              L6ACO_TE
       MESSAGE TRANSFER FAILURES ---
          POTS MSGS BLOCKED                                  L6MRPBC
          UNEQUIPPED POTS LABEL (NO TRANSLATION)             L6MRPNT
          DIRECT SIG MSGS REFUSED (BLOCKED)                  MRSBCO6+L6MRSBC
          DIRECT SIG MSGS REFUSED (NO TRANSLATION)           MRSNTO6
          TRANMIT BUFFER OVERFLOW                            L6BOFX
          INITIAL ADDRESS MSGS DROPPED                       MRUNVL
          LOOPED DIRECT SIG MSGS                             MGSLOOP
          DS & 511 MSGS DROPPED (RPC/DLN CONGESTION)         DRP6MSG1+2+3


Page 1 of 5
```

Figure 5-1. Layout of the Scheduled SNPR1 Report (Sheet 1 of 4)

```
xx REPT SMR SNPR1 IN PROG

   SIGNALING LOAD ---              RECEIVED        TRANSMITTED
    SS7 MSU BYTES:                  BYMSUR            BYMSUX
    SS7 ROUTED MSGS:                MGMSUR            MGMSUX
    ECIS MESSAGES:                 L6MGRV_           L6MGXV_
    TOTAL GTR MSGS REC'D:          SC7RGTR

   SIGNALING PERFORMANCE ---                                  PEG          TIME
                                                             COUNT        (SEC.)
    SS7 PERFORMANCE ---                                      ------       ------
       SIG LINK CONGESTION ONSET (LEVEL 1)                 L7LCON1X     L7LCON1XT
       DECLARED LINK FAILURES                                L7FLD        L7FLDT
       AUTOMATIC CHANGEOVERS                                 L7ACO
       RECEIVE BUFFER OVERFLOW                               L7BOFR
       RECEIVE BUFFER OVERLOAD                               L7BOLR       L7BOLRT
       TRANSMIT BUFFER DISCARD LEVEL 1                    L7LCDIS1X
       ROUTING AUDIT FAILURES
       EXCEPTION REPORTS (THRESHOLDS EXCEEDED) ---
          ERRORED SECONDS                                  ERSECTE
          DETECTED ERRORS                                  CRCERTE
          BYTES RETRANSMITTED                               BYRXTE
          AUTOMATIC CHANGEOVERS                            L7ACOTE
       MESSAGE TRANSFER FAILURES ---
          ECIS MSGS REFUSED - BLOCKED                      L7MRPBC
          ECIS MSGS REFUSED - NO TRANSLATION               L7MRPNT
          DCIS MSGS REFUSED - BLOCKED                      MRSBCO7
          DCIS MSGS REFUSED - NO TRANSLATION               MRSNTO7
          ECIS6 MSGS DROPPED - RPC/DLN CONGESTION          DRPEMSG1+2+3
          LOOPING CCS7 MSGS                                MSG7LOOP
          GIT REFUSED - BLOCKED                            GTTUNBC
          GIT REFUSED - NO TRANSLATION                     GTTUNNT
          SIG LINK MESSAGES DISCARDED                       MSUDISC0+1+2
          MSGS DROPPED - RPC/DLN CONGESTION                DRP7MSG1+2+3
          SCCP MSGS - UNKNOWN ADDRESS       (LN7)          SC7RERUA
          SCCP MSGS - UNKNOWN ADDRESS TYPE (LN7)           SC7RERUATY
          SCCP MSGS - UNEQUIPPED SUBSYSTEM (LN7)           SC7RERUNE
          SCCP MSGS - PROHIBITED SUBSYSTEM (LN7)
          SCCP MSGS - UNKNOWN ADDRESS       (OFC)           SCRERUA
          SCCP MSGS - UNKNOWN ADDRESS TYPE (OFC)           SCRERUATY
          SCCP MSGS - UNEQUIPPED SUBSYSTEM (OFC)           SCRERUNE
          SCCP MSGS - PROHIBITED SUBSYSTEM (OFC)           SCRERPRO

Page 2 of 5
```

Figure 5-1. Layout of the Scheduled SNPR1 Report (Sheet 2 of 4)

```
xx REPT SMR SNPR1 IN PROG

   SIGNALING LOAD ---              RECEIVED        TRANSMITTED
    CCITT7 MSU BYTES:              BYMSUR            BYMSUX
    CCITT7 ROUTED MSGS:            MGMSUR            MGMSUX
    TOTAL GTR MSGS REC'D:          SC7RGTR

   SIGNALING PERFORMANCE ---                          PEG          TIME
                                                      COUNT        (SEC.)
    CCITT7 PERFORMANCE ---                            ------       ------
       SIG LINK CONGESTION ONSET (LEVEL 1)
       DECLARED LINK FAILURES
       AUTOMATIC CHANGEOVERS
       RECEIVE BUFFER OVERFLOW
       RECEIVE BUFFER OVERLOAD
       TRANSMIT BUFFER DISCARD
       ROUTING AUDIT FAILURES
       EXCEPTION REPORTS (THRESHOLDS EXCEEDED) ---
          ERRORED SECONDS
          DETECTED ERRORS
          BYTES RETRANSMITTED
          AUTOMATIC CHANGEOVERS
       MESSAGE TRANSFER FAILURES ---
          LOOPING CCITT7 MSGS
          SIG LINK MESSAGES DISCARDED
          MSGS DROPPED - DLN/RPC CONGESTION

PAGE 3 OF 5

xx REPT SMR SNPR1 IN PROG

   SIGNALING PERFORMANCE ---                          PEG          TIME
                                                      COUNT        (SEC.)
    SS7 & CCITT7 PERFORMANCE ---                      ------       ------
       SIGNALING POINT ISOLATION                      SPISP        SPISPT
       LINK SET FAILURE                               CLFSP        CLFSPT
       MESSAGE TRANSFER FAILURES ---
         MSUS DISCARDED - ROUTING DATA ERROR

PAGE 4 OF 5
```

Figure 5-1. Layout of the Scheduled SNPR1 Report (Sheet 3 of 4)

```
xx REPT SMR SNPR1 IN PROG

   SIGNALING LOAD ---              RECEIVED        TRANSMITTED
     PBX BYTES:                      BYRL_            BYXL_
     PBX MESSAGES:                MGMSURL_         MGMSUXL_
     PBX Q.931 MSGS:              Q931MGRL_        Q931MGXL_

   SIGNALING PERFORMANCE ---                                    PEG          TIME
                                                               COUNT        (SEC.)
     PBX PERFORMANCE ---                                       ------       ------
        SIGNALING PATH FAILURE
        DECLARED LINK FAILURE                                  LPFLDL_      LPFLDTL_
        TEMPORARY LINK FAILURE                                 LPTMPFLDL_   LPTMPFLDTL_
        RECEIVE BUFFER OVERLOAD                                LPBOLRL_     LPBOLRTL_
        TRANSMIT BUFFER FULL EVENTS                            XBFFULLL_    XBFFULLTL_
        NUMBER OF LINK RESTARTS                                LKESTAB_
        SIGNALING SWITCHOVERS SUCCESSFUL
        SIGNALING SWITCHOVERS FAILURES
        MESSAGE TRANSFER FAILURES ---
           MSGS RECEIVED FOR UNAVAILABLE LINK                  MGUNAL_
           MSGS RECEIVED WITH INVALID ADDRESS


PAGE 5 OF 5

xx REPT SMR SNPR1 COMPL
```

Figure 5-1. Layout of the Scheduled SNPR1 Report (Sheet 4 of 4)

Header Information

The SNPR1 header information includes the following:

- Office identification
- Report type
- Time
- Data coverage.

CCS7 Signaling Load and Signaling Performance Measurements

The CCS7 signaling load and signaling performance measurements identify the number of messages received and transmitted for various CCS7 message types and various failure conditions for CCS7 links (that is, signaling point isolations, buffer congestion, declared failures, changeovers). They include counts and exception threshold measurements for certain error conditions that indicate poor link performance. Also shown are message counts discarded due to blockage or translation failure, counts of looping messages, the number of routing audit failures, and global title translation counts, total and failures. A few points to consider when interpreting the measurements are the following:

- Byte and signal unit load counts are pegged in the link interface. They do not include SYNC, ACU, or PRO messages. They do include signal units received in error.
- Message counts, based on a determination of message type, are pegged in the node. They include messages that may subsequently be blocked at the outgoing node.
- The ECIS signaling load measurements count all CCIS 6 messages that are sent or received on CCS7 virtual links. Furthermore, the count of SS7 routed messages includes the ECIS type.
- Signaling point isolation is similar to the EMR condition; they both indicate failure of all signaling paths to an adjacent signaling point. A signaling path failure is indicated by local link failure, far-end processor outage, or receipt of TFx messages indicating some link in a path to the destination has failed.
- Discarding messages due to link congestion is related to the transmit buffer occupancy and the priority of the message to be transmitted. If the priority level is less than the congestion level, the message is discarded. Depending on several factors, a return message may be sent indicating the reason for discard.
- Level 1 congestion is the lowest congestion state for the link. The duration measurement for this state indicates the length of time the buffer occupancy is above normal. The peg count indicates how often occupancy is above normal, but not the severity of the congestion.
- Errored seconds is the number of 1-second intervals during which signal units are received with errors, not a count of signal unit errors. Detected errors is the number of signal units that failed the parity check. An excess of these could cause the link to be declared failed.
- Looping messages are usually caused by congestion or blockage at an outgoing link combined with messages returned from some far-end office. When looping counts are high, look for other counts indicating congestion, blockage, no translation, and possibly discarded messages.

PBX Signaling Load and Signaling Performance Measurements

This feature is not applicable in the LEC environment.

Signaling Network Performance Report, Part 2

General

The Signaling Network Performance Report, Part 2 (SNPR2) is a detailed report of signaling link performance. The SNPR2 is output automatically once each day; the data coverage should be 288/288. The purpose of the report is to

provide enough detail on each signaling link in the office to allow troubleshooting of faulty links and the compilation of statistical data on each link. Due to the amount of data provided in this report, many pages of output can be expected. Each page of the report is output as a single message; that is, the printer prints each page of the report with no other output interspersed, but the entire report may not be contiguous.

The SNPR2 report and the thirty-minute marginal performance report (30MRP) are the main sources for analyzing link failures and marginal performance. The SNPR2 provides an overview of signaling capabilities for the office giving a detailed description of SS7 link performance. This report should be checked whenever link problems are indicated. Of particular concern are the counts in the SS7 link performance sections. Most of this data is an expansion of similar total office data provided on the SNPR1 report. The SNPR2 reports should be compared each day to determine trends in signaling link problems and provide long-term analysis of intermittent problems.

In the link performance sections of the SNPR2 report, data is provided for each equipped link, if all measurements on the particular report line in question are nonzero. If there is no data available for a link, the type field is set to "*." The measurements for each link are listed on separate lines with link identification (far-end CLLI code, layer number, link type, group number, and member number) to the left of each. The basic layout of the SNPR2 report is shown in Figure 5-2. The following are four sections of the report:

- Header information
- Loss of signaling capability
- SS7 signaling link performance
- PBX signaling link performance.

Header Information

The header information chapter provides office identification, report type, time, and data coverage. In addition, this chapter shows the number of equipped links in the office and the combined active time for all links.

Loss of Signaling Capability

The loss of signaling capability chapter indicates how often and for how long particular categories of links were unable to provide signaling. The degree that signaling can be impaired is identified as follows:

- The emergency restart indicates loss of signaling to an adjacent signaling point. This data is cumulative for all SS7 links.
- A signaling point isolation indicates loss of signaling to an adjacent office. The count that pegs in this case is the SPI count for the link type of the last link to fail causing the isolation.

- A link set failure indicates alternate routing is necessary to the far-end office and all affected destinations. If the link set failure results in failure of the combined link set, then the far-end becomes isolated.

CCS7 Signaling Link Performance

The SS7 signaling link performance chapter provides the most important measurements for analyzing CCS7 link performance. There are four separate groups of measurements in this chapter:

- Failed time, errored seconds, detected signal unit errors, and bytes retransmitted
- Automatic changeovers, declared failures, and link set failures
- Signaling point isolations, discarded message signal units, and transmit buffer congestion
- Emergency restarts.

Refer to the SS7 performance description of the SNPR1 report for important points to consider when analyzing the CCS7 signaling link performance measurements.

PBX Signaling Link Performance

This process is not applicable in the LEC environment.

```
xx REPT SMR SNPR2 STARTED
   SIGNALING NETWORK PERFORMANCE REPORT - PART II

   REPORTING OFFICE: local CLLI code            REPORT INTERVAL:  daily
   CURRENT GENERIC: gen_id                   AUTOMATIC REPORT
   DATE: mm/dd/yy,  TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss   THRU  mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

                                      CCIS6      SS7       CCITT7   PBX
   TOTAL NO. OF EQUIPPED LINKS:        nn        nn         nn      nn
   TOTAL LINK OOS TIME (SECS):      (Note 1)  (Note 2)   (Note 2)
   DURATION RCV'D PROCESSOR OUTAGE: L6PORT    L7PORT     L7PORT
   TOTAL NO. OF POOLS/LINK SETS:       nn        nn         nn      nn

   LOSS OF SIGNALING CAPABILITY ---
                 ------EMR------
                   PC       SEC
   A/E LINKS:     EMRA     EMRAT
   B LINKS:       EMRB     EMRBT
   C LINKS:       EMRC     EMRCT

   LOSS OF SIGNALING CAPABILITY ---
                 --SS7 SPI--       --SS7 LSF--
                   PC       SEC      PC       SEC
   A/E LINKS:     SPIA     SPIAT    CLFA     CLFAT
   B LINKS:       SPIB     SPIBT    CLFB     CLFBT
   C LINKS:       SPIC     SPICT    CLFC     CLFCT

   LOSS OF SIGNALING CAPABILITY ---
               --CCITT7 SPI--       --CCITT7 LSF--
                PC        SEC        PC       SEC
   W LINKS:     SPI       SPIT       CLF      CLFT
```

Notes:

1. **Sum of L6AFLT and L6MFLT.**
2. **Sum of L7AFLT and L7MFLT.**

Figure 5-2. Layout of the Scheduled Daily SNPR2 Report (Sheet 1 of 4)

```
xx REPT SMR SNPR2 IN PROG

CCIS6 SIGNALING LINK PERFORMANCE ---
                                                  ---ACO---    -SU-ERR-    -SU-RXMT-   -R&S-ACU-
   FAR END CLLI-LAYER    T  GR-MEM VFL  PC     TE     PC     TE     PC     TE     PC     TE
   --------------------  -  ------ --- ---------    ---------    ---------    ---------

   nnnn  nn  nn  nnn-nn  a  nn-nn   A    L6ACOB_      SUERB_       SURXB_       AURS_
   nnnn  nn  nn  nnn-nn  a  nn-nn   B    L6ACOA_      SUERA_       SURXA_       AURS_

CCIS6 SIGNALING LINK PERFORMANCE ---
                                       OOS-TIME    -DCL-FLR-   --EMR--     -EMR-PO-
   FAR END CLLI-LAYER    T  GR-MEM     HH MM SS    PC    SEC   PC    SEC    PC  SEC
   --------------------  -  ------    ---------   ---------   ---------    ---------

   nnnn  nn  nn  nnn-nn  a  nn-nn     (Note 1)      L6FLD_      EMR_         EMRPO_
   nnnn  nn  nn  nnn-nn  a  nn-nn     (Note 1)      L6FLD_      EMR_         EMRPO_

CCIS6 SIGNALING LINK PERFORMANCE ---
                                       ---XMIT BUFFER---
                                        OVFL      --OVLD--     PRO XMTD     PRO-RCVD
   FAR END CLLI-LAYER    T  GR-MEM       PC       PC SEC       PC SEC       PC SEC
   --------------------  -  ------    ------      -------      --------     --------

   nnnn  nn  nn  nnn-nn  a  nn-nn     L6BOFX       L6BOLX_      L6POX_       L6POR_
   nnnn  nn  nn  nnn-nn  a  nn-nn     L6BOFX       L6BOLX_      L6POX_       L6POR_

SS7 SIGNALING LINK PERFORMANCE ---
                                                  ---ACO---   --ERSEC--   --CRCER--   -BYT-RXMT
   FAR END CLLI-LAYER    T  GR-MEM     PC     TE    PC     TE    PC     TE    PC     TE
   --------------------  -  ------ ---------    ---------    ---------    ---------

   nnnn  nn  nn  nnn-nn  a  nn-nn     L7ACO_       ERSEC_       CRCER_       BYRX_
   nnnn  nn  nn  nnn-nn  a  nn-nn     L7ACO_       ERSEC_       CRCER_       BYRX_

CCIS7 SIGNALING LINK PERFORMANCE ---
                                       OOS-TIME     ----LSF---      --DCL-FLR-
   FAR END CLLI-LAYER    T  GR-MEM     HH MM SS    PC    SEC       PC     SEC
   --------------------  -  ------    ---------   ---------      ----------

   nnnn  nn  nn  nnn-nn  a  nn-nn     (Note 2)    CLF   CLFT     L7FLD L7FLDT
   nnnn  nn  nn  nnn-nn  a  nn-nn     (Note 2)    CLF   CLFT     L7FLD L7FLDT
```

Notes:

1. **Sum of L6AFLT and L6MFLT.**
2. **Sum of L7AFLT and L7MFLT.**

Figure 5-2. Layout of the Scheduled Daily SNPR2 Report (Sheet 2 of 4)

```
xx REPT SMR SNPR2 IN PROG
CCS7 SIGNALING LINK PERFORMANCE ---
                                ---XMIT BUFFER---
                                MSURMV  CONG-LEV1  PRO-XMTD  PRO-RCVD
  FAR END CLLI-LAYER T GR-MEM       PC   PC  SEC   PC  SEC   PC  SEC
  ------------------- - ------  ------- --------- --------  --------
  nnnn nn nn nnn-nn   a nn-nn   (NOTE 1) L7LCON1X_  L7POX_    L7POR_
  nnnn nn nn nnn-nn   a nn-nn   (NOTE 1) L7LCON1X_  L7POX_    L7POR_
SS7 SIGNALING LINK PERFORMANCE ---
                                --EMR--   --EMR-PO--    --SPI--    --SPI-PO--
  FAR END CLLI LAYER T GR-MEM    PC SEC     PC  SEC       PC  SEC     PC  SEC
  ------------------- - ------  -------    ---------     --------    ----------
  nnnn nn nn nnn-nn   a nn-nn   L7EMR_     L7EMRPO_      SPI_        SPIP_
  nnnn nn nn nnn-nn   a nn-nn   L7EMR_     L7EMRPO_      SPI_        SPIP_
CCITT7 SIGNALING LINK PERFORMANCE ---
                                --ACO--   --ERSEC--   --CRCER--   -BYT-FORRX-
  FAR END CLLI-LAYER T GR-MEM    PC TE      PC   TE      PC   TE     PC      TE
  ------------------- - ------  -------   ---------   ---------   ------------
  nnnn nn nn nnn-nn   a nn-nn   L7ACO_     ERSEC_       CRCER_      FORRXBY
  nnnn nn nn nnn-nn   a nn-nn   L7ACO_     ERSEC_       CRCER_      FORRXBY
CCITT7 SIGNALING LINK PERFORMANCE ---
                                OOS-TIME   ----LSF---      --DCL-FLR-
  FAR END CLLI-LAYER T GR-MEM   HH MM SS     PC  SEC         PC  SEC
  ------------------- - ------  --------   ---------       ---------
  nnnn nn nn nnn-nn   a nn-nn    (NOTE 2)   CLF  CLFT     L7FLD L7FLDT
  nnnn nn nn nnn-nn   a nn-nn    (NOTE 2)   CLF  CLFT     L7FLD L7FLDT
CCITT7 SIGNALING LINK PERFORMANCE ---
                                ---XMIT BUFFER---
                                MSURMV  CONG-LEV1  PRO-XMTD  PRO-RCVD
  FAR END CLLI-LAYER T GR-MEM       PC   PC  SEC   PC  SEC   PC  SEC
  ------------------- - ------  ------- --------- --------  --------
  nnnn nn nn nnn-nn   a nn-nn   (NOTE 1) L7LCON1X_  L7POX_    L7POR_
  nnnn nn nn nnn-nn   a nn-nn   (NOTE 1) L7LCON1X_  L7POX_    L7POR_
CCITT7 SIGNALING LINK PERFORMANCE ---
                                    ----SPI----       ----SPI-PO----
  FAR END CLLI-LAYER T GR-MEM        PC     SEC         PC      SEC
  ------------------- - ------      -----------       --------------
  nnnn nn nn nnn-nn   a nn-nn           SPI_               SPIP_
  nnnn nn nn nnn-nn   a nn-nn           SPI_               SPIP_
```

Notes:

1. **Sum of MSUDISC0, MSUDISC1, and MSUDISC2.**
2. **Sum of L7AFLT and L7MFLT.**

Figure 5-2. Layout of the Scheduled Daily SNPR2 Report (Sheet 3 of 4)

```
xx REPT SMR SNPR2 IN PROG

PBX SIGNALING LINK PERFORMANCE* ---
                    OOS TIM      OOS-AUTO      OOS-MAN       SIG  FLR
TYPE  GR-MN-C-P     HR  MIN        (SEC)         (SEC)        PC  SEC
----  ---------     --------     --------      --------      --------
aaaa  nn-nn-n-n     LP_FLTL_     LPAFLTL_      LPMFLTL_      LPSPFAIL_
aaaa  nn-nn-n-n     LP_FLTL_     LPAFLTL_      LPMFLTL_      LPSPFAIL_

PBX SIGNALING LINK PERFORMANCE* ---
                    DCL FLR      TMP LK FLR      LINK        MSGS RCV
TYPE  GR-MN-C-P      PC SEC       PC    SEC     RESTARTS      UNAVL
----  ---------     --------     ----------   ------------   --------
aaaa  nn-nn-n-n     LPFLD_       LPTMPFL_      LKESTAB_      MGUNAL_
aaaa  nn-nn-n-n     LPFLD_       LPTMPFL_      LKESTAB_      MGUNAL_

PBX SIGNALING LINK PERFORMANCE* ---
                    MSGS   RCV  XMT BUF FULL  RCV BUF OVLD  SWITCHOVRS
TYPE  GR-MN-C-P     INVLD ADDR   NODE  SEC     NODE  SEC     SUC  FLD
----  ---------     --------     ------------  ------------  ----------
aaaa  nn-nn-n-n     MGRUAL_      XBFFULL_      LPBOLR_     LPSWITCH LPINSWITCH
aaaa  nn-nn-n-n     MGRUAL_      XBFFULL_      LPBOLR_     LPSWITCH LPINSWITCH

  * Not applicable in LEC environment
```

Figure 5-2. Layout of the Scheduled Daily SNPR2 Report (Sheet 4 of 4)

Signaling Equipment Performance Report

The Signaling Equipment Performance Report (SEPR) is a detailed report on node performance. The SEPR is output once each day; the data coverage should be 288/288. The purpose of the report is to provide a profile of each node's status for the reporting period.

The report should be examined to note any excessive counts. Of particular concern are the automatic out-of-service (OOS) count and duration (OOSAU_), and reconfigured OOS count and duration (OOSCFG_) columns. This is especially true with the RPC node chapter. Proper RPC operation is critical to the message switching function.

Any node out of service may be caused by node processor or ring interface problems. In the case of a link node, it may also be caused by poor link performance. When a link is declared failed, the node is automatically removed from service to perform diagnostics. However, keep in mind that a normal link is not necessarily declared failed when the node is removed due to other problems.

Likewise, in the case of an RPCN, it may be caused by D-channel node (DSCH) problems. The report may indicate problems with a specific node or the ring in general.

The SEPR report does not provide a detailed analysis of why a node failed. Out-of-service counts and durations are provided for each node according to the major cause of the change to the OOS or standby state.

Three conditions that are mutually exclusive in effect may cause this report to be generated: Automatic action due to a node or link fault, Manual action, and Ring reconfiguration affecting a normally operating node.

Also, a total count of the number of times the node restarted for any reason is provided. A few points to consider when interpreting this report are:

- The duration counts are cumulative for all occurrences (i.e., not associated with a single occurrence).
- The OOS counts indicate the *initial* reason for a node being removed. The node maintenance state may change without affecting the OOS measurements as long as the major state remains the same. For example, a node removed due to failing diagnostics causes the OOS automatic count to peg. Later changing the node state to MOOS does not cause the OOS manual count to peg.

The data is provided one node per line with group and member number identification to the left. A node that has not been in the OOS state at any time during the reporting period is not shown in the report. The basic layout of the SEPR report is shown in Figure 5-3. The following are the five sections to the report:

1. Header information
2. SS7 link node performance
3. Ring peripheral controller node (RPCN) performance.

```
xx REPT SMR SEPR STARTED
   SIGNALING EQUIPMENT PERFORMANCE REPORT

   REPORTING OFFICE: local CLLI code          REPORT INTERVAL: daily
   CURRENT GENERIC: gen_id                  AUTOMATIC REPORT
   DATE: mm/dd/yy, TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

   CCIS6 LN PERFORMANCE
     GRP   MEM       ERROR        OOS_AUTO          OOS_MAN          OOS_CNFG
     NUM   NUM       COUNT       COUNT    SEC      COUNT    SEC     COUNT    SEC
     ---   ---       -------     ---------------   ---------------   ---------------
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT

   SS7 LN PERFORMANCE
     GRP   MEM       ERROR        OOS_AUTO          OOS_MAN          OOS_CNFG
     NUM   NUM       COUNT       COUNT    SEC      COUNT    SEC     COUNT    SEC
     ---   ---       -------     ---------------   ---------------   ---------------
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT

   SADC LN PERFORMANCE*
     GRP   MEM       ERROR        OOS_AUTO          OOS_MAN          OOS_CNFG
     NUM   NUM       COUNT       COUNT    SEC      COUNT    SEC     COUNT    SEC
     ---   ---       -------     ---------------   ---------------   ---------------
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT

   DCHN LN PERFORMANCE*
     GRP   MEM       ERROR        OOS_AUTO          OOS_MAN          OOS_CNFG
     NUM   NUM       COUNT       COUNT    SEC      COUNT    SEC     COUNT    SEC
     ---   ---       -------     ---------------   ---------------   ---------------
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT

   RPC NODE PERFORMANCE
     GRP   MEM       ERROR        OOS_AUTO          OOS_MAN          OOS_CNFG
     NUM   NUM       COUNT       COUNT    SEC      COUNT    SEC     COUNT    SEC
     ---   ---       -------     ---------------   ---------------   ---------------
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT
     nn    nn        RSTTRMT     OOSAU    OOSAUT   OOSMN    OOSMNT   OOSCFG   OOSCFGT

xx REPT SMR SEPR COMPL

 * Not applicable in LEC environment
```

Figure 5-3. Layout of the Scheduled Daily SEPR Report

Machine Performance Report

General

The Machine Performance Report (MPR) is a total office report that is output automatically for each hour (the data coverage should be 12/12) and once for the entire day (data coverage 288/288). Make particular note of the time of the report. The purpose of the report is to provide an overall view of the message switching capability for the office.

The report does not provide detailed measurements for each link or node. The MPR shows cumulative counts for the entire office. This report can be used to determine the message switching status of the office in general (that is, the number of times it initialized and how long CCS messages were not processed) or the status of the ring in general (that is, node OOS counts, ring reconfigurations, and ring congestion levels).

This report should be checked daily for counts indicating ring node failures or degraded ring performance. The hourly reports from many periods should be compared for trends and abnormalities. Keep in mind that a high count on one report is not necessarily an indication of problems. Also, the same count(s) occurring at the same time each day may point to externally induced problems. If problems are indicated, the user should then refer to the Signaling Equipment Performance Report (SEPR) or Ring Exception (RINGEX) report for detailed measurements of specific nodes.

The basic layout of the MPR report is shown in Figure 5-4. The following are the seven sections to this report:

1. Header information
2. System initializations
3. No message signal unit processing
4. RPCN performance
5. Link node (LN) performance
6. Ring performance
7. Internal congestion.

Header Information

The MPR header information contains the following:

a. Office identification
b. Report type
c. Time
d. Data coverage.

System Initializations

The system initialization chapter shows how many times specific levels occurred and how long for each subsystem. The application starts the CNI initialization, and the CNI starts IMS. Since initialization of each subsystem is triggered by a higher level subsystem, the counts for a particular level are normally the same for all subsystems. A few points to consider when interpreting the measurements in this chapter are as follows:

- A UNIX RTR Operating System or application level 1 leads to either a 1A or 1B IMS level; there is no level 1 in the IMS initialization strategy. The message switch is stopped by the level 1B but not by the level 1A.
- Levels 0, 1, 1A, or 1B do not include a boot.
- The UNIX RTR Operating System 5x levels generally correspond to the application x levels.

The meaning of each initialization level is as follows:

0 — Audit Level:	No interruption of message switching. This is currently not implemented.
1 — Recovery level:	Process communication and data tables are reinitialized. No processes are recreated but some messages may be lost.
3 — Lowest boot level:	All processes are recreated and RPCs are pumped.
4 — Highest boot level:	All processes are recreated and all nodes are pumped.

No Message Signal Unit Processing

The No Message Signal Unit Performance chapter indicates how many times the CNI entered a state in which it could not process CCS messages. This should be at least the sum of the IMS levels 1B, 3, and 4; although the state could occur without an initialization.

Ring Peripheral Controller (RPC) Node Performance

The RPCN performance chapter provides out-of-service counts and durations, for RPCs in general, according to the major cause of the change to the OOS or standby state. There are three conditions, all mutually exclusive in effect, that may cause this report to be generated:

1. Automatic action due to a node or link fault
2. Manual action
3. Ring reconfiguration affecting a normally operating node.

Also, a cumulative count of the number of times any node restarted for any reason is provided. The data provided in this chapter and the LN Performance chapter is similar to the per-node data in the Signaling Equipment Performance Report (SEPR).

The following are a few points to consider when interpreting the measurements:

- The OOS counts indicate the initial reason for a node being removed. The node maintenance state may change without affecting the OOS measurements as long as the major state remains the same. For example, a node removed due to failing diagnostics causes the OOS automatic count to peg. Later changing the node state to MOOS does not cause the OOS manual count to peg.
- A node changing to the OOS state does not necessarily result in a corresponding ring reconfiguration, shown under Ring Performance. If the state of the ring interface hardware is quarantined usable, the node may be OOS yet still part of the active ring.

Link Node (LN) Performance

The link node performance chapter provides out-of-service counts and durations for link nodes in general according to the major cause of the change to the OOS or standby state. The data shown is the sum for SS7 and PBX link nodes.

Ring Performance

The ring performance chapter provides a profile of ring performance during the reporting period, including counts and durations of automatic ring isolations, manual ring isolations, and ring down time. The following are a few points to consider when interpreting the data:

- An isolated segment is considered automatically generated if the most recently isolated node is isolated by automatic action. It is considered manually generated if the most recently isolated node is isolated by manual action. The RNIMN count pegs for zero, one, or more nodes isolated.

- The single and multiple node isolation durations are mutually exclusive.
- Multiple node isolated segments are of particular concern not only due to their larger impact on message switching but also because they may contain normally operating nodes that are innocent victims of the reconfiguration. Quick restoration of these nodes is important.
- When growing nodes, begin by manually reconfiguring the ring with an isolated segment (zero nodes isolated) where the nodes are to be grown.
- The ring has two transient states, *configuring and restoring,* and three quiescent states, *normal, isolated,* and *down.* These are minor maintenance states. Only the down state is explicitly counted. The total ring normal time, including transient states, is the reporting period less single and multiple isolation times and less ring down time.

Internal Congestion

The internal congestion chapter indicates the general level of congestion in the ring. A RPC count pegs each time any RPC node enters a particular level of ring-receive buffer congestion. A link node count pegs each time any LN or PBX node enters a particular level of ring receive buffer congestion. The buffers become congested if IMS is delivering messages to the node faster than it is processing the messages already in the buffers. The congestion controls become progressively more severe as the occupancy level of the buffer increases; at RPC level 1, LNs are warned of imminent overflow at their home RPC. A few points to consider when interpreting the data are:

- Messages are discarded only in IUNs. However, the RPC congestion levels are more critical for two reasons:
  1. All IUNs are affected by them.
  2. Communication between the central processor and ring is affected.
- There are both IMS actions and CNI actions based on the congestion level. The CNI actions are intended to preclude any discarding of messages by IMS. For more information on the number of messages discarded, refer to the DRP_MSG_ measurements.
- The IMS maintenance-type messages are affected only at level 4 congestion.

```
xx REPT SMR MPR STARTED
   MACHINE PERFORMANCE REPORT

   REPORTING OFFICE: local clli code          REPORT INTERVAL: hourly or daily
   CURRENT GENERIC: gen_id                  AUTOMATIC REPORT
   DATE: mm/dd/yy   TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss THRU mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

   SYSTEM INITIALIZATIONS

            LEVEL-0          LEVEL-1         LEVEL-1A        LEVEL-1A
          COUNT   SEC      COUNT   SEC    COUNT    SEC    COUNT    SEC
          ------------   -------------- -------------- --------------
   CNI   CINIT0 CINIT0T  CINIT1 CINIT1T       N/A             N/A
   IMS   INIT0   INITOT       N/A        INIT1A INIT1AT  INIT1A INIT1AT

   SYSTEM INITIALIZATIONS

            LEVEL-2          LEVEL-3          LEVEL-4
          COUNT   SEC      COUNT   SEC      COUNT   SEC
          -------------   -------------   -------------
   CNI   CINIT2 CINIT2T   CINIT3 CINIT3T  CINIT4 CINIT4T
   IMS   N/A              INIT3  INIT3T   INIT4  INIT4T

   NO MESSAGE SIGNAL UNIT PROCESSING

      COUNT     SEC
     -------  -------
      NOCMG   NOCMGT

   RPC/DLN NODE PERFORMANCE - RPC COUNT: nn

    ERRORS        OOS-AUTO           OOS-MAN           OOS-CNFG
     COUNT     COUNT       SEC     COUNT       SEC    COUNT       SEC
    -------   ---------------     ---------------    ---------------
    RSTTRMT   OOSAU    OOSAUT     OOSMN    OOSMNT    OOSCFG   OOSCFGT

   LN NODE PERFORMANCE - LN COUNT: nn

    ERRORS        OOS-AUTO           OOS-MAN           OOS-CNFG
     COUNT     COUNT       SEC     COUNT       SEC    COUNT       SEC
    -------   ---------------     ---------------    ---------------
    RSTTRMT   OOSAU    OOSAUT     OOSMN    OOSMNT    OOSCFG   OOSCFGT
```

Figure 5-4. Layout of the Scheduled MPR Report (Sheet 1 of 2)

```
RING PERFORMANCE

  SNGL ISOLAT     MULT ISOLAT      RING DOWN   MAN NODE ISOLAT
  COUNT    SEC    COUNT    SEC     COUNT  SEC  COUNT        SEC
 -------------   -------------   ----------  ---------------
 SRNIAU SRNIAUT MRNIAU MRNIAUT  RDWN RDWNT  RNIMN     RNIMNT


INTERNAL CONGESTION

                                OVERFLOW    OVERFLOW    OVERFLOW
                                LEVEL_1     LEVEL_2     LEVEL_3
                                --------    --------    --------
 RPC RING RECEIVE BUFFER       RRBOVFLW1   RRBOVFLW2   RRBOVFLW3
  LN RING RECEIVE BUFFER         N/A       RRBOVFLW2   RRBOVFLW3

xx REPT SMR MPR COMPL
```

Figure 5-4. Layout of the Scheduled MPR Report (Sheet 2 of 2)

Fifteen-Minute Marginal Performance Report

General

The Fifteen-Minute Marginal Performance Report (15MPR) is a detailed exception report of signaling link performance. The 15MPR can be output automatically each 15 minutes and is output only if one of the measurements contained in the report exceeds some predefined threshold. The purpose of the report is to identify links that are showing marginal performance. The 15MPR provides a set of measurements that indicate various problems with the link, such as parity errors in received signal units, alignment problems, excessive changeovers, or excessive downtime.

This report should be checked whenever link problems are indicated. The fifteen-minute reports from many periods should be compared for trends and abnormalities. Look for failures associated with an individual link, a group of links, or a particular far-end office.

The basic layout of the 15MPR report is shown in Figure 5-5. For additional information on the 15MPR report, refer to the I/O manual.

```
xx RING REPT SMR  A15MPR15  STARTED
   MACHINE RESOURCE PERFORMANCE REPORT

   REPORTING OFFICE: local clli        REPORT INTERVAL: hourly or daily
   CURRENT GENERIC: gen_id                  AUTOMATIC REPORT
   DATE: mm/dd/yy,  TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

IDLE  KERN  KPROC  USER  PAGES   PAGES    APS     PROC  PROC
TIME  TIME  TIME   TIME  SWAPIN  SWAPOUT  DKRATE  CRTD  TERM
%040  %020  %025   %011  000000  000000   0009    0119  0120

CCS7   BYTES     MSUS      FLD  DLN    BASE/    BLOCKS    MESGS     ERR
NODES  IN/OUT    IN/OUT    CNT  NODES  TBSY     IN/OUT    IN/OUT    IN/OUT
00-01  00015514  00000775  000  00-05  088515   00000823  00001917  000015
       00016160  00000794              000288   00004115  00004432  000000
00-06  00000000  00000000  000  00-10  088542   00000000  00000000  000000
       00000000  00000000              000000   00000000  00000000  000000
00-08  00000000  00000000  000  32-05  088532   00002729  00003031  000000
       00000000  00000000              000128   00000937  00002195  000000
00-12  00000000  00000000  000  32-10  088541   00000000  00000000  000000
       00000000  00000000              000000   00000000  00000000  000000
06-02  00000000  00000000  000
       00000000  00000000  000
06-02  00000000  00000000  000
       00000000  00000000  000
06-07  00000000  00000000  000
       00000000  00000000  000
32-01  00025678  00001376  000
       00027789  00001456  000
32-06  00000000  00000000  000
       00000000  00000000  000
32-08  00000000  00000000  000
       00000000  00000000  000
32-12  00000000  00000000  000
       00000000  00000000  000
38-02  00000000  00000000  000
       00000000  00000000  000
38-07  00000000  00000000  000
       00000000  00000000  000
08/08/90   08:01:09   #007879

xx RING REPT SMR A15MPR15  COMPL
```

Figure 5-5. Layout of the Scheduled 15MPR Report

Thirty-Minute Marginal Performance Report

General

The Thirty-Minute Marginal Performance Report (30MPR) is a detailed exception report of signaling link performance. The 30MPR can be output automatically every 30 minutes (the data coverage should be 6/6) and is output only if one of the measurements contained in the report exceeds some predefined threshold. The purpose of the report is to identify links that are showing marginal performance. The 30MPR provides a set of measurements that indicate various problems with the link, such as parity errors in received signal units, alignment problems, excessive changeovers, or excessive downtime.

This report should be checked whenever link problems are indicated. The thirty-minute reports from many periods should be compared for trends and abnormalities. Look for failures associated with an individual link, a group of links, or a particular far-end office.

If any measurement in a particular section exceeds its threshold as specified in the measurement output control table (MOCT), all equipped links are printed in that section. Those measurements that exceed their threshold are identified by an "+3*–3". If no measurements in a section exceed their threshold, the section is not printed. Depending on how many links are included in the report, there may be many pages of output.

The basic layout of the 30MPR report is shown in Figure 5-6. The following are the four sections of this report:

- Header information
- SS7 Links
- SS7 clusters
- PBX links.

Header Information

The 30MPR header information comtains the following:

- Office identification
- Report type
- Time
- Data coverage.

```
xx REPT SMR 30MPR STARTED

   SIGNALING LINK 30 MINUTE MARGINAL PERFORMANCE REPORT

   REPORTING OFFICE: local clli            REPORT INTERVAL: half hourly
   CURRENT GENERIC: gen_id                   AUTOMATIC REPORT
   DATE: mm/dd/yy,  TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/288

  CCIS6 LINKS:
                                        OOS TIM     SU ERR   SU RXMT     AURS
   FAR END CLLI-LAYER T GR-MEM VFL MIN  SEC
   ------------------ - ------ --- --------  -------  -------    ------
   nnnn nn nn nnn-nn  a nn-nn   B  (NOTE 1)   SUERB     SURXB      AURS
   nnnn nn nn nnn-nn  a nn-nn   A  (NOTE 1)   SUERA     SURXA      AURS

  CCIS6 LINKS:
                                      AUT CHG OVER      CB SM
   FAR END CLLI-LAYER T GR-MEM VFL
   ------------------ - ------ --- ------------     -------
   nnnn nn nn nnn-nn  a nn-nn   B      L6ACOB        L6CBSMB
   nnnn nn nn nnn-nn  a nn-nn   A      L6ACOA        L6CBSMA

  CCIS6 LINKS:
                                 OOS TIM   CRCER    BY RX       AUTO
   FAR END CLLI-LAYER T GR-MEM   MIN  SEC                    CHG OVER
   ------------------ - ------  --------  -----    -------   --------
   nnnn nn nn nnn-nn  a nn-nn   (NOTE 2)  CRCER     BYRX      L7ACO
   nnnn nn nn nnn-nn  a nn-nn   (NOTE 2)  CRCER     BYRX      L7ACO

  CCS7 LINKS*:
                                   ERSEC   UNVL
   FAR END CLLI-LAYER T GR-MEM
   ------------------ - ------     -----  ------
   nnnn nn nn nnn-nn  a nn-nn      ERSER   UNVL
   nnnn nn nn nnn-nn  a nn-nn      ERSER   UNVL
```

Notes:

1. **Calculated from L6CCTA or L6ACTB (the desription details how to derive total link OOS time)**
2. **This is the sum of L7AFLT and L7MFLT.**

* Not applicable in LEC environment

Figure 5-6. Layout of the Scheduled 30MPR Report (Sheet 1 of 2)

```
CCS7 CLUSTERS*:
                              ROUTE SET UNAVAILABLE
 CLUSTER      TYPE            COUNT          SEC
 -------    ------    ---------------------
   aaa        aaaa       RTESETUN  RTESETUNT

xx REPT SMR 30MPR IN PROG

 PBX LINKS*:
                          OOS TIME
   TYPE    GR-MN-C-P      (MINS)        ERSEC       CRCER
   ----    ---------    ---------     --------    --------
   aaaa    nn-nn-n-n    LP_FLTL_      ERSECL_     CRCERL_
   aaaa    nn-nn-n-n    LP_FLTL_      ERSECL_     CRCERL_

 PBX LINKS*:
                                                  MSG RCV'ed    PROTOCOL
   TYPE    GR-MN-C-P    BY RX     MSG RXMT      FOR UNA LINK  EX RCVD
   ----    ---------    ------    --------    ------------    --------
   aaaa    nn-nn-n-n    BYRXL_    MGRXL_        MGUNAL_       PROTEXRL_
   aaaa    nn-nn-n-n    BYRXL_    MGRXL_        MGUNAL_       PROTEXRL_

 PBX LINKS*:
                          NUMBER OF LINK  TEMP LINK FAIL
   TYPE    GR-MN-C-P       RESTARTS        TIME (SEC)
   ----    ---------     ------------    --------------
   aaaa    nn-nn-n-n       LKESTAB_        LPTMPFLT_
   aaaa    nn-nn-n-n       LKESTAB_        LPTMPFLT_

xx REPT SMR 30MPR COMPL

 * Not applicable in LEC environment
```

Figure 5-6. Layout of the Scheduled 30MPR Report (Sheet 2 of 2)

Common Channel Signaling 7 Links

This chapter is not applicable in the LEC environment.

Common Channel Signaling 7 Clusters

This chapter is not applicable in the LEC environment.

Private Branch Exchange (PBX) Links

This chapter is not applicable in the LEC environment.

Five-Minute Ring Exception Report

The Five-Minute Ring Exception (RINGEX) report is a detailed exception report of RPC congestion status. It can be output automatically every 5 minutes (the data coverage should be 1/1). The report is output only if one of the measurements contained in the report exceeds some predefined threshold. If no measurements exceeded their thresholds, the message **NO RPC OVERFLOWS ENCOUNTERED** is output.

The purpose of the report is to identify RPC nodes experiencing various levels of congestion. It should be used in conjunction with the machine performance report (MPR) to determine possible causes of the congestion and appropriate actions to relieve it. Give particular attention to overflow levels 2 and 3 (RRBOVFLW2_ and RRBOVFLW3_).

This is a one-page report with the basic layout shown in Figure 5-7. There are two sections to this report:

1. Header information
2. Details of congestion status.

The header information includes office identification, report type, time, and data coverage. The details of congestion status identifies data relevant to congested RPCN ring receive buffers. Congestion of the RPCN ring receive buffers indicates messages are being sent to the RPCN faster than the RPCN can process them. The report shows peg counts for levels 0, 1, 2, and 3 and duration counts for levels 1, 2, and 3. All IUNs are notified of the home RPCN congestion status. A few points to consider when interpreting the measurements are as follows:

- Level 0 is the normal no discard state. Messages are discarded at higher levels (only in IUNs however).
- The peg count indicates how many times the buffer occupancy reached the indicated level.

```
xx REPT SMR RINGEX STARTED
   RPC OVERFLOW REPORT

   REPORTING OFFICE: local clli code   REPORT INTERVAL: five minutes
   CURRENT GENERIC: gen_id               AUTOMATIC REPORT
   DATE: mm/dd/yy,  TIME: hh:mm:ss
   REPORT PERIOD (NWT): mm/dd/yy, hh:mm:ss  THRU  mm/dd/yy, hh:mm:ss
   DATA COVERAGE: nnn/001

   GRP MEM   OVFLW LVL 0    OVFLW LVL 1     OVFLW LVL 2    OVFLW LVL 3
   NUM NUM       PC          PC   TIME       PC   TIME      PC   TIME
   --- ---   ----------     ----------     ----------     ----------
    nn  nn    RRBOVFLW0     RRBOVFLW1_     RRBOVFLW2_     RRBOVFLW3_
    nn  nn    RRBOVFLW0     RRBOVFLW1_     RRBOVFLW2_     RRBOVFLW3_

xx REPT SMR RINGEX COMPL
```

Figure 5-7. Layout of the Scheduled RINGEX Report

Description of Critical Events

Introduction

The CCS Network *Critical Events* (CNCE) are predefined events that are considered indicators of abnormal network operation. They are of primary importance to both network operation and the proper functioning of the office. Both on-site and support system personnel must be immediately aware of events affecting the CCS network. The CNCE messages are output as the critical events occur. The critical event messages provide necessary real-time monitoring of the CCS network.

The CNCE messages are output as critical events occur in the office or as network events are recognized and acted upon. There are approximately 70 critical events in a CNI system. Some critical events pertain to the CCS network in general, while others have significance to the CNI also. A CNCE could represent an occurrence, the beginning of some state, or the ending of some state. Events indicating the beginning or ending of a state should occur in pairs, if not, investigate. A critical event never represents a length of time.

The naming convention used for critical events is similar to the naming convention used for measurements. The naming convention is as follows:

a. The mnemonic represents as closely as possible the actual event. The mnemonic is derived from a set of abbreviations representing typical signaling events. These abbreviations are combined to describe the event.

b. The suffix **E** means the state indicated by the mnemonic has ended.

c. Names may include letters, digits, or special characters.

d. Names are unique and contain no more than 12 characters.

The names given to critical events are used by the measurement output control table (MOCT). The MOCT controls the reporting of critical events.

Critical Event Logging

The recognition of critical events, occurrences to be reported, takes place in the central processor. The following information is provided to the central processor:

a. Identification of the event that occurred (the CNCE name)

b. If required, identification of the peripheral units involved.

Upon recognition of critical events, a CNCE message (**REPT CNCE**) is immediately output to users and automatically recorded in a critical event log file. This log file is a circular file stored on disk (/etc/log/CNCELOG). The file content is estimated to be a minimum of 90 minutes of the most recent CNCE messages. The messages in the log file can be retrieved. The file can be output using the **OP:LOG;CNCELOG** message. Refer to the *Input/Output Manual* for a description. Support system users cannot use this command when communications are via BX.25 data links.

The CNCE messages are sent to users both locally and at various support system centers. The office has several operation, administration, and maintenance organizations involved in its day-to-day functioning. These support systems use BX.25 data links for reception of critical event messages.

Critical event messages are generated by the critical event handler in short and long forms. The short form is intended mainly for support systems which have a reference data base containing details on the hardware identified. The long form is meant for use by the maintenance work force. Therefore, detailed information, in addition to what the short form provides, must be included. In particular, office identification (CLLI code), speed, type, layer (or SLK code), and protocol of the link must be included with the long form. If applicable, the long form also includes the VFL identification, function number, or subsystem number. When a critical event occurs, the log file is sent a long form message identifying the critical event. See I/O manual for detailed explanation.

The MOCT critical event table controls the reporting of critical events. This table includes information indicating which users are to be informed of any particular critical event. The critical event table also designates what form, long or short, of the message that a user receives. When the critical event handler records the message in the log file, a message is also sent to any users specified in the critical event table. Automatic reporting of critical events is in real time.

The following are examples of long and short CNCE messages. Refer to the *Output Message Manual* for a description of the fields in a CNCE message. Note that a CNCE message cannot be generated by an input command:

```
REPT CNCE
C7LCABM1X    14:00:36:59 7 02-00     ATLN_GA_TL_MS2_06 56. A
(Long form)


REPT CNCE
C7LCABM1X    14:00:36:59 7 02-00
(Short form)
```

Common Channel Signaling Network Critical Event Descriptions

The event names appearing in CNCE output messages are derived from the MOCT. Critical events that are reported by the CNCE messages are identified and described in Table 5-D. The descriptions are presented alphabetically by event name. Note that the table shows data provided by the CNCE message enclosed in parentheses. This field is either the group and member, point code, or link set identification.

Often an occurrence not only causes a CNCE message, but is also counted as a measurement. Some of the critical events in the table can be better understood by referring to the corresponding measurement. The corresponding measurement contains a more detailed description of certain "events." The measurement name should be similar to the critical event name.

Measurement Output Control Table

Overview

The Measurement Output Control Table (MOCT) is used to control the format, frequency, destination, and content of network critical event messages and measurement reports. The following five tables are contained in the MOCT:

1. Critical Event Table (CET)
2. User View Descriptor Table (UVDT)
3. Exception Table (EXCP)
4. History File Descriptor Table (HFDT)
5. Scheduler Table (SCHD).

The CET enables users to select which critical event messages they wish to receive. A threshold can be assigned to a particular critical event which will either permit or prevent the critical event message from being transmitted. By use of the threshold, notification of a particular critical event can be stopped for a while and then resumed again later. The user can also elect to receive either a long or short form of the critical event message.

This flexibility also applies to reporting measurements. Users can define reports tailored to their specific needs. These flexible format reports can contain as many measurements as the CNI. The presence of a particular set of measurements in a report can be made contingent upon the measurement values. The measurement values can be drawn from files covering different periods of time. A report can be generated on a regular basis or when the user requests a report. In short, a measurement report can be whatever the user specifies it to be in the MOCT.

The responsibility of the user is to have an operational, administrative, and maintenance plan for the MOCT. If unmanaged, an inconsistent flow or even a loss of data and reports could result. Someone in the user's organization must take the responsibility to define which of the many possible plans is the most effective for meeting the needs and capabilities of the network. Once the plan for the operation, administration, and maintenance of the MOCT is determined, the initial CNI MOCT can be administered. The initial MOCT has been designed according to the input of users. As the need of the user changes, the MOCT changes to reflect the changes of the user.

Critical Event Table

A CCS network critical event is an event occurring in the network due to the result of an abnormality in network operations or as a potential cause of abnormalities. Messages that report such events are called CCS network critical event (CNCE) messages. There are a variety of critical events that can be reported by the office. Since not all critical event messages are desired by a network monitor, the Critical Event Table (CET) provides a means of selecting the ones desired to be delivered to a specified destination in the proper format. Each critical event may be directed to several destinations where each destination is represented by an output class number.

Critical event messages can be output in long or short form. The user specifies whether the long or short form is desired in the "message type" field of the CET entry. The short critical event message contains the critical event name, network time of occurrence, association field, and virtual link number. The long critical event message contains the same data items as the short critical event message plus the Common Language Location Identifier (CLLI) code, link speed and protocol, link type, and VFL ID.

The threshold determines whether a report is generated and sent to a particular destination. For this application, the threshold has two states (on and off). The threshold is on when it equals 1; and consequently, the report is generated and sent to the destination as defined. But in the off state, when it equals zero, the report is not generated or sent to the specified destination. The use of the off state is for user flexibility. With this flexibility, a user can receive a particular critical event message if desired. Should the user elect not to receive a particular critical event message, all that is required is to perform a recent change on the threshold value. Note, however, that changing the threshold affects all users assigned to the specified destination class. The following is a sample entry in the CET:

CRITICAL EVENT

EVENT NAME: c6fldcol

DESTINATION	MESSAGE TYPE	THRESHOLD
001	cmcesrpt	1
002	cmcelrpt	0
133	cmcesrpt	0
232	cmcelrpt	1

In the CET, all critical events are assigned to the destination representing the critical event log file. The critical event log file is a circular log file in the central processor. All critical event messages are sent to this log file in an on-occurrence basis. Critical event messages are stored in this log file in short form only. The log file receives all critical event messages and stores them until log file buffers are full. Once the log file is filled, the oldest CNCE messages are discarded to make room for a new CNCE message that the log file receives.

A user can look up a critical event message which has recently occurred by accessing the critical event log file. In the 4ESS switch application, the critical event log file is identified as "CNILOG". To access the critical event log file, the PDS command *OP:LOG:CNILOG* is used. If the user enters this option only, all the critical events contained in the critical event log file (CNILOG) are be printed. The user must specify additional options to receive specific data from the critical event log file (CNILOG). Refer to AT&T IM-4A001-01 — ***4ESS** Switch/APS Input Message Manual* for all applicable options and a description of each.

The event name, destination, message type, and threshold values for the initial critical event table (CET) are identified in Table 5-E.

Administering Measurement Reports

The purpose of the remaining tables that comprise the MOCT is to specify how, what, when, and where to generate measurement reports for users. Measurements provide past, raw statistics of performance, while critical events reflect current conditions of the CNI. Measurements are periodically collected by the CNI and are stored in memory and on disk. Although the measurement process is constant, the software only collects the measurements every 5 minutes. Reporting of the CNI's performance is said to be in nonreal time, since the data contained in these reports is not immediately relayed to the user. The measurements or statistics are presented to users in measurement reports. Reports present the selected measurements in a form acceptable to users, be it a fixed format or flexible format. The fixed format reports are predefined reports whose output is specifically designed and therefore, should not be changed. Although the user has the ability to change the contents of these fixed format reports, the report generator designated for these reports cannot be changed. Thus, the designed output limits the user's ability to change the contents of these reports. The flexible format reports are defined by the user to attain a report tailored to a user's specific needs. These reports can be defined and redefined, via recent change procedures, as the user's needs change.

There are four tables used to define the contents of a particular report. These are the User View Descriptor Table, Exception Table, History File Descriptor Table, and Scheduler Table. Each of these tables is described in the following paragraphs.

Table 5-E. Initial Critical Event Table

Event Name	Destination	Message Type	Threshold
C7ACB	64	Long	1
	65	Short	1
C7ACBFLD	64	Long	1
	65	Short	1
C7ACOCOV	64	Long	1
	65	Short	1
C7ACOER	64	Long	1
	65	Short	1
C7BOLR	64	Long	1
	65	Short	1
C7BOLRE	64	Long	1
	65	Short	1
C7FLDCOL	64	Long	1
	65	Short	1
C7FLDCOV	64	Long	1
	65	Short	1
C7FLDER	64	Long	1
	65	Short	1
C7FLDSNT	64	Long	1
	65	Short	1
C7LCABM1X	64	Long	1
	65	Short	1
C7LCABM2X	64	Long	1
	65	Short	1
C7LCABM3X	64	Long	1
	65	Short	1
C7LCDIS1X	64	Long	1
	65	Short	1
C7LCDIS2X	64	Long	1
	65	Short	1
C7LCDIS3X	64	Long	1
	65	Short	1

Table 5-E. Initial Critical Event Table (Contd)

Event Name	Destination	Message Type	Threshold
C7LCON1X	64	Long	1
	65	Short	1
CPARSFLD	64	Long	1
	65	Short	1
CPMOOS	64	Long	1
	65	Short	1
CTREDAL	64	Long	1
	65	Short	1
C7LCON2X	64	Long	1
	65	Short	1
C7LCON3X	64	Long	1
	65	Short	1
C7LSF	64	Long	1
	65	Short	1
C7LSFE	64	Long	1
	65	Short	1
C7MCB	64	Long	1
	65	Short	1
C7MCOF	64	Long	1
	65	Short	1
C7MCON	64	Long	1
	65	Short	1
C7POR	64	Long	1
	65	Short	1
C7POR	64	Long	1
	65	Short	1
C7PORE	64	Long	1
	65	Short	1
C7SPI	64	Long	1
	65	Short	1
C7SPIE	64	Long	1
	65	Short	1
C7SPIPO	64	Long	1
	65	Short	1

Table 5-E. Initial Critical Event Table (Contd)

Event Name	Destination	Message Type	Threshold
CPFLD	64	Long	1
	65	Short	1
CPMOOSE	64	Long	1
	65	Short	1
CTREDALC	64	Long	1
	65	Short	1
CTYELAL	64	Long	1
	65	Short	1
CT1FAFL	64	Long	1
	65	Short	1
CTYELALC	64	Long	1
	65	Short	1
CT1FARCVRY	64	Long	1
	65	Short	1

The first step in defining any measurement report is to define the measurement IDs desired in the report. This is done in the User View Descriptor Table (UVDT). This table simply contains lists of measurement IDs grouped under different view names. This view name is then used to reference the list of measurement IDs when generating the report.

The next step is to assign each measurement a threshold if this option is desired. If a threshold value is assigned to a measurement, the measurement value must exceed the threshold value in order to be included in the specified report. The assignment of thresholds to measurement IDs is done in the Exception Table (EXCP).

The next step in defining a measurement report is to define the source of the measurement values. As discussed earlier, measurements are gathered every 5 minutes. These 5-minute blocks of data are stored in the core memory in a file called LPM. Every 5 minutes, the LPM file is accumulated to form a file covering 15 minutes. The resultant 15-minute file and each subsequently accumulated history file is stored on disk. Therefore, the information in a measurement report is gathered from one of two sources:

1. LPM—In-core 5-minute data structure containing measurements collected for the last 5 minutes.
2. History file—On disk multiples of 15-minute coverages.

All sources contain the same number of measurement items. Each source differs only in the time of day covered or the length of time covered in any particular file. The history file descriptor table (HFDT) describes how various history files are accumulated.

The final step in the MOCT's generation of a report is to gather all the ingredients of the report at the specified time and output the report to the specified destination(s). This task is performed by the Scheduler Table (SCHD). There are two ways to generate a report:

1. ***Scheduled:*** Internal stimulus as a history file is completed. Once a history file is completed, the Scheduler Table is scanned for all entries which use the newly created history file as its source. From these entries, using the newly completed history file, a report is generated for each entry specifying the present time for activation of the report.
2. ***Demanded:*** OP:SMR command as stimulus. A user can specify the ingredients of a report in the Scheduler Table and not specify that the report be generated at any certain time. The user can then request or demand the report at any time with the **OP:SMR** input command.

User View Descriptor Table

The User View Descriptor Table (UVDT) contains the lists of measurement IDs that the user designates for particular reports. Each list of measurement IDs is assigned a user view name. This view name is used as a reference to access the list of measurement IDs contained in a measurement report. Each user has different needs and therefore, requests different measurement IDs in their measurement reports. Each view name, assigned in the UVDT, defines the contents of one or more reports.

To create a new report, a new view name must be added to the UVDT. This new view name must have all the measurement IDs for the report assigned to it. To change the content of an existing report, the user must add or delete measurement IDs from the existing user view name to meet the present needs. If the user view is being used by one or more group names in the Exception Table, then the threshold(s) assigned to the measurement ID is affected also. If a measurement ID is being added, then the measurement ID and a threshold of zero is assigned to the group name in the Exception Table. If the measurement ID is being deleted, then the measurement ID and its assigned threshold are also deleted from the corresponding group name in the Exception Table.

There are five fixed format reports whose views are contained in the UVDT. However, it must be pointed out that more than one user may be receiving a particular report and would also be affected by any changes to the view name. It is therefore highly recommended that all changes be administered by a centralized administrative entity. These views should not be changed since the report generators assigned to them are designed for a certain output and cannot

be changed. The following example shows a list of measurements assigned to the user view name "ct100" in the UVDT.

```
VIEW NAME:     ct100

MEASUREMENT ID

      sux
      sur
    mgansx
    mgansr
```

The user view and associated measurement identifications for the initial user view descriptor table (UVDT) are identified in Table 5-F.

Exception Table

In many instances a user only wants to see a set of measurements in a report if one of them exceeds a certain threshold level. Some thresholds refer to the number of accumulated counts, while others refer to the number of seconds involving the exception. These exceptions or threshold values are assigned to a particular measurement ID in the Exception Table (EXCP). In the EXCP, a view and its associated thresholds are assigned to a group name. In this group name every measurement ID is assigned a threshold. While the requested report is being generated, the measurement values and the threshold values are compared. The measurement and the other measurements in the same group are then placed in the report only if one of them has exceeded the defined threshold value. Sets of measurements are grouped according to one of three categories:

1. Per link
2. Per node
3. Per office.

An exception report can contain several sets of measurements from one or all of these three categories. The placement of each set of measurements in the exception report is individually dependent upon the measurement values of that set exceeding the threshold values assigned to the set.

Table 5-F. Initial User View Descriptor Table

User View	Measurement IDs			
A30MPR	AURS RTESETUNT L7MFLT SURXB ERSECL0 PROTEXRL0	BYRX ERSEC SUERA UNVL CRCERL0 MGRXL0	CRCER L7ACO SUERB LPAFLTL0 BYRXL0	RTESETUN L7AFLT SURXA LPMFLTL0 MGFMTERL0
AMPR	CINIT0 INIT0 INIT4 NOCMGT OOSCFGT RSTTRMT	CINIT1 INIT1A MRNIAU OOSAU OOSMN SRNIAU	CINIT3 INIT1B MRNIAUT OOSAUT OOSMNT SRNIAUT	CINIT4 INIT3 NOCMG OOSCFG RDWNT
ASEPR	OOSAU OOSMN	OOSAUT OOSMNT	OOSCFG RSTTRMT	OOSCFGT
ASNPR1	AURSTE GTTUNBC CRCERTE ERSECTE L7BOLR	BYR CLFSP MRBADRTG L7ACO L7BOLRT	BYRXTE CLFSPT EMRSP L7ACOTE	BYX GTTUNNT EMRSPT L7BOFR
	L7FLD L7LCON1XT MGMSUR MSUDISC0 SPISPT	L7FLDT L7MRPBC MGMSUX MSUDISC1 SUERATE	L7LCDIS1X L7MRPNT MRSBCO7 MSUDISC2 SUERBTE	L7LCON1X MSG7LOOP MRSNTO7 SPISP SUR
	SURXATE SC7RGTR LPFLDL3 LPFLDL7 LPFLDTL3	SURXBTE LPFLDL0 LPFLDL4 LPFLDTL0 LPFLDTL4	SUX LPFLDL1 LPFLDL5 LPFLDTL1 LPFLDTL5	L7RTGAUD LPFLDL2 LPFLDL6 LPFLDTL2 LPFLDTL6
	LPFLDTL7 LPTMPFL3 LPTMPFL7 LPTMPFLT3 LPTMPFLT7	LPTMPFL0 LPTMPFL4 LPTMPFLT0 LPTMPFLT4 LKESTBL0	LPTMPFL1 LPTMPFL5 LPTMPFLT1 LPTMPFLT5 LKESTBL1	LPTMPFL2 LPTMPFL6 LPTMPFLT2 LPTMPFLT6 LKESTBL2

Table 5-F. Initial User View Descriptor Table (Contd)

User View	Measurement IDs			
ASNPR1 (Contd)	LKESTBL3	LKESTBL4	LKESTBL5	LKESTBL6
	LKESTBL7	MGUNAL0	MGUNAL1	MGUNAL2
	MGUNAL3	MGUNAL4	MGUNAL5	MGUNAL6
	MGUNAL7	BYXL0	BYRL0	MGMSUXL0
	MGMSURL0	LPBOLRL0	LPBOLRTL0	MGRUAL0
	Q931MGXL0	Q931MGRL0	XBFFULLL0	XBFFULLTL0
	BYXL1	BYRL1	MGMSUXL1	MGMSURL1
	LPBOLRL1	LPBOLRTL1	MGRUAL1	Q931MGXL1
	Q931MGRL1	XBFFULLL1	XBFFULLTL1	BYXL2
	BYRL2	MGMSUXL2	MGMSURL2	LPBOLRL2
	LPBOLRTL2	MGRUAL2	Q931MGXL2	Q931MGRL2
	XBFFULLL2	XBFFULLTL2	BYXL3	BYRL3
	MGMSUXL3	MGMSURL3	LPBOLRL3	LPBOLRTL3
	MGRUAL3	Q931MGXL3	Q931MGRL3	XBFFULLL3
	XBFFULLTL3	BYXL4	BYRL4	MGMSUXL4
	MGMSURL4	LPBOLRL4	LPBOLRTL4	MGRUAL4
	Q931MGXL4	Q931MGRL4	XBFFULLL4	XBFFULLTL4
	BYXL5	BYRL5	MGMSUXL5	MGMSURL5
	LPBOLRL5	LPBOLRTL5	MGRUAL5	Q931MGXL5
	Q931MGRL5	XBFFULLL5	XBFFULLTL5	BYXL6
	BYRL6	MGMSUXL6	MGMSURL6	LPBOLRL6
	LPBOLRTL6	MGRUAL6	Q931MGXL6	Q931MGRL6
	XBFFULLL6	XBFFULLTL6	BYXL7	BYRL7
	MGMSUXL7	MGMSURL7	LPBOLRL7	LPBOLRTL7
	MGRUAL7	Q931MGXL7	Q931MGRL7	XBFFULLL7
	XBFFULLTL7			
ASNPR2	AURSTE	BYRX	BYRXTE	CRCER
	CRCERTE	EMR	EMRT	CLF
	CLFT	L7EMR	L7EMRT	ERSEC
	ERSECTE	L7ACO	L7ACOTE	L7AFLT
	L7FLD	L7FLDT	L7LCON1X	L7LCON1XT
	L7MFLT	L7PORT	MSUDISC0	MSUDISC1
	MSUDISC2	SPI	SPIT	SUERA
	SUERB	SURXA	SURXB	SUERATE
	SUERBTE	SURXATE		

Table 5-F. Initial User View Descriptor Table (Contd)

User View	Measurement IDs			
ASNPR2 (Contd)	SURXBTE	LPFLDL0	LPFLDL1	LPFLDL2
	LPFLDL3	LPFLDL4	LPFLDL5	LPFLDL6
	LPFLDL7	LPFLDTL0	LPFLDTL1	LPFLDTL2
	LPFLDTL3	LPFLDTL4	LPFLDTL5	LPFLDTL6
	LPFLDTL7	LPAFLTL0	LPAFLTL1	LPAFLTL2
	LPAFLTL3	LPAFLTL4	LPAFLTL5	LPAFLTL6
	LPAFLTL7	LPMFLTL0	LPMFLTL1	LPMFLTL2
	LPMFLTL3	LPMFLTL4	LPMFLTL5	LPMFLTL6
	LPMFLTL7	LPTMPFLT0	LPTMPFLT1	LPTMPFLT2
	LPTMPFLT3	LPTMPFLT4	LPTMPFLT5	LPTMPFLT6
	LPTMPFLT7	LPTMPFL0	LPTMPFL1	LPTMPFL2
	LPTMPFL3	LPTMPFL4	LPTMPFL5	LPTMPFL6
	LPTMPFL7	LKESTBL0	LKESTBL1	LKESTBL2
	LKESTBL3	LKESTBL4	LKESTBL5	LKESTBL6
	LKESTBL7	MGUNAL0	MGUNAL1	MGUNAL2
	MGUNAL3	MGUNAL4	MGUNAL5	MGUNAL6
	MGUNAL7	MGRUAL0	MGRUAL1	MGRUAL2
	MGRUAL3	MGRUAL4	MGRUAL5	MGRUAL6
	MGRUAL7	LPBOLRL0	LPBOLRTL0	XBFFULLL0
	XBFFULLTL0	LPBOLRL1	LPBOLRTL1	XBFFULLL1
	XBFFULLTL1	LPBOLRL2	LPBOLRTL2	XBFFULLL2
	XBFFULLTL2	LPBOLRL3	LPBOLRTL3	XBFFULLL3
	XBFFULLTL3	LPBOLRL4	LPBOLRTL4	XBFFULLL4
	XBFFULLTL4	LPBOLRL5	LPBOLRTL5	XBFFULLL5
	XBFFULLTL5	LPBOLRL6	LPBOLRTL6	XBFFULLL6
	XBFFULLTL6	LPBOLRL7	LPBOLRTL7	XBFFULLL7
	XBFFULLTL7			
LFTADM	L7BYTO3B			
NFDISK	EMR	EMRPO	EMRPOT	EMRT
	L7EMR	L7EMRPO	L7EMRPOT	L7EMRT
	L7AFLT	L7BOLR	L7BOLRT	L7LCDIS3X
	L7LCON1X	L7LCON1XT	L7LCON2X	L7LCON2XT
	L7LCON3X	L7LCON3XT	L7MFLT	L7POR
	SPI	SPIT		

Table 5-F. Initial User View Descriptor Table (Contd)

User View	Measurement IDs			
NFLPM	EMR L7EMR L7AFLT L7LCON1X L7LCON3X SPI	EMRPO L7EMRPO L7BOLR L7LCON1XT L7LCON3XT SPIT	EMRPOT L7EMRPOT L7BOLRT L7LCON2X L7MFLT	EMRT L7EMRT L7LCDIS3X L7LCON2XT L7POR
RINGEX	IUNOVLD0 RRBOVFLW1 RRBOVFLW3	IUNOVLD1 RRBOVFLW1T RRBOVFLW3T	IUNOVLD2 RRBOVFLW2	RRBOVFLW0 RRBOVFLW2T

There must be a view defined in the UVDT for every exception group in the EXCP. However, two exception reports may use the same view. This allows the user the flexibility to assign different threshold values to the same measurement IDs for a view name. Different exception groups may be required because the two reports use different history files. To do this, the view name and its assigned measurements must appear in more than one exception group in the EXCP. Each group name specifies different threshold values, yet each group uses the same user view. The Scheduler Table (SCHD) specifies which exception group is used with which user view in the creation of the report.

GROUP NAME: ce2001

VIEW NAME: ce200

MEASUREMENT ID	THRESHOLD
l6bolr	0000000001
l6bolrt	0000000300
l6bolx	0000000001
l6bolxt	0000000060

In the preceding example, the exception group ce2001 contains all the measurements assigned to the user view name ce200. These measurements are listed in the MEASUREMENT ID column. The EXCP is then used to assign these measurements the threshold values listed in the THRESHOLD column.

The exception group, measurement user view, measurement identification, and measurement threshold values for the initial exception table (EXCP) are identified in Table 5-G.

History File Descriptor Table

Most report generators can be applied over different time periods. These time periods are defined in the History File Descriptor Table (HFDT). The HFDT is simply a set of instructions constructing history files covering different time periods. All history files contain the same measurement IDs. One history file differs from another in the time interval it covers. The valid periods covered by history files are 5 minutes, 15 minutes, 30 minutes, hour, day to hour, and last day. Because the HFDT is constructed to meet the common requirements of all CNI reports, it is less volatile than any of the other tables. For example, a 15-minute collection period is used to accumulate a 30-minute collection period and also generate reports covering 15-minute periods of data. Should a user manipulate the history file containing this 15-minute collection period, each subsequently accumulated history file is affected. Therefore, changes to the HFDT are discouraged.

The software collects measurements and stores them in a 5-minute file in core memory called lpm. When the lpm file is complete, its contents are copied into a current 15-minute file (c15m) in core memory. Five minutes later, the lpm file is overwritten with the most current 5-minute collection period. This new data is added to the previous 5 minutes of data in the c15m file to accumulate 10 minutes of data. Five minutes later, the lpm file is again overwritten with the most current 5-minute collection period. This new data is then added to the previously accumulated 10 minutes of data to fill the current 15-minute file (c15m). Once the c15m file is filled, it is copied into the last 15-minute (l15m) file in disk memory for further accumulation. The l15m file is used to accumulate larger history files on disk. The first step in this process is to copy the l15m file into a current 30-minute (c30m) file to begin the accumulation of a 30-minute collection period. Five minutes later, the cycle repeats itself. When the lpm file is overwritten, it is then copied into the c15m file which overwrites the 15 minutes of data previously stored there. As the lpm file is updated, it adds two more 5-minute collection periods to fill the c15m file. Once the c15m file is filled, it is copied into the l15m file overwriting the 15 minutes of data previously stored there. The new l15m file is added to the c30m file to accumulate 30 minutes of data in that history file. Once the c30m file is filled, it is copied into the last 30-minute l30m file for further accumulation of larger history files. The l30m file is copied into another history file called chrm to begin the accumulation of a 60-minute data collection period. Five minutes later, the cycle again repeats itself. The 5-minute lpm file is used to accumulate a current 15-minute collection period in the c15m file which is copied into the l15m file. The last 15-minute (l15m) file is used to accumulate a new current 30-minute collection period in the c30m file which is copied into the l30m file. The last 30-minute (l30m) file is added to chrm to accumulate 60 minutes of data in that history file. Once chrm is filled, it is copied into another 60-minute history file called lhrm for the accumulation of a current day history file. Repetition of this process allows these 60-minute files to

be accumulated 24 times to create a history file covering an entire day (cday). Once the cday file has accumulated an entire day's data, it can be copied into the lday file for further use. As the new file is being created for the next day, the cday file is filled while the previous day's data is stored in the lday file. The accumulation process stops here since history files are presently limited to a single day's coverage. The cycle does not stop though. The next day, the lday file is simply overwritten with more current measurements. In summary, the cycle flow according to the following list:

1. The software collects and stores measurements in core memory in a 5-minute file called lpm.
2. The lpm file is accumulated in core memory in a current 15-minute file called c15m.
3. The c15m file is copied to another 15-minute history file in disk memory called l15m.
4. The l15m file is accumulated in disk memory in a current 30-minute history file called c30m.
5. The c30m file is copied to another 30-minute history file in disk memory called l30m.
6. The l30m file is accumulated in disk memory in a current 60-minute history file called chrm.
7. The chrm file is copied to another 60-minute history file in disk memory called lhrm.
8. The lhrm file is accumulated in disk memory in a current day history file called cday.
9. The cday file is copied to another day history file in disk memory called lday. The accumulation process stops here since history files are presently limited to a single day's coverage. The cycle does not stop though. The next day, the lday file is simply overwritten with more current measurements.

The functional use of the data items used in the HFDT is described in the following paragraphs. It is followed by an example which illustrates how the preceding data items are implemented in the HFDT. Following the example is a detailed explanation of what is happening in each time interval shown on the example.

Every 5 minutes, the HFDT is scanned. The record number depicts the order in which the entries are executed. Each time the HFDT is accessed, the lowest record number to be executed at that time is done first; the remaining record numbers are done in ascending order for the specified time.

Table 5-G. Initial Exception Table

Exception Group	Measurement User View	Measurement ID	Measurement Threshold
A30MPR30	A30MPR	AURS	0000000003
		BYRX	0000021222
		CRCER	0000005500
		RTESETUN	0000000001
		RTESETUNT	0000000001
		ERSEC	0000001000
		L7ACO	0000000002
		L7AFLT	0000000001
		L7MFLT	0000000001
		SUERA	0000000300
		SUERB	0000000300
		SURXA	0000000300
		SURXB	0000000300
		UNVL	0000000015
		LPAFLTL0	0000000001
		LPMFLTL0	0000000001
		ERSECL0	0000000001
		CRCERL0	0000000001
		BYRXL0	0000000001
		MGFMTERL0	0000000001
		PROTEXRL0	0000000001
		MGRXL0	0000000001
NFDISKEXHR	NFDISK	EMR	0000000001
		EMRPO	0000000001
		EMRPOT	0000000001
		EMRT	0000000001
		L7EMR	0000000001
		L7EMRPO	0000000001
		L7EMRPOT	0000000001
		L7EMRT	0000000001
		L7AFLT	0000000001
		L7BOLR	0000000001
		L7BOLRT	0000000001
		L7LCDIS3X	0000000001
		L7LCON1X	0000000001
		L7LCON1XT	0000000001
		L7LCON2X	0000000001
		L7LCON2XT	0000000001
		L7LCON3X	0000000001

Table 5-G. Initial Exception Table (Contd)

Exception Group	Measurement User View	Measurement ID	Measurement Threshold
NFDISKEXHR (Contd)		L7LCON3XT	0000000001
		L7MFLT	0000000001
		L7POR	0000000001
		SPI	0000000001
		SPIT	0000000001
NFLPMEXHR	NFLPM	EMR	0000000001
		EMRPO	0000000001
		EMRPOT	0000000001
		EMRT	0000000001
		L7EMR	0000000001
		L7EMRPO	0000000001
		L7EMRPOT	0000000001
		L7EMRT	0000000001
		L7AFLT	0000000001
		L7BOLR	0000000001
		L7BOLRT	0000000001
		L7LCDIS3X	0000000001
		L7LCON1X	0000000001
		L7LCON1XT	0000000001
		L7LCON2X	0000000001
		L7LCON2XT	0000000001
		L7LCON3X	0000000001
		L7LCON3XT	0000000001
		L7MFLT	0000000001
		L7POR	0000000001
		SPI	0000000001
		SPIT	0000000001
RINGEXLPM	RINGEX	IUNOVLD0	0000000001
		IUNOVLD1	0000000001
		IUNOVLD2	0000000001
		RRBOVFLW0	0000000001
		RRBOVFLW1	0000000001
		RRBOVFLW1T	0000000001
		RRBOVFLW2	0000000001
		RRBOVFLW2T	0000000001
		RRBOVFLW3	0000000001
		RRBOVFLW3T	0000000001

The history file is the result of the action or the file receiving the measurements to be accumulated. The source file is the file from which the measurements are being taken to build the specified history file. The source file may be another history file which was built from other source files. The smallest source file is a 5-minute file called lpm. This file resides in core memory and is predefined to be accumulated into a 15-minute file called l15m. The history file l15m resides in disk memory and is the smallest source file available to the user in the HFDT. Each subsequently accumulated history file resides in disk memory and is built in the HFDT.

The coverage represents the number of 5-minute accumulation periods which can be contained in the specified history file. This can range from 3 to 288, since the smallest history file available for HFDT use covers 15 minutes, and the largest is a 1-day file.

The action defines how the source file is entered into the history file. If the action is "copy," the history file does not accumulate or increase the time period covered but receives the measurements in the source file and stores them under a new history file name. This is done to store the measurements to be accumulated in a larger file when the need exists. If the action is "add," the source file is accumulated in the history file to increase the time covered by the file. For the "add" action, the source file overwrites the contents of the history file and is then added to the history file until the history file is filled.

The disposition determines what happens next. If the action is "add," the disposition is void because the disposition has no affect on the process. If the disposition is "continue," the process proceeds to the Scheduler Table where all the reports using the updated history file are generated and returned to the HFDT. If the action is "stop," the process terminates. This is necessary if the Scheduler Table doesn't use the history file that was updated, and the process doesn't need to proceed to the Scheduler Table. A detailed discussion of the interaction of the UVDT, EXCP, HFDT, and SCHD in the generation of reports is provided later in this chapter.

The "**when**" field is used to determine the time the specified action takes place. If repeat equals N, the action occurs at the time specified in the "**when**" field. The number in this field multiplied by 5 minutes (smallest network measurement file time) is the network time of the action. For example, if a user wants a report generated at 01:30 network time, the entry in the "**when**" column would be 018 (018 x 5 minutes = 90 minutes = 01:30). An action in the history file can then be repeated by entering a **Y** in the "**repeat**" field. A repeat causes the action to occur at every multiple of the time specified in the "**when**" column. For example, if the "**when**" entry is 012 and the "**repeat**" entry is **Y**, then the action involved occurs every hour (12 x 5 minutes = 60 minutes = 1 hour). If the entry in the "**repeat**" field is N, then the action occurs only at the time specified by the "**when**" entry. The following example illustrates the use of each of these data items and is followed by a more detailed description of the process.

NOTE:
History files updated with the "**add**" action are called current history files. These files cannot be used to cause scheduled reports to occur. This task is reserved for those files updated with the copy action.

RECORD NUMBER	HISTORY FILE	COVERAGE	ACTION	DISP	SOURCE	WHEN	REPEAT
00010	c30m	006	add		l15m	003	Y
00020	l30m		copy	cont	c30m	006	Y
00030	chrm	012	add		l30m	006	Y
00040	lhrm		copy	cont	chrm	012	Y
00050	cday	288	add		lhrm	012	Y
00060	lday		copy	cont	cday	010	N

c30m - current 30-minute history file
l30m - last 30-minute history file
chrm - current hour history file
lhrm - last hour history file
cday - current day history file
lday - last day history file
cont - continue
Y - yes
N - no

The previous example is described below according to time of occurrence.

At 00:15 network time, the following occurs:

00010 The last 15-minute (l15m) file is copied to the current 30-minute (c30m) file. The network time 00:15 was calculated by multiplying the number in the "**when**" column (003) by 5 minutes. The coverage tells us that the history file c30m covers a 30-minute time period (006 x 5 minutes). The **Y** in the "**repeat**" column causes this action to occur every 15 minutes (003 x 5 minutes). Since the action is "add," the disposition is not recognized. Therefore, it is entered as void.

At 00:30 network time, the following occurs: record number 00010 is repeated, and then record numbers 00020 and 00030 are initiated.

00010 History file l15m is added to c30m a second time. Now c30m has accumulated 30 minutes of current measurements.

00020 The current 30-minute (c30m) file is copied into history file l30m to be stored as the last 30 minutes. This saves the current 30-minute data for future accumulation. There is no entry in the coverage column because there is no change in the time period covered by the history file with the copy action. This action is repeated every 30 minutes starting at the present network time 00:30 (006 x 5 minutes). Once this action is complete, the "continue" entry in the disposition column (continue) tells the Scheduler Table to continue and process any reports using l30m.

00030 The last 30-minute l30m file is copied to current hour (chrm) file. This begins the accumulation of a 1-hour history file. The 012 entry in the "coverage" column tells us that the history file chrm covers 60 minutes (012 x 5 minutes). The **Y** entry in the "**repeat**" column causes this action to occur every 30 minutes (006 x 5 minutes).

At 00:45 network time, the following occurs:

00010 The last 15-minute (l15m) file is copied to the current 30-minute (c30m) file.

At 00:50 network time, the following occurs:

00060 The current day (cday) file is copied into the last day (lday) file. This time is represented by the 010 entry in the "**when**" column (010 x 5 minutes). This time was selected because of the many actions which congest the data base on the quarter hours immediately following 00:00 network time. The current day (cday) file could be copied into the last day (lday) file any time after the last hour of the day that it is accumulated (00:00) and before the first hour of the next day is accumulated (01:00 network time). Yet, there are many reports and files being sent and updated during the hour directly following the end of a network day. Therefore, a large volume copy, such as the copy of a current day file, should be done during a time of lesser congestion in the data base. The least congested times available for such actions are those 5-minute divisions between quarter hours, such as 00:25 and 00:50. This action is not repeated during this day due to the **N** entry in the "**repeat**" column. Once this action is complete, the "continue" entry in the disposition column tells the Scheduler Table to continue, and process any reports using the lday file.

At 01:00 network time, the following occurs:

00010 History file l15m is added to the history file c30m which then contains 30 minutes of current measurements.

00020 History file c30m is copied into history file l30m so that the 30 minutes of current measurements can be further accumulated in another larger history file.

00030 History file l30m is added to history file lhrm which will then contain 60 minutes of current data.

00040 The current hour (chrm) file is copied into the last hour (lhrm) file to be used to accumulate an even larger history file. This action occurs every hour,:w as defined by the 012 entry in the "**when**" column and the Y entry in the "**repeat**" column (012 x 5 minutes). Once this action is complete, the "continue" entry in the "disposition" column allows the Scheduler Table to continue to generate measurement reports using the lhrm file created. Note that there is no entry in the "coverage" column because there was no change in the time period covered by the new history file with the copy action.

00050 The last hour history (lhrm) file is copied to the current day history (cday) file. This action also occurs every hour as defined by the entries in the "**when**" column and "\f3repeat" column. The history file lhrm is added to the history file cday 24 times throughout the day. Therefore, the cday file contains all the 288 possible 5-minute measurement periods in a day as is shown in the "coverage" column.

At 01:15 network time, the following occurs:

00010 The last 15-minute (l15m) file is copied to the current 30-minute (c30m) file. This action continues to occur every 15 minutes.

At 01:30 network time, the following occurs:

00010 Source file l15m is added to history file c30m. This action continues to occur every 15 minutes.

00020 Source file c30m is copied to history file l30m. This action continues to occur every 30 minutes.

00030 Source file l30m is copied to history file chrm. This action continues to occur every 30 minutes.

At 01:45 network time, the following occurs:

00010 Source file l15m is copied to history file c30m. This action continues to occur every 15 minutes.

At 02:00 network time, the following occurs:

00010 Source file l15m is added to history file c30m. This action continues to occur every 15 minutes.

00020 Source file c30m is copied to history file l30m. This action continues to occur every 30 minutes.

00030 Source file l30m is added to history file chrm. This action continues to occur every 30 minutes.

00040 Source file chrm is copied to history file lhrm. This action continues to occur every hour.

00050 Source file lhrm is added to history file cday. This action continues to occur every hour.

The record number, history file, action, disposition, source file, when, coverage, and repeat values for the initial history file descriptor table (HFDT) are identified in Table 5-H.

Table 5-H. Initial History File Descriptor Table

Record Number	History File	Action	Disposition	Source File	When	Coverage	Repeat
00010	C30M	ADD	VOID	L15M	003	006	YES
00020	L30M	COPY	CONT	C30M	006	000	YES
00030	CHRM	ADD	VOID	L30M	006	012	YES
00040	LHRM	COPY	CONT	CHRM	012	000	YES
00050	CDAY	ADD	VOID	LHRM	012	288	YES
00060	LDAY	COPY	CONT	CDAY	010	000	NO

Scheduler Table

The Scheduler Table (SCHD) draws all the ingredients of a report together. The report type specified in SCHD provides a skeleton of the report. The report must then be provided with the measurement data from data bases. The combination of a report type and a history file uniquely define a report. With all the ingredients for report generation defined in HFDT, UVDT, and EXCP, one may compose a report by properly combining the ingredients in an entry in the SCHD. The name of the report, representing the entry, is defined by the user. An entry in the SCHD consists of several fields:

a. **Report name:** The name specified to represent the entry in the SCHD.

b. **Destination:** Represented by an output class number.

c. **Report type:** Representing a report generator to be used.

d. **History file:** Drawn from the HFDT.

e. **View name:** Drawn from the UVDT.

f. **Group name:** Drawn from the EXCP. This entry is blank, if the report is not an exception report.

g. **Activation time:** Represents the time the report begins generating. This field is only valid for scheduled reports (when repeat does not equal zero).

h. **Repeat:** Specifies how many times the report should be generated per day. If repeat equals zero, the report is generated upon demand only.

i. **Print if empty:** Specifies whether or not to print certain reports if they are empty (contain all zeros).

j. **Output type:** Specifies how the report should be output:
   1. Polled - output to a file
   2. Autonomous - output to a spooler output class
   3. Both - output to a file and a spooler output class.

k. **Output delay** - specifies the amount of time (in seconds) that a report should be delayed before being output (maximum 5 minutes).

Every entry in the SCHD is labeled with a report name. This item is defined by the user and is used for any future reference of the entry. A skeleton of the report is defined by the report generator specified in the report type field. There are different report generators for different types of reports, and each report generator has a specific use. Each of the five standard reports has its own fixed format report generator. These fixed format report generators only generate the desired output when used with their particular user view. There are also four flexible format report generators available for user-defined reports. Yet, each of these also has a specific use. Their use depends on the type of measurements, exception or regular, contained in the report and the source of the measurement values (core memory, lpm or disc memory, history files). A listing of the valid report generators and their characteristics is provided in Table 5-I.

For every report generated by the MOCT, there must be a view defined for it in the UVDT. Only those measurement IDs listed in the view are included in the report. If the SCHD entry is an exception report, the user must enter the group name in the EXCP which contains the required list of the measurement IDs and their thresholds in addition to the user view. A view in the UVDT serves as a screen over a history file. Where history files contain all measurements, only those listed in the user view are included in the report.

Table 5-I. Report Generators

Report Generator	Report Format	Measurement Type	Source
AM30MPR	Fixed	Exception	Disk
AMMPR	Fixed	Regular	Disk
AMSEPR	Fixed	Regular	Disk
AMSNPR1	Fixed	Regular	Disk
AMSNPR2	Fixed	Regular	Disk
CMRINGEX	Fixed	Exception	LPM
CMNFLPM	Flexible	Regular	LPM
CMNFDISK	Flexible	Regular	Disk
CMNFLPMEX	Flexible	Exception	LPM
CMNFDISKEX	Flexible	Exception	Disk

The "**repeat**" field is used to determine whether an SCHD entry is a scheduled report or a demand report. If repeat field is set to 0, the report is generated on demand only. The user only receives a demand report when a report is requested, which should only be if the user knows how to use the report and needs the report. To demand a report, a valid entry must first be placed in the MOCT. The user can then demand the report at any time using the OP:SMR command as outlined in the *Input/Output Manual*. If repeat field is greater than 0, the report is scheduled. The activation time is then used to determine when the report can begin being generated. The SCHD is scanned every time a history file is completely updated. If the history file used by the SCHD entry is a 30-minute file, then the report is generated every 30 minutes for as many times as is noted in the "**repeat**" field. If the "**repeat**" field equals four and the history file is a 30-minute file, then a report is generated four times, separated by 30 minutes each time. Thus, this example covers 2 hours of data. Should the entry in the "**repeat**" field be 1, then the report is generated once a day, at the time specified in the activation field.

The actual output of the report can be done in different ways. Using the "**output type**" field, the user can specify that the report be output to a spooler output class specified in the "**destination**" field, to a file, or both. The user can prevent a report from being output when all of its measurements equal zero via the "**print if empty**" field. The output of a report can be delayed up to 5 minutes by specifying the delay time (in seconds) in the "**output delay**" field. Delaying the output of a report could help prevent spooler congestion at peak periods of spooler use.

The following is an example of six sample entries in the SCHD. The first four of these entries are scheduled reports, while the last two are demand reports.

REPORT NAME	DEST	REPORT TYPE	VIEW NAME	HIST FILE	ACT TIME	GROUP	RPT	PRINT EMPTY	OUT TYPE	DELAY
SC30MPR30	42	SM30MPR	SC30MPR	L30M	0000	SC30MPR30	048	YES	A	000
SCSNPR1HR	42	SMSNPR1	SCSNPR1	LHRM	0000	NULL	024	YES	A	000
SCMPRLDAY	41	SMMPR	SCMPR	LDAY	0000	NULL	001	YES	A	000
REPORT_XX	50	CMNFLPMEX	VIEW_XX	LPM	0000	GROUP_XX	288	YES	A	000
SCSEPRHR	96	SMSEPR	SCSEPR	LHRM	0000	NULL	000	YES	A	000
REPORT_YY	152	CMNFLPM	VIEW_YY	LPM	0000	NULL	000	YES	A	000

The first entry in the report example is a scheduled report named **sc30mpr30**. The report name is defined by the user and assigned in SCHD. The measurements which comprise this report are recorded in the user view sc30mpr. Since this is an exception report, the thresholds are assigned to the measurement IDs in the exception group sc30mpr30. The actual values for the specified measurements are drawn from the history file l30m which covers 30 minutes. The report is generated the first time l30m is updated after 00:00 network time and at each 30-minute increment after that throughout the day. The initial report time is determined by the activation time while the repetition has several inputs. The report is generated in 30-minute intervals because l30m is a 30-minute history file as defined in HFDT. The report is repeatedly generated throughout the day because the value entered in the "**repeat**" column encompasses every 30-minute increment available in a day. Once all the ingredients are collected, they are sent to the report generator sm30mpr. The report generator creates the report and sends it to the specified destination 042. The devices assigned to this destination are defined by the output class number in UNIX RTR Equipment Configuration Data (ECD).

The second entry in the example is a scheduled report named **scsnpr1hr**. The measurements which comprise this report are recorded in user view scsnpr1. Since none of the measurements contained in scsnpr1 is exception related, there is a null entry for the group name. The measurement values are drawn from the history file lhrm which covers one hour. Since the history file's coverage is an hour, the report is repeated throughout the day in 1-hour increments. It is repeated all day starting at 01:00 and ending at midnight because the 024 entry in the "**repeat**" column encompasses the entire 24-hour period of a day. Once all the ingredients are collected, they are sent to the report generator smsnpr1. The generated report is then forwarded to the specified destination 042.

The third entry in the example is for a scheduled report named **scmprlday**. The measurements which comprise this report are recorded in the user view scmpr. Since none of the measurements contained in scsnpr1 are exception related, there is a null entry for the group name. The measurement values are extracted from the history file lday which covers a full day. The report is only generated once a day after 00:00 network time as defined by the "**activation**" and "**repeat**" fields. The ingredients are collected and the report is generated by the report generator smmpr. The final output of scmprlday is then sent to the devices assigned to destination 041 as defined by the output class number in the UNIX RTR ECD.

The fourth entry in the example is for a scheduled report named **report_xx**. The measurements which comprise this report are recorded in the user view "view_xx." Since this is an exception report, the thresholds are assigned to the measurement IDs in the exception group "group_xx." The measurement values are drawn from lpm which covers the smallest collection period available (5 minutes). The first exception report is generated at 00:00 network time. Since the history file covers 5 minutes and the entry in the "**repeat**" column is 288, the exception report is created after each 5-minute time period in a day. Each of these 5-minute exception reports is generated using the report generator cmnflpmex and directed to the devices assigned to the destination 50 as defined by the output class number in the UNIX RTR ECD.

The fifth entry in the example is a demand report named **scseprhr**. Since there is a zero entry in the repeat field, the report is not scheduled and therefore is not generated unless it is demanded by the user. The measurements which comprise this report are recorded in the user view scsepr. Since none of the measurements contained in scsepr is exception related, there is a null entry for the group name. The measurement values are drawn from the history file l30m which covers 30 minutes. The destination listed in the entry is not used. When the report is demanded, it is generated by smsepr and sent to the user demanding the report.

The sixth entry in the example is a demand report named **report_yy**. Since repeat equals zero, this report is not generated unless a user demands it. The measurements which comprise this report are recorded in the user view "view_yy." Since none of the measurements contained in "view_yy" is exception related, there is a null entry for the group name. This demand report extracts its measurement values from lpm which covers a 5-minute time period. The destination listed in the entry is not used. When the report is demanded, it is generated by cmnflpm and sent to the user demanding the report.

The report name, report type, view name, history file, activation time, repeat, and delay values for the initial scheduler table (SCHHD) are identified in Table 5-J.

Table 5-J. Initial Scheduler Table (Notes 1 through 4)

Report Name	Report Type	View Name	History File	Act Time	Repeat	Delay
A30MPR30	AM30MPR	A30MPR30	L30M	0000	048	060
AMPRCDAY	AMMPR	AMPR	CDAY	0000	000	000
AMPRHR	AMMPR	AMPR	LHRM	0000	024	120
AMPRLDAY	AMMPR	AMPR	LDAY	0000	001	120
ASEPRCDAY	AMSEPR	ASEPR	CDAY	0000	000	000
ASEPRHR	AMSEPR	ASEPR	LHRM	0000	024	180
ASEPRLDAY	AMSEPR	ASEPR	LDAY	0000	001	180
ASNPR1CDAY	AMSNPR1	ASNPR1	CDAY	0000	000	000
ASNPR1HR	AMSNPR1	ASNPR1	LHRM	0000	024	240
ASNPR1LDAY	AMSNPR1	ASNPR1	LDAY	0000	001	240
ASNPR215	AMSNPR2	ASNPR2	L15M	0000	000	000
ASNPR2CDAY	AMSNPR2	ASNPR2	CDAY	0000	000	000
ASNPR2HR	AMSNPR2	ASNPR2	LHRM	0000	024	300
ASNPR2LDAY	AMSNPR2	ASNPR2	LDAY	0000	001	300
MEASLFT15	MEASLFT	LFTADM	L15M	0000	096	000
NFDISK	CMNFDISK	NFDISK	L15M	0000	000	000
NFDISKEX	CMNFDISKEX	NFDISKEXHR	L15M	0000	000	000
NFLPM	CMNFLPM	NFLPM	LPM	0000	000	000
NFLPMEX	CMNFLPMEX	NFLPMEXHR	LPM	0000	000	000
RINGEXLPM	CMRINGEX	RINGEXLPM	LPM	0000	288	000
SLMLFTLDAY	SLMLFT	LFTADM	LDAY	0000	001	000

Notes:

1. GROUP NAME is initially set equal to the VIEW NAME for A30MPR30, for A30MPR30, NFDISKEX, NFLPMEX, and RINGEXLPM. It is initially null for all other reports.
2. DESTINATION designation is 64 for all reports.
3. PRINT EMPTY designation is **YES** for all reports.
4. OUT TYPE designation is **A** for all reports.

MOCT Interaction When Generating Scheduled Reports

The generation of scheduled reports begins in the HFDT. As measurements are collected, the lpm file is updated. Each time the lpm file is updated, SCHD is scanned to see if any of its entries use the lpm file. Therefore, SCHD is scanned every 5 minutes. Of those entries using the lpm file, SCHD checks to see if the activation time is past. If the activation time is past, SCHD checks to see if the report has been generated as many times that day as the repeat value specifies. If not, the report is generated. The SCHD table draws the ingredients it needs from the lpm file, the user view, and the exception group specified in the entry.

The lpm file is then used to update the history file l15m. Each time the l15m file is updated, SCHD is scanned for its use of that file. Of those entries using the l15m file, SCHD checks to see if the activation time is past. If the activation time is past, SCHD checks to see if the report has been generated as many times that day as the repeat value specifies. If not, the report is generated. The SCHD table draws the ingredients it needs from the l15m file, the user view, and the exception group specified in the entry.

The l15m file is now used to update the history files in the HFDT. Each time an updated current file is copied into another file, the "**disposition**" field is checked. If the "**disposition**" field entry is continue, SCHD is scanned for the use of the updated file. This process begins with the copy of the c30m file to the l30m file. If the "**disposition**" field entry is continue, SCHD is scanned to see if any of its entries use the l30m file each time the copy occurs. Of those entries using the l30m file, SCHD checks to see if the activation time is past. If the activation time is past, SCHD checks to see if the report has been generated as many times that day as the repeat value specifies. If not, the report is generated. The SCHD table draws the ingredients it needs from the l30m file, the user view, and the exception group specified in the entry.

The l30m file is used to update the chrm file. Once the chrm file is completely updated, it is copied into the lhrm file. If the "**disposition**" field entry is continue, SCHD is scanned for the use of the lhrm file. Of those entries using the lhrm file, SCHD checks to see if the activation time is past. If the activation time is past, SCHD checks to see if the report has been generated as many times that day as the repeat value specifies. If not, the report is generated. The SCHD table draws the ingredients it needs from the lhrm file, the user view, and the exception group specified in the entry.

The lhrm file is used to update the cday file. Once the cday file is completely updated, it is copied into the lday file. If the "disposition" field entry is continue, SCHD is scanned for the use of the lday file. Of those entries using the lday file, SCHD checks to see if the activation time is past. If the activation time is past, SCHD checks to see if the report has been generated as many times that day as

the repeat value specifies. If not, the report is generated. The SCHD table draws the ingredients it needs from the lday file, the user view, and the exception group specified in the entry.

Maintenance Guidelines

6

Contents

Contents

Maintenance Guidelines

6

Introduction

The CNI ring maintenance includes both preventive and corrective maintenance tools. Preventive maintenance in a CNI office environment ensures that basic procedures are used to detect potential troubles and maintain normal system operation. Corrective maintenance provides for trouble detection, service recovery, trouble notification and verification, trouble isolation, and repair. Maintenance must be performed to preserve as much machine sanity as possible while operating in fault situations.

Common Network Interface Ring Maintenance Description

All ring nodes are constructed of hardware that perform specific functions. The hardware that controls the logic and processing functions of the ring node is identified as the node processor (NP) circuitry. The hardware that interfaces the node processor (NP) to the ring is identified as the ring interface (RI) circuitry. There are two types of ring interface circuitry RI0 and RI1. *The node processor (NP) and ring interface (RI) circuitry combined are referred to as a ring node.*

Ring nodes are connected serially via a data bus to form the ring. Ring 0 and Ring 1 are independent of each other. Ring 0 is normally used for traffic and message handling and is the ACTIVE ring. Ring 1 is the STANDBY ring and is normally used to carry maintenance messages. The rings propagate data in opposite directions and are designed so that faulty equipment may be temporarily removed from the active system. A special message called the "token message" travels around each ring and allows other messages to be placed onto the ring without causing congestion. Each RI has a pair of

independent ring access circuits (RACs) which allow messages to be placed onto, removed from, or passed along a specific ring. Data on the ring is passed from one RAC to the next in an asynchronous fashion to assist in assuring proper ring operation (Figure 6-1).

Ring nodes (RNs) are peripheral processors where digital information enters or leaves the ring or is processed further. Ring nodes are classified into different types, depending upon their function:

- Application link node (LN)
- Ring Peripheral Controller Node (RPCN)
- Direct Link Node (DLN).

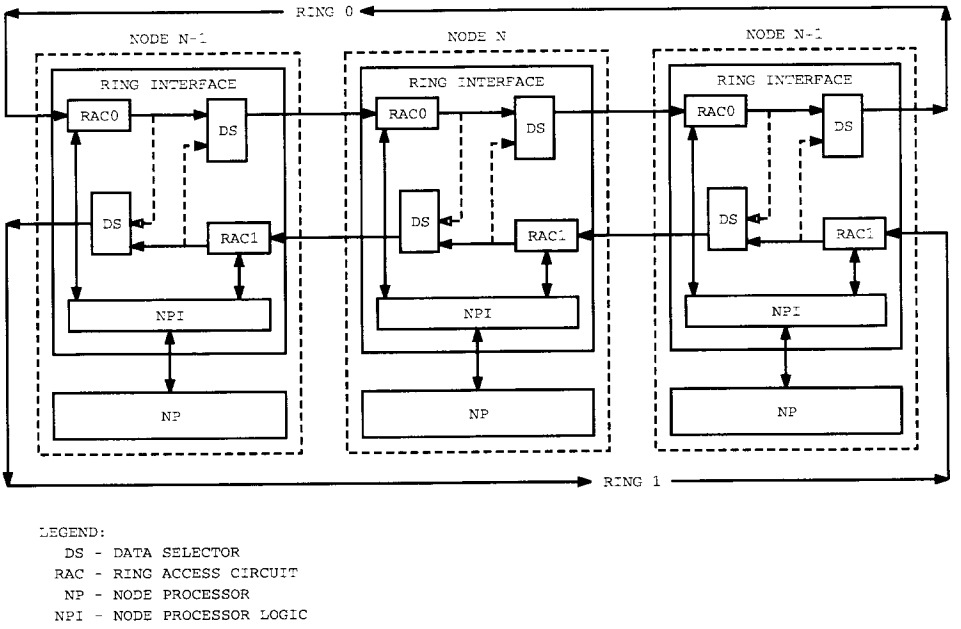


Figure 6-1. Common Network Interface Dual Ring Structure

Application LNs, RPCNs, and DLNs are constructed using circuit packs and are located in the ring node cabinet (RNC).

An *application link node* consists of a node processor (NP), two ring interface (RI0 and RI1), and link interface (LI) circuit packs, and is located on the ring where user information enters or exits via a signaling link to be processed. It is responsible for detecting and reporting ring, node processor, and link interface failures to the 3B20 Duplex (3B) Computer. The Common channel signaling (CCS) node is an example of a specific application link node. The *SS7* node provides a ring interface for the common channel signaling network.

The *RPCN consists of a NP, two RI (RI0 and RI1), a 3B Computer interface (3BI), and a dual duplex serial bus selector (DDSBS) circuit pack (Figure 6-2), and is located on the ring. This node is used to remove digital information from the ring and then transfer the digital information to the 3B Computer for farther processing or to enter information back onto the ring after processing. It is also responsible for detecting ring failures and reporting them to the 3B Computer for analysis. In some failures, the RPCN autonomously attempts recovery. However, severe failures require the aid of the 3B Computer.*

The *DLN* is a node on the ring used to process special application messages. The DLN sends and receives applicable signaling messages to and from the 1A/1B Processor Attached Processor Interface (API) circuitry via 3B Computer direct memory access (DMA) buffers. It is also responsible for detecting ring, NP, and application processor circuitry failures, and reporting them to the 3B Computer. Two DLNs are provided in a dual active/standby mode in order to circuit pack (Figure 6-2). Although the DLN is functionally more like an application LN, with the exception of direct memory access (DMA) abilities, it consists of the same circuit packs used in a RPCN plus an attached processor (AP) circuit pack. The enhanced direct link node (DLNE) operates in a similar manner as the DLN. An increased traffic handling capability is made possible by using AP/LI (LI4E) board instead of the API. The LI portion of the board is not used. The standard configuration consists of two to four DLNEs per office.

The CNI hardware and software contains logic for detecting faulty equipment. Upon detecting such equipment, the 3B Computer can remove the equipment from service, configure the ring around the faulty equipment, diagnose, and restore the equipment to service. Equipment failures associated with the ring are grouped in the following 4 major failure classes:

- Ring down
- Multiple node isolation
- Single node isolation
- Node out-of-service (OOS) - quarantined.

The *ring down* failure is a state in which the ring is unable to handle traffic. In this state, communication with the 3B Computer, except for maintenance purposes, and other nodes on the ring is lost. All LNs are in the OOS state, and all ring peripheral controller nodes (RPCNs) are in the OOS maintenance state. The RPCNs are left in this standby state to eliminate the need to restore them if service can be restored. This state affects all system operations; therefore, the problem must be corrected as soon as possible.

A *multiple link node isolation* failure is a condition in which there are two or more failures that occur on the ring, causing a potentially large isolated segment. When there is an isolated segment of multiple nodes with an established BISO and EISO node, the most probable faulty node(s) are the isolated nodes adjacent to the beginning of isolation (BISO) and end of isolation (EISO) nodes. This is assumed because both the BISO and EISO nodes of a multiple node isolation are most likely to be established adjacent to the faulty node when attempting to recover from ring error conditions. Therefore, by troubleshooting the nodes adjacent to the BISO and EISO nodes, faults are corrected with the least amount of time and service interruption.

A *single node isolation* failure is a condition on the ring where a node has been placed in the out-of-service isolated (OOS-ISO) maintenance state. A node in this state has been isolated from the active ring. The node in isolation is enclosed by a BISO and an EISO node. Single node isolation can be caused by faulty node processors (NPs), ring interface (RI), link interfaces, interframe buffers (IFBs), cabling and/or backplane faults. The node in isolation should first be diagnosed, faults corrected, restored to service, and included back into the active ring. An isolated link node is a serious problem; immediate action must be taken to correct the problem.

A *link node out-of-service* failure is a condition on the ring where a node is removed from active service and placed in the OOS state for various reasons. A link node may be placed in either of the OOS maintenance states (OOS-NORM or OOS-ISO). When a node is placed in the OOS-ISO state, the node is first removed from service (OOS-NORM), and then isolated from the active ring (OOS-ISO). When a node is removed from service for maintenance or faults that do not interfere with system operations, the node is placed in the OOS-NORM state. A node in the OOS-ISO state is not able to communicate with the ring or perform normal node functions. However, a node in the OOS-ISO state is capable of performing and handling maintenance functions. In the OOS-NORM state, the node is quarantined and not allowed to communicate with either the 3B Computer or the ring.

When failure conditions are detected on the ring, the affected equipment is removed from service and grouped in one of the four failure classes described above. It is also possible to remove one or more nodes from service or to configure the ring via input commands from the maintenance CRT (MCRT).

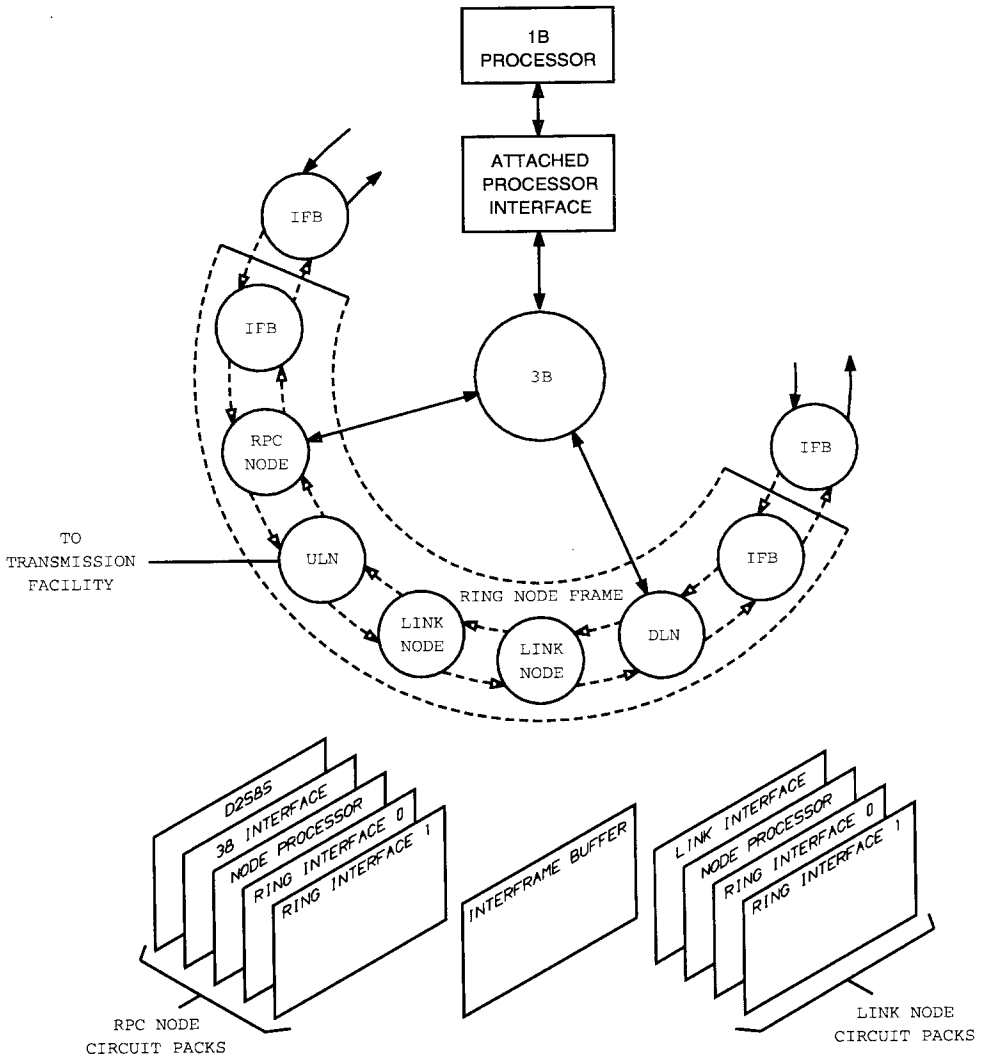


Figure 6-2. Common Network Interface Link Node Architecture

Ring and Ring Node Operation

Message Propagation on the Ring

In a fully operational ring (all 3B Computer equipment and link nodes functioning), a message arrives at the link node, is processed in the link interface and node processor circuitry, is placed onto the normal traffic ring (Ring 0), and is then passed to the destination node using the assigned address. The message reaches the destination node, is processed by the node processor circuitry and is then transmitted to the link interface as outgoing messages on the link. Thus, each node must be able to propagate messages from one node to the next on both rings (0 and 1) for a ring to be fully operational. In addition, each node must be able to transmit and receive messages.

The source ring access circuit (RAC) transfers messages, one byte at a time, to the next RAC on the ring. The destination address is compared to that node's address, and if the address fails to match, the message is sent to the next RAC. This transfer from RAC to RAC continues until the message reaches the node address which matches the message destination address.

The token message continuously travels around the ring and allows messages to be placed on the ring without causing congestion. When a node is ready to place a message onto the ring, it must wait for the arrival of the token message at the output of the previous node. When instructed to do so by the node processor, the RAC detains the token at the output of the previous RAC and allows the message(s) to be placed onto the ring. When the transfer is complete, the token is allowed to proceed to the next node on the ring.

Node Addressing

A message which contains the address of both the source and destination nodes is placed on the ring via the node's RAC. The addressing of nodes on the ring are identified in terms of an integer sequence number. Nodes are interconnected so that any downstream node on Ring 0 has a higher sequence number, and any upstream node has a lower sequence number, except at the junction of the highest and lowest numbered cabinet. Addresses only have hardware and software significance and are invisible to the user. The physical ring identification is interpreted by software and presented to the user as *RPCNxx 0* or *LNxx y*, depending on the node type. The *xx* identifies the group number and the *y* identifies the node member number—position in the cabinet.

Example: RPCN00 0

LN00 12

LN32 15

Addresses are assigned consecutively to RPCNs and LNs. To calculate the address of any RPCN, multiply the group number by 16. For example, the address for RPCN in group 32 is 512 (16 x 32 = 512).

The LN addresses are calculated by multiplying the group number by 16 and adding LN member number. For example, the address for LN 15 in group 32 is 527 (16 x 32 + 15 = 527).

Ring Configuration and Isolation

Ring Configuration

During normal operating and traffic handling conditions, there are two separate rings. If trouble is encountered on either ring and Automatic Ring Recovery (ARR) cannot correct it, the ring is reconfigured by the 3B Computer to isolate the faulty segment. Each RAC has a data selector at its output that allows data to be directed to the mate ring. At the node preceding the faulty segment, the output of Ring 0 is redirected to the input of Ring 1. This results in one continuous ring excluding the faulty segment (Figure 6-3). The maintenance messages, on the standby ring, consume a small amount of space and do not reduce ring message capacity during ring configuration.

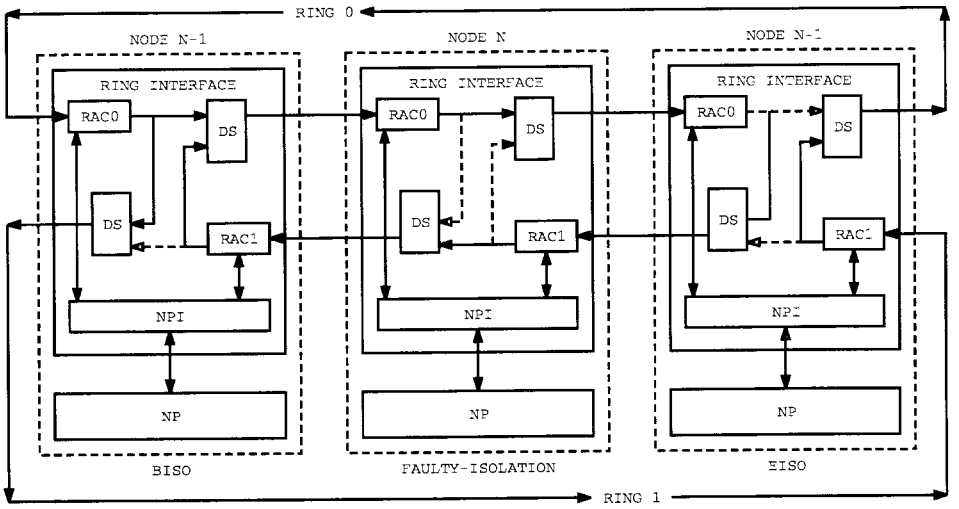


Figure 6-3. Common Network Interface Ring Structure During Isolation

User input commands are used to manually include or exclude a node on the active ring. The **CFR:RING;INCLUDE** command is used to include ring nodes on the active ring. With the use of this command, only the nodes that are specified are included on the active ring segment. If no nodes are specified with this command, then all nodes in the appropriate maintenance state that are not in the active ring segment at the time of the request are included on the active ring. The **CFR:RING;EXCLUDE** command is used to isolate specified nodes from the active ring segment. This command may cause the isolation of other nodes to form a workable ring. The ring cannot be reconfigured using the INCLUDE or EXCLUDE options if either the current beginning of isolation (BISO) and/or end of isolation (EISO) nodes are not active. A ring with an inactive BISO and/or EISO node is in a transient state, and restoral of this node is given top priority.

Ring configuration is requested either automatically or manually. When faults are detected on the ring that involve ring interfaces, the 3B Computer automatically reconfigures the ring around the faults. Manual configuration, using the **CFR:RING** commands, is used to create an isolated segment on the ring to configure the ring around faults. Manual configuration requires that nodes be already removed from service when the they are to be isolated. If the nodes are not removed from service the configuration request will be denied.

On a small ring, automatic ring error analysis cannot always determine which of the two adjacent nodes is at fault. When this occurs, the **CFR:RING;MOVFLT** command is used to correct ring configuration. The command initiates a requests to move an indication of a faulty ring interface from the currently isolated ring node to the adjacent ring node and reconfigure the ring so that the new node becomes the isolated node.

Ring Isolation

An isolated segment on the ring consists of one or more nodes (RPCNs or LNs) that are not permitted to handle traffic or messages, or allowed to communicate with the 3B Computer except for maintenance purposes. When an isolated segment is created on the ring, two boundary nodes identified as the BISO and EISO nodes are established to distinguish this segment of the ring. The *BISO* node is the node in the active segment that is adjacent to the faulty or isolated segment.

An *EISO* node is the node in an active segment that is adjacent to the end of the isolated segment. The BISO and EISO nodes are not faulty nodes. They serve to identify the isolated segment and are also used to direct maintenance messages in and out of the isolated segment (Figure 6-3).

Nodes within an isolated segment are classified into two categories. These are faulty nodes and nonfaulty nodes. An isolated segment can have single isolated nodes or a multitude of nodes. When there is a fault on the ring that causes an isolation, the BISO and EISO nodes are established. Later, if this isolation is not cleared and another fault develops, the ring again reconfigures, creating a new

isolated segment containing the original faults and the last faults detected. When the ring reconfigures the second time, the BISO and EISO nodes can change, depending on the location and direction of the second fault. When a new BISO or EISO node is created, the new BISO or EISO node must be a fully operational node in the AVAIL or OOS state.

When a BISO or EISO node is diagnosed, a request is made to remove the node from service. This request may be accepted or denied. If the system denies permission to diagnose the BISO or EISO, then, unless absolutely necessary, the system should not be forced into this condition (diagnosing, configuration, etc.).

When a DLN failure occurs, the failure is detected by either the 3B Computer or the neighbor node audit which in turn isolates or quarantines the DLN from the ring. Messages are routed to the standby DLN when this condition occurs. The 3B Computer applies diagnostics to the failed DLN via access through the RPCNs and attempts to recover the DLN. An output message is received when the active DLN is or has been congested. Congestion means the DLN is at or near processing capacity and is attempting to reduce its load. The severity of the congestion is indicated by the output message. This message has no effect on ring operation; but if it appears consistently, technical assistance should be obtained.

Maintenance Functions, Hardware, and Equipment

Ring maintenance normally involves using diagnostics to identify problems at the circuit pack level. When problems cannot be resolved using this approach, additional testing is required. To aid the user under these conditions, maintenance test equipment and hardware are utilized. This equipment includes the following:

a. A maintenance terminal (MCRT) to provide the interface and communications necessary for system control and display (C&D), input/output messages, and emergency action interface (EAI) control and display.

b. A maintenance receive-only printer (MROP) to provide hard copies of input/output messages, status report information, fault/error conditions, diagnostic results, audits, and other data.

c. Voice frequency link (VFL) test equipment and a transmission measuring set (TIMS) are used to test analog SLKs.

Equipment Handling Procedures

Specific equipment handling procedures must be observed when performing CNI ring maintenance functions. Failure to follow these procedures could result in damage to the integrated circuit packs or loss of service caused by a partially isolated or totally interrupted ring. These procedures cover the handling and replacement of all CNI equipment.

Ring Node Cabinet Circuit Pack Description

The units that make up the CNI ring are located in the ring node cabinet (RNC) and consists of the following.

- The DLN unit Ring peripheral controller node (RPCN) unit
- Link node (LN) unit (A and B)
- Direct link node (DLN) unit
- Fan unit
- Power converters
- Visual status indicators
- Internal and external connectorized cabling.

The units within the ring node cabinet house individual circuit packs which provide the circuitry for specific nodes. A RPCN unit is equipped with one RPCN and up to two application link nodes. The RPCN is used to remove information from the ring and transfer it to the 3B Computer for processing or

return processed information back onto the ring. All ring node cabinets are equipped with an RPCN. The RPCN consists of the following circuit packs:

- Dual Duplex Serial Bus Selector (DDSBS) -- TN69B
- 3B Computer Interface (3BI) -- TN914
- Node Processor (NP) -- TN913 or TN922
- Ring Interface 0 (RI0) -- UN122, UN122B or UN122C
- Ring Interface 1 (RI1) -- UN123 or UN123B
- IRN/IRN2 - UN303B or UN304B.

A link node unit can be equipped with up to three application link nodes. Link node units are designated as A or B. Link node unit A houses nodes within the ring node cabinet that are identified and addressed from left to right; whereas, link node unit B houses nodes that are identified and addressed from right to left. This node identification and addressing sequence has been implemented to allow the output of a link node, unit A, to be directly connected to the input of a link node, unit B; and the output of that link node, unit B, to be directly connected to the input of another link node, unit A. The basic application link node can contain the following circuit packs:

- Ring Interface (RI0) -- UN122, UN122B or UN122C
- Ring Interface (RI1) -- UN123 or UN123B
- Node Processor (NP) -- TN913 or TN922
- Link Interface (LI) -- TN916 (LI), TN1315 (LI4D), TN1316 (LI45), or TN1317
- T1 Facility Access (T1FA) -- UN291
- IRN/IRN2 -- UN303B or UN304B.

The DLN unit is equipped to house one DLN and up to two application link nodes. The DLN is used to normally process signaling messages to and from the 3B Computer. Although the DLN is functionally more like a link node, it consists of all circuit packs that make up a RPCN plus an attached processor (AP). The DLN consists of the following circuit packs:

- Dual Duplex Serial Bus Selector (DDSBS -- TN69B
- 3B Computer Interface (3BI) -- TN914
- Node Processor (NP) -- TN913 or TN922
- Ring Interface 0 (RI0) -- UN122, UN122B, or UN122C
- Ring Interface 1 (RI1) -- UN123 or UN123B

- Attached Processor (AP) -- AP30 - TN1630B for DLNE or TN1630 for DLN30
- IRN/IRN2 -- UN303B (for DLNE) or UN304B for DLN30.

In addition to RPCN, DLN, and application link node circuit packs, the ring node cabinet also houses interframe buffer (IFB) circuit packs. The IFBs provide buffering circuitry between nodes in different ring node cabinets. There are two types of IFBs:

a. Padded IFBs (IFB-P) -- TN915

b. Unpadded IFBs (IFB-U) -- TN1508

Power Descriptions

The power converters, located in the power distribution frame and each individual CNI equipment frame provide, the necessary power required for CNI system operations. Fan units provide the necessary equipment cooling.

Power Distribution

The CNI system requires a power plant with a single point ground to isolate all equipment from building ground. A -48V power supply is used to supply all load units associated with the CNI ring. Each cabinet power feeder powers one unit. A single 495FA power converter is used to supply power to link nodes within the unit. This minimizes the number of nodes that fail due to a single converter failure. Each RPCN is powered from a single converter. The link interface and node processor are not powered by separate converters.

The digital facility access (DFA) cabinet power is diversified in such a way that in case of a fuse failure, only half of the units are lost.

Fuse Description

System interruption and/or the loss of nodes may be caused by the loss of a 10 amp fuse located in the ring node cabinet or a 20 amp fuse located in the power distribution frame (PDF). System interruptions may also be caused by the loss of a 250 amp fuse in the battery plant. The loss of the 20 amp fuse in the power distribution frame causes a failure to one half of the nodes in all shelf units. However, if the 250 amp fuse that is associated with the battery plant is lost, total service is adversely affected. When problems occur with fusing, an alarm is triggered; the problem must be corrected as soon as possible. In addition, the digital facility access (DFA) and analog facility access (AFA) cabinets contain fuses and power failure circuitry.

Fan Unit Description

The fan unit assemblies contain three fans and monitor circuitry to monitor each fan. Each fan is powered through individual fuses. The fuses are in a panel

located at the base of associated cabinets. The fan unit assemblies are located in the bottom of all cabinets to force cooled air up through the units to maintain the proper operating temperature. Cabinets should be able to function properly with the loss of one fan; but with the loss of two fans, the equipment rapidly overheats. If there is only one operational fan in a cabinet and there are no office spares, a fan must be taken from another cabinet and placed in the faulty unit. It is imperative that each cabinet have at least two operational fans. It is also recommended that the office have two spare fans.

Fan Maintenance

When a fault is detected in one of the fans, the fan alarm (ALM) lamp, on the unit, and the power alarm (PWR ALM) lamp, at the control panel, illuminate. Because the fans are used to cool cabinet equipment, corrective action must be taken as soon as possible when faults occur. The fans should be checked for proper operation every 6 months. Each fan unit assembly is equipped with a removable wire mesh air filter.

Filter Maintenance

The air filters are intended to eliminate dust from the cooling air. Dust buildup on frame circuitry could lead to improper system operation. Although no alarms are associated with the fan filters, they must be properly maintained by cleaning or replacing the filters every 6 months.

The filters are positioned horizontally, just above the fan unit in the cabinet. To replace the fan filter, simply pull the old filter from the front of the frame; remove the handle from the old filter, and attach it to the new filter; then slide the new filter, with handle, back into the frame.

Circuit Pack Handling Precautions

Before any maintenance procedures are performed on a functional ring, certain equipment handling precautions must be observed. Before removing, installing, or handling any circuit pack, proper personnel grounding techniques must be made to avoid further damage to the equipment. If a proper ground is not made before handling equipment, static electricity may damage it. To avoid the possible damage caused by the discharge of static electricity, a static control wrist strap must be worn when handling equipment. The wrist strap is used by connecting the clip lead to a nonelectrical metallic portion of the cabinet and placing the strap around the wrist. The wrist strap must be worn at all times when handling new or old equipment.

New circuit packs are always wrapped in a antistatic protective wrapper to avoid static discharge damage. Therefore, when handling new circuit packs, keep the circuit pack enclosed in the static proof wrapper until the appropriate ground connections are made and the pack is ready to be installed. When handling old or defective circuit packs, the same static discharge precautions must be observed to prevent further damage to the pack. The old or defective circuit pack

should be wrapped in the protective wrapping and returned for repair. Always include diagnostic failure information with the defective circuit pack.

When a circuit pack or other equipment is removed for inspection or replacement, connections must be checked to assure that backplane pins are not damaged. Use care when handling circuit packs. Some circuit packs require considerable force to remove and insert.

Circuit Packs and Fans

There are times when diagnostics and circuit pack replacement does not correct a problem. When this occurs, it may be necessary to check the backplane wiring, pins, and other connections for shorts or other faults that could interrupt normal system operation.

Some circuit packs contain LEDs which indicate their status or the status of the ring. The circuit packs are designed to be removed and/or replaced without powering down. Before removing any circuit pack be sure to verify its status. A wrist strap must be worn to guard against electrostatic discharge, when replacing circuit packs. No circuit pack should be removed or replaced in the system unless appropriate LEDs are illuminated.

The ring node cabinets (RNCs) contain a fan unit. The fan unit contains three -48V DC fans to provide forced air cooling for the electronic components in the cabinet. Each fan is equipped with a connector to facilitate replacement if a fan fails. In the event of fan failure, a door closes automatically to minimize air leakage from the inoperative fan opening. When a fan fails, it should be replaced before another fan or system operation is affected.

Equipment Visual Indicators

Most equipment have visual indicators that indicate faulty or out-of-service (OOS) states. These indicators show the status of many maintenance functions. Indicators found on the node processor (NP), ring interface (RI), integrated ring node (IRN/IRN2), attached processor (AP), and link interface (LI) circuit packs are the ring quarantine (RQ), ERROR and no token (NT) lamps.

The RQ lamp is located on the NP, IRN/IRN2, and the LI4 circuit packs. This lamp indicates that either the NP or one of the LI circuit packs is presently in the OOS maintenance state but is still part of the active ring. The NT lamp is located on the RI, IRN/IRN2, circuit pack and indicates that there is no token message transversing around the ring. When the NT lamp is illuminated, any circuit pack may be removed from that node without affecting system operation. A red LED is used on the AP circuit pack to indicate an error.

The PWR ALM lamp illuminates on the cabinet control panel when there is a fuse failure, a power converter is unplugged, or a fan failure occurs. If more than one fan fails, a major alarm sounds.

Before any interframe buffer (IFB) circuit pack can be replaced, the NT lamp on both adjacent nodes must be illuminated. There are only two IFBs per ring node cabinet, and they are located before the first and after the last node in the cabinet. Since an IFB is adjacent to one node within its own ring node cabinet and another node in the next ring node cabinet, the NT lamp on both nodes must be illuminated before the IFB circuit pack can be extracted.

There are three LEDs on the T1FA circuit pack. The red LED indicates a near-end facility failure, the yellow LED indicates a far-end facility failure and the green LED indicates normal operation. A red/green combination indicates a self-test failure. A reset button is also provided on the T1FA board to aid in running self-tests.

Removing Equipment From Service

Caution must be exercised when removing nodes while an isolated segment exists on the ring. Due to this action, the creation of larger isolated segments on the ring is avoided when equipment is removed from service. Therefore, all isolated segments on the ring should be corrected before other maintenance functions are performed. All affected nodes and equipment must first be removed from service before any associated equipment can be replaced.

System software may remove faulty equipment from service by taking it OOS and leaving it in the OOS-NORM maintenance state. In this state, the equipment is still part of the active ring. In addition, system software may remove faulty equipment from service and place it in the OOS-ISO maintenance state. In this state, the equipment is isolated from the active ring and is not a functional part of the ring, except for maintenance purposes.

Maintenance States

Before any manual maintenance action is invoked, ring and node maintenance states must be considered. The CNI maintenance involves both major and minor maintenance states. The following are the classes of these states:

- Ring maintenance state
- Node major state
- Node minor state: ring position
- Node minor state: NP hardware
- Node minor state: RI hardware
- Node minor state: maintenance mode.

Ring Maintenance State

The ring maintenance state defines the overall operational state of the ring. The ring maintenance state consists of the following:

a. **Ring Normal**: The ring is operating normal on a two ring configuration. There are no isolated nodes on the ring.

b. **Ring Isolated:** The ring contains an isolated segment. The nodes referred to as the beginning of isolation (BISO) and end of isolation (EISO) are active.

c. **Ring Restoring**: The ring contains an isolated segment and restoral activity is in progress. This is a transient state but can last several minutes.

d. **Ring Down**: The ring is totally unusable from the 3B Computer. However, the LNs may be able to communicate among themselves.

e. **Ring Normal-Listen**: Same as Ring Normal but in "listening" mode.

f. **Ring Isolated-Listen**: Same as Ring Isolated but in "listening" mode. This is a transient state.

g. **Ring Restoring-Listen**: Same as Ring Restoring but in "listening" mode. This is a transient state.

h. **Ring Configuring**: The ring is initializing, configuring, or fault recovery is in progress. This is a transient state.

i. **Ring Configuring-No BISO/EISO**: Same as Ring Configuring but ring is a normal two ring configuration without BISO and EISO nodes. This is a transient state.

j. **Ring Configuring-Isolated**: Same as Ring Configuring but ring contains an isolated segment. This is a transient state.

Node Major State

During normal system operation, each node is classified into one of the system major states. The major state is the same as the equipment configuration data (ECD) and shows the overall status of a node. Node major states include the following:

a. Active (ACT): The node is active and performing on-line functions.

b. Standby (STBY): If the node is an RPCN, the node is operational, but the ring configuration is not complete or the ring is down. If the node is a DLN, it is the inactive DLN and can be made active through manual or automatic intervention.

c. Initializing (INIT): The node is initializing. This is a transient state and is used to restart nodes on the ring.

d. Off-line (OFL): The node is OOS and neither restoral or removal is permitted. The node can be diagnosed and included into the active ring when appropriate.

e. Out-of-service (OOS): The node is OOS and unavailable for normal use but can be used for maintenance and diagnostic purposes.

f. Grow (GROW): The node is physically being added to or removed from the ring. The node must always be configured within an isolated segment of the ring.

g. Unequipped (UNEQ): The node is unequipped but an ECD record can exist for the node.

Node Minor State: Ring Position

The ring-position minor state indicates the position of the node, relative to the current configuration of the ring. The state values of ring positions are as follows:

a. Normal (NORM): The node is included on the active ring and is not a BISO or EISO node.

b. Begin isolated segment (BISO): The node is included on the active ring and forms the beginning of the isolated segment.

c. End isolated segment (EISO): The node is included on the active ring and forms the end of the isolated segment.

d. Isolated (ISO): The node is contained in the isolated segment.

Node Minor State: Node Processor Hardware

The node processor hardware minor state describes the node processor hardware maintenance state of a node. The node processor includes any user supplied hardware that is tested by diagnostics. The state values of the node processor hardware minor state are as follows:

a. Usable (USBL): The node processor is usable.

b. Faulty (FLTY): The node processor is known to be or is suspected to be faulty.

c. Untested (UNTSTD): The condition of the node processor is unknown.

Node Minor State: Ring Interface Hardware

This describes the ring interface hardware maintenance state of a node. The ring interface hardware state also indicates whether a node can be included on the active ring. The ring interface hardware states are as follows:

a. Usable (USBL): The ring interface hardware is usable.

b. Quarantine Usable (QUSBL): The ring interface hardware is partially usable. The node can be included on the active ring but the node must be in the quarantine (OOS) state.

c. Faulty (FLTY): The ring interface hardware is faulty and the node must be isolated.

d. Untested (UNTSTD): The condition of the ring interface hardware is unknown.

Node Minor State: Maintenance Mode "Node Minor State: Maintenance Mode"

The state of maintenance mode indicates whether automatic restoral of the node is attempted. The maintenance mode states are as follows:

a. Automatic (AUTO): The node is under automatic control.

b. Manual (MAN): The node is under manual control, and only manual-user action can restore the node to service.

Automatic Ring Recovery (ARR)

The CNI provides for fault detection and analysis that requires the removal and restoral of ring nodes. This removal and restoral of ring nodes may be accomplished either automatically or manually via input commands.

Within the CNI, problems are detected by nodes and reported to the 3B Computer through the RPCNs; the RPCNs forwards the problem to error analysis and recovery (EAR). The EAR is responsible for determining the probable cause of a fault, locating the fault, and requesting a ring configuration to remove the faulty equipment from the active ring. Traffic is routed around the affected equipment while automatic ring recovery (ARR) attempts to restore the faulty equipment.

The ARR is responsible for automatically restoring faulty nodes, innocent victim nodes, and nodes marked OOS that are found to be in the appropriate maintenance states. These maintenance states and the appropriate corresponding circuit packs are listed in Table 6-A. This table identifies treatment for all combinations of minor and ring maintenance states associated with the OOS major state.

Table 6-A. Automatic Ring Recovery Response to Isolation and CP Maintenance States

Isolated	RI State	NP State	NM State	ARR Action
Yes	FLTY, QUSBL	Any	Auto	Cond RST*
Yes	UNTSTD	Any	Auto	Cond RST*
Yes	USBL	Any	Auto	None
Yes	ANY	Any	Man	None
No	USBL	USBL	Auto	UCL RST
No	USBL	UNTSTD,FLTY	Auto	Cond RST
No	USBL	Any	Man	None
No	QUSBL	Any	Auto	Cond RST
No	QUSBL	Any	Man	None
No	UNTSTD,FLTY	Any	Any	ERRLOG, RI = QUSBL, Reprocess

* Recovery from nondeferrable removal and isolation due to problems (that is, recovery of a node with a "faulted" RI). The conditional restore requests inclusion in the ring if the RI tests pass. Usable hardware states are transient during the conditional restore.

Legend:

ARR = Automatic Ring Recovery
CP = Circuit Pack
NM = Node Maintenance
NP = Node Processor
RI = Ring Interface
RST = Restore

The ARR procedures respond to any node in the OOS major state that has not been manually placed out of service. The ARR procedures normally attempt to restore any node once. If diagnostics fail, the faulty equipment is marked faulty and manual action is required. If diagnostics are started and aborted but no test failures are indicated, the ARR procedures attempt to restore the node a maximum of three times before any manual actions are requested.

It is important to note that if equipment is automatically removed from service for fault reasons, then manual actions should be avoided until the ARR procedures have attempted to restore the equipment and identified it for manual actions. If manual actions are desired, the ARR procedures may be inhibited using the **INH:DMQ;SRC ARR** input command. When ARR procedures are inhibited, unconditional restorals are still active. Inhibiting the ARR procedures only inhibits conditional restorals.

Nodes eligible for automatic restorals are determined by priority. The priority listing and order of node restoral is as follows:

a. Nominated critical nodes (BISOs and EISOs)
b. Nodes with faulty ring interfaces
c. RPCNs eligible for unconditional restorals
d. RPCNs eligible for conditional restorals
e. LNs nodes eligible for unconditional restorals
f. LNs eligible for conditional restorals.

When diagnosing and attempting to restore nodes within an isolated segment of the ring, the ARR procedures attempt to restore the end nodes of the isolated segment. The end nodes are those adjacent to either the BISO or EISO nodes. The inner nodes of the isolated segment are called innocent victim nodes, when the inner nodes are not faulty.

Ring Node Equipment Removal

When performing CNI ring maintenance, it may be necessary to manually or automatically remove a node from the active ring. To manually remove a node from service, use the **RMV:LN** or **RMV:RPCN** input command.

There are two OOS states, OOS-NORM and OOS-ISO. When a node is found to be faulty, insane, ready to be grown/degrown, or some other manual maintenance function needs to be performed, the node is first removed from service (OOS-NORM). In this state, the node is said to be quarantined and not permitted to communicate with the ring. If a node must be isolated from the active ring, the node is first removed from service (OOS-NORM). Upon successful removal from service, the node can then be excluded from the active ring and placed in the OOS-ISO state. In either OOS, state the node is allowed to communicate with only the 3B Computer for maintenance purposes. Nodes are removed from service or removed from service and isolated automatically by EAR when faults are detected.

Link Node Removal

When a request is received to remove a link node from service, the major state of the node is checked, and an attempt is made to remove the node. If successful, the major state of the link node is changed to OOS-NORM, and the node is placed in the quarantine state. Success for removing the node from service depends on the associated application. For example, if the signaling link (SLK) is in service at the time of the request, and the mate SLK is not capable of handling the load that was handled by both links; the request may be denied. A **CHG:SLK** input command should be entered to request a change in the SLK minor state. If the request is accepted, the SLK minor state is changed to the appropriate maintenance state. Upon successful removal of the SLK, the node can be removed from service efficiently.

To successfully remove a DLN from service, the standby DLN must be able to handle the active DLN's functions. Otherwise, the remove request is denied.

Ring Peripheral Controller Node Removal

The removal of a RPCN from service follows the same rules and restrictions as specified for the removal of a LN, with the exception that removal of the last active RPCN on the ring is always denied. A **RMV:RPCN** input command is used to manually remove a RPCN from service. When a request is received to remove a RPCN from service, the major state of the node is checked and an attempt is made to remove the node. If successful, the RPCN's major state is changed to OOS-NORM, and the node is placed in the quarantine state. Success for removing the node from service depends on the traffic handling ability of the 3B Computer. If the traffic cannot be handled by the 3B Computer with the RPCN removed from service, the request is denied. Otherwise, the request is accepted.

Ring Node Equipment Restoral

Restoral of LNs and RPCNs are performed either conditionally or unconditionally. Manual restorals are accomplished using the **RST:LN** and **RST:RPCN** input commands.

Conditional Restore

A conditional restore is used to restore a ring node when problems are detected and diagnostics need to be run on the node. A conditional restore first attempts to remove the node from service if it is not already OOS and run diagnostic. If the node is not already isolated, diagnostics request the node to be isolated so that all diagnostic phases can be run. The isolation request could be denied if, for example, there is another node already isolated and the ring interface hardware state of the node, being restored, is unusable (USBL). This could lead to a CATP diagnostics result.

At the conclusion of diagnostics, a request is made to include the node on the active ring. If the ring interface hardware state is USBL or QUSBL and the overall condition of the ring allows it, the node is included on the active ring. If the diagnostic results were either ATP or CATP, the node is restored to service (node software downloaded, execution started, major state changed to ACTIVE). If the diagnostic results were STF, the restore is terminated and the node left either OOS-NORM or OOS-ISO.

Unconditional Restore

An unconditional restore is used when diagnostics have run and all problems have been corrected. Also, an unconditional restore is used when a node has been removed from service for some reason (that is, innocent victim nodes), and no diagnostics need to be performed. When this is the case and no problems are evident, the unconditional restore may be used.

Do not perform an unconditional restore unless one of the following has occurred:

a. A complete diagnostics has produced an all-tests-passed (ATP) response.
b. A complete diagnostics has produced a conditional all-tests-passed (CATP) response, and the ring interface and node processor minor states are both USBL.

The unconditional restore of a node is halted if the node major state is not OOS. If the major state is OOS, an attempt is made to include the node onto the active ring. If the inclusion fails, the restoral stops. If the inclusion is successful, the node is restored to service—pumped with operational code and placed into execution—and its major state is changed to ACT.

Office Alarms and Trouble Indications

When trouble is encountered on the active ring, the system has four methods of alerting the user. These methods are provided by audible alarms, visual alarms, visual alarms at the 3B interface (3BI), and teletypewriter (TTY) reports.

To aid the user in the maintenance activities of the office, an alarm structure has been established. Audible alarms are used to alert the user to abnormal conditions in the office. These alarms can be set by either hardware or software failures. These alarms are used to indicate a specific degree of system failure. A priority of action has been assigned for each of the major alarms. The priority of action used for output messages result in an associated level of office alarms being triggered. These office alarms and their associated priority of action are listed as follows:

a. CRITICAL -- A double stroke of the tone bar. This is set by the 3B Computer indicating a severe fault with a loss of service. The MROP indicator is * C.
b. MAJOR -- A single stroke on the tone bar. This is set by hardware or software failures indicating a major fault that can affect service. The MROP indicator is **.
c. MINOR -- This is not a service affecting alarm but indicates a minor problem in the hardware or software. This alarm is identified by a bell. The MROP indicator is *.
d. MANUAL -- This is a response to a manual request.
e. AUTOMATIC -- This is a response to an automatically generated request.
f. POWER PLANT MAJOR -- A bell that indicates a major fault in the power plant that can affect the system. There is no MROP indicator for this alarm.

An audible alarm sounds whenever any of the following conditions exist:

a. Ring access circuit (RAC) errors occur
b. IMS driver faults occur
c. Certain levels of initialization occur
d. A RPCN or LN is automatically removed from service
e. Ring faults occur
f. A fuse blows
g. A power board is removed from the 3BI unit
h. Ring is being reconfigured.

All alarms are sent to the 3B Computer. Audible alarms can be silenced by the user without correcting the fault. However, visual status indicators remain in effect until the office returns to normal operation.

To aid the user in maintenance activities, there are visual indicators associated with the alarms to assist in determining faulty equipment. These visual indicators serve as aids in determining when circuit packs and cabling can be replaced or changed without affecting system operation and function. These visual indicators are found on the following equipment:

a. Ring interface 1
b. Node processor
c. Link interface (LI4D)
d. T1FA
e. Attached processor.

A visual alarm is displayed when the system detects any of the following conditions:

a. A RPCN is automatically removed from service
b. A LN is removed from service
c. A link is removed from service
d. Ring is being reconfigured
e. Ring is down
f. A power failure.

The visual indicators are identified as the ring quarantine (RQ) lamp and the no-token (NT) lamps. The RQ lamp is located on both the node processor and link interface. When illuminated, the RQ lamp indicates that the node processor and link interface are presently in the OOS state but the node may still be on the active ring. This indicates that messages and traffic may be passing through the node's link interface to and from other nodes on the ring but data other than maintenance messages cannot be processed by the affected node. When the RQ lamp is illuminated, only the node processor or link interface circuit pack can be removed without affecting system operation.

The NT lamp is located on the ring interface 1 (RI1) circuit pack and indicates that there is no token message appearing at either ring access circuit (RAC) serving this node. When the NT lamp is illuminated, the node is OOS and in an isolated segment of the ring. In this state, all node circuit packs can be removed without affecting any additional system operations. The ring is considered inactive if a token message is not present on the ring for more than 40 milliseconds.

The NT lamps are also adjacent to nodes equipped with interframe buffers functions may require replacing IFB circuit packs or making cable changes. When IFB circuit packs are replaced, the pack should not be removed unless one of the adjacent node's NT lamp is illuminated.

NOTE:
Both NT lamps on nodes adjacent to IFB packs are not in the same ring node cabinet. Therefore, extreme caution must be taken to ensure that appropriate NT lamps are illuminated in the correct cabinets. ***This guideline must be followed to avoid affecting system operation.***

Additional visual alarms exist in the ring node cabinet when the following conditions are observed:

a. The RQ lamp illuminates on the node processor (NP) circuit pack when a RPCN is OOS or insane.
b. The NT lamp illuminates on the ring interface 1 (RI1) circuit pack when there is no token circulating on either ring. This indicates that the node is isolated or the ring is down.
c. The PWR ALM lamp lights on the control panel when there is a blown fuse or the power board is unplugged.

T1FA Maintenance

There are three LEDs on the T1FA circuit pack. The red LED indicates a near-end facility failure, the yellow LED indicates a far-end facility failure and the green LED indicates normal operation. In addition, a red/green LED combination indicates a self-test failure.

Also contained on the T1FA circuit pack is a RESET button used for running self-tests. If the RESET button is pressed, all LEDs extinguish and one of the following events occurs:

a. If a facility is connected to the T1FA and the T1FA passes self-tests, the green LED lights in approximately 4 seconds.

b. If a facility is **not** connected to the T1FA and the T1FA passes self-tests, the green LED lights in approximately 4 seconds; and after approximately an additional 4 seconds, the red LED lights and the green LED extinguishes.
c. If the T1FA **does not** pass self-tests, the red and green LEDs both light in approximately 4 seconds.

If the T1FA is functioning properly, the green LED is lit, and a near-end or far-end facility failure occurs; the red or yellow LED lights in approximately 4 seconds, and the green LED extinguishes. After the facility problem is corrected, the green LED lights in approximately 12 seconds, and the red or yellow LED extinguishes.

There are cases where a less severe trouble condition may be masked from the user by a more severe trouble condition, thus causing the less severe trouble condition not to be cleared. The following list contains trouble conditions from most severe to least severe.

CT1FAFL	T1FA hardware or firmware failure
CTREDALM	Red alarm (near-end facility failure)
CTYELALM	Yellow alarm (far-end facility failure).

Troubles reported by the CT1FAFL critical event obstruct the sensing of all less severe trouble conditions, and troubles reported by the CTREDALM critical event obstruct the sensing of the trouble conditions reported by the CTYELALM critical event. As an example, if a yellow alarm condition exists and a red alarm condition occurs before the yellow alarm condition is cleared, visibility of the yellow alarm is lost. If the red alarm condition is cleared and the yellow alarm condition is also cleared, only the CTREDALC (red alarm cleared) critical event message is issued. If the red alarm condition is cleared and the yellow alarm condition still exists, the yellow alarm condition is again reported with a CTYELALM critical event message. If a yellow alarm condition occurs after a red alarm condition occurs, the yellow alarm condition is not reported until the red alarm condition is cleared, assuming the yellow alarm condition still exists.

Trouble Indicators and Display Pages

Trouble Indicators

Trouble indicators are used to identify and recognize faults that occur on an active ring. The most common and recognizable trouble indicators that aid in the recognition of ring and system related problems are as follows:

- Audible alarms
- Visual alarms
- Output messages.

Audible Alarms

Abnormal conditions in an office are identified by both audible and visual alarms. Hardware failures, software faults, and power faults cause alarms in an office. These alarms fall into major categories. Associated with each alarm category is an audible alarm used to notify the system user by sound. These alarms and their associated tones are as follows:

a. **Critical Alarm**: A critical alarm is set by the 3B Computer and indicates a severe fault has occurred causing a loss of service. Two strokes on the office tone bar indicates a critical alarm.
b. **Major Alarm**: A major alarm is set by a hardware or software fault. This alarm type could also be service affecting but reacting immediately upon the fault may prevent service interruption. One stroke on the office tone bar indicates a major alarm.
c. **Power Plant Major Alarm**: A power plant major alarm indicates a major fault in the power plant and is service affecting. This alarm rings a bell to indicate power plant problems.
d. **Minor Alarm**: A minor alarm is set by a minor software or hardware fault and is not service affecting. This alarm rings a bell to identify a fault.

These alarms may be transferred to remote locations for monitoring in addition to being monitored by the affected CNI site.

Visual Alarms

Visual alarms are used in conjunction with audible alarms to more precisely locate faulty equipment and assist in understanding what a problem may be. Visual alarms are normally located on the MCRT, affected equipment, and aisle cabinets where the affected equipment is located.

The visual alarms associated with the MCRT are located on the top of each display page. The visual alarms are in the form of CRITICAL, MAJOR and MINOR indicators. These alarms are illuminated when there is an associated audible alarm. There are additional alarm indicators on the display pages.

There are other visual alarms used to clearly pinpoint affected and faulty equipment in an office. These visual alarms are in the form of light emitting diodes (LEDs) and are located on control panels in the cabinets. The LEDs identify equipment that may be the cause of audible and visual alarms in the office.

Output Messages

Another type of trouble indicator is output messages. Output messages are used to more accurately determine what is causing a problem with faulty hardware and/or software. Output messages are printed at the MCRT and are directly related to the visual and audible alarms that occur in the office.

The following tables identify a summary of the trouble indicators that may occur in a CNI equipped 4ESS Switch office. These tables may be used to quickly analyze trouble indicators, locate and determine faulty equipment, and to direct the user to appropriate documentation.

The tables provide quick reference information listed under several major headings. This information includes the following:

a. **Indication:** Identifies the categories of trouble indicators encountered (output messages, visual, and audible).
b. **Location:** Identifies various locations that different alarms can be found (MCRT, affected equipment locations, etc.)
c. **Message or Alarm Type:** Identifies the type of alarm (output message, visual, or audible).
d. **Alarm Severity:** Identifies the severity of the alarm.
e. **Affected Equipment:** Identifies equipment affected by the fault that caused alarm.
f. **Service Affect:** Identifies whether service will be interrupted or not.

The columns of each table are marked with an "x" or "+" to denote the alarm severity, affected equipment and service affected. In some instances, more than one field may be marked. All alarm severity fields are sometimes marked indicating that any of the alarms may occur for the particular incident. The service affected equipment columns are marked "Yes or No" indicating if service is affected. If both columns (Yes and No) are marked, this indicates that service may or may not be affected.

Table 6-B. Common Network Interface Trouble Indicators and Analysis — Output Messages

Alarm Indications						Affected Equipment					Service Affect and Documents			
Indication	Location	Message	Alarm Severity			Power	Ring		Link	3B	Service		References	
			CRIT	MJ	MN		LN*	RPC			Yes	No	CNI	OM
Output Messages	MROP	ALM BATTERY ALM		x		x						x	3-10	+
		CO BATTERY DISCH		x		x						x		+
		LOST PROTECTED AC		x	x	x				x	x	x		+
		POWER FAILURE ON		x	x	x				x	x	x		+
		PWR RM ALM		x	x	x	x	x		x	x			+
		REPT CNCE	x						x		x	x	3-6,7,8,9	+
		REPT DB INIT	x							x	x		3-2	+
		REPT DLN CNGST					DLN				x	x		+
		REPT ERROR		x	x		x	x	x	x	x	x		+
		REPT IMSDRV FLT			x		x	x	x		x	x	3-2	
		REPT IMSDRV INIT		x	x		x	x	x	x	x		3-2	+
		REPT LN			x		x					x	3-5	+
		REPT RING CFR			x		x	x			x	x	3-4	+
		REPT RING GROWTH			x		x	x				x	2-2	+
		REPT RING INIT		x			x	x	x	x	x		3-2	+
		REPT RING TRANSPORT ERROR			x		x	x				x		+
		REPT RPC STAT	x					x			x		3-4	+
		RMV:LN			x		x					x	3-5	+
		RMV:RPCN		x	x			x			x	x	3-5	+

* Includes DLNs, D-channel (DCHN) nodes, and special access data channel (SADC) nodes.

Table 6-C. Common Network Interface Trouble Indicators and Analysis — Visual Alarms

Alarm Indications				Affected Equipment					Service Affect and Documents			
					Ring				Service Affected		Reference	
Indication	Location	Alarm Type		Power	LN*	RPC	Link	3B20D	Yes	NO	CNI	OM
Visual Alarms	At MCRT	Critical				x		x	x		3-3	+
		Major		x	x	x	x	x	x		3-3, 6, 7, 8, 9	+
		Minor		x	x	x	x	x		x	3-3, 6, 7, 8, 9	+
		BLDG/PWR		x	x	x		x	x	x	3-3	+
		SLK					x		x		3-3, 6, 7, 8, 9	+
		SYS EMER		x				x	x		3-3	+
		Other										
	Leds at Affected Equipment Location**	RNF	RQ		x	x			x	x	3-4	+
			NT		x				x		3-4	+
			ALM		x	x				x	3-10	+
			RED LED		T1FA				x		3-9	+
			YEL LED		T1FA				x		3-9	+
			Error		AP				x	x	3-10	+
			PWR ALM	x						x	3-10	+
		AFAF	FAN ALM	x	x	x				x	3-10	+
			133K ALM	x						x	3-10	+
			130D ALM	x						x	3-10	+

* Includes DLNs, DCHN nodes, and SADC nodes.

** Most office frames are equipped with a control panel. Located on each panel is a PWR ALM lamp. If a frame is not shown in the tables, and if the PWR ALM lamp for that frame is illuminated, check the fuses and the related power faults for the affected equipment as detailed in the "Equipment Handling Procedures" section.

Table 6-D. Common Network Interface Trouble Indicators and Analysis — Audible Alarms

Alarm Indications			Affected Equipment					Service Affect and Documents			
				Ring				Service Affected		Reference	
Indication	Location	Alarm Type	Power	LN*	RPC	Link	3B20D	Yes	No	CNI	OM
Audible Alarm	Office	ALM BAT SUPPLY	x						x		+
		CRITICAL			x	x	x	x			+
		MAJOR	x	x	x	x	x	x	x		+
		MINOR	x	x	x	x	x		x		+
		PWR PL MAJOR	x				x	x	x		+

* Includes DLNs, DCHN nodes, and SADC nodes.

Display Pages

The on-site user is provided with status information and maintenance functions in the form of display and menu pages. Application display pages are provided by the 4APS<x> generic software.

Index Page (100)

The Index page is the source from which all other display pages can be accessed (Figure 6-4). Several display pages show the status of the associated devices in the office. If a device fails, the appropriate page entry on the index page is identified with a red background. The user can access any desired display page listed on the "index display page" by entering the associated page number. For example, the user would enter page number "101" following **CMD>** to display the "Status Summary Area" page.

```
NAME          TYPE        GENERIC                    <C>      DATE      TIME
SYS EMER   CRITICAL   MAJOR  MINOR    BLDG/PWR    BLD INH   CKT LIM   SYS NORM
TRAFFIC    SYS INH     CU  CU PERPH   OSS LINK
CMD>                                          100 - PAGE INDEX

CMD   PAGE TITLE                                CMD    PAGE TITLE

101 - STATUS SUMMARY AREA                      1105 - RING STATUS SUMMARY
102 - COMMON PROCESSOR DISPLAY                 1106 - RING GROUP STATUS
103 - C-D UPDATE                               1107 - API/DLN STREAM STATUS
104 - OS STATUS PAGE                           1108 - LINK STATUS SUMMARY
105 - CRAFT FM 01
106 - CRAFT FM 01
109 - FIELD UPDATE
110 - DISK FILE SYSTEM ACCESS INDEX
198 - RCV/SG
199 - RCV/ECD
```

Figure 6-4. Example of Index Page (100)

Ring Status Summary Page (1105)

The Ring Status Summary page (Figure 6-5) displays the IMS state of every equipped node on the ring. This page is in the form of a character map where each node corresponds to a character. Characters in lower case correspond to isolated nodes. The legal states are as follows:

A = Active
i = Isolated and out-of-service
O = Out of service
S or s = Standby
U or u = Unavailable
F or f = Off line
B or b = Initializing
G or g = Growth
. or blank = Unequipped

```
NAME         TYPE     GENERIC                      <C>     DATE      TIME
SYS EMER  CRITICAL    MAJOR   MINOR                                  SYS NORM
OVERLOAD  SYS INH     CU     CU PERPH          OS LINKS       CNI   API   NSC

                                                --1105 - RING STATUS SUMMARY--
                      [RING MAINTENANCE STATE]    [NODE DATA INVALID FLAG]

00 AAAOAAAiigAOO...      01 AAAAOOii...AAAAA      02 AAAAAAAAAAA...AA
03 AAAOAAA.........      04 AAAOAAAAAAAAAAAA      05 AAOAAOOAAAAAAAAA
06       .               07       .               08       .
09       .               10       .               11       .
23       .               24       .               25       .
26       .               27       .               28       .
29       .               30       .               31       .
32 AAAAAAAAOOOAAA..      33 AAAAAAAAAAAAAAAA      34 AAOOOOAAAAAAAAAA
35       .               36       .               37       .
38       .               39       .               40       .
41       .               42       .               43       .
55       .               56       .               57       .
58       .               59       .               60       .
61       .               62       .               63       .

400 - OP:RING;DETD
```

Figure 6-5. Example of Ring Status Summary Page (1105)

Ring Node Status Page (1106)

The Ring Node Status page (Figure 6-6) displays the status and detailed information for a particular range of nodes (up to 16) in a ring group. The left side of the display page provides overall status of the ring along with input controls and the right side of the display provides detailed ring node status summaries.

```
CMD< 400 OK                                        - 1106 - RING NODE STATUS -
NODE NAME:                                                 RING MAJOR RI    NP   MAINT
                                          NODE  NAME  POS STATE STATE STATE MODE
RING STATUS: ISOLATED                  01 LN00  04    BISO ACT  USBL  USBL  AUTO
ARR RESTORE: LN00 05                   02 LN00  05    ISO  OOS  FLTY  USBL  AUTO
[ARR Restart]                          03 LN00  06    ISO  OOS  USBL  USBL  AUTO
[ACNR Restore or Restart]              04 LN00  07    ISO  OOS  FLTY  FLTY  AUTO
CMD     FUNCTION                       05 RPCN32 00   EISO ACT  USBL  USBL  AUTO
2xx     RMV node (line xx)             06
3xx     RST node (line xx)(UCL)        07
400     BISO-EISO                      08
401/402 all non-ACT(next/prev)         09
403/404 all Equipped(next/prev)        10
500     DGN Isolated Segment           11
5xx     DGN node (line xx)             12
6nn     Group nn                       13
7nn     RST NODE (line xx) COND        14
TOTAL BISO-EISO NODES: 5               15
                                       16
```

Figure 6-6. Example of Ring Group Display Page (1106)

DLN/API Stream Status Page (1107)

The direct link node/attached processor interface (DLN/API) Stream Status page (Figure 6-7) supplies the user with status information on the DLNs, the DLN stream, both Attached Processor Interface units, and the DLN/API stream. The status information for up to four DLNs is displayed on the 1107 page. This page also shows the hardware state, application state, mode, and stream status.

```
NAME          TYPE       GENERIC                  <CHANNEL>  DATE      TIME
SYS EMER    CRITICAL   MAJOR    MINOR                                  SYS NORM
OVERLOAD    SYS INH    CU       CU PERPH        OS LINKS     CNI  API  NSC HSL

                                        - 1107 - DLN/API STREAM STATUS PAGE -

                        HDWR       APPL
                        STATE      STATE        MODE         STREAM
   LN00 05              ACT        ACT          1WAYOUT      SCANOUT
   LN00 10              ACT        STBY         1WAYIN       SCANIN
   LN32 05              ACT        ACT
   LN32 10              ACT        STBY
   API 0                ACT                     TWOWAY       BOTH
   API 1                STBY
```

Figure 6-7. Example of DLN/API Stream Status Page (1107)

Link Status Display Page (1108)

The Link Status Display page (Figure 6-8) displays the status of the SS7 signaling links. This page shows up to eight links and can scroll forward, backward, or choose a particular link. Information displayed on the Link Status Display page includes the following:

a. Link member number (group, node, and link number)
b. Link protocol type (SS7)
c. Far-end CLLI* code
d. Node mate (if applicable)
e. Link state
f. Node state.

```
NAME          TYPE       GENERIC                  <CHANNEL>  DATE      TIME
SYS EMER    CRITICAL    MAJOR    MINOR                                SYS NORM
OVERLOAD    SYS INH     CU       CU PERPH        OS LINKS     CNI  API  NSC  HSL

                                          - 1108 - SIGNALING LINK STATUS PAGE -
ENTER GROUP-MEMBER: _ _  _ _                        TOTAL LINK FAILURES

CMD          FUNCTION          NEXT/PREV    FUNCTION          NEXT/PREV  FUNCTION
20X  CHG SLK MOOS (line x)     400/401   LOCAL LINK FAILURES   430/431  DCHN LINKS
30X  CHG SLK ARST (line x)     406/407   ALL EQUIPPED LINKS    440/441  SADC LINKS
                               410/411   CCS7 LINKS            450/451  SSN LINKS
                               420/421   CIT7 LINKS            460/461  SIN LINKS

GROUP   PROT    LS              CIN              LINK      NODE     PRO
MEMBER  TYPE    LACID  SLC      CLLI     MATE    STATE     STATE    RCVD

00 01   CCS7     1      1    clli_code  32 01  AVL-IS      ACT      NO
00 03   CCS7     2      2    clli_code  32 03  AVL-IS      ACT      NO
32 01   CCS7     1      2    clli_code  00 01  AVL-OOS     ACT      NO
32 03   CCS7     2      1    clli_code  00 03  AVL-IS      ACT      NO
```

Figure 6-8. Example of Link Status Summary Page (1108)

* COMMON LANGUAGE is a registered trademark and CLEI, CLLI, CLCI, and CLFI are trademarks of Bell Communications Research, Inc.

Signaling System No. 7 Digital Signaling Link Maintenance

General

A *digital signaling* link is defined as the link running from the LN, not including RI circuit pack, through a digital service adapter (DSA), digital service unit (DSU), and optional channel service unit (CSU) to the transmission facility and voice frequency link (VFL) access circuit.

The objective of the signaling link maintenance strategies is to use automatic and semiautomatic actions when applicable. Signaling link troubles are automatically detected in real time. If possible, the system reconfigures to protect service. The system then diagnoses and tests the faulty signaling link prior to notifying the user of trouble.

Maintenance aids to help in locating actual and potential signaling link failures are provided in the form of signaling link display pages, audible alarms, output messages, and measurement reports. The signaling link display pages provide information on the status of signaling link states. Signaling link alarms, output messages, and measurement reports are discussed later in this part. Signaling link failures or potential failures must be corrected as soon as possible to minimize service disruption.

Signaling Link and Transmission Link Control

Signaling link control is responsible for classifying signaling link failures for the following:

- Beginning of the signaling link
- End of signaling link
- Intervening signaling link.

The transmission link is the part of the signaling link contained between the CSUs. Transmission link control is responsible for isolating troubles within a transmission link and ultimately referring an isolated trouble to a field work group for repair. The various control responsibilities for digital signaling links should be defined by the application.

Signaling Link Process Characteristics

Much of the maintenance process for signaling links is automatic. The complete sequence for hard failures which involves user interaction are invoked only when repairs are necessary. Before repairs are required, automatic trouble detection mechanisms should determine when signaling link performance is unacceptable and reconfiguration is required.

In the event that a performance of a signaling link deteriorates past an acceptable level, the automatic recovery mechanisms transfer traffic to other signaling links and attempt to reestablish the original signaling link. This is classified as a changeover. Changeovers occur when an unacceptable performance threshold is exceeded. For a 4-wire circuit, the end detecting the unacceptable performance informs the other end that the traffic should be transferred. After a successful traffic transfer, attempts are made to prove-in the defective link. A successful prove-in within 3 minutes results in a transfer of the traffic back to the original signaling link. This is classified as a changeback. In an encrypted digital signaling link, this could take up to 13 minutes due to the long key exchange. This is an encryption code exchange which may take up to 10 minutes to complete. A complete automatic recovery procedure is called a *changeover/changeback.*

Failure to reestablish the original signaling link after three attempts by Automatic Ring Recovery (ARR) procedures initiates the need for user interaction. This involves manually testing signaling link hardware, replacing any faulty equipment, and performing diagnostics until the problem is fixed. User interaction is required only when an exception report is sent or an alarm is output.

Signaling Link Trouble Detection Mechanisms

Mechanisms for detecting unacceptable signaling link performance include the following:

a. Monitoring signal units in error (SUIE) rates
b. Detecting near-end LN failures.

Marginally acceptable signaling link performance is detected by monitoring the following:

a. Counts of SUIE rate
b. Changeover/changeback rates
c. Signaling quality measurements.

Signaling Link Alarms

Three different signaling link alarm severity levels exist as described below:

a. *Critical* -- The last signaling link connected to another office has failed. It is most likely caused by signal point isolation (SPI).

b. *Major* -- A signaling link has failed for longer than 3 to 13 minutes with a satisfactory transfer of the signaling load.

c. *Minor* -- The signaling link performance has been below established criteria over the last 30 minutes.

Diagnostics

Classifying a signaling link failure requires automatic and manually requested diagnostics on the link nodes. Link node diagnostics can be automatically invoked as part of the failure declaration/classifying sequence or manually initiated via an input message.

Measurement Reports

Measurement reports are output either automatically or on demand via input messages. The following reports are useful when performing signaling link maintenance:

1. Thirty-Minute Marginal Performance Report
2. Signaling Network Performance Report, Part 1
3. Signaling Network Performance Report, Part 2

Thirty-Minute Marginal Performance Report

Signaling link thirty-minute marginal performance reports (30MPRs) provide information on marginal performing signaling links. These reports highlight the measure of performance deterioration of the signaling links. The decision to test a marginal signaling link should be made on the basis of the data provided. The following lists show the information provided by the 30MPRs for digital signaling links:

a. SUIE rate: The default threshold is 200 per signaling link per half hour.

b. Retransmission request: The default threshold is 200 per signaling link per half hour.

c. Number of automatic changeovers/changebacks: The default threshold is two changeovers per half hour.

d. Clock half hour signaling quality: The calculation is defined as the percentage of in-service seconds that are service-free.

e. Current day count of clock half hours: The calculation is defined as the number of 1-second intervals where at least 1 error threshold has been exceeded.

f. Availability of digital signaling link: The calculation is defined as the percentage of time that the signaling link is unavailable for service.

Signaling Network Performance Report

There are two parts to the signaling network performance report, *SNPR1* and *SNPR2*. The *SNPR1* provides a summary of the signaling performance in an office. The SNPR1 is a part of the total office report and is output on-site every hour.

The *SNPR2* provides a close look at the individual links. There are separate measurements for each link in the office. Thusly, the reports provide information helpful in isolating problems to a particular link. The *SNPR2* is a part of the detailed performance reports and is output on-site every day.

Critical Events

Critical event messages are output as critical events occur in the signal point or as network events are recognized by the signaling point.

Signaling Link States

The state of a signaling link must be taken into consideration when performing signaling link maintenance. There are major and minor signaling link states. The following is a list of the major signaling link states:

- UNEQUIPPED
- UNAVAILABLE
- AVAILABLE.

To change from one major state to another, a recent change function must be used. The following is a list of the minor signaling link states associated with the major signaling link state UNAVAILABLE:

- GROW
- TEST.

The following is a list of the minor signaling link states associated with the major signaling link state AVAILABLE:

- ACT
- OOS
- MOOS.

To change from one minor state to another, program documentation standard commands must be used.

Trouble Conditions

Signaling Point Isolation

Signaling point isolation (SPI) is defined as the office not being able to signal other adjacent signaling network nodes due to signaling link failures. This could be due to a local signaling link failure or the receipt messages indicating a failure of some other signaling link in a path to the far-end. Signaling point isolation is a critical alarmed condition.

Each signaling point isolation occurrence increments the SPI peg count associated with each affected signaling link. There is also a per-link count of the time that each affected signaling link spent in isolation. Total office SPI occurrence peg and time counts are separated by type (that is, A-link, C-link, E-link etc.).

Declared Signaling Link Failure

A declared signaling link failure occurs because automatic recovery mechanisms have not succeeded within the allotted 13 minutes to clear near-end link node failures or because processor signaling congestion (PSC) signals have been received every 8 to 10 seconds for 30 seconds from the far-end office. A declared signaling link failure requires trouble notification, and human intervention if automatic recovery procedures are not able to return the signaling link to service. A declared link failure is a major alarmed condition.

The occurrence of each link failure increments the FLD peg count associated with the affected link. The time the link is out-of-service is accumulated in the FLD-T peg count associated with the affected link. The declared link failure peg counts and times contribute to a total office FLD peg count and a total office declared link failure time. An automatic recovery from a signaling link failure is a changeover/changeback that occurs after the detection of a link failure.

Link Set Failure

A link set failure is defined as a failure of a link set or combined link set. A link set failure is a major alarmed condition. Each occurrence of a link set failure causes the CLF peg count to be incremented and the per-link time count to be accumulated for the affected signaling link.

Diagnostics

Diagnostics for the IMS and CNI serve two major purposes. First, diagnostics are run for fault detection and resolution and are invoked by manual requests. Diagnostics are also invoked by error analysis programs as part of the automatic ring recovery (ARR) of equipment that has been removed from service due to a faultly condition. Secondly, diagnostics are run for the purpose of repair verification.

The IMS/CNI system diagnostics provide diagnostic testing for the IMS and CNI hardware. These diagnostics are performed in a manner similar to those of the 3B Computer system but diagnose totally different equipment. The IMS utilizes the 3B Computer as the central processing unit. The function of the IMS is to receive messages from incoming applications and route the message to an outgoing application. The IMS utilizes a ring communication bus to totally interconnect all application terminations and the 3B Computer. The ring is a dual bus configuration and is designed such that faulty circuits can be eliminated from the active system for an indefinite period of time.

The IMS diagnostics primarily test ring nodes that is contained in the ring node cabinet (RNC). There are several types of ring nodes:

1. Ring Peripheral Controller Nodes (RPCNs)
2. Direct Link Nodes (DLNs)
3. Signaling System No. 7 (SS7) nodes

The RPCN is used to remove data from the ring and transfer it to the 3B Computer for processing or insert processed data back onto the ring. The DLNs are used to provide direct access to the 3B Computer. The DLNs function like application link nodes but have direct memory access (DMA) capability. The DLNs contain the same circuit packs as the RPCN plus an attached processor (AP) circuit pack. The SS7 node is identified as an application link node and are used to provided entrance and exit points on the ring for specific applications. The CNI utilizes the link interface of these nodes to provide communications between the ring and the various applications offered by the network.

Local maintenance access and diagnostic status information for IMS, CNI and 3B Computer functions are obtained through maintenance terminals and receive-only printers. The maintenance terminal provides the primary interface for system control and display functions, input/output messages and 3B Computer emergency action interface (EAI) functions. Inputs entered at the maintenance terminal can be monitored via remote support organizations.

The maintenance receive-only printer provides hard copies of input/output messages, report status information, fault conditions, audits, and diagnostic results. If remote maintenance is provided, it has the same terminal access and terminal capabilities as the on-site user. Because both the remote and local

users have simultaneous access to system diagnostics, it is advised that diagnostic input requests be coordinated through the on-site user.

Performing Diagnostics

When performing manual diagnostics, input and output messages are entered and interpreted from the maintenance terminal. For this reason, basic terminal familiarization and operating knowledge is required. An understanding of input messages and knowledge of the message data fields and formats are also important.

UNIX RTR software provides assistance to users for entering input messages. It can be used to complete or correct errors caused by the user. Invalid values are rejected accompanied by an appropriate error acknowledgment. Further help can then be obtained by entering a question mark (?). Help is provided for only one input message at a time. A prompting mode can be used to lead the user through the input message. A user may either execute or cancel a complete input message once the message has been constructed. The help session is then completed.

Diagnostic Message Structure

Listed within the following paragraphs are basic guidelines for understanding the input message format. For a detailed explanation of the message structure, refer to Input/Output message manuals. An input message can contain 96 characters separated by colons into fields. The fields of an input message are identified as the action, identification, and data field. Each field is variable in length. These fields are briefly explained as follows:

a. Action Field: An action verb that identifies the action the system should perform. This field is always a verb such as diagnose (DGN), inhibit (INH), remove (RMV), restore (RST), etc.

b. Identification Field: Consists of one, two, or three fields called subfields. These subfields are separated by semicolons with each containing one or more keywords. The identification field aids in structuring the message to permit a complete specification or provides additional information identifying the object of the action.

c. Data Field: This field is either null or composed of keywords separated by commas, providing additional information pertaining to the message.

A typical diagnostic input message and format varies in length and field identifiers. The sample message below provides field separation and identification.

DGN:nodexx y[;[RPT n] [,RAW] [,UCL]] [:PH n [,TLP]]

Where:

DGN: = Action field
nodexx y[;[RPT n] [,RAW] [,UCL]] [: = Identification field
PH n [,TLP]] = Data field.

System Diagnostics

Diagnostics on the IMS/CNI system may be performed manually. However, when the system detects a faultly condition, diagnostics are performed automatically via the automatic ring recovery (ARR) procedures. The diagnose (DGN) command is used to perform manual diagnostics in an office. Several formats of the diagnose command are detailed in Table 6-E. For a complete listing of all diagnostic input messages, refer to the input/output message manuals.

When performing IMS/CNI diagnostics, it may be necessary to obtain the status of the system, the ring, or the a particular node. One manner that a status report can be obtained is with the use of input messages. Table 6-F provides a list of input message formats used to produce status reports.

Table 6-E. DGN Message Input Variations

Command	Function
DGN:nodexx y	Runs all automatic phases on nodexx y.
DGN:nodexx y:PH a	Runs only the specified phase (a) on nodexx y.
DGN:nodexx y:PH a-b	Runs all automatic phases within the specified range (a through b) on nodexx y.
DGN:nodexx y;RPT n	Runs all automatic phases on nodexx y and repeats execution "*n*" times, where *n* is equal to or less than 255.
DGN:nodexx y;RAW	Runs all automatic phases on nodexx y and prints the diagnostic results of every phase at the MROP.
DGN:nodexx y;UCL	Runs all automatic phases on nodexx y. Early terminations built into data tables are ignored.

Table 6-F. OP:RING Input Message Variations

Input Message	Function
OP:RING,nodexx y	Provides status information for the specified node (RPCN or IUN).
OP:RING,GRP xx	Provides status information for all nodes on a specified frame/cabinet (GRP xx).
OP:RING	Provides summary information of the ring.
OP:RING;SUM	
OP:RING;DETD	Provides detailed status of the ring.
OP:OOS	Provides status information of all equipment which is out-of-service
OP:SLK	Provides link status information for DCHNs and SADC nodes.

Diagnostic Phases

Diagnostic routines are broken down into phases. Phases are designed to test a unique group of functionally related hardware. Each phase may test all or part of the hardware on a single circuit pack or group of circuit packs. In addition, each node is diagnosed by its own set of diagnostic phases. Certain node hardware, such as the node processor, is used by all node types. Therefore, diagnostic phases that test this type hardware are the same for all node types.

Associated with each piece of hardware that is tested by a diagnostic phase is a list of suspected or possibly faulty circuit packs. When diagnostic failures still exist after replacing suspect hardware, analysis of the diagnostic test results must be performed. This is accomplished using the diagnostic output message and diagnostic listings. Generally, the first failing phase and the first few failing tests within that phase are most useful for analysis. If this data is not available, run diagnostics using the **RAW** option to print all test failures.

A diagnostic listing consists of a prologue followed by one or more program units. Each program unit contains a PROLOGUE, HARDWARE TESTED and HOW TESTING IS PERFORMED. The remainder of the program unit consists of program data specifying diagnostic commands.

Each diagnostic command begins with a statement number. This is the statement number that is referred to in the interactive diagnostics. Some diagnostic command lines are preceded by one or more comment lines. These are lines that begin with the character "C." They are intended to identify the purpose of the command line.

Ring Node Addressing

The addressing of ring nodes and the manner in which cabinets are identified are for maintenance purposes. An address is identified in terms of an integer sequence number and may be represented in decimal or hexadecimal notations. The decimal notations represent the physical node identification ranging from 0 to 1023. Another decimal notation ranging from 3072 to 4095 represents the physical node addresses in machine logic. These notations are not usually seen by the users. Node addresses are listed in hexadecimal notations. These addresses are important when analyzing mismatched data. Suspected faulty nodes as well as the beginning of isolation (BISO) and the end of isolation (EISO) nodes are identified by hexadecimal node addresses. Tables 6-G through 6-J identify the physical node identifications and physical node addresses in both decimal and hexidecimal formats.

Table 6-G. Physical Node Identification — Decimal Representation

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
01	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
02	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
03	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
04	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
05	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
06	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
07	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
08	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
09	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
10	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
11	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
12	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
13	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
14	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
15	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
16	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271
17	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287
18	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303
19	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319

Table 6-G. Physical Node Identification — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
20	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335
21	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351
22	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367
23	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383
24	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399
25	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415
26	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431
27	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447
28	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463
29	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479
30	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495
31	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511
32	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527
33	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543
34	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559
35	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575
36	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591
37	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607
38	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623

Table 6-G. Physical Node Identification — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
39	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639
40	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655
41	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671
42	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687
43	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703
44	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719
45	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735
46	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751
47	752	753	754	755	756	758	759	760	761	762	762	763	764	765	766	767
48	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783
49	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799
50	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815
51	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831
52	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847
53	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863
54	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879
55	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895
56	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911
57	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927

Table 6-G. Physical Node Identification — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
58	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943
59	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959
60	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975
61	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991
62	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007
63	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023

Table 6-H. Physical Node Addresses — Decimal Representation

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	3072	3073	3074	3075	3076	3077	3078	3079	3080	3081	3082	3083	3084	3085	3086	3087
01	3088	3089	3090	3091	3092	3093	3094	3095	3096	3097	3098	3099	3100	3101	3102	3103
02	3104	3105	3106	3107	3108	3109	3110	3111	3112	3113	3114	3115	3116	3117	3118	3119
03	3120	3121	3122	3123	3124	3125	3126	3127	3128	3129	3130	3131	3132	3133	3134	3135
04	3136	3137	3138	3139	3140	3141	3142	3143	3144	3145	3146	3147	3148	3149	3150	3151
05	3152	3153	3154	3155	3156	3157	3158	3159	3160	3161	3162	3163	3164	3165	3166	3167
06	3168	3169	3170	3171	3172	3173	3174	3175	3176	3177	3178	3179	3180	3181	3182	3183
07	3184	3185	3186	3187	3188	3189	3190	3191	3192	3193	3194	3195	3196	3197	3198	3199
08	3200	3201	3202	3203	3204	3205	3206	3207	3208	3209	3210	3211	3212	3213	3214	3215
09	3216	3217	3218	3219	3220	3221	3222	3223	3224	3225	3226	3227	3228	3229	3230	3231
10	3232	3233	3234	3235	3236	3237	3238	3239	3240	3241	3242	3243	3244	3245	3246	3247
11	3248	3249	3250	3251	3252	3253	3254	3255	3256	3257	3258	3259	3260	3261	3262	3263
12	3264	3265	3266	3267	3268	3269	3270	3271	3272	3273	3274	3275	3276	3277	3278	3279
13	3280	3281	3282	3283	3284	3285	3286	3287	3288	3289	3290	3291	3292	3293	3294	3295
14	3296	3297	3298	3299	3300	3301	3302	3303	3304	3305	3306	3307	3308	3309	3310	3311
15	3312	3313	3314	3315	3316	3317	3318	3319	3320	3321	3322	3323	3324	3325	3326	3327
16	3328	3329	3330	3331	3332	3333	3334	3335	3336	3337	3338	3339	3340	3341	3342	3343
17	3344	3345	3346	3347	3348	3349	3350	3351	3352	3353	3354	3355	3356	3357	3358	3359
18	3360	3361	3362	3363	3364	3365	3366	3367	3368	3369	3370	3371	3372	3373	3374	3375
19	3376	3377	3378	3379	3380	3381	3382	3383	3384	3385	3386	3387	3388	3389	3390	3391

Table 6-H. Physical Node Addresses — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes															
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
20	3392	3393	3394	3395	3396	3397	3398	3399	3400	3401	3402	3403	3404	3405	3406	3407
21	3408	3409	3410	3411	3412	3413	3414	3415	3416	3417	3418	3419	3420	3421	3422	3423
22	3424	3425	3426	3427	3428	3429	3430	3431	3432	3433	3434	3435	3436	3437	3438	3439
23	3440	3441	3442	3443	3444	3445	3446	3447	3448	3449	3450	3451	3452	3453	3454	3455
24	3456	3457	3458	3459	3460	3461	3462	3463	3464	3465	3466	3467	3468	3469	3470	3471
25	3472	3473	3474	3475	3476	3477	3478	3479	3480	3481	3482	3483	3484	3485	3486	3487
26	3488	3489	3490	3491	3492	3493	3494	3495	3496	3497	3498	3499	3500	3501	3502	3503
27	3504	3505	3506	3507	3508	3509	3510	3511	3512	3513	3514	3515	3516	3517	3518	3519
28	3520	3521	3522	3523	3524	3525	3526	3527	3528	3529	3530	3531	3532	3533	3534	3535
29	3536	3537	3538	3539	3540	3541	3542	3543	3544	3545	3546	3547	3548	3549	3550	3551
30	3552	3553	3554	3555	3556	3557	3558	3559	3560	3561	3562	3563	3564	3565	3566	3567
31	3568	3569	3570	3571	3572	3573	3574	3575	3576	3577	3578	3579	3580	3581	3582	3583
32	3584	3585	3586	3587	3588	3589	3590	3591	3592	3593	3594	3595	3596	3597	3598	3599
33	3600	3601	3602	3603	3604	3605	3606	3607	3608	3609	3610	3611	3612	3613	3614	3615
34	3616	3617	3618	3619	3620	3621	3622	3623	3624	3625	3626	3637	3628	3629	3630	3631
35	3632	3633	3634	3635	3636	3637	3638	3639	3640	3641	3642	3643	3644	3645	3646	3647
36	3648	3649	3650	3651	3652	3653	3654	3655	3656	3657	3658	3659	3660	3661	3662	3663
37	3664	3665	3666	3667	3668	3669	3670	3671	3672	3673	3674	3675	3676	3677	3678	3679
38	3680	3681	3682	3683	3684	3685	3686	3687	3688	3689	3690	3691	3692	3693	3694	3695

Table 6-H. Physical Node Addresses — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
39	3696	3697	3698	3699	3700	3701	3702	3703	3704	3705	3706	3707	3708	3709	3710	3711
40	3712	3713	3714	3715	3716	3717	3718	3719	3720	3721	3722	3723	3724	3725	3726	3727
41	3728	3729	3730	3731	3732	3733	3734	3735	3736	3737	3738	3739	3740	3741	3742	3743
42	3744	3745	3746	3747	3748	3749	3750	3751	3752	3753	3754	3755	3756	3757	3758	3759
43	3760	3761	3762	3763	3764	3765	3766	3767	3768	3769	3770	3771	3772	3773	3774	3775
44	3776	3777	3778	3779	3780	3781	3782	3783	3784	3785	3786	3787	3788	3789	3790	3791
45	3792	3793	3794	3795	3796	3797	3798	3799	3800	3801	3802	3803	3804	3805	3806	3807
46	3808	3809	3810	3811	3812	3813	3814	3815	3816	3817	3818	3819	3820	3821	3822	3823
47	3824	3825	3826	3827	3828	3829	3830	3831	3832	3833	3834	3835	3836	3837	3838	3839
48	3840	3841	3842	3843	3844	3845	3846	3847	3848	3849	3850	3851	3852	3853	3854	3855
49	3856	3857	3858	3859	3860	3861	3862	3863	3864	3865	3866	3867	3868	3869	3870	3871
50	3872	3873	3874	3875	3876	3877	3878	3789	3880	3881	3882	3883	3884	3885	3886	3887
51	3888	3889	3890	3891	3892	3893	3894	3895	3896	3897	3898	3899	3900	3901	3902	3903
52	2904	3905	3906	3907	3908	3909	3910	3911	3912	3913	3914	3915	3916	3917	3918	3919
53	3920	3921	3922	3923	3924	3925	3926	3927	3928	3929	3930	3931	3932	3933	3934	3935
54	3936	3937	3938	3939	3940	3941	3942	3943	3944	3945	3946	3947	3948	3949	3950	3951
55	3952	3953	3954	3955	3956	3957	3958	3959	3960	3961	3962	3963	3964	3965	3966	3967
56	3968	3969	3970	3971	3972	3973	3974	3975	3976	3977	3978	3979	3980	3981	3982	3983
57	3984	3985	3986	3987	3988	3989	3990	3991	3992	3993	3994	3995	3996	3997	3998	3999

Table 6-H. Physical Node Addresses — Decimal Representation (Contd)

Ring Node	RPC	IMS User Nodes															
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
58	4000	4001	4002	4003	4004	4005	4006	4007	4008	4009	4010	4011	4012	4013	4014	4015
59	4016	4017	4018	4019	4020	4021	4022	4023	4024	4025	4026	4027	4028	4029	4030	4031
60	4032	4033	4034	4035	4036	4037	4038	4039	4040	4041	4042	4043	4044	4045	4046	4047
61	4048	4049	4050	4051	4052	4053	4054	4055	4056	4057	4058	4059	4060	4061	4062	4063
62	4064	4065	4066	4067	4068	4069	4070	4071	4072	4073	4074	4075	4076	4077	4078	4079
63	4080	4081	4082	4083	4084	4085	4086	4087	4088	4089	4090	4091	4092	4093	4094	4095

Table 6-I. Physical Node Identification — Hexadecimal Representation

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	000	001	002	003	004	005	006	007	008	009	00A	00B	00C	00D	00E	00F
01	010	011	012	013	014	015	016	017	018	019	01A	01B	01C	01D	01E	01F
02	020	021	022	023	024	025	026	027	028	029	02A	02B	02C	02D	02E	02F
03	030	031	032	033	034	035	036	037	038	039	03A	03B	03C	03D	03E	03F
04	040	041	042	043	044	045	046	047	048	049	04A	04B	04C	04D	04E	04F
05	050	051	052	053	054	055	056	057	058	059	05A	05B	05C	05D	05E	05F
06	060	061	062	063	064	065	066	067	068	069	06A	06B	06C	06D	06E	06F
07	070	071	072	073	074	075	076	077	078	079	07A	07B	07C	07D	07E	07F
08	080	081	082	083	084	085	086	087	088	089	08A	08B	08C	08D	08E	08F
09	090	091	092	093	094	095	096	097	098	099	09A	09B	09C	09D	09E	09F
10	0A0	0A1	0A2	0A3	0A4	0A5	0A6	0A7	0A8	0A9	0AA	0AB	0AC	0AD	0AE	0AF
11	0B0	0B1	0B2	0B3	0B4	0B5	0B6	0B7	0B8	0B9	0BA	0BB	0BC	0BD	0BE	0BF
12	0C0	0C1	0C2	0C3	0C4	0C5	0C6	0C7	0C8	0C9	0CA	0CB	0CC	0CD	0CE	0CF
13	0D0	0D1	0D2	0D3	0D4	0D5	0D6	0D7	0D8	0D9	0DA	0DB	0DC	0DD	0DE	0DF
14	0E0	0E1	0E2	0E3	0E4	0E5	0E6	0E7	0E8	0E9	0EA	0EB	0EC	0ED	0EE	0EF
15	0F0	0F1	0F2	0F3	0F4	0F5	0F6	0F7	0F8	0F9	0FA	0FB	0FC	0FD	0FE	0FF
16	100	101	102	103	104	105	106	107	108	109	10A	10B	10C	10D	10E	10F
17	110	111	112	113	114	115	116	117	118	119	11A	11B	11C	11D	11E	11F
18	120	121	122	123	124	125	126	127	128	129	12A	12B	12C	12D	12E	12F
19	130	131	132	133	134	135	136	137	138	139	13A	13B	13C	13D	13E	13F

Table 6-I. Physical Node Identification — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
20	140	141	142	143	144	145	146	147	148	149	14A	14B	14C	14D	14E	14F
21	150	151	152	153	154	155	156	157	158	159	15A	15B	15C	15D	15E	15F
22	160	161	162	163	164	165	166	167	168	169	16A	16B	16C	16D	16E	16F
23	170	171	172	173	174	175	176	177	178	179	17A	17B	17C	17D	17E	17F
24	180	181	182	183	184	185	186	187	188	189	18A	18B	18C	18D	18E	18F
25	190	191	192	193	194	195	196	197	198	199	19A	19B	19C	19D	19E	19F
26	1A0	1A1	1A2	1A3	1A4	1A5	1A6	1A7	1A8	1A9	1AA	1AB	1AC	1AD	1AE	1AF
27	1B0	1B1	1B2	1B3	1B4	1B5	1B6	1B7	1B8	1B9	1BA	1BB	1BC	1BD	1BE	1BF
28	1C0	1C1	1C2	1C3	1C4	1C5	1C6	1C7	1C8	1C9	1CA	1CB	1CC	1CD	1CE	1CF
29	1D0	1D1	1D2	1D3	1D4	1D5	1D6	1D7	1D8	1D9	1DA	1DB	1DC	1DD	1DE	1DF
30	1E0	1E1	1E2	1E3	1E4	1E5	1E6	1E7	1E8	1E9	1EA	1EB	1EC	1ED	1EE	1EF
31	1F0	1F1	1F2	1F3	1F4	1F5	1F6	1F7	1F8	1F9	1FA	1FB	1FC	1FD	1FE	1FF
32	200	201	202	203	204	205	206	207	208	209	20A	20B	20C	20D	20E	20F
33	210	211	212	213	214	215	216	217	218	219	21A	21B	21C	21D	21E	21F
34	220	221	222	223	224	225	226	227	228	229	22A	22B	22C	22D	22E	22F
35	230	231	232	233	234	235	236	237	238	239	23A	23B	23C	23D	23E	23F
36	240	241	242	243	244	245	246	247	248	249	24A	24B	24C	24D	24E	24F
37	250	251	252	253	254	255	256	257	258	259	25A	25B	25C	25D	25E	25F
38	260	261	262	263	264	265	266	267	268	269	26A	26B	26C	26D	26E	26F

Table 6-I. Physical Node Identification — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
39	270	271	272	273	274	275	276	277	278	279	27A	27B	27C	27D	27E	27F
40	280	281	282	283	284	285	286	287	288	289	28A	28B	28C	28D	28E	28F
41	290	291	292	293	294	295	296	297	298	299	29A	29B	29C	29D	29E	29F
42	2A0	2A1	2A2	2A3	2A4	2A5	2A6	2A7	2A8	2A9	2AA	2AB	2AC	2AD	2AE	2AF
43	2B0	2B1	2B2	2B3	2B4	2B5	2B6	2B7	2B8	2B9	2BA	2BB	2BC	2BD	2BE	2BF
44	2C0	2C1	2C2	2C3	2C4	2C5	2C6	2C7	2C8	2C9	2CA	2CB	2CC	2CD	2CE	2CF
45	2D0	2D1	2D2	2D3	2D4	2D5	2D6	2D7	2D8	2D9	2DA	2DB	2DC	2DD	2DE	2DF
46	2E0	2E1	2E2	2E3	2E4	2E5	2E6	2E7	2E8	2E9	2EA	2EB	2EC	2ED	2EE	2EF
47	2F0	2F1	2F2	2F3	2F4	2F5	2F6	2F7	2F8	2F9	2FA	2FB	2FC	2FD	2FE	2FF
48	300	301	302	303	304	305	306	307	308	309	30A	30B	30C	30D	30E	30F
49	310	311	312	313	314	315	316	317	318	319	31A	31B	31C	31D	31E	31F
50	320	321	322	323	324	325	326	327	328	329	32A	32B	32C	32D	32E	32F
51	330	331	332	333	334	335	336	337	338	339	33A	33B	33C	33D	33E	33F
52	340	341	342	343	344	345	346	347	348	349	34A	34B	34C	34D	34E	34F
53	350	351	352	353	354	355	356	357	358	359	35A	35B	35C	35D	35E	35F
54	360	361	362	363	364	365	366	367	368	369	36A	36B	36C	36D	36E	36F
55	370	371	372	373	374	375	376	377	378	379	37A	37B	37C	37D	37E	37F
56	380	381	382	383	384	385	386	387	388	389	38A	38B	38C	38D	38E	38F
57	390	391	392	393	394	395	396	397	398	399	39A	39B	39C	39D	39E	39F

Table 6-I. Physical Node Identification — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
58	3A0	3A1	3A2	3A3	3A4	3A5	3A6	3A7	3A8	3A9	3AA	3AB	3AC	3AD	3AE	3AF
59	3B0	3B1	3B2	3B3	3B4	3B5	3B6	3B7	3B8	3B9	3BA	3BB	3BC	3BD	3BE	3BF
60	3C0	3C1	3C2	3C3	3C4	3C5	3C6	3C7	3C8	3C9	3CA	3CB	3CC	3CD	3CE	3CF
61	3D0	3D1	3D2	3D3	3D4	3D5	3D6	3D7	3D8	3D9	3DA	3DB	3DC	3DD	3DE	3DF
62	3E0	3E1	3E2	3E3	3E4	3E5	3E6	3E7	3E8	3E9	3EA	3EB	3EC	3ED	3EE	3EF
63	3F0	3F1	3F2	3F3	3F4	3F5	3F6	3F7	3F8	3F9	3FA	3FB	3FC	3FD	3FE	3FF

Table 6-J. Physical Node Addresses — Hexadecimal Representation

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	C00	C01	C02	C03	C04	C05	C06	C07	C08	C09	C0A	C0B	C0C	C0D	C0E	C0F
01	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C1A	C1B	C1C	C1D	C1E	C1F
02	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C2A	C2B	C2C	C2D	C2E	C2F
03	C30	C31	C32	C33	C34	C35	C36	C37	C38	C39	C3A	C3B	C3C	C3D	C3E	C3F
04	C40	C41	C42	C43	C44	C45	C46	C47	C48	C49	C4A	C4B	C4C	C4D	C4E	C4F
05	C50	C51	C52	C53	C54	C55	C56	C57	C58	C59	C5A	C5B	C5C	C5D	C5E	C5F
06	C60	C61	C62	C63	C64	C65	C66	C67	C68	C69	C6A	C6B	C6C	C6D	C6E	C6F
07	C70	C71	C72	C73	C74	C75	C76	C77	C78	C79	C7A	C7B	C7C	C7D	C7E	C7F
08	C80	C81	C82	C83	C84	C85	C86	C87	C88	C89	C8A	C8B	C8C	C8D	C8E	C8F
09	C90	C91	C92	C93	C94	C95	C96	C97	C98	C99	C9A	C9B	C9C	C9D	C9E	C9F
10	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CA7	CA8	CA9	CAA	CAB	CAC	CAD	CAE	CAF
11	CB0	CB1	CB2	CB3	CB4	CB5	CB6	CB7	CB8	CB9	CBA	CBB	CBC	CBD	CBE	CBF
12	CC0	CC1	CC2	CC3	CC4	CC5	CC6	CC7	CC8	CC9	CCA	CCB	CCC	CCD	CCE	CCF
13	CD0	CD1	CD2	CD3	CD4	CD5	CD6	CD7	CD8	CD9	CDA	CDB	CDC	CDD	CDE	CDF
14	CE0	CE1	CE2	CE3	CE4	CE5	CE6	CE7	CE8	CE9	CEA	CEB	CEC	CED	CEE	CEF
15	CF0	CF1	CF2	CF3	CF4	CF5	CF6	CF7	CF8	CF9	CFA	CFB	CFC	CFD	CFE	CFF
16	D00	D01	D02	D03	D04	D05	D06	D07	D08	D09	D0A	D0B	D0C	D0D	D0E	D0F
17	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D1A	D1B	D1C	D1D	D1E	D1F
18	D20	D21	D22	D23	D24	D25	D26	D27	D28	D29	D2A	D2B	D2C	D2D	D2E	D2F
19	D30	D31	D32	D33	D34	D35	D36	D37	D38	D39	D3A	D3B	D3C	D3D	D3E	D3F

Table 6-J. Physical Node Addresses — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
20	D40	D41	D42	D43	D44	D45	D46	D47	D48	D49	D4A	D4B	D4C	D4D	D4E	D4F
21	D50	D51	D52	D53	D54	D55	D56	D57	D58	D59	D5A	D5B	D5C	D5D	D5E	D5F
22	D60	D61	D62	D63	D64	D65	D66	D67	D68	D69	D6A	D6B	D6C	D6D	D6E	D6F
23	D70	D71	D72	D73	D74	D75	D76	D77	D78	D79	D7A	D7B	D7C	D7D	D7E	D7F
24	D80	D81	D82	D83	D84	D85	D86	D87	D88	D89	D8A	D8B	D8C	D8D	D8E	D8F
25	D90	D91	D92	D93	D94	D95	D96	D97	D98	D99	D9A	D9B	D9C	D9D	D9E	D9F
26	DA0	DA1	DA2	DA3	DA4	DA5	DA6	DA7	DA8	DA9	DAA	DAB	DAC	DAD	DAE	DAF
27	DB0	DB1	DB2	DB3	DB4	DB5	DB6	DB7	DB8	DB9	DBA	DBB	DBC	DBD	DBE	DBF
28	DC0	DC1	DC2	DC3	DC4	DC5	DC6	DC7	DC8	DC9	DCA	DCB	DCC	DCD	DCE	DCF
29	DD0	DD1	DD2	DD3	DD4	DD5	DD6	DD7	DD8	DD9	DDA	DDB	DDC	DDD	DDE	DDF
30	DE0	DE1	DE2	DE3	DE4	DE5	DE6	DE7	DE8	DE9	DEA	DEB	DEC	DED	DEE	DEF
31	DF0	DF1	DF2	DF3	DF4	DF5	DF6	DF7	DF8	DF9	DFA	DFB	DFC	DFD	DFE	DFF
32	E00	E01	E02	E03	E04	E05	E06	E07	E08	E09	E0A	E0B	E0C	E0D	E0E	E0F
33	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E1A	E1B	E1C	E1D	E1E	E1F
34	E20	E21	E22	E23	E24	E25	E26	E27	E28	E29	E2A	E2B	E2C	E2D	E2E	E2F
35	E30	E31	E32	E33	E34	E35	E36	E37	E38	E39	E3A	E3B	E3C	E3D	E3E	E3F
36	E40	E41	E42	E43	E44	E45	E46	E47	E48	E49	E4A	E4B	E4C	E4D	E4E	E4F
37	E50	E51	E52	E53	E54	E55	E56	E57	E58	E59	E5A	E5B	E5C	E5D	E5E	E5F
38	E60	E61	E62	E63	E64	E65	E66	E67	E68	E69	E6A	E6B	E6C	E6D	E6E	E6F

Table 6-J. Physical Node Addresses — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
39	E70	E71	E72	E73	E74	E75	E76	E77	E78	E79	E7A	E7B	E7C	E7D	E7E	E7F
40	E80	E81	E82	E83	E84	E85	E86	E87	E88	E89	E8A	E8B	E8C	E8D	E8E	E8F
41	E90	E91	E92	E93	E94	E95	E96	E97	E98	E99	E9A	E9B	E9C	E9D	E9E	E9F
42	EA0	EA1	EA2	EA3	EA4	EA5	EA6	EA7	EA8	EA9	EAA	EAB	EAC	EAD	EAE	EAF
43	EB0	EB1	EB2	EB3	EB4	EB5	EB6	EB7	EB8	EB9	EBA	EBB	EBC	EBD	EBE	EBF
44	EC0	EC1	EC2	EC3	EC4	EC5	EC6	EC7	EC8	EC9	ECA	ECB	ECC	ECD	ECE	ECF
45	ED0	ED1	ED2	ED3	ED4	ED5	ED6	ED7	ED8	ED9	EDA	EDB	EDC	EDD	EDE	EDF
46	EE0	EE1	EE2	EE3	EE4	EE5	EE6	EE7	EE8	EE9	EEA	EEB	EEC	EED	EEE	EEF
47	EF0	EF1	EF2	EF3	EF4	EF5	EF6	EF7	EF8	EF9	EFA	EFB	EFC	EFD	EFE	EFF
48	F00	F01	F02	F03	F04	F05	F06	F07	F08	F09	F0A	F0B	F0C	F0D	F0E	F0F
49	F10	F11	F12	F13	F14	F15	F16	F17	F18	F19	F1A	F1B	F1C	F1D	F1E	F1F
50	F20	F21	F22	F23	F24	F25	F26	F27	F28	F29	F2A	F2B	F2C	F2D	F2E	F2F
51	F30	F31	F32	F33	F34	F35	F36	F37	F38	F39	F3A	F3B	F3C	F3D	F3E	F3F
52	F40	F41	F42	F43	F44	F45	F46	F47	F48	F49	F4A	F4B	F4C	F4D	F4E	F4F
53	F50	F51	F52	F53	F54	F55	F56	F57	F58	F59	F5A	F5B	F5C	F5D	F5E	F5F
54	F60	F61	F62	F63	F64	F65	F66	F67	F68	F69	F6A	F6B	F6C	F6D	F6E	F6F
55	F70	F71	F72	F73	F74	F75	F76	F77	F78	F79	F7A	F7B	F7C	F7D	F7E	F7F
56	F80	F81	F82	F83	F84	F85	F86	F87	F88	F89	F8A	F8B	F8C	F8D	F8E	F8F
57	F90	F91	F92	F93	F94	F95	F96	F97	F98	F99	F9A	F9B	F9C	F9D	F9E	F9F

Table 6-J. Physical Node Addresses — Hexadecimal Representation (Contd)

Ring Node	RPC	IMS User Nodes														
Group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
58	FA0	FA1	FA2	FA3	FA4	FA5	FA6	FA7	FA8	FA9	FAA	FAB	FAC	FAD	FAE	FAF
59	FB0	FB1	FB2	FB3	FB4	FB5	FB6	FB7	FB8	FB9	FBA	FBB	FBC	FBD	FBE	FBF
60	FC0	FC1	FC2	FC3	FC4	FC5	FC6	FC7	FC8	FC9	FCA	FCB	FCC	FCD	FCE	FCF
61	FDO	FD1	FD2	FD3	FD4	FD5	FD6	FD7	FD8	FD9	FDA	FDB	FDC	FDD	FDE	FDF
62	FE0	3E1	3E2	3E3	3E4	3E5	3E6	3E7	3E8	3E9	3EA	3EB	3EC	3ED	3EE	3EF
63	FF0	FF1	FF2	FF3	FF4	FF5	FF6	FF7	FF8	FF9	FFA	FFB	FFC	FFD	FFE	FFF

Audits

Even with powerful automatic recovery abilities such as application boot, the effects of software mutilation may seriously degrade system performance for several minutes at a time. Therefore, to ensure high reliability and availability, defensive techniques must be applied to minimize the effect of software errors and reduce the incidence of severe recovery actions. These defensive techniques are known as audits. Audits are a collection of programs used for monitoring the occurrence of errors, taking corrective action whenever possible, and reporting errors and inconsistencies encountered in application software. Types of errors that audits search for are as follows:

a. Errors in the state of data where a unit may be reported to be out-of-service when the unit is actually in service

b. Linkage errors between tables that cause messages to be lost as messages are passed from one function to another.

c. Application integrity errors preventing jobs from running or running too long that would eventually result in a system reinitialization

d. Consistency in errors between related tables where in many cases different subsystems have their own version.

Most audits detect and report errors, and, in some cases, correct the errors that are found. The most common error correction strategy for inconsistencies is to copy the more reliable version into the conflicting version. Other audits simply initialize the erroneous data.

When an audit relates to a data base, the ausit determines whether or not the related tables contain valid data, have been properly updated, and are consistent. Software mutilation could occur with any of these situations. If the error cannot be corrected via recent change, the audit corrects the problem at the time the problem is encountered. If this is not possible, the audit provides more detailed data on the detected error. The reports returned by the audit enable the user to manually locate and correct the errors.

NOTE:
Mismatches between the 3B Computer memory and disk memory can be corrected via recent change and are therefore **NOT** corrected by any audits.

Audit Scheduling and Control

Audits can be routine, run automatically without user intervention; user dependent, input messages must be used to initiate the audit, or a combination of both. Also, certain audits automatically run during system initialization.

Audit records reside in the equipment configuration database (ECD) and are under control of the software integrity subsystem "audit manager". The audit manager schedules both routine and demand audits.

The audit control subsystem consists of the following:

a. *System Integrity Monitor* (SIM) - Software integrity and audit control processes responsible for scheduling and dispatching all audits.

b. *Equipment Configuration Database* (ECD) - Software integrity records containing information concerning the execution of audits and audit error recovery.

c. *Output Formatter* - Provides output message format for reporting audit results to the user.

d. *Audit Commands - UNIX* RTR operating system input commands (STOP:AUD, OP:AUD, OP:AUDERR, INH:AUD, and ALW:AUD) used to query and request software integrity services. Both CNI and *UNIX* RTR operating system input commands are provided to run specific audits.

e. *Audit Requests* - Requests from trouble clearing software processes to run automatically generated audits.

f. *Plant Measurements Interface* - Counts of audit attempts and failures stored in the plant measurements database and output on the hourly PMCR report.

Audit Equipment Configuration Database (ECD) Records

Audits are identified and controlled by ECD records. All software integrity information used by system integrity monitor (SIM) is stored in the ECD. The ECD contains information used by both the operating system and the application. The ECD is maintained by the operating system. Problems with audits not running properly are most likely in the ECD. During the initialization of the audit manager after a boot and while running routine audits, SIM must access the records in the ECD. Audits are temporarily inhibited and a message is output if SIM encounters a problem accessing the ECD. If unable to allow all audits within 5 minutes, another status message is output. If the user fixes a problem in the ECD, the **ALW:AUD:ALL** command must be used to reinitialize the audit manager and begin running routine audits.

The following are the two types of records:

a. A control record that contains information that regulates the percentage of system time to be spent running audits, the parameters that control the scheduling of manually requested audits, and a master inhibit state that is used to turn off the scheduling of all routine audits.

b. Several control records for each audit that uniquely identify the audit by name and member number. These records contain all of the information that SIM needs to schedule an audit, dispatch an audit, and report errors found by the audit.

All audits are categorized on the basis of audit type such as file manager, link and band status, or database. Each of these categories is referred to as a family, and each family has a name that contains up to six characters. In addition, a member number is used to distinguish between audits in the same family.

Each audit record contains one or more audit "instances." For an audit with only one instance, the name and member number of the audit is used to identify the audit while the instance name is null.

Execution Modes

There are two aspects to any audit invocation. First, audits are grouped into either a segmented or nonsegmented category that is based on how they utilize CPU time. This is an attribute of the audit program that cannot be changed. Segmented audits relinquish the CPU after a predetermined amount of time. This is a time-slicing environment; therefore, most kernel audits execute in this mode. Running in this mode normally causes an audit to run slower than in the nonsegmented mode. However, because the continuous execution of kernel level audits could result in the lockout of lower level processes, kernel audits should execute in the segmented mode if possible. Nonsegmented audits run to completion, and report the amount of CPU time used. All operating systems or users, supervisors, and demand audits are nonsegmented. Because the time sharing of supervisor processes is controlled by the *UNIX* RTR operating system scheduler, supervisor audits execute in a nonsegmented mode.

Secondly, the audit manager provides four types of audit invocations:

a. *Routine* - Audits that are executed at a given frequency or at specified times during normal system operation. The audit manager permits one routine audit and a limited number of requested audits to run simultaneously. The maximum number of simultaneously requested audits is specified by the ECD. Routine audits run at half their normal speed while a requested audit is running.

b. *Manual* - Audits that are manually requested by means of input commands.

c. *External* - Audits that are requested by processes other than input commands. The next routinely scheduled audit may be delayed to compensate for the CPU time used by the requested audit.

d. *Demand* - Audits that are demanded by SIM as a result of a system error.

These aspects of the audit invocation are indicated in the ECD. They allow SIM to control when any particular audit runs and how much of the processor's time is used by the audit. The audit manager attempts to limit the total amount of time consumed by all routine, manual, and externally requested audits. Also, it is flexible enough to allow an audit to execute in any of the four execution modes, depending on the nature of the audit invocation. All execution modes might not be appropriate for all audits. Again, the permitted execution modes of each audit are specified in one of the ECD records for that audit.

When an audit is invoked, the sequence of events shown in Table 6-K typically occurs.

Table 6-K. Audit Execution Sequence

Step	Action
1	If the audit resides in a transient process, SIM creates the process. Otherwise, it finds the audit process using information in the ECD record of the audit.
2	SIM dispatches the audit.
3	The audit may find and possibly correct errors. It reports each error to the audit interface library, which increments an error counter. One or more of the error reports results in the printing of a raw data output message.
4	The audit finishes its work and reports its termination status to the interface library, which reports the total error counts to SIM. SIM updates the error counters in the ECD record of the audit, and a final output message is printed. SIM also updates the audit's counts of attempts and failures in the PMS data base.
5	If an error threshold has been exceeded, SIM takes recovery action as specified in the ECD record of the audit.

Blocking and Inhibiting Audits

The following two mechanisms are available to prevent the running of audits:

Blocking — A process specifically requests the blocking of an audit. This is explicit blocking and prevents the audit from being executed in any mode. When scheduling audits, SIM implicitly blocks certain audits. It ensures that no two audits with the same name are run simultaneously.

Inhibiting — This prevents audits from being scheduled to run routinely. Separate inhibit states are provided for all audits. The **INH:AUD** and **ALW:AUD** commands are used to control these inhibit states. Setting or resetting the master inhibit state for all audits does not affect the inhibit states of individual audits.

Because audit inhibit states are stored in the ECD, audit inhibit states are not lost across an operating system level 2 initialization (boot). However, they are lost across an operating system level 3 or 4 initialization. When the system is booted in minimum configuration, all audits remain inhibited. Also if IMS or CNI is not running, certain audits pertaining to those subsystems are automatically inhibited. In full configuration, SIM allows all audits approximately 5 minutes after the boot; unless, the audits have been inhibited manually before the boot (level 2 only). Manually inhibited audits are not allowed automatically by SIM.

A periodic output message (**REPT AUDSTAT**) reports the inhibit status of audits when the system is running in full configuration.

Scheduling Routine Audits

Routine audits are scheduled in two ways:

Frequency Groups — Some audits need to run often taking a small amount of time to ensure the integrity of critical system resources that are in a constant state of flux. Many *UNIX* RTR operating system audits use this type of scheduling. How often an audit is scheduled depends on what effect an undetected error would have on the system. Each frequency group audit is assigned a specific frequency of execution. Each frequency group executes audits twice as often as the next frequency group. The frequency group of each audit is specified in one of the audit's ECD records. An audit in any specific frequency group cannot be guaranteed to execute repeatedly at a predetermined time interval. Review the Plant Measurements Common Reports (PMCR) report for details on how many times each audit is executed.

Timed — Other audits need to run only occasionally to check on resources that change less often and some audits may need to be coordinated with other timed activities. Examples of these include database audits and file system audits. Audits that must be executed at given times of the day use the timed audit facility. Each timed audit must be scheduled to execute at a specific hour of the day (0000 to 2300) and on a specific day of the week (Sunday through Saturday). This information is maintained in the ECD records of the audit. The same audit may not be both timed and in a frequency group.

Error Reporting and Recovery

Errors detected by audits are grouped into categories for purposes of reporting and recovery. The error categories used by an audit are specified in its ECD records. For each category, there is an error threshold; a time interval during which errors are counted; and a list of recovery actions that should be taken, if the threshold is exceeded. Separate error counts are accumulated for each audit. No error counts are accumulated when an audit is run in the noncorrecting mode.

There are specific recovery actions taken by the audit manager. When an audit fails, a report is generated and SIM attempts to reschedule the audit. If an audit aborts, SIM attempts to run it once more in demand mode. The ECD control record may specify that SIM not demand the audit in this situation. If the ECD allows it and the audit aborted while correcting errors, SIM demands the audit once. If the audit aborts the same way a second time, SIM inhibits the audit and outputs a message. There are two stages of audit recovery:

0 Errors detected by the audit exceeded a threshold. The audit may be demand invoked by SIM.

1 The audit reported abnormal completion and errors exceeded a threshold. A different audit may be demanded.

Output messages are printed for routine and externally requested audits only if the audits report errors or abnormal completion. Output messages are always printed for manual and demand audits. However, when a demand audit is run as a recovery action for a manual audit that failed, its output may not be printed on the same terminal from which the initial input message was entered.

Audit Analysis

Although information on audit execution is reported to the user via the **AUD** output messages, there are other messages that provide important audit information to the user. They should be used when an audit unexpectedly starts reporting a lot of errors. Some of these messages are produced in response to manual requests by the user, when additional audit information is needed. Some are generated automatically—giving error and status reports. In addition, there are processor recovery messages (PRMs) that provide information to aid the user during 3B Computer recovery. Message descriptions should be referenced for suggested actions to be taken. The user should also refer to the specific audit descriptions.

Currently, two PRMs provide audit-related information to the user during 3B Computer recovery. Both messages are output by SIM. Both PRMs provide information that describes the function or possible error and any corrective action that should be taken:.

a. PRM FBxx xx07 xxxx xxxx xx xx xx
Function code 07 indicates an audit manager initialization failure. This means that SIM was unable to initialize the audit manager because of a failure while attempting to access the ECD. Perform the following corrective actions:

1. Verify and correct the SIM control records or audit records in the ECD. Changes to the ECD should only be made by the technical support group.
2. Attempt to initialize the audit manager (**ALW:AUD:ALL**)
3. Obtain technical assistance if the audit manager does not initialize.

b. PRM FBxx xx08 xxxx xxxx xx xx xx
Function code 08 indicates that SIM was unable to attach to the plant measurement system (PMS) database. Perform the following corrective action:

1. Verify and correct the PMS database. Changes to this database should be verified by the technical support group.
2. Attempt to attach the PMS database to SIM (**ALW:AUD:ALL**)
3. Obtain technical assistance if SIM is still unable to attach to the PMS data base.

There are basically four types of output when analyzing audit errors:

1. **AUD** message
2. PMCR report
3. Various related messages
4. PRMs.

By correlating the information provided by these messages and reports, patterns can be identified. Also, specific data on uncorrected errors can be used to identify the suspect software or hardware causing the audit to fail. It is important to note that most audits are *correcting* audits. Nevertheless, recurrent error correction by the same audit indicate problems outside the scope of the audit. This is where identified patterns can lead to a solution of the problem.

The major items to check on the messages and reports are as follows:

- Check the types and frequencies of specific errors encountered
- Identify errors corrected, errors not corrected and quantity of errors found. The PMCR report indicates quantity of errors found by each audit. It should be noted that if an audit runs automatically and finds no errors, there is no printout associated with the audit.

- Identify when and if specific audits were executed. It should be noted that CNI system audits are considered low priority processes. If the system is loaded with a large amount of CCS traffic or other non-deferrable work, audits may not run as scheduled.
- Identify if particular audits aborted or completed.
- Identify other messages indicating changes in the state of particular units made suspect by audit errors.

A particular audit taking a long time to complete is not necessarily an indication of problems. Most audits are considered deferrable, other work could slow them down. Also, because most audits check office-dependent data structures, the amount of time required to complete depends on how the office is equipped. Audit descriptions indicate the approximate time it takes for the audit to complete. The times indicated are based on the amount of time required to execute the audit. When an audit is manually requested, it may or may not execute immediately. In a busy office, the amount of time required to execute an audit is often insignificant compared to the length of time the audit is deferred.

Audit (AUD) output messages report audit execution results to the user. There are two types of audit output messages. The first type reports raw data that pertains to specific errors found by an audit. The second type reports the termination status of the audit.

The data reported by an **AUD** error message includes four words of raw data designated DATA1, DATA2, DATA3, and DATA4. These words are printed in hexadecimal notation. Each audit prints a limited number of raw data reports which are specified in the ECD. The definitions of these data words and the maximum number of reports possible is specific to each audit. This information is provided in the output message manual. Some audits do not use the data words, and they are therefore identified with zeros in their respective fields. Many audit error messages provide supplementary data to facilitate analysis of the reported error conditions. The data words and supplementary data present the user with the state of various software facilities being checked by the audit.

The audit completion messages report the termination status, COMPLETED, STOPPED, or ABORTED, of the audits. If the termination status is COMPLETED, the total number of errors found and the number of errors corrected by the audit are reported in the message. If the termination status is STOPPED, errors may have been reported before manual action stopped the audit. If the termination status is ABORTED, an abort code is provided to specify why the audit was aborted. Table 6-L identifies the audit abort codes.

The PMCR report is generated by the *UNIX* RTR operating system both hourly and daily. It includes a section identified as "System Performance" that details audit activity for the preceding hour. The number of attempts SIM attempted to run the audit and the number of errors detected are identified for each audit.

The actual number of successful completions of the audit and the number of errors corrected must be obtained using the **OP:AUD** input command. If an audit appears on the PMCR report, the audit is in the ECD and has tried to run.

Table 6-L. Audit Abort Codes

Code	Meaning
3	Audit aborted internally without completing its work
4	Audit was faulted while correcting errors
5	SIM could not start or dispatch the audit
6	Error was encountered in the audit control/audit library interface
7	Audit exceeded its time-out or segment limit
8	SIM aborted an executing routine audit because of a blocking request
9	Transient process that was running the audit terminated
10	A segmented audit exceeded an error threshold

The **OP AUDERR** output message outputs the error counts that were extracted from the ECD records for audits controlled by SIM. Such information can be useful to the user as historical data. The **OP AUDERR** output message simply furnishes statistical information reguarding audits to the user.

The **REPT AUDSTAT** output message is produced automatically by the system approximately every 30 minutes. This report prints the status of inhibited audits controlled by SIM. When this message is output, one or more audits are either inhibited or blocked.

The **REPT SIMCHK** output message reports failures in SIM. If the audit manager fails to initialize after a system boot, SIM temporarily inhibits all audits and outputs this message. In addition, if SIM has difficulty accessing the ECD when routinely running audits, this message is generated. If SIM cannot allow audits to run within 5 minutes, it outputs another message. Manual action is required by the user to determine the cause of the problem.

Central Node Control Audit

The central node control (CNC) audit is a routine audit that is run automatically a number of times every hour. The purpose of the audit is to detect and correct any inconsistencies or errors in the status of various scheduled jobs related to nodes. Internal ring node maintenance records are checked for inconsistencies which could prevent jobs, such as RST:LN, from progressing or cause jobs to be unnecessarily aborted. The two main types of jobs checked by the audit are those for node pumping and node restoral. If errors are detected, all jobs associated with the node are cancelled. Should an inconsistency be caused by some undetected problem, this audit only cancels those jobs associated with the

node affected by the inconsistency. Therefore, the same jobs may be canceled every time the audit runs. If those jobs must run and the problem cannot be identified by examination of the output, a system initialization may be necessary.

If the audit is running automatically or the detailed option (DETL) was specified, up to 20 detailed reports are provided. These reports, four data words and no supplementary data, provide the restore job's state, source, and associated node address.

This audit normally takes less than 10 seconds to run depending on the number of equipped nodes in the office. If IMS is very busy at the time the audit is requested, the execution time could be lengthened considerably. This audit corrects any errors found.

Node State Audit

The node state audit is a routine audit that is run automatically several times every hour. The purpose of the audit is to detect and correct any inconsistencies in the node state data maintained by IMS in the central processor. The audit currently has only one member. Member 1 compares the node availability map with the IMS driver node state data. The node availability map indicates whether a node is available or not. The node state audit is used by other software, such as the neighbor node audit, to determine node states. Normally, audit data is updated simultaneously with the IMS driver data. This audit corrects any inconsistencies by copying the IMS driver data to the node availability map.

If the audit is running automatically or the detailed option (DETL) was specified, up to 10 detailed reports are provided. These reports provide ring node identification, group and member, and node states maintained by the node availability map and IMS driver. This audit usually takes approximately 2.5 minutes to run depending on how busy the IMS is at the time. The node state audit corrects all errors found.

Direct Link Node Audit

The direct link node (DLN) audit is a routine audit that is run automatically at a frequency dependent on the real-time load of the 3B Computer. The DLN audit function resides in both the 3B computer and the DLN. Data in the DLN is updated only after associated data in the 3B Computer is updated. It is required that the data in the DLN be updated correctly and not be altered accidentally at any time. The purpose of DLN audits is to ensure the integrity and accuracy of all the data/tables updated in the 3B Computer and DLN.

The data/tables of both the 3B Computer and DLN are divided into segments. Only one segment is audited at a time. All the segments are audited sequentially to complete one audit cycle. An audit failure detected against any one segment of the DLN triggers another audit request against the failed segment. If a segment fails the audit twice, the DLN audit function updates the failed segment of the DLN.

If the audit is running automatically, up to 16 reports are provided. The function is scheduled to be run by default, unless it is otherwise directed by the ECD entry. The DLN audit function can also be run manually. The DLN audit usually takes about 75 seconds to run depending on the office load and should be run at a medium or low priority band so as not to consume too much of the Audit Manager's resources.

Internal Data Audits

The internal data audits compare the tables contained in main memory with tables maintained on disk and report any mismatches. The tables are also checked for invalid data within a table and inconsistencies across tables. The audit reports all errors that are found via the appropriate **AUD:NIDATA** output message. The error code received with the output message can be used to identify the action to be taken to correct the problem in the tables. If any errors are identified that cannot be corrected via recent changes, then the audit corrects the error as necessary and reports the correction.

The internal data audits are manual audits only. To run these audits, the user must manually invoke the audit by entering **AUD:NIDATA** x where x represents the specific audit to be run (1-6). It is suggested that these audits be run weekly to ensure the reliability of the CNI data base. It is also suggested that these audits be run after completion of recent change activity to audit the success of the session. It is not necessary to run these audits after each recent change order is completed. However, once the user has completed all recent change activity for a session it is suggested that these audits be activated. Any errors found by these audits should be referred to the database administrator.

Processor Recovery Messages (PRMs)

During system recovery, the common network interface initialization (CNIINIT) process may produce a 16-digit hexadecimal failure PRM. The PRMs are displayed on the maintenance cathode ray tube (MCRT) and printed at the maintenance receive-only printer (MROP). Failing PRMs are always output. By selecting the emergency action interface (EAI) PRM-TRAP option, the first failing PRM is trapped and displayed in reverse video on the MCRT.

Processor Recovery Message Format

A PRM output identifies the process encountering the failure, states the reason for failure, and in many cases, includes failure data. The general format of a PRM is shown in Figure 6-9.

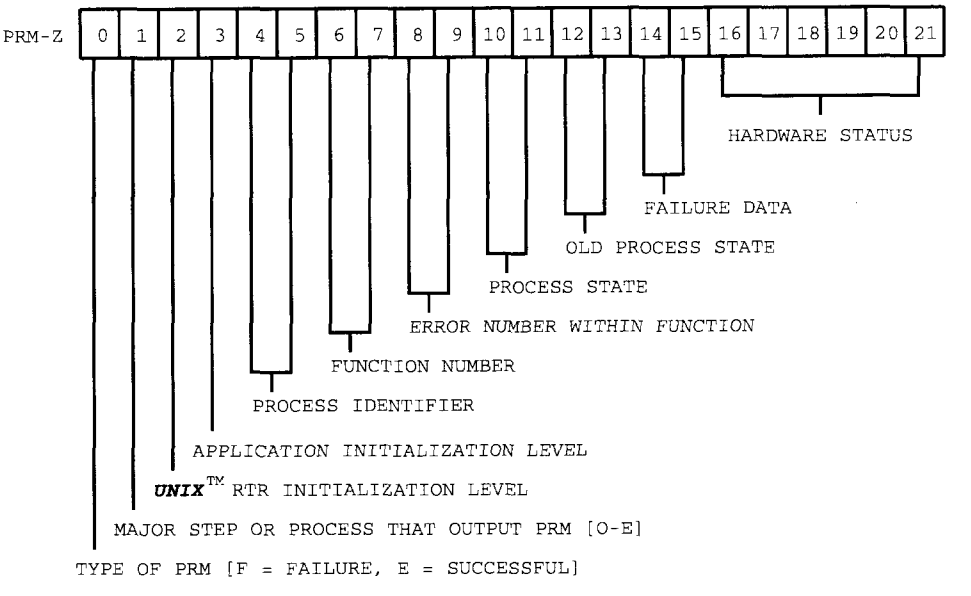


Figure 6-9. Processor Recovery Message (PRM) Format

The definition of each digit in the PRM is as follows:

Letter Z	= Identifies active control unit (CU) Zero (0) for CU0. One (1) for CU1.
Digit 0	= Message type: F = Failure E = Success A failure PRM (F) occurs when an error is considered fatal and a phase is called. A success PRM (E) is an information message which describes a function or a possible error and any corrective action that should be attempted.
Digit 1	= Major step or process that output PRM. CNI PRM major step is "E" (IMS Application Process)
Digit 2	= *UNIX* RTR level of initialization.
Digit 3	= Application level of initialization.
Digit 4 & 5	= Two-digit process identifier. CNI PRM process identifier is 7F" (CNIINIT process)
Digits 6 & 7	= Two-digit hexadecimal function code.
Digits 8 & 9	= Two-digit code identifying error within function.
Digits 10 & 11	= Two-digit code identifying internal state originating process was in when the error was detected.
Digits 12 & 13	= Two-digit code identifying previous state originating process was in subsequent to state where the error was detected.
Digits 14 & 15	= Two-digit code identifying error data. These digits are not always used.
Digits 16-21	= Six-digit code representing hardware status.

Analyzing Processor Recovery Messages

To analyze a PRM, complete the following procedure:

1. Examine PRM Z field to determine processor that produced PRM (CUO=0 or CU1=1).
2. Examine PRM digit 0 to determine if PRM is a success (E) or failure (F) PRM.
3. Locate received PRM in Processor Recovery Message Manual by the number or letter in digit positions 0, 1, 4, 5, 6 and 7. The underlined characters in the following example indicate the digit positions used to locate the PRM:

   F_E_xy 7_F_3_4_ eess oo00 hh hh hh

4. Read comments under **RECOVERY STEP** heading to identify the major step or process that outputs PRM.
5. Read comments under **FUNCTION** heading to determine which function within the recovery step was being performed.
6. Read comments under **PRM EXPANSION** heading to interpret any failure information provided.
7. Read comments under **EXPLANATION** heading for additional information.
8. Follow actions suggested under **CORRECTIVE ACTION** heading to correct any failures.
9. Examine PRM digits 16 through 21 to determine hardware status of 3B Computer when PRM was generated.
10. Contact appropriate technical support organization if additional information is required.

3B Computer Maintenance Functions

The 3B Computer is the central processing unit (CPU) and must be able to communicate with any node on the ring in the maintenance mode. The handlers associated with each type of peripheral contain the functions needed to perform the following tasks:

a. In-service software functions

b. Fault detection and recovery actions

c. Software audits

d. Hardware audits

e. Neighbor audits

f. Ring audits

g. Blockage

h. Message format errors

i. Abnormal end of process

j. Parity errors

k. Quarantine

l. Reset.

The 3B Computer also has the function of providing system and ring initialization, node processor initialization, and reconfiguration. The 3B Computer has ultimate control of ring actions. It has the responsibility of determining fault locations and the configuration of the ring. The 3B Computer also determines whether to fault a piece of hardware, diagnose, or restart it. These decisions are based on error messages received from RPCNs and the peripheral performance history.

Glossary

GL

Contents

Glossary

A

Analog Signaling Link
The link running from the link node (LN) (but not including the ring interface [RI] board) through a data set and voice-frequency link (VFL) access circuit to the transmission facility.

Attached Processor (AP)
A circuit pack used with the direct link node (DLN) that provides expanded storage for added processing capacity on the ring.

Available
While in the minor state "In-Service (IS)," the signaling link is available for handling traffic. The minor state "Out of Service (OOS)" is a transient state that is automatically accessed when putting a signaling link in service or when an error condition occurs on an in-service signaling link. The minor state "Manual Out of Service (MOOS)" is used when it is necessary to manually remove the signaling link from service.

B

Beginning of Isolation (BISO) Node
A node on the ring that is located before the beginning of an isolated segment but is not isolated itself.

C

CCITT
An international body that controls the standards of communication protocols.

CLLI Code
The common language location identification code used to uniquely identify an office.

Cluster Member
A cluster member is a single node within a cluster. A cluster member is used to uniquely identify a specific node within a known cluster.

Collection Period
The time span over which report measurement data is to be collected and stored.

Common Network Interface (CNI)
A common subsystem software component supplied to various network components whose primary function is providing CCS network access and CCS message routing.

Critical Event
Events that occur in the CCS network that may affect network operations. These events are reported to users immediately.

D

D-Channel (DCHN)
Refers to both the signaling link and the node that is used to provide a DCHN interface between customer premises equipment (CPE) and a CNI- equipped office and is associated with a T1 facility access (T1FA) board used for multiplexing/demultiplexing DS0 signals.

Destination Point Code (DPC)
A unique value associated with every network component used for routing.

Digital Signaling Link
The link running from the link node (LN) (but not including the RI board) through a digital service adapter (DSA), digital service unit (DSU), and channel service unit (CSU) (optional) to the transmission facility.

Direct Link Node (DLN)
A node on the ring that functions like an interprocess message switch (IMS) user node (IUN) but contains the hardware of a ring peripheral controller node (RPCN) plus an attached processor and direct memory access (DMA) capability.

E

End of Isolation (EISO) Node
A node on the ring that is located after the end of an isolated segment but is not isolated itself.

Equipment Configuration Data (ECD)
The ECD is a UNIX® RTR-provided memory-resident data base that contains the attributes and current status of various system entities. These entities include all known processor and peripheral hardware and most software facilities. Data is stored in individually accessible records. Virtually all operations and maintenance of CNI/IMS are dependent on the ECD.

I

IMS User Node (IUN)
A basic node (minimum hardware components) on the ring that provides an interface between the ring and the transmission facility.

Integrated Service Digital Network Extended D-Channel (DCHX)
Feature of CNI 10.4 generic program that increases tunable number of D-Channel nodes from 40 to 60. Increases maximum number of DCHNs supported per 4ESS Switch from 40 to 54.

Interprocess Message Switch (IMS)
A common subsystem software component that provides a ring-based interfunction, interprocessor transport mechanism.

ISDN Network
A configuration in a CNI equipped office which supports an integrated services digital network (ISDN) interface directly to customer premises equipment (CPE).

L

Link Node (LN)
A node on the ring where digital information enters from or exits to the transmission facility.

Link Set Routing
CCS7 routing using point codes to identify the destination of link messages associated with a link set.

M

Message Transfer Part (MTP)
The functional part of CCS7 that transfers signaling messages as required by all the users and that also performs the necessary subsidiary functions (e.g., error control and signaling security).

N

Node Processor (NP)
The node processor (NP) is the central processing unit (CPU) portion of a ring node (RN). The NP controls and schedules the processes in the ring node.

O

Overflow
A condition that occurs when buffer occupancy exceeds some predetermined level. If related to link transmit/receive buffers, this term means the buffer is full and additional messages are necessarily discarded. If related to ring buffers (overflow states), it does not necessarily mean any buffer is full, but messages may be discarded according to some congestion strategy that is usually associated with some onset and abatement thresholds.

Overload
A condition that occurs when the load on some resource is excessive. This could be a lack of real time as in the buffer overload case. The latter is synonymous with buffer congestion. Messages may be discarded even though the buffer is not full. This is usually associated with some onset and abatement thresholds.

R

Raw Measurement
This is the data values taken from buffers in the ring nodes. After a value is aggregated with the corresponding value from other nodes, it is known as a measurement. This measurement is cumulated with new values over time to be output after some collection period has elapsed.

Ring
Refers collectively to the RPCNs, DLNs, and application link nodes that are serially connected to dual circular busses. The ring provides 4-megabyte data paths in both directions between adjacent nodes and can uniquely address up to 1024 nodes.

Ring Configuration
A reconfiguration of the ring via the 3B20D Computer to isolate faulty segments.

Ring Interface (RI)
One of two circuits in a ring node that interfaces the node processor to the ring. Each ring interface can access either ring 0 or ring 1 to insert messages onto, or remove messages from the active ring. The heart of the circuit is a first-in first-

out (FIFO) buffer that provides access to the ring and allows messages to circulate on the ring independent of the node.

Ring Isolation
A ring configuration where one or more nodes are isolated from the active ring.

Ring Peripheral Controller Node (RPCN)
A node on the ring where digital information is removed from the ring for transferral to the 3B20D computer for processing or placed back on the ring after processing.

S

Self-Looped
A condition that exists when both ends of a signaling link terminate on the same ring node. All messages sent over the signaling link are looped back; thus, they are transmitted and received by the same signaling link.

Signaling Connection Control Part (SCCP)
An adjunct to the message transfer part (MTP) layer of CCS7 that performs interpoint code subsystem status.

Signaling Link (SLK) States
The signaling link states indicate the status of the signaling link. A brief description of the three major states and their associated minor states follow:

T

T1 Facility Access (T1FA)
A board that multiplexes and demultiplexes 24 DS0 64-kb/s links into one DS1 1.544 Mb/s bit stream. A single T1FA board can serve up to 24 DCHN signaling links.

T1FA Control Node (TCN)
A DCHN node that contains a T1FA and has responsibility for monitoring and controlling the T1FA circuitry in addition to its normal DCHN node functions.

U

Unavailable
This state is used as an interim state for testing purposes before putting the signaling link in service. While in the minor state "Grow," no link usage information is provided to the user. While in the minor state "Test," link usage information is provided to the user but the signaling link does not alarm and/or interact with the network.

Unequipped
In this state, no link configuration data has been assigned to the signaling link.

V

Virtual Link
A virtual link allows one physical link to be used for carrying traffic for eight "logical software" links.

Abbreviations

2

2STP
No. 2 Signal Transfer Point

3

30MPR
Thirty-Minute Marginal Performance Report

3BI
3B20D Computer Interface

4

4ESS™
4ESS Switching System

A

AAR
Automatic Ring Recovery

ABT
Abort

ACI
AT&T Communications ISDN

ACO
Alarm Cutoff

ACRT
Administrative Cathode-Ray Tube

ACT
Active

ACU
Acknowledgment Unit

AFA
Analog Facility Access

AFAF/C
Analog Facility Access Frame/Cabinet

ALM
Alarm

ANS
Answer Message

ANSI
American National Standards Institute

AP
Attached Processor

API
Attached Processor Interface

APS
Attached Processor System

ARR
Automatic Ring Recovery

ARS
Alarm Reset

ASCII
American Standard Code for Information Interchange

ASUR
Application Specified Unconditional Restore

ATP
All Tests Passed

AUTO
Automatic

AVL
Available

B

b/s
Bits Per Second

BAT
Battery

BCD
Binary Coded Decimal

BISO
Beginning of Isolation

BLDG
Building

BWM
Broadcast Warning Message

C

C&D
Control and Display

CATP
Conditional All Tests Passed

CCIS
Common Channel Interoffice Signaling

CCITT
International Telephone and Telegraph Consultative Committee

CCS
Common Channel Signaling

CCS6
Message format conforming to domestic version of CCITT 6 signaling

CCS7
Common Channel Signaling No. 7

CD
Circuit Drawing

CDR
Call Detail Recording

CDRP
Call Detail Reording Platform

CET
Critical Event Table

CHRM
Current Hour

CIC
Circuit Identification Code

CLLI
Common Language Location Identification

CNCE
CCS Network Critical Event

CNI
Common Network Interface

CNIINIT
Common Network Interface Initialization

COV
Changeover

CP
Circuit Pack

CPE
Customer Premises Equipment

CPU
Central Processing Unit

CRC
Cyclic Redundancy Check

CRCER
Cyclic Redundancy Check Error

CRI
Continuity Recheck Incoming

CRO
Continuity Recheck Outgoing

CRT
Cathode-Ray Tube

CSU
Channel Service Unit

CU
Controller Unit

D

DACS
Digital Access and Cross-Connect System

dB
Decibel

DBA
Data Base Administration

dBm
Decibels referred to 1 milliwatt

dBrn
Decibels referred to reference noise

DCHN
D-Channel

DCHX
Extended D-Channel

DCIS6
Destination Routed CCIS 6

DDS
Digital Data System

DDSBS
Dual Duplex Serial Bus Selector

DETL
Detailed Option

DFA
Digital Facility Access

DFAF/C
Digital Facility Access Frame/Cabinet

DFC
Disk File Controller

DGN
Diagnose

DLN
Direct Link Node

DLN-AP
Direct Link Node-Attached Processor

DLNE
Enhanced Direct Link Node

DMA
Direct Memory Access

DMERT
Duplex Multi-environment Real-time

DPC
Destination Point Code

DPRAM
Dual-Port Random Access Memory

DS
Data Selector

DSA
Digital Service Adapter

DSCH
Dual Serial Channel

DSSBS
Duplex Dual Serial Bus Selector

DSU
Digital Service Unit

DSX
Digital Cross-connect

E

EAI
Emergency Action Interface

EAR
Error Analysis and Recovery

ECD
Equipment Configuration Data

ECIS6
Embedded CCIS 6

EIA
Electronic Industries Association

EISO
End of Isolation

ELT
Emergency Load Transfer

EMC
Electromagnetic Compatibility

EMER
Emergency

EMI
Electromagnetic Interference

EML
Expected Measured Loss

EX
Interactive Diagnostics

EXCP
Exception Table

EXCT
Exception Table

F

FIFO
First-In First-Out

FLTY
Faulty

FPI
Full Process Initialization

G

GSC
Group Signaling Congestion

GT
Global Title

GTT
Global Title Translation

H

HD
High Density

HDB
High Density Backplane

HFDT
History File Descriptor Table

Hz
Hertz

I

IAD
Integrated Access Distributor

IAM
Initial Address Message

IFB
Interframe Buffer

IFB-P
Interframe Buffer - Padded

ILN
International Link Node

IM
Input Manual

IMS
Interprocess Message Switch

INH
Inhibit

INIT
Initializing

IOP
Input/Output Processor

IRN
Integrated Ring Node

IS
In-Service

ISC
International Switching Center

ISDN
Integrated Services Digital Network

ISUP
Integrated Services Digital Network User Part

IUN
IMS User Node

K

kb/s
Kilobits Per Second

L

L30M
Last 30 Minutes

LAP-B
Link Access Protocol-Balanced

LAP-D
Link Access Protocol-DCHN

lday
Last Day

LED
Light-Emitting Diode

LI
Link Interface

LI4
Four-Port Link Interface

LKPLID
Logical-to-Physical Link Identifier

LL
Local Loopback

LN
Link Node

LNU
Link Node Unit

LO
Local

LPM
Last Period Measurement

M

MAN
Manual

Mb/s
Megabits per Second

MCRT
Maintenance Cathode-Ray Tube

MDCT
Minor Device Chain Table

MH
Message Handler

MHD
Moving Head Disk

MJ
Major

MML
Man-Machine Language

MN
Minor

MOCT
Measurement Output Control Table

MOOS
Manual Out of Service

MPR
Machine Performance Report

MROP
Maintenance Receive-Only Printer

MSG
Message

MSU
Message Signal Units

MTP
Message Transfer Part

MTTY
Maintenance Teletype

N

NCN
Noncontrol Node

NEBS
New Equipment Building Standards

NI
Network Interconnect

NID
Network Identifies

NP
Node Processor

NPI
Node Processor Interface Logic

NRM
Node Recovery Monitor

NT
No Token

NTR
No Test Run

NUT
Node Under Test

O

OA&M
Operation, Administration, and Maintenance

OFL
Overflow

OM
Output Manual

OMAP
Operations, Maintenance, and Administration Part

OOS
Out of Service

OPC
Originating Point Code

OSI
Open Systems Interconnection

OSWF
On-Site Work Force

P

PA
Power Alarm

PAS
Protected Application Segment

PD
Power Distribution

PDF
Power Distribution Frame

PDS
Program Documentation Standards

PDT
Page Descriptor Table

PLID
Physical Link Identification

PMCR
Plant Measurement Common Reports

POA
Priority of Action

POTS
Plain Old Telephone Service

PR
Peripheral Routing

PRM
Processor Recovery Message

PRO
Processor Outage

PSC
Processor Congestion

PSM
Power Switch Monitor

PWR
Power

Q

QUSBL
Quarantine Usable

R

RABT
Received Abort

RAC
Ring Access Circuit

RAM
Random Access Memory

RC
Recent Change

RC/V
Recent Change and Verify

REL
Release Message

REX
Routine Exercise

RF
Radio Frequency

RGDP
Ring Group Display Page

RI
Ring Interface

RINGEX
Ring Exception

RMV
Remove

RN
Ring Node

RNA
Ring Node Address

RNC
Ring Node Cabinet

RNF/C
Ring Node Frame/Cabinet

RNR
Receive Not Ready

ROM
Read Only Memory

ROP
Read-Only Printer

RPC
Ring Peripheral Controller

RPCN
Ring Peripheral Controller Node

RQ
Ring Quarantine

RST
Restore

RTR
Real-Time Reliable

S

SAPI
Service Access Point Identifier

SCC
Switching Control Center

SCCP
Signaling Connection Control Part

SCHT
Scheduler Table

SCMG
Signaling Connection

SCP
Service Control Point

SCSI
Small Computer Systems Interface

SD
Schematic Drawing

SDN
Software Defined Network

SDT
Segment Descriptor Table

SEP
Signaling End Point

SEPR
Signaling

SIM
System Integrity Monitor

SIN
Small Computer Systems Interface Node

SIO
Service Indicator Octet

SLK
Signaling Link

SLMK
Signaling Link Maintenance Kernel

SLS
Signaling Link Selection

SNPR1
Signaling Network Performance Report—Part 1

SNPR2
Signaling Network Performance Report—Part 2

SP
Signaling Point

SPC
Stored Program Control

SPI
Signaling Point Isolation

SRM
Signaling Route Management

SSI
Small Scale Integration

SSN
Signaling Point and Subsystem Number

STBY
Standby

STF
Some Tests Failed

STP
Signal Transfer Point

SU
Signal Unit

SUIE
Signal Units In Error

SYS
System

T

T1FA
T1 Facility Access

TC
Transaction Capabilities

TCA
Transfer Cluster Allowed

TCN
T1FA Control Node

TCR
Transfer Cluster Restricted

TEI
Terminal Endpoint Identifier

TFA
Transfer Allowed

TFP
Transfer Prohibited

TFR
Transfer Restricted

TG4
4 ESS Switch Translation Guide

TIMS
Transmission Impairment Measuring Set

TLP
Transmission Level Point

TMS
Transmission Measuring Set

TSN
Trunk Scanner Number

TTFF
Token track flip flop

U

UCB
Unit Control Block

UDS
Unitdata Service

UDT
Unitdata

UL
Underwriters Laboratories

UNAV
Unavailable

UNEQ
Unequipped

UNTSTD
Untested

USBL
Usable

UVDT
User View Descriptor Table

V

VFL
Voice Frequency Link

VLSI
Very Large Scale Integration

Index

3

5

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V