Critical Release Notice

Publication number: 297-8991-500
Publication release: Standard 05.01

The content of this customer NTP supports the SN06 (DMS) software release.

Bookmarks used in this NTP highlight the changes between the NA015 baseline and the current release. The bookmarks provided are color-coded to identify release-specific content changes. NTP volumes that do not contain bookmarks indicate that the NA015 baseline remains unchanged and is valid for the current release.

Bookmark Color Legend

Black: Applies to content for the NA015 baseline that is valid through the current release.

Red: Applies to new or modified content for NA017 that is valid through the current release.

Blue: Applies to new or modified content for NA018 (SN05 DMS) that is valid through the current release.

Green: Applies to new or modified content for SN06 (DMS) that is valid through the current release.

Attention!
Adobe Acrobat Reader 5.0 is required to view bookmarks in color.

Publication History

September 2003

For the SN06 (DMS) release, 05.01, updates were mad according to CR Q00319430, Q00508407, and Q00544114

DMS-100 Family

All Product Computing-Module Loads

Maintenance and Operations Manual

2001Q1   Standard   04.02   March 2001

NORTEL NETWORKS™

THIS PAGE INTENTIONALLY LEFT BLANK

DMS-100 Family

All Product Computing-Module Loads

Maintenance and Operations Manual

Publication number: 297-8991-500
Product release: All Product Computing-Module Loads
Document release: Standard 04.02
Date: March 2001

Trademarks

AccessNode™, AccessNode Express™, ADAS™, BNR™, Directory One™, Compu CALL™, DMS™, DMS1U™, DMS-10™, DMS-100™, DMS-100/200™, DMS-200™, DMS-250™, DMS-300™, DMS-300/250™, DMS-500™, DMS-Bus™, DMS-Core™, DMS-MTX™, DMS-STP™, C-SCAN™, DE-4E™, Digitone™, DPN™, DPN-100™, DPX™, Fiberworld™, Internet Thruway™, Magellan™, MAP™, Meridian™, Meridian Digital Centrex™, Meridian 5009™, Meridian 5209™, Meridian 5209-T™, Meridian M5112™, Meridian 5317T™, Meridian M209™, Meridian M312™, Meridian M518™, Meridian M536™, Nortel Networks™, S/DMS™, MSL-100™, SLC™, SuperNode™, BRISC™, TOPS™, and the globemark are trademarks of Nortel Networks Corporation.

Datapath™ is a trademark used by Nortel Networks under license.

EADAS™ is a trademark of Lucent Technologies.

Ethernet™ is a trademark of Xerox Corporation.

SEAS™ and CLASS™ are trademarks of Telcordia Technologies, Inc.

All other trademarks that are found within this document and were not listed above are the property of their respective holders.

Revision history

Software	Date	Revisions
thru NA014	**March 2001**	Added Data Grooming section
		Corrected error in SDM overview and maintenance section for CSR
thru NA014	**January 2001**	added 1-Meg Modem Overview and Maintenance section
		added XPM (XMS-based Peripheral Module) Overview and Dual Shelf Maintenance section
		added TOPS IP Overview and Maintenance
		added Star Remote System Overview and Maintenance section
		added ISDN Line Drawer for Remotes (ILD-R) Overview and Maintenance
		added TOPS ISUP Overview and Maintenance

Software (continued)	Date (continued)	Revisions (continued)
		Added UEN/UE9000 Overview and Maintenance section
		retired References (made obsolete by PCL)
		updated for Product Computing-module Loads (PCL) thru NA014
		removed tag line from brand
		corrected level3ix and level4ix index problems
		updated Abbreviations and Acronyms
		updated questionnaire and contact information
		added www.nortelnetworks.com references
thru NA012	January 2000	updated ENET section to include 32K ENET overview and maintenance
		added Input/Output Module (IOM) overview and maintenance section
		added SuperNode Data Manager (SDM) overview and maintenance section
		added DMS-Spectrum Peripheral Module (SPM) overview and maintenance section
		added Extended Architecture Core (XA-Core) overview and maintenance section
		updated documentation section to include CD-ROM recycling program, deleted microfiche
		updated for Product Computing-module Loads (PCL) thru NA012
		removed SEA/SEB (no longer updated)
		made editorial updates and corporate name changes in all sections
thru NA010	April 1999	updated for Product Computing-module Loads (PCL) thru NA010
		updated "Training" section
		updated all sections for content and references

Software (continued)	Date (continued)	Revisions (continued)
		added new acronyms
thru NA006	**January 1997**	NTP 297-8991-500, release 01.01, replaces NED 0003, release 10.01 of the MOM. Revision history of NED 0003 has been retained for the first issue of NTP 297-8991-500.
		updated for Product Computing-module Loads (PCL) thru NA006
		updated "Training" section courses
		updated all sections for content and references
		revised entire document for addition to HELMSMAN
		added new subsection called "AIN Overview and Maintenance"
		added new acronyms
thru NA004	**February 1996**	updated for Product Computing-module Loads (PCL) thru NA004
		updated "Training" section courses
		updated all sections for content and references
		moved topics that were under several subsections into one subsection—such as all the previous separate subsections for Operational Measurements (OMs) are now in one subsection called "Operational Measurements"
		added new subsection for "Remote Switching Center"
		added new subsection called "Carrier Maintenance"
		added new subsection call "Software Optionality Control"
		updated "Routine Tasks" subsection with the latest recommendations from Nortel Networks

Software (continued)	Date (continued)	Revisions (continued)
		updated "Office Parameters" subsection
BCS36	**Jan 1995**	updated for BCS36 and preliminary PCL load topics
		added "References" subsection within the last tab to support documentation references for the MOM—including PCL documentation
		moved the "User Index" to the last tab
		updated "Training" section courses
		updated all sections for content and references
		moved "DRAM Maintenance" subsection from the *Corrective Maintenance* section to the *System Products* section
		added "MPC Maintenance" subsection to the *System Products* section
		moved individual section Table of Contents to the "Table of Contents" tab in front of the MOM
BCS35	**June 1993**	added BCS34 & BCS35 topics to MOM
		added new "System Products" section and moved ISDN, SS7, TOPS, Datapath, ENET, and Meridian Digital Centrex Terminals within this tab
		added "User Index"
		updated "Training" section courses
		updated all sections for content and references
		restructured topic content and removed redundant material in some areas
		added routine maintenance tables for the "Routine Task" subsection

Software (continued)	Date (continued)	Revisions (continued)
BCS33/34	**Aug 1992**	added Traffic Operator Position System (TOPS) subsection in the "Preventive Maintenance" section
		added ENET subsections in the "Preventive Maintenance" section
		revised the "Performance" section for ENET
		revised and updated the ISDN subsections in the "Preventive Maintenance" section
		updated the "Training" section
		updated all sections for content and references
		removed STORE FILE Exhibits until they can be reviewed, evaluated, and tested
BCS30/31/32	**April 1991**	added ISDN subsections in the "Preventive Maintenance" section
		added SS7 Maintenance subsection in the "Preventive Maintenance" section

Customer Documentation Questionnaire

You may use this form to communicate your comments or concerns about this document, its organization or subject matter, with the understanding that Nortel Networks may use or distribute whatever information you supply without incurring any obligations to you. Your views will be sent to the originating department for review and action, if any is deemed appropriate.

NTP 297-8991-500: Issue_____Date:_____

Does the publication meet your needs?..YES___   NO___

Did you find the information:

Accurate?...YES___   NO___

Easy to read and understand?.. YES___   NO___

Organized for convenient use?.. YES___   NO___

Legible?..YES___   NO___

Complete? Well illustrated?.. YES___   NO___

Written for your technical level?...................................... YES___   NO___

If your answer to any of the above questions was NO, please explain under comments.

What new topics should be included in the next issue of this document?

Comments:

_____

_____

_____

_____

_____

_____

_____

_____

What is your function within your Company? _____

If you would like a reply, please fill in your: Name: _____

Address: _____

_____

Telephone: _____

Thank you for your time. Please return to the following address:

Nortel Networks, Global Professional Services - Technical Services, Dept. 1773,

MDN MS49D030F5, 2520 Meridian Pkwy, Durham, NC 27713

PLEASE FOLD, TAPE, AND MAIL—NO POSTAGE NECESSARY
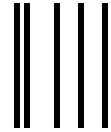
NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES
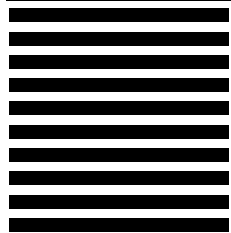
BUSINESS REPLY MAIL

FIRST CLASS   PERMIT NO. 1024   DURHAM, NC

POSTAGE WILL BE PAID BY ADDRESSEE

NORTEL NETWORKS
Global Professional Services - Technical Services
Dept. 1773, MDN MS49D030F5
2520 Meridian Parkway
Durham, NC 27713

DMS-100F
MAINTENANCE & OPERATIONS MANUAL
NTP 297-8991-500 Standard 04.02 March 2001

ORDERING FORM

The next planned release of this manual is 1Q2002. To order additional paper copies of NTP 297-8991-500, *DMS-100F Maintenance & Operations Manual* release 04.02 please complete the form including the quantity and your purchase order number.

Number of Paper Copies   Quantity_____

Purchase Order Number   P.O. #_____

Shipping Address:

Company Name_____

Address_____

City_____State_____Zip_____

Attention_____Tel #_____

Billing Address:

Company Name_____

Address_____

City_____State_____Zip_____

Attention_____Tel #_____

Fold and mail to the Nortel address listed on the reverse side of this form. If you wish to order by telephone, please call 1-800-684-2273.

PLEASE FOLD, SEAL AND MAIL—NO POSTAGE NECESSARY

BUSINESS REPLY MAIL

FIRST CLASS   PERMIT NO. 1024   DURHAM, NC

POSTAGE WILL BE PAID BY ADDRESSEE

Nortel Networks
Merchandise Order Desk
Dept. 6611
P.O. Box 13010
Research Triangle Park, NC 27709-3010
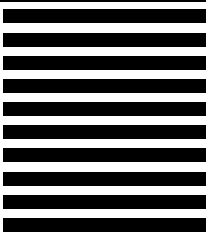
Table of Contents

Notes:

- Trademarks (located before Table of Contents)
- Revision history (located before Table of Contents)
- Customer Documentation Questionaire (located before Table of Contents)
- Document Order Form (located before Table of Contents)
- Figures and Tables listed in back of Table of Contents
- User Index in back of manual

Summary of Operations, Administration, & Maintenance Tools   1-19

New & Changed Logs, Commands, and OMs   1-31

Preventive Maintenance —General   2-1

Routine Tasks   2-3

Operational Measurements   2-21

Focused Maintenance   2-114

Line Maintenance 2-131

Trunk Maintenance   2-152

Carrier Maintenance 2-260

Corrective Maintenance — General   3-1

Maintenance, Troubleshooting, and Recovery References   3-2

Trouble Indicators   3-8

Trouble Repair   3-17

Trouble Analysis Tools   3-23

DISPCALL & SHOWAUD Commands   3-31

Data Grooming DMS-100F Networks   3-36

TOPS Overview and Maintenance   4-1

ISDN Overview and Maintenance   4-95

ENET Overview and Maintenance   4-225

Datapath Overview and Maintenance   4-252

MDC Overview and Maintenance   4-269

XA-Core Overview and Maintenance   4-355

SPM Overview and Maintenance   4-376

IOM Overview and Maintenance   4-390

1-Meg Modem Overview and Maintenance 4-405

Star Remote System Overview and Maintenance   4-417

XMS-based Peripheral Module Overview and Maintenance   4-427

Real Time Performance Indicators   5-42

Service Analysis System   5-48

DMSMON   5-50

Maintenance Managers Morning Report   5-52

Technical Assistance – General   6-1

Technical Support Services   6-2

Office Security   8-66

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

Manual Objectives

Purpose

The *2001 DMS-100F Maintenance and Operations Manual* (MOM) is structured to provide working levels of management and technicians with a single document that gives an overview of DMS-100F switch maintenance features and tools—including administrative maintenance procedures with typical examples and suggestions. Also included are references to supporting Nortel Networks documents that provide the details needed to perform various maintenance tasks referenced throughout this manual. The tools, procedures, and suggestions presented in this manual are recommended to provide good customer service and maintain the DMS-100F switch at expected performance levels.

The MOM provides a minimum starting point to achieve acceptable and realistic levels of service and performance. Supported by sound technical and administrative advice, the information in this manual may be modified by the operating company to meet specific service, performance, and operating cost requirements.

The DMS-100F switch maintenance process described in the MOM utilizes the maintenance and administration position (MAP) visual display unit (VDU) as the user interface for initiating and responding to the various machine tests, diagnostics, surveillance, and resident test program features. This same maintenance process applies when centralizing the maintenance functions for several DMS sites. Additional savings and operating efficiencies may be realized when the centralized testing, surveillance, and administrative work operations are supported by computerized operational support systems.

Material contained within this manual is intended to supplement material presented in Nortel Networks Publications (NTPs), not replace them. This manual can be used as a quick reference when first learning about DMS switch announcement and maintenance strategy. Where procedural problems or any conflicts arise when using this manual, the current NTPs are the final authority and should be used.

The switch features presented in this document are considered as basic requirements for performing operations, administration, and maintenance functions for the DMS-100F switch. See the "Summary of Operations, Administration, & Maintenance Tools" subsection within this tab for a summary of the various tools and features which are described within several subsections of this manual.

DMS-trained personnel are essential for maintaining and operating any DMS switch. This manual does not circumvent the need for formal training as recommended in the *Training* section of this manual.

The Nortel Networks Technical Education Centers have several courses that teach many of the topics and ideas presented in this manual. For example, Course 4500, "DMS SuperNode System Switch Performance Management" provides an overview of maintenance, surveillance, and administrative tools for the DMS-100F switch. For information on training courses, see the *Training* section in the back of this manual.

For managers that need an overview of the various maintenance tools and a strategy for maintaining a DMS-100F switch, see the following "Maintenance Strategy" and "Maintenance by Exception" subsections. If further details are needed on the tools described within the "Introduction" tab, then reference the other supporting sections within this manual.

Comments concerning the *DMS-100F Maintenance and Operations Manual* are invited, as are other inquiries related to DMS-100F maintenance and performance. For your convenience, a pre-addressed Customer Documentation Questionnaire is provided at the front of this manual. Your feedback, through the Customer Documentation Questionnaire form, would assist us in the further development of this manual.

Nortel Networks updates the *DMS-100F Maintenance and Operations Manual* yearly—to include the latest maintenance features with current and future software releases.

Besides updating this manual, ongoing efforts are being made to restructure the manual. Restructuring will make the manual easier to use and help reduce duplication of content. Future efforts will also be made to add new product topics and additional useful material—such as "Quick Reference" items—to the manual.

Each colored tab within the MOM is called a section. Within the tabs are titled subsections providing various topics. It is suggested that the "Table of Contents" be referenced to find the starting page location of each subsection. The "User Index" within the last tab can be used to locate various subject matter within the manual.

Maintenance Strategy

Strategy Description

The DMS-100F switch maintenance strategy described in this subsection—when administered—will produce the desired level of customer service satisfaction and switch performance that is expected. This is achievable through structured operating, technical, and administrative processes which provide cost-effective maintenance.

A DMS-100F switch maintenance strategy recommended by Nortel Networks is based upon utilization of the following switch maintenance tools, reports, and other supporting groups:

- OM THRESHOLDING — A real time switch surveillance tool that uses selected key operational measurement (OM) indicators to generate alarms and log messages when bogey (a numerical standard of performance set up as a mark to be aimed at) settings are reached. It can be used as a warning tool for service index related OMs, or as a corrective maintenance tool for troubleshooting problem areas that peg OMs.

- OM MANAGEMENT AND BOGEY SETTINGS — Prime indicator for determining switch maintenance. Provides suggested bogey values for some selected OM registers to help identify problem areas based upon numerical factors.

- USER INTERFACE — The mechanism that allows the switch and user personnel to communicate. The interface, described later, provides uniform input commands and outputs for simplicity of control for all DMS-100F switches.

- LOG SYSTEM ADMINISTRATION— User oriented functional structure of system output messages routed to logging device(s). When properly administered through the use of tables and parameters, log messages can be significantly reduced and prevented from being lost due to log buffer overflows.

- FOCUSED MAINTENANCE — A real time surveillance tool which replaces tedious manual analysis of specific TRK, LINE, and NET log messages by collecting the ten worst faults. Line and trunk faults are collected by line concentrating device or trunk group in a selectable buffer—resulting in a significant reduction in line and trunk log messages.

- SWITCH PERFORMANCE MONITORING SYSTEM (SPMS) — An automated system that produces a set of composite indexes which measures switch

performance, maintenance, and provisioning. An SPMS report highlights any specific area requiring corrective maintenance activity.

- MAINTENANCE MANAGERS MORNING REPORT — A management tool which reports on the performance of the DMS-100F switch. The report is broken down into two parts, "DMS Switch Performance" and "Scheduled Test Results." The report is generated automatically and allows management and technicians to focus on abnormal operating areas.

- DMS MONITORING SYSTEM (DMSMON) — The DMSMON utility provides data which can be used to measure office performance. DMSMON is an on–demand report which maintenance personnel can use to review some areas for office performance and system configuration.

- RESIDENT SURVEILLANCE AND TEST PROGRAMS — Automated preventive maintenance test programs which identify problems prior to impacting service and switch performance. Operating companies have the option to implement and manage these programs through table and parameter settings.

- SUPPORT GROUPS — The hierarchy of support groups for effective maintenance includes: technical, analysis, engineering, administrative, and training.

Each of the above tools may be implemented individually; however, it is advisable to apply them collectively as a maintenance strategy for either single or multiple switch entities as is shown in Figure 1-1.

Figure 1-1 — DMS-100F Maintenance & Administrative Tools
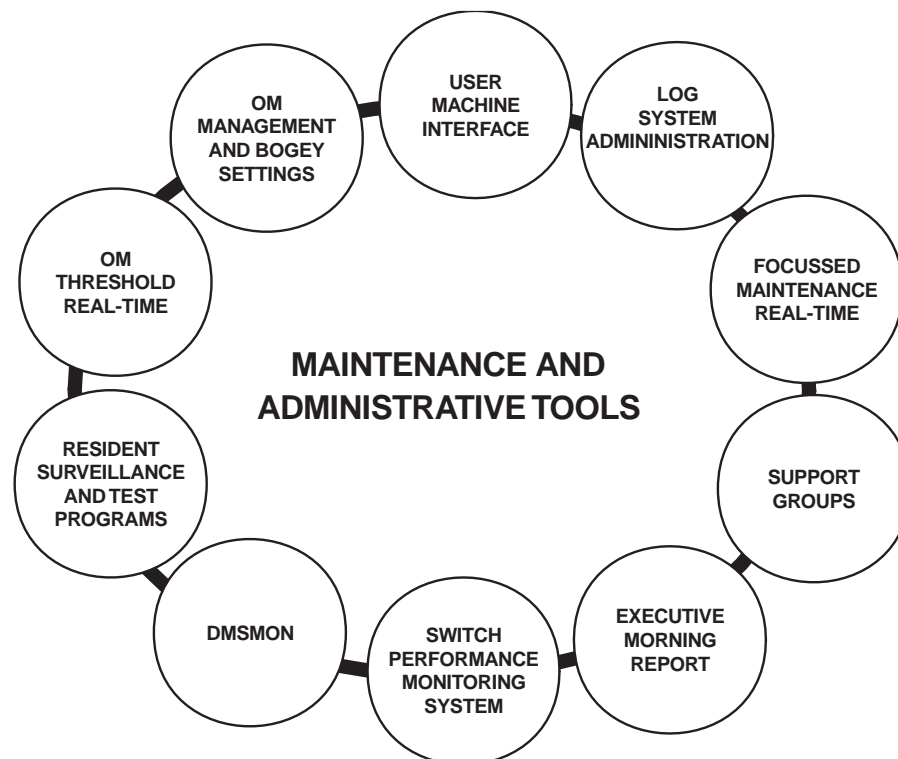
A prime objective of DMS-100F switch maintenance should be to achieve 'Maintenance by Exception' (see next subsection). This is possible when the maintenance strategy is to use some or all the switch maintenance tools in an effective manner.

Successful maintenance—no matter what strategy is used—includes not only system operations, but also administrative procedures, technical support group interfaces, appropriate staff training, and an attitude and motivation toward providing good service to customers.

OM thresholding

Operational measurements (OMs) are machine-generated real time system events which— through structured *accumulators*—can only be viewed or analyzed after the fact from scheduled or manual requested reports. OM thresholding dramatically increases OM surveillance capabilities. This is done by selectively choosing discrete registers that indicate immediate maintenance is required when their peg counts exceed specified thresholds and time frames.

Specific details for using this feature are described in the "Operational Measurements" (OMs) subsection within the *Preventive Maintenance* tab.

OM management and bogey setting

Operational measurement data provides information regarding the operation, performance, and utilization of the switching system's software and hardware resources. Over 2000 unique registers are provided to measure events or usage. To effectively manage a switch or group of switches, these registers must be selectively combined into functionally defined, multiple- user classes.

The OM accumulating classes effectively manage switch resident data and should not normally be output unless needed for trouble analysis, thereby eliminating needless data output. Switch resident programs circumvent manual paper analysis.

With larger operating company centralized maintenance operations, predefined and structured groupings are required. Commonality provides ease of maintenance, provisioning, and administration, both within the operating company and with outside support groups, such as the emergency technical assistance service (ETAS) center described within the *Technical Assistance* tab of this manual.

Bogeys or benchmarks (the expected OM peg count for normal operation) must be determined before OMs can be used effectively for real time and subsequent analysis. Operational measurement and bogey setting guidelines are provided in the "Operational Measurements" (OMs) subsection within the *Preventive Maintenance* tab.

User interface

The maintenance and administration position (MAP) is the communication mechanism between the switch and people for inputting commands, data modifications, interrogation, and receiving messages and scheduled output reports. The MAP is very user friendly and flexible, utilizing menus, prompts, and verification procedures. The *Corrective Maintenance* and *Office Administration* tabbed sections provide guidance for the administration and security of terminal devices, such as the MAP.

Log system administration

The output messaging system provides printable information of machine events of various levels and detail. The messages are comprised of over 3,000 log message types divided into over 200 subsystem groupings. The messages provide data for various users such as technicians, technical support groups, and design and maintenance engineers. To effectively manage the messaging system output, the assigned routing of various messages to appropriate recording devices within the system is essential. A strategy for managing log messages is very important. It is often neglected by many companies and can have an impact on problem solving and customer service.

Details for the management of the log messaging system are described in the "Log System Administration" subsection within the *Office Administration* tab of this manual.

Focused Maintenance for Lines and Trunks

The Focused Maintenance feature for both lines and trunks provides a real time trouble message surveillance mechanism. This feature filters out incidental trouble occurrences and focuses the maintenance efforts directly to the most logical trouble area. The feature also permits reduction in the quantity of log message printouts, savings in machine time, as well as faster trouble identification and resolution time due to the real time nature of the feature.

Specific details for implementation of this feature are contained in the *Preventive Maintenance* tab within subsection "Focused Maintenance."

Switch Performance Monitoring System (SPMS)

The switch performance monitoring system (SPMS) is an optional feature that can assist maintenance personnel in the analysis of OMs to identify and correct switch problems. SPMS is a totally automated system that provides on-demand performance index reports at user selected intervals, such as day, week, and report month. The output report highlights indices with asterisk(s) (**) that do not meet specified switch performance objectives.

The monthly report is suitable for input to an operating company switch measurement plan. Whether or not SPMS is used for this purpose, it should be used as a maintenance tool on a daily basis to detect and correct maintenance and provisioning problems that have not been detected by other means.

The *Performance* section in this manual describes the SPMS plan, key concerns, and indicators pertinent to operating company operations and customer service. In addition, a standard plan enables inter- and intra-company assessment of both the DMS-100F systems and the operating company's ability to effectively maintain the switching system.

Maintenance Managers Morning Report

The "Maintenance Managers Morning Report" software feature is an automated tool that can provide a daily printout of the switch performance and specific maintenance activities. It is also known as the "Executive Morning Report," "Good Morning Report," or the "AM Report." Further information on this feature can be found in the *Performance* section of this manual.

DMS Monitoring (DMSMON) System

The DMS monitoring (DMSMON) system provides data that can be used to manually evaluate office performance and configuration. DMSMON is available on all DMS-100F systems. With DMSMON, maintenance personnel can manually compare OM and log counts against known bogeys or benchmarks to identify areas in the DMS that need attention, thus reducing analysis time. For further information, see the *Performance* section and the DMSMON subsection within this manual.

Resident surveillance and test programs

Full utilization of available switch resident surveillance and test features is required to detect fault conditions and correct them before they affect customer service. When the automated features are used, it reduces the labor intensive effort for manual testing.

These standard features are software programs that the operating company can control to identify both internal and external machine abnormal conditions, which, if left unattended, will affect service or switch performance levels.

The following maintenance related features are described within the MOM:

- *Preventive Maintenance* section
    — Focused Maintenance for Lines and Trunks
    — Trunk maintenance
    — Carrier maintenance
    — KT (Killer Trunk)
    — ATT (Automatic Trunk Test)
    — SIGTST (Diagnostic Signaling Test)
    — STKSDR (Stuck Sender MTCE)
    — PRDTKMTC (Periodic Trunk Maintenance Report)
    — Line maintenance
    — ALT (Automatic Line Test)
    — ALMSTAT (Alarm Status - Lines)
    — BERT (Bit Error Rate Testing)
    — BERP (Bit Error Rate Performance)
    — NETFAB (Network Fabric Testing)
    — BERT for trunks
    — NETPATH (Diagnostic Testing)
    — ICTS (Integrity Check Traffic Simulator)
    — NETINTEG (Analysis Tool)
    — XBERT (XPM BERT Testing)

- *Corrective Maintenance* section
    — DISPCALL (Display Call Failure Details)
    — Trouble analysis tools

- *Performance* section
    — Switch performance monitoring system (SPMS)
    — Real time performance indicators
    — Service analysis system
    — DMS monitoring (DMSMON) system
    — Maintenance managers morning report

Support groups

A support force, either permanent or contracted, is essential for an effective DMS-100F maintenance strategy. This support force would provide technical training, technical support for escalated trouble situations, and an effective administrative system,

including related mechanized systems. For further details about support groups and services, see the following tabbed sections:

- *Office Administration* section
    — Log system administration
    — Software optionality control (SOC)
    — Office security
    — Nortel Networks documentation
    — Office parameters
    — Store file administration

- *Technical Assistance* section
    — Technical Assistance Service (TAS)
    — Emergency Technical Assistance and Support (ETAS)
    — Service Reports (SRs)
    — Maintenance services
    — Software application
    — C-SCAN
    — Customer Information Management (Canada)
    — Circuit pack replacement
    — DMS-100 warning and bulletins
    — Change application services
    — Engineering complaint services

- *Maintenance Administration* section
    — On-site and control center operations
    — Key work items

- *Training* section
    — Training curriculum

Maintenance by Exception

Maintenance by Exception Description

Maintenance by exception involves the automated surveillance of a spectrum of selected machine indicators(for example, alarms, alarm lamps, maintenance and administrative position (MAP) indicators, log message errors and faults, and operational measurements (OMs) which, truly represent the health of the switch. DMS maintenance by exception operates in real-time or near real-time to identify fault conditions using the essential surveillance and trouble indicators generated by the various machine features. When the incidents of trouble reach a predetermined threshold setting, an alarm will be generated to alert the maintenance staff of a problem before the customer reports the trouble. The maintenance by exception process brings the problem to the attention of the maintenance force in real-time or near real-time; therefore, a continual review of all output log messages is not required. Once the fault is identified, the control center will assess the severity and set priorities. In some cases, the technician will initiate tests or open log messages to confirm the trouble condition and to get such information as the details of equipment type and reason for the fault or failure.

A block diagram indicating the key maintenance by exception elements is shown in Figure 1-2. It uses various switch features and administrative processes which are exploited in a complimentary manner to achieve maintenance by exception. The functions recorded in Figure 1-2 are based on available features. Further enhancements, which will increase productivity and lessen technician frustration, are possible by using auxiliary computer systems (OSSs) and custom programs.

The maintenance by exception process highlights actionable information from a comprehensive source of service and performance indicators, which truly reflect the whole state of the system minute-by-minute. The DMS-100F switching system generates this type of information, but the data must be managed adequately by using resident tools to analyze and pattern the information into actionable items.

Figure 1-2 — DMS Maintenance Strategy—Maintenance By Exception

OTHER ACTIVITY ADMIN ─ MTCE

MAINTENANCE ADMINISTRATION PROCEDURES
• LOGUTIL
• OM OUTPUT
• LOG OUTPUT
• COMMANDS
• SECURITY HMI
• THRESHOLD
• SETTING
• EVALUATIONS
• VERIFY

POP & NTP SPECIFIED ROUTINES
• IMAGE
• REPAIR & RETURN
• NT & TELCO SPECIFIED ROUTINES
• OTHER

ESSENTIAL INDICATORS FOR EFFECTIVE SURVEILLANCE

NEAR REAL-TIME | REAL-TIME | SUBSEQUENT

OPERATIONAL MEASUREMENTS

SUBSEQUENT ANALYSIS & TREND ANALYSIS

SPMS PREVIOUS DAY(S)

MTCE OMs

CONTROL RECORDS & LOG RECORDS POST

MTCE SYS STATUS DISPLAY
CC | CMC | IOD | NET
PM | CCS | LNS | TRK
EXT | CM | WS
LOGS | ALARMS

OM THRESHOLD
LOGS | ALARMS

OM ALARMTAB
LOGS | ALARMS

LOGS

ANALYZE SPECIFIC LOGS–OMs–SPMS AS REQUIRED

INITIATE DIAGNOSTIC TEST TO IDENTIFY H/S FAULTS

LOCATE FAULT REPAIR & VERIFY

HMI INITIATED RESIDENT TEST & SURVEILLANCE PROGRAMS

FM | FM NET
TRKS
FM LNS
LOGS | ALARMS

ACT UPON THE EXCEPTIONS BY EXPLOITING THE TOOLS — "LET IT INFORM US"

ANALYSES/DECISIONS/PRIORITIES
• DECISIONS/PRIORITIES
• CORRECTIVE ACTION
• VERIFY RESULTS
• CONTROL/DISPATCH
• TREND INFORMATION

ROUTINE ACTIVITY
TRK | NET
BERT | FAB
BERP | ALT | ATT
LOGS/RPTs

SYSTEM ROUTINE DIAGNOSTICS
• CMC REX
• MEMORY REX
• CPU REX
• XPM REX
• IMAGE TEST
• DATA STORE
LOGS | ALARMS

SURVEILLANCE
PRD TRKMTC
KT REPORTS
LOGS & RPTs

SURVEILLANCE
ALMSTAT
LOGS & RPTs

LOCAL ADMIN STORE FILES
MAINTENANCE MANAGERS MORNING REPORT
OTHER A/R

EXAMINE OUTPUTS FROM ROUTINE AND SURVEILLANCE FEATURES FOR EXCEPTION

CUSTOMER REPORTED PROBLEMS

Maintenance by exception is attainable when the following administrative and switch resident maintenance procedures are operated in a complimentary manner:

- system alarms
- machine initiated audits and diagnostic tests
- resident surveillance and test features
- related administrative procedures
- customer trouble reports

Alarms, OMs and thresholding of fault indicators within the DMS are the basic triggering processes for identifying problem areas to maintenance personnel. Once activated through tables and parameter settings, the surveillance processes continue indefinitely. When the incidents of trouble reach or exceed the established threshold or bogey values, an alarm condition is generated which identifies the equipment on the MAP and within log messages—alerting maintenance personnel to problem(s).

Realistic settings for threshold/bogey values, scan time intervals, and alarm classes, are crucial for the proper identification of trouble conditions in real-time. Periodically check threshold values, scan times, and alarm levels to ensure validity.

The various elements that make up the maintenance by exception process are described in the following paragraphs:

Near real-time indicator tools

The near real-time resident test and surveillance indicators should be interrogated periodically, especially at the start of a shift, to find hard or potential troubles that need corrective action. Where summary reports are automatically provided, a review of the report for problems should be made before or at the beginning of the first shift,. Taking this initiative early will help reduce customer trouble reports. When not done, customers will most likely initiate trouble reports until the problem is resolved. Following are some of the near real-time tools that make up the maintenance by exception process.

Automatic line testing feature

The automatic line testing (ALT) feature tests subscriber lines without manual intervention by maintenance personnel. Line maintenance is defined at the ALT level of the MAP. The system start and stop times are also defined. If needed, manual tests can be run without defining a schedule. Information on the use and recommended operation frequency can be found within the "Line Maintenance" subsection within the *Preventive Maintenance* tab of this manual. Further details can be found in NTP 297-1001-594, *Lines Maintenance Guide*.

Lines status

Line status should be reviewed at least once a day—preferably, before the first shift, or at least the beginning of the first shift. Command ALMSTAT, on the LTP level of

the MAP, displays a summary of the office line failures, threshold levels, and office dial-tone delay status when input without parameters. The failure results from the Automatic Line Testing (ALT) routine are part of the summary. Information on the ALMSTAT command can be found within the "Line Maintenance" subsection. Detailed use of the ALMSTAT command can be found in NTP 297-1001-594, *Lines Maintenance Guide* and NTP 297-1001-822, *Commands Reference Manual*.

Babbling line status

Babbling lines,—sometimes known as showering lines—are lines that cause rapid on-hook off-hook seizures. Babbling lines can cause a serious overload on the switch; however, the incoming message overload (ICMO) handler switch feature handles the fault conditions. The babbling lines can be listed, posted, and printed using ALM-STAT and other commands described in NTPs previously listed under "Lines status." Further information on babbling lines can be found within the "Line Maintenance" subsection of this manual.

Automatic trunk test

The automatic trunk testing (ATT) feature automatically performs routine trunk transmission, bit error rate test (BERT), and operational tests. Pre-scheduled tests are performed on outgoing trunks (one-way or two-way trunk groups) to terminating offices with the appropriate responders. Tests that may be performed are: loss, noise, tone detection, BERT, signaling, and operational. ATT tests should be run nightly. When all trunks have been tested through scheduled testing, they should be recycled for further testing. For surveillance purposes, exception reporting should be used and the related failure log messages should be routed to a printer designated for trunk reports. Review the exception ATT log messages daily and take corrective action before the trunk problems impact the network.

Further information on the ATT feature can be found within the "Trunk Maintenance" subsection. A description of the ATT feature can be found in NTP 297-1001-121, *Automatic Trunk Testing Description*, NTP 297-1001-595, *Trunks Maintenance Guide*, and NTP 297-1001-822, *Commands Reference Manual*.

Trunk performance

Periodic trunk maintenance (PRDTKMTC) report summarizes trunk group performance. The key items are from the TRK OM group. Since the report is lengthy, schedule printing before the first shift. See the "Trunk Maintenance" subsection for a description on the use of the PRDTKMTC feature. Also see NTP 297-1001-318, *Service Problem Analysis Administration Guide*, for further information and references on the PRDTKMTC feature.

Killer trunk feature

The killer trunk (KT) feature output identifies individual trunk problems by monitoring the performance and recording by trunk member the following irregularities: always busy, always idle, short holding time, and long holding times. See the "Trunk

Maintenance" subsection which describes the KT setup and provides suggested data-fill using tables KTPARMS, KTGROUP, KMINMAX, and DIRPSSYS.

Also see NTP 297-1001-318 for further information and KT feature references.

Stuck sender maintenance

The stuck sender (STKSDR) maintenance feature identifies trunks that have timed out (transmitter time-outs) due to out-pulsing problems. Suggestions for finding stuck sender problems can be found within the "Trunk Maintenance" subsection. Actual use of the STKSDR command off the TTP MAP level is described in NTP 297-1001-822, *Commands Reference Manual*.

Remember that senders are not used with CCS7 trunks; therefore, stuck sender failures improve after converting conventional trunks to CCS7. CCS7 trunk failures exhibit themselves in other ways, such as continuity (COT) failures. With CCS7, the killer trunk feature (previously described) becomes a very important tool to detect continuity type failures. Stuck senders will continue to exist with direct inward dial (DID) trunks and other trunk groups that use sender outpulsing.

BERT for trunks

The bit error rate testing (BERT) for trunks feature measures bit error rates (BER) on individual trunks at the DS0 rate. The path being tested includes the digital switch trunks and the facility. Manual testing is initiated from the MAP level to perform the individual DS0 trunk BER tests. Automated BERT tests can be set up using the ATT feature for individual trunks.

It is important that routine BER tests be performed on the trunks and within the switch network in order to provide the high-speed data service required in today's and tomorrow's market. To further understand more about the BERT tools for trunks, see the "Network Maintenance" and "Carrier Maintenance" subsections within the *Preventive Maintenance* tab.

Bit error rate performance

The high-speed data performance of a DMS-100F switch is assessed by bit error rate performance (BERP) testing. This assessment is made by running several BER tests randomly through the network transmission paths of the switch. BERP tests and reports can be set up using commands at the BERP level of the MAP. Further information on BERP and BERT testing can be found in the *Preventive Maintenance* section under the "Network Maintenance" subsection. The supporting practice for BERP is NTP 297-1001-533, *Bit Error Rate Performance Testing*.

NETFAB/ENETFAB routine testing

Network fabric (NETFAB) for junctored networks and Enhanced Network Fabric (ENETFAB) for enhanced networks are automated routine testing features that provide the ability to schedule testing of network call paths. The term "network fabric" refers to the numerous call paths through the network modules of the switch.

As more high-speed data services are being deployed with new technology, it is essential that tools such as NETFAB and ENETFAB be used to provide good service. To understand more about this tool, see the "Network Maintenance" subsection. The supporting document for NETFAB and ENETFAB is NTP 297-1001-591, *Network Maintenance Guide.*

System routine diagnostics

Routine exercise (REX) tests programs can be run nightly on the front end equipment and peripherals. Automatic testing of images is also provided. The operating company can schedule the nightly routines. Several days may be needed to complete the tests. Examine related log messages daily to verify that tests are run, all equipment is routined progressively, and identified troubles are corrected and remain clear. See "Routine exercise (REX) tests" in the "Routine Tasks" subsection within the *Preventive Maintenance* tab for more details. Also, see the "Maintenance Managers Morning Report" subsection in the *Performance* section. The NAG400 log report also provides REX information

DMS schedule (DMSSCHED)

This feature allows commands to be scheduled for execution once or multiple times. A custom store file (SF) program can be scheduled for execution using the DMSSCHED utility. A routine could be established for the manager or technician to review results before or at the start of the first shift. A custom report can be developed to provide machine indicators for the SuperNode CM, Networks, Peripheral Modules, AMA, trunks, and lines etc. The type of information can include such things as: alarms, system busy, man busy, lockouts, remote busy, percent out of service, off line, carrier failures, line diagnostic failures, and users logged in. Further information can be found in the *Technical Assistance* section of this manual.

Customer reported troubles

Customer trouble reports are originated by subscribers and record the difficulty encountered while using their provided service. The reports are usually received by the Repair Service Bureau (RSB) for testing and sectionalization, and are then referred to other support groups responsible for investigation and correction. Common examples of troubles are: no-dial-tone, can't call, can't be called, can't hear, and cut-off. Most individual reports can be tested and resolved by using the regular LTP MAP level testing facilities.

An influx of customer trouble reports should trigger the maintenance staff to examine other machine indicators such as the Alarm Status Display, Carrier, Focused Maintenance, or current machine activity to determine a common cause for the increased customer reporting. The reports and dispositions should be tracked with particular emphasis on test-ok and found-ok conditions, which may require more in-depth analysis. Customer trouble reports should be resolved swiftly to restore customer service and prevent subsequent trouble reports. See the *Corrective Maintenance* section and the "Trouble Indicators" subsection for further information.

Real-time indicator tools

There are several real-time indicator features that can alert maintenance personnel to problems or potential problems as they occur. Two well-known indicators are visual lamps and audible alarms. Some other indicators include: system status displays on the MAP, the focused maintenance feature for lines and trunks, and the OM thresholding and OM alarmtab features. See the "Real-Time Performance Tools' subsection within the *Performance* tab of this manual.

MAP system status display

The MAP system status display is the watchdog feature that alerts the maintenance staff when hardware or software alarms are generated by internal maintenance subsystem CM & MS (SuperNode), IOD, NET, PM, CCS, Lns, Trks, EXT and APPL. The display is dynamic—as the alarm situation changes, the display is automatically updated to display the highest severity of abnormal condition. In most cases, a log message is generated when the alarm condition is displayed or changed. The visual information is located on the top of the MAP VDU screen.

Each maintenance subsystem contains the software necessary for maintaining its own hardware by initiating diagnostic tests to identify and isolate fault conditions and alert the maintenance staff via alarms. Corrective action would include interrogating the specific MAP subsystem to determine the exact fault condition, examining log messages and other related indicators, and initiating additional MAP tests. For further information on this important resident feature that every DMS-100F technician should be familiar with, see the *Corrective Maintenance* section and subsection "Trouble Indicators". Also see NTP 297-1001-520, *Maintenance System Man-Machine Interface Description.*

Focused maintenance feature for lines & trunks

The focused maintenance feature for lines and trunks is an administrative tool for managing call processing identified line and trunk trouble log messages. It uses a system of buffers, thresholds, and alarms to identify the worst line and trunk problems so that work can be focused on those problems. For each Line Concentrating Device (LCD) and each Common Language Location Identifier (CLLI) trunk group, the 10 worst lines and trunk members are recorded respectively. When set thresholds are reached, the MAP alarm status bar is activated for a real-time indication of problems.

If equipped with this feature, it should be a daily routine requirement to display the line and trunk groups for maintenance action. The activation, setup, and operating procedures are described in the *Preventive Maintenance* section within subsection "Focused Maintenance."

OM thresholding feature

The operational measurement (OM) thresholding feature (NTX385AA) is a powerful real-time switch maintenance surveillance tool. Switching problems can be identified in real-time by monitoring up to 128 key maintenance OMs—against preset thresh-

olds (bogeys)—over a moving time frame. When the threshold is reached or exceeded for any selected OM register, an alarm and log message OM2200 is generated that alerts the technician of a problem. These key OMs and threshold values that trigger the alarms and logs can be selected and set by the operating company. Once the maintenance staff has been alerted to the problem by the OM thresholding feature alarm and log message, immediate action could be taken to resolve the problem or analyze it with other related conditions within the switch.

If equipped with this feature, learn to use it for troubleshooting and possible correlation with other OMs, SPMS, or log messages. To get started with the OM thresholding feature, see subsection "Operational Measurements (OMs)."

OM ALARMTAB table

The OM alarmtab feature performs in the same manner as the OM thresholding feature. However, the ALARMTAB table used for this feature is read-only and the threshold counts are set at one minute intervals. In table OMTHRESH for the OM thresholding feature, the time is specified by the operating company. The ALARM-TAB table is write protected and predatafilled by Nortel Networks. Predatafilled OMs are normally resource overflow registers. When an alarm is activated for an OM defined in table ALARMTAB, a log report OM2200 is generated and alarm generation for the entry is suppressed for 15 minutes.

Analysis tools

Analysis tools present in the DMS or in any operational support system should be reviewed periodically by operating company personnel. These tools, when used, will identify problems and potential problem areas of the DMS. After problem areas are identified, it is possible to perform corrective maintenance before a problem results in customer trouble reports or a switch outage. Following are some examples of analysis tools in the DMS switch.

Nortel Networks Customer Network Services Group has developed a special analysis program that combines key indicators from several reports and analysis tools to provide a single report to manage the DMS switch. Contact this group at 1 (919) 997-7745 for further information on this and other services provided by this group.

Switch Performance Monitoring System

The Switch Performance Monitoring System (SPMS) software feature (NTX738AC) is a switch analysis tool that provides on-demand indices. It describes how well the switch is operating at various levels of detail. The process is totally automated and uses operational measurements for the input data. For further information on the use of SPMS, see the *Performance* section of this manual, or NTP 297-1001-330, *Switch Performance Monitoring System Application Guide*.

Maintenance Managers Morning Report

The Maintenance Managers Morning Report—supported by NTP 297-1001-535—is available as an early morning report. Besides providing a status review of SPMS, call processing performance, CPU occupancy, and SWACT information, it will provide a quick overview of test count results for some maintenance tools. This report should be reviewed before or at the start of the first shift. Further information on this feature can be found in the *Performance* section of this manual.

Key maintenance OMs

The *Preventive Maintenance* section lists the key maintenance OMs to be tracked for subsequent analysis. It also records the factors for determining related benchmarks or bogeys for meaningful evaluation of OM data. The key OM data should be tracked on a control record for subsequent analysis when SPMS is not used. Intermittent, hard, or obscure fault conditions can be identified by reviewing this data periodically as part of a local analysis program.

DMS monitoring system (DMSMON)

The DMSMON utility provides on-demand reports via CI level DMSMON subcommands on the MAP. It has been found to be a useful tool in determining office performance and highlighting potential problem areas. The report provides: peripheral configurations; PM load information (counts of lines, trunks, receivers, peripheral modules); system restarts; downtime information; types and number of memory cards equipped; and available store. The report also displays high runner and counts of all log reports, a summary of traps, swerrs, mismatches, and counts of selected OMs. For further information on DMSMON see the *Performance* section tab and the "DMSMON" subsection.

Summary of Operations, Administration, & Maintenance Tools

Tool Precautions

The real-time call carrying capacity of the DMS switch can be maximized by curtailing some operations, administration, and maintenance (OAM) activities during the peak busy hour period. However, the latest BRISC processors with increased real-time call capacity should now allow us to utilize most tools 24 hours a day.

If, for some reason, the switch is exhausting its call carrying capacity, the following steps can be taken to curtail activities:

- Suspend all SERVORD or *table editor* activity (emergency changes only).
- Log out all unnecessary users, including disconnected users executing store files.
- The maintenance MAP position may be set to the "PREF" mode of operation which uses real-time capacity. See NTP 297-1001-129, *Input/Output System Reference Manual*, for use of the PRIORITY command.
- Resident tools such as Automatic Line Test (ALT), Automatic Trunk Test (ATT), and Killer Trunk (KT) should be suspended.
- In LOGUTIL, the STOPDEV command should be used to suspend spooling to devices that are not necessary.
- Suspend network diagnostics in the NET level of the MAP.
- Suspend Bit Error Rate Performance (BERP) testing and other Bit Error Rate (BER) tests executed from the MAP.
- Devices left logged into the switch should not be in the MAP level unless absolutely necessary.

Tool Exhibits

For information on any DMS SuperNode operations, administration, and maintenance (OAM) features that are not listed within this manual, see the latest *DMS-100/200 System Feature Planning Guide*.

The following exhibits provide a summary of commonly used operations, administration, and maintenance (OA&M) tools and include many that are topics within the MOM.

Exhibit A   Summary of Maintenance Test Tools

> **NOTE:** Included with the NTX code and name is the related PCL order code and order code name. <u>In future issues of the MOM, the NTX and feature ID may be discontinued.</u> Many of the following maintenance test tools are presented in more detail within other sections of this manual.

MAINTENANCE TEST TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
NTX001AA BASE0001	BASE Common Basic BASE (This SOC is not visible in the SOC application)
AC0285	LOOPBACK ON TRUNKS — Provides a digital transmission loopback on an individual trunk when the trunk is seized and the loopback number is dialed. The loopback takes place in the network module. This feature is required for all BER testing on individual trunks using the TTP or ATT access. Also, see the 108 test line in the Preventive Maintenance section as a supporting tool.
AG0273	DTU (Digital Test Unit) — Facilitates BER testing for tandem and toll switching offices. The DTU performs the IBERT functions of the 6X99 ILC card in a local office.
BC1611	ICTS (Integrity Check Traffic Simulator) — Test capability expanded to include LMs NETFAB (Network Fabric) NETWORK MAINTENANCE ENHANCEMENTS — Extends NETFAB testing into LMs.
BR0588	SIGNALING TEST (SIGTST) — Provides an optional *signaling test* as part of the trunk diagnostic tests.
NTX051AA TEL00001	Automatic Trunk Test TEL Telecom Layer Function (This SOC is not visible in the SOC application)
BT0241	ATT (Automatic Trunk Test) — Tests trunks for proper operation, call-through tests and transmission noise.
NTX052AB BAS00003	Remote Office Test Line (ROTL) BAS Generic (This SOC is not visible in the SOC application)
BC0128 BR0069	ROTL ATT INTERFACE — Enables maintenance testing over a specific circuit.
BC1146	ROTL TRUNK NUMBER TABLE — Provides a mapping facility between the CLLI group numbers residing in the Centralized Automatic Recording Of Trunks (CAROT) database and the actual CLLI groups residing in the DMS.

MAINTENANCE TEST TOOLS (continued)

Technical Reference | **PCL Name, Test Tool Name, and Test Tool Description**

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
NTX053AA BAS00003	Maintenance Assistance Package BAS Generic (This SOC is not visible in the SOC application)
BC0426	NETINTEG ANALYSIS — Provides a tool that identifies faulty network cards that are causing problems.
BC1460	KILLER TRUNK (KT) REPORT SEPARATION — Provides a new report separation output capability for the killer trunk report.
BR0210	SILENT SWITCHMAN — Provides the capability of opening the tip and ring of the cable pair at the cutoff relay on the line card. This action is taken by the installer/repair person at the station end (no central office involvement). The line returns to normal after a time based upon the SILENT_SWITCHMAN_TIMEOUT parameter.
F6309	KILLER TRUNK (KT) feature updated for improved detection and reporting.
BR0017	KILLER TRUNK (KT) TEST I.D. — Detects any trunks which have one of the following properties: Short Holding Time; Slow Release; Always Busy; and Always Idle.
NTX054AA BAS00003	Line Test Position BAS Generic (This SOC is not visible in the SOC application)
BT0095	ALT (Automatic Line Testing) BAL — Sets the *hybrid balance network* in the line card to provide transmission balance. DIAGN — Checks line card circuits for correct operation. SDIAG — Verifies the transmission function of the line card.
BV0061 BV0062 BV0063	LTP — Descriptions of various line tests which can be performed from the LTP.
NTX055AA TEL00001	Trunk Test Position TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AG1240	TTP (Trunk Test Positions) DETACHED USER — Permits the creation of detached (software only) Trunk Test Positions. A detached TTP has all the capabilities of a regular TTP except those which require any dedicated hardware.
BC0091	MONITOR TALK (also requires BR0245, BT0233, and BV0042).
BR0021	TTP — Scheduled status report.
BR0196	TTP — Call transfer—local (also requires BV0041).
BR0245	MONITOR TALK (also requires BC0091, BT0233, and BV0042).
BT0233	MONITOR TALK (also requires BC0091, BR0245, and BV0042).
BV0039	STUCK SENDER — Identify and system busy stuck senders in a specified truck group.

MAINTENANCE TEST TOOLS (continued)

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
BV0041	TTP — Call transfer—local (also requires BR0196).
BV0042	MONITOR TALK (also requires BC0091, BR0245, and BT0233).
NTX106AA MDC00007	MDC - Meridian Business Set MDC MBS Minimum
AG0409	EBS (Electronic Business Set) MAINTENANCE — Maintains the volume setting at the station while the loop is opened for testing. Requires Metallic Test Unit (MTU) hardware and firmware (NTX124AA).
AG0979	CKTTST — An additional ALT test function. Applies to EBS, DU, AIM and IBERT line cards. Performs a *circuit test* between the station and line card to validate transmission.
NTX167AB ISP70001	CCS7 Trunk Signaling SS7 Trunk Signaling
AC0199	ISUP105 TEST LINES — Extends ISUP capabilities to include manual or automatic 105 test line testing.
NTX250AA DTP00001	Datapath - Basic DTP Datapath
AC0105 BC2051	IBERT BIT ERROR RATE TEST ENHANCED — 2047 Pattern enhancement to existing IBERT capabilities for: Error-free Second Measurements Error Injection Capabilities T-Link Version 2 Compatibility
BC2052 BF0952 BT1088 BZ0592	IBERT – 511 BIT PATTERN — Integrated Bit Error Rate Testing (IBERT) enables the technician to perform maintenance messaging from a MAP position as follows: Datapath Bit Error Rate Testing Datapath Extension (DPX) Maintenance
NTX259AA DTP00001	Datapath Extension - DPX DTP Datapath
BC2240 BF0726	DPX COMPATIBILITY WITH IBERT — Extends existing data line maintenance and Bit Error Rate Testing (BERT) to the DPX line and its associated Data Line Card (DLC) and Data Unit (DU).
NTX272AA BAS00003	Focussed Maintenance BAS Generic (This SOC is not visible in the SOC application)
BC1288 BC1289 BC1290 BV1573	FOCUSSED MAINTENANCE FOR LINES — To manage line call processing failure messages utilizing a system of buffers, thresholds and alarms.

MAINTENANCE TEST TOOLS (continued)

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
BV1572	FOCUSSED MAINTENANCE FOR TRUNKS — To manage software identified trunk trouble messages utilizing a system of buffers, thresholds and alarms.
NTX277AA BAS00003	Dialable Line Circuit ID BAS Generic (This SOC is not visible in the SOC application)
BR0569	CABLE LOCATOR TONE — The DMS-100, upon receiving a security/access code followed by a seven digit DN from any line circuit, should provide the desired tone across the tip and ring leads of the dialed DN.
BR0570	SHORT CIRCUIT — Provides the capability of applying a timed short circuit across the tip and ring leads of DMS-100 line.
NTX750AB NTX750AC NTX750AD	ISDN Basic Access (MD's in BCS35) ISDN Basic Access (MD's in BCS36) NI0 ISDN Basic Access
AL0596	BERT ISDN ACCESS LOOPS — Enables performance of Bit Error Rate Testing at 56 Kbps or 64 Kbps on ISDN basic rate access loops using existing DMS Integrated BERT facility.
NTX875AA ISP70001	CCS7 MASS Trunk Conversion SS7 Trunk Signaling
AL0520	Will save the operating company time and effort when converting conventional trunks to SS7 trunks as well as reducing trunk down time.
NTX881AC BAS00003	Switch Bit Error Rate Maintenance BAS Generic (This SOC is not visible in the SOC application)
AG0360	BIT ERROR RATE INDICATOR — A tool for measuring switch Bit Error Rate Performance (BERP) using random test sampling.
AG0665	IBERT RESOURCE MANAGEMENT — Integrated Bit Error Rate Testers NT6X99 (ILC) and NT4X23 (DTUs) can now be allocated to specific BER applications or shared between a number of applications.
AG0949	BERP and LM/LCM LOOPAROUND — Extends BERP testing to all LCMs and LMs. Reduces the requirement for NT6X99 ILCs (IBERT Line Cards).
NTX882AA TEL00001	Bit Error Ratio Indicator - Toll TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AG0521	BERP FOR TRUNKS — Provides Bit Error Ratio Performance (BERP) testing on trunks with or without loopbacks at the DS1 card or DS30 Link Card.
NTX883AA TEL00001	Interoffice Trunk BERT TEL Telecom Layer Function (This SOC is not visible in the SOC application)

MAINTENANCE TEST TOOLS (continued)

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
AG0520	BERT FOR TRUNKS — Provides BER testing for digital outgoing and two trunks to the next digital office which must be equipped with the "DIALED LOOPBACK ON TRUNKS FEATURE" (NTX001AA F6528). Also provides automated ATT BER trunk testing capability.
NTX885AC TEL00001	Switch Path Diagnostics TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AL0154	NETPATH — A troubleshooting tool for network fault isolation/verification testing. Allows the tester to specify and select specific paths through the network for troubleshooting.
AL0478	XBERT — A fault detection and isolation tool for identifying bit error transmission problems in XPM, LCM, and RLCM type circuit packs. XBERT supports LTC, LGC, DTC, RCC, IAC, MSB7, and ILGC.
AL0511	ICTS — Integrity Check Traffic Simulator (ICTS) is a resident software tool for identifying integrity/parity errors between two end points of a network connection.
AJ0473	ICTS ENHANCEMENTS — Allows the Integrity Check Traffic Simulator (ICTS) and Network Fabric (NETFAB) to test inservice trunk channels associated with New Peripherals (XPMs).
AL0153	(NETFAB) Scheduled Testing of DMS Networks — Essentially automates the ICTS testing process. Scheduled to run four hours each night, starting where it stopped the previous night. When all link and junctor channels have been tested, it starts again.
AG1214	NETPATH AUTOMATION — Provides automation of the AG1214 existing NETPATH feature to perform isolation/verification on the network links and components of a speech path.
NTX901AA BAS00003	Local Features I BAS Generic (This SOC is not visible in the SOC application)
BR0283	STATION RINGER — Performs dial test, off-hook ground test, and DN on-hook ground test. Also requires BT0063.
BR0623	STATION RINGER 3-DIGIT — Permits Station Ringer access via a single access code followed by a 7-digit DN.
BT0063	STATION RINGER — Performs dial test, off-hook ground test, and DN on-hook ground test. Also requires BR0283.
AG0156	ALT (Automatic Line Testing) — for improved administration: table driven, improved scheduling, logs, and user interface; eliminates the requirement for multiple users.
BR0511	ALT SPEED-UP — Speeds up ALT functions
BT0095	ALIT — Identifies cable pair faults (i.e., grounds, shorts, FEMF).

Exhibit B   Summary of Operations, Administration & Maintenance Tools

NOTE: Included with the NTX code and name is the related PCL order code and order code name. <u>In future issues of the MOM, the NTX and feature ID may be discontinued.</u>

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description
BASE 08	**BASE**
AR2212	WARM SWACT RECOVERY INFRA-STRUCTURE — This feature provides the implementation of a Switch of Activity (SWACT) infrastructure that safeguards the SWACT environment against applications or SWACT steps that trap.
SD0003	PRESERVE LOG SETTINGS OVER ONE NIGHT PROCESS (ONP) — This feature implements a method of maintaining various log control information over a software upgrade and Maintenance Switch of Activity (MTCSWACT). The information about logs that is handled by this feature includes class assignments, log suppression, and threshold values. These are the settings displayed by the LOGUTIL commands LISTREPS SPECIAL, LISTTIME, and LISTREPS CLASS X, where X = 0 through 31.
AR1917	TABAUDIT ENHANCEMENT — This enhancement feature mainly focuses on the improvement of the autotabaudit scheduling capabilities and the user interface. The main purpose of this feature is to: • Eliminate One Night Process (ONP) lab dry runs as much as possible. • Increase the usability of TABAUDIT, especially automated TABAUDIT. • Decrease the number of failed tables and tuples during the table transfer portion of the ONP The main activities involved in this feature include: • Modify TABAUDIT to allow multiple iterations of data checking. • Modify some CI commands to include more options thereby providing users with a more flexible user interface. • Redesign the architecture to make the tool more robust and easier to expand.
BASE00003	**BASE (This SOC is not visible in the SOC application)**
XPM10 Planned AF7565	MAINTENANCE ARBITRATOR — This fault-handling enhancement automates the isolation of potential problems with system hardware before they become serious.
GA = NA009	LOCAL SCAN POINT for LINK ALARMS — This feature assigns an SS7 link failure alarm to a scan point so a control center can be alerted.
AN0753 GA = NA002	SWITCH STATUS REPORT — A report that provides a single concise log on various aspects of switch status such as call originations and call traps. An SSR CI level command and subcommand DISPLAY outputs either a short or verbose format of the SSR600 report.
AN0754 GA = NA002	NODE ASSESSMENT GRAPH — A feature that generates an hourly log report (NAG400) which contains a snapshot of nodes in the system that are out-of-service or have a REX problem. A NAG command at the CI level controls the output display.

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description (continued)
BAS00041	**DMS Base Service — Enhanced Permanent Signal**
AG3384 GA = NA003	ENHANCED PERMANENT SIGNAL — A feature that automatically provides an analysis of a line that has been detected as being off-hook for an extended period of time. Identifies faulty or hazardous lines and alerts by logs to take action on resolving the problem.
PLATFORM **No ordering codes**	**DMS SuperNode Platform — Standard Features**
AG3548 GA = NA002	SPMS RECALIBRATION — Enhancement to recalibrate the Switch Performance Monitoring System (SPMS) with new OMs added since BCS32—and provide stricter performance and thresholds criteria.
AL2666 GA = NA002	TELCO-DEFINED LOGIN BANNER — Enhancement to provide a banner that warns the user that this is a private database. Allows the customer to edit the banner as needed.
GA = BCS36	NORESTARTSWACT — Provides a significant enhancement by reducing system interruption during maintenance activities from between three and five minutes to less than 30 seconds
AF5766AA GA = NA004	MAINTENANCE (MTC) SWACT — Automates NORESTARTSWACT steps required for setting up and performing in-sync maintenance activities that require a manual restart—such as parameter and table changes and software retrofits.
AF5950, 51, & 52 GA = NA004	POST RELEASE SOFTWARE MANAGER (PRSM) — PRSM is a new software patching system that replaces the existing DMS Patcher Utility. It provides a simplified user interface, flexible recording, and consistent command syntax across all patchable DMS nodes.
GA = NA009	ENHANCED POST RELEASE SOFTWARE MANAGER (PRSM) — An enhanced version that expedites patch removal by automatically identifying software that is dependent on any patch in the current load, and it simplifies troubleshooting through an automatic time stamp that records the time and date each patch is activated.
GA = NA004	ENHANCED LOG FORMAT — Upgrades the LOGFORMAT utility for retrieving logs by date and time.
GA = NA004	ENHANCED TRUNK MAINTENANCE FRAMEWORK — Enhancement provides a verification report of Analog Trunk Test Signal timing in accordance with Bellcore specification TR-TSY-0005067, Sections 5.2 and 6.3.
GA = NA002	BRISC CAPACITY USAGE MONITOR — Introduces OMs and a usage table to track processor-capacity usage trends and allow pay-per-use pricing implementation.
NTX001AA **BASE00001**	**Common — Basic** **BASE (This SOC is not visible in the SOC application)**
AF1452	MEMORY ADMINISTRATION — New operational measurements that give actual memory usage information.

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description (continued)
AF1780	DIRP SPACE ROTATION — A new method of managing the room taken up by DIRP files on disk.
AG0724	PARMCALC PHASE II — A CI command that displays recommended values of office parameters, now will output the amount of memory increase or decrease in words for the changed value.
AG1006 AG1007	SCHEDULED CC/CM & XPM PATCHING feature automates the patch application process, once the patch is downloaded to the switch. The operating company has complete control over the patch process through table control and may select the patches to be either automatically or manually applied.
AG1524	JFFREEZE-DMO ENFORCEMENT FOR JOURNAL FILE — When invoked after a system image is taken for a Dump and Restore, it maintains a record of all Journal Files created. All changes that cannot be restored with JFDUMP and DMOPRO commands will be stored in a separate file for manual re-entry.
AL0044	OUTAGE FOOTPRINT — Provides a quick means of determining the cause of serious switch outages. Captures a snap shot of the system when an outage occurs.
BC1925	QUERY COMMAND ENHANCEMENTS — Allows the user to find out, using QUERY command, when a module was last modified.
BR0165	INPUT COMMAND SCREENING I/O PORT — Allows operating company to restrict command usage on the basis of terminal identity instead of user ID. (also requires BV0018 and BV0040)
BR0536	CRITICAL MESSAGE PRIORITIZATION — Provides for an optional method of report prioritization in the log system.
BR0817	PROTECTION OF UNEXPIRED TAPES — Prevents tape over-writing and formatting when using the MOUNT command and the tape has not expired.
BT0043 BT0249 BV0006	DEAD OFFICE ALARM — Indicates a loss of call processing ability in the DMS office.
BV0018 BV0040	INPUT COMMAND SCREENING I/O PORT — Allows operating company to restrict command usage on the basis of terminal identity instead of user ID. (also requires BR0165)
BV0409	INPUT COMMAND SCREENING LOG-IN — Allows automatic login at terminal. (see BR0165, BV0018, and BV0040)
F1062	INPUT COMMAND SCREENING USER RESTR. — A user is allowed to input only those commands assigned to that user.
NTX044AA BAS00003	Central Automatic Message Accounting (CAMA) BAS Generic (This SOC is not visible in the SOC application)
BR0020	BLUE BOX FRAUD — Enables identification and billing of blue box fraudulent calls.

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description (continued)
NTX074AA BASE0001	Disk Data Storage System BASE (This SOC is not visible in the SOC application)
AG1004	LOG RETRIEVE FACILITY FOR E1 INCIDENTS — Enables telcos to potentially capture all logs on permanent store, including logs which can be threshold or suppressed.
AG1043	AUTOMATIC IMAGE DUMP — Provides the operating company with a method to automate the office IMAGE process. It is table controlled; the IMAGE is taken following a successful CC REX test.
NTX177AA CNBS0001 CNBS0005 CNBS0006	Non-resident General Utilities CNBS COPYTSUB CNBS SELECTIVE CMD Executive CNBS DISP meaning of name
BV0261 BV0397	COMMAND SCREENING — Enables the assignment of commands to devices which will be allowed to use these commands.
NTX178AA CNBS0004	Nonresident Diagnostic Utilities CNBS OM Tape Dump Command
BC0354	LOG ANALYSIS PROGRAM (SCANLOG) — Allows for selection, sorting and analysis of specific log output reports.
NTX210AA TEL00001	No. 2 SCC Interface TEL Telecom Layer Function (This SOC is not visible in the SOC application)
BR0513	NO. 2 SCC INTERFACE — Provides central control maintenance support for remote maintenance and control hardware.
NTX292AB BASE0001	Enhanced Security Package I — Password Encrytion BASE (This SOC is not visible in the SOC application)
BC0904	ENHANCED COMMAND SCREENING — Allows commands to be assigned any subset of 31 classes.
BC0905	PASSWORD CONTROL — Password control is restricted to the user (if old password is known).
BC1041	AUDIT TRAIL (SECURITY LOGS) — Provides an audit trail to track all user security related events on a DMS switch.
BC1042	ACCESS CONTROL (LOGIN CONTROL) — Allows control of login access to consoles.
BC1044	AUTOMATIC LOGOUT OF DIAL-UP — Terminal users are automatically logged out, and the connection is dropped when a *facility open* condition is detected.
BC1305	SECURITY TABLE ENHANCEMENTS — Allow the operating company to monitor who is accessing which customer tables.

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description (continued)
NTX293AA BASE0001	Enhanced Security Package II BASE (This SOC is not visible in the SOC application)
BC1043	AUTOMATIC DIALBACK — Enhances the security of remote access to DMS using dial-up ports by optionally requiring dial back via a companion CTS 212 AH SMART Modem.
BC1451	DIALBACK ON OTHER MODEMS — Enhances the security of remote access to DMS using dial-up ports by optionally requiring dial back via a RIXON R212A Intelligent Modem.
NTX385AA TEL00001	OM Thresholding and Alarms TEL Telecom Layer Function (This SOC is not visible in the SOC application)
BR0576	OM THRESHOLDING — Provides real-time switch surveillance by measuring key OM maintenance registers against preset bogeys and a scan time interval.
NTX445AB BASE0001	OM Selective Output BASE (This SOC is not visible in the SOC application)
BR0578	OM SELECTIVE OUTPUT — Enables scheduling of operational measurement data by selected tuples.
BR0664	OM GROUP TOTALS — Adds totals by register to a operating company-defined selection of OM groups.
NTX738AC TEL00001	Switch Performance Monitoring System TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AG0469	SPMS (Switch Performance Monitoring System) — Provides minor improvements for the SPMS which include a new sub-index for attendant console performance and a new CI SPMS sub-command DESCRIBE.
AC0048	(SPMS) Switch Performance Monitoring System – Phase II — Adds new sub-commands to the SPMS CI commands, SET and DISPLAY, permitting improved display of index results. New OMs are added, allowing the full set of TRAFFIC indices to be implemented.
BS0604	(SPMS) Switch Performance Monitoring System – Phase I — Adds new SPMS CI command, with sub-commands, allowing interrogation of index values.
AG1495	SPMS ENHANCEMENTS II — Switch Performance Monitoring System has been expanded by adding forty seven new indices. The new indices provide information on the performance of the DMS switch that was previously not measured by SPMS.
NTX812AA TEL00001	Centralized MAP TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AG0375	SCC MAP AUTO RESTART — Ensures that after a DMS restart or a communications link failure, the SCC remote log port with the name CMAPSCCS will have log message routing restarted.

OPERATIONS, ADMINISTRATION, & MAINTENANCE TOOLS

Technical Reference	PCL Name, Test Tool Name, and Test Tool Description (continued)
NTX901AA BAS00003	Local Features BAS Generic (This SOC is not visible in the SOC application)
BR0653	"COD" OPTION OFFICE BASIS — Provides operating company the ability to supply, on every line in a DMS-100F office, an 800 ms open battery signal at disconnect to either the originating or terminating agent in a call.
BT0045	PURPLE BOX — Prevents purple box wire tap fraud by employing both timed and called party clear and calling party clear connection release on normal types of call.
NTX942AA BASE0001	SuperNode System Load Module BASE (This SOC is not visible in the SOC application)
AG1385	PRESCHEDULED IMAGE TAKING ON THE SLM — Allows the Computing Module and Message Switch image dumps to be taken automatically to a System Load Module without user intervention.
NTXJ35AA TEL00001	Manager's Maintenance Report TEL Telecom Layer Function (This SOC is not visible in the SOC application)
AJ0190	EXECUTIVE MORNING REPORT — An automated tool which reports on the DMS switch performance and scheduled test results. See the "Maintenance Managers Morning Report" subsection within the *Performance* section of this manual.
AJ0472	EXECUTIVE MORNING REPORT — Provides enhancements to the first version of the report and the capability to tailor the report.
HSTP0002	Nortel Networks 1-Meg Modem (GA NA007)
AF7630 GA NA011	PROVISIONING & OAM ENHANCEMENTS FOR 1-MEG MODEM Enables the service provider to automate the 1-Meg Modem line option datafill using SERVORD. Provides OAM capability to query a 1-Meg Modem Media Access Control (MAC) address by using the Query XNET (QXNET) command.

New & Changed Logs, Commands, and OMs

The tables within this subsection provide a summary of new and changed schema tables, OM groups, logs, office engineering parameters, and user interface commands for LEC0011 through LEC0014 releases. Detailed information for each item can be found for the corresponding PCL release in NTP 297-XXXX-100, *North American DMS-100 OAM&P Change Document Reference Manual*.

LEC0011

Table 1-1   LEC0011 New and Changed Tables, OM Groups, and Logs

Table 1-2   LEC0011 New and Changed Office Parameters

Table 1-3   LEC0011 New and Changed User Interface Commands

LEC0012

Table 1-4   LEC0012 New and Changed Tables, OM Groups, and Logs

Table 1-5   LEC0012 New and Changed Office Parameters

Table 1-6   LEC0012 New and Changed User Interface Commands

Table 1-7   LEC0012 Deleted Command Interface Elements

Table 1-8   LEC0012 New Alarms

Table 1-9   LEC0012 Deleted Alarm Elements

LEC0013

Table 1-10   LEC0013 New and Changed Tables, OM Groups, and Logs

Table 1-11   LEC0013 New and Changed Office Parameters

Table 1-12   LEC0013 New and Changed User Interface Commands

Table 1-13   LEC0013 Deleted Command Interface Elements

Table 1-14   LEC0013 New Alarms

LEC0014

NOTE: Text that does not fit on a single line within the table column is underlined to improve readability.

NOTE: Tables that contain italicized items in the "Changed" column identifies items that have been deleted.

NOTE: Tables 1-7 through 1-9 are new with LEC0012

Table 1-1 — LEC0011 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
C7LKPARM	ACDGRP	C7HSLAL1	AINICSUB	AUD673	AIN600
IPINV	ACDIPINV	C7HSLAL2	AINOGSUB	CCS120	AIN601
MNPRIIID	ACDMISPL	C7HSLATM	CALLWAIT	CCS121	AIN602
MTRLNET	AMAOPTS	C7HSLCAR	ECANRMAN	CCS124	AINT700
MTRMOG	AMATKOPT	C7LINK4	EXT	CCS125	CCS103
MTRMOTS	AOCBASIC	MWICTCAP	EXT 198	ISDN401	CCS163
MTRNAMES	C7CNGSTN	PRIMWIC	ISUPUSAG	ISDN402	CCS164
MTRNETIF	C7LINK	RLDBD	OAPCALP9	PES200	CCS173
MTRSYSPM	C7LKSET	RLDBRA	PRADCHL	PES201	E911231
MTRTARIF	C7TIMER	RLDMSGCT	SCAISRV2	PES202	EQAC600
MTRTTS	C7UPTMR	RLDSTAT	SCAISRV3	SCAI500	ISDN100
PILOTGRP	CARRMTC	RND	TRMTCM2	SCAI501	ISDN101
RATEAREA	CFW	SCAISRV3	TROUBLEQ	SCAI502	ISDN102
SRASCRN	CMDS	SCAISRV4	TWCIBN	SIM600	ISDN103
TONESGRP	CSGRP	SEIUTRAN	TWCPOTS	SPM310	ISDN106
TRKSGRP	CUSTENG	SIMRING		SPM502	ISDN107
XLAPLAN	CUSTHEAD	SRAOM		SPM503	ISDN108
	CUSTNTWK	U3WC		SPM504	ISDN109
	CUSTSTN			SPM660	ISDN115
	DIGMAN			SPM661	ISDN116
	DNATTRS			SPM705	LINE100
	DNCTINFO			SPM706	LINE101
	DNFEAT			SPM707	LINE150
	DNATTRS			SPM708	LINE605
	DNROUTE			TOPS604	PM179
	ENG640I1			Unable to pass LNP info through VFG	PM180
	HNPACONT			V5260	PM181
	HNPACONT$HNPACODE				PM182
	HUNIGRP				PM183
	IBNFEAT				PM184
	IBNLINES				SDMB530
	IBNRT2				SNAC100
	IBNRT3				SPM310

—continued—

Table 1-1 — LEC0011 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	IBNRT4				SPM660
	IBNRTE				SPM661
	IBNXLA/XLANAME				SPRF670
	IBNXLA				SPRF671
	ISDNVAR				
	KSETFEAT				
	KSETLINE				
	LCCOPT				
	LCMDRINV				
	LCMINV				
	LENFEAT				
	LENLINES				
	LINEATTR				
	LIUINV				
	LNINV				
	LTCALLS				
	LTCPSINV				
	LTDATA				
	LTDEF				
	LTDEF and PRIPROF				
	LTMAP				
	MNHSCARR				
	MSRTAB				
	MTRMOG				
	MTRMOTS				
	MTRTARIF				
	MTRTTS				
	NCOS				
	OFCAUT				
	OFCENG				
	OFRT				
	OPTOPT				
	PODPATTR				

—continued—

Table 1-1 — LEC0011 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	RESFEAT				
	RESOFC				
	RMPCKT				
	SACB				
	SCAICOMS				
	SCAIPROF				
	SCAISSRV				
	SPMECAN				
	SVPRIGRP				
	TCAPTRID				
	TMTCNTL/TREAT				
	TMTMAP				
	TONES				
	TRA125I1				
	TRA125I2				
	TRA250I1				
	TRIGITM				
	TRKGRP				
	TRKOPTS				
	TRKSGRP				
	V5SIG				
	VFGDATA				
	VIRTGRPS				
	XESAINV				
	XLAMAP				
	XLANAME				
	SCRNCL deleted				
	HSTS deleted				
	PRTNM deleted				
	ZEROMPOS deleted				
	RESINFO deleted				
	LCANAME deleted				
	MRSA deleted				
	LATANM deleted				
	MAXTAIL deleted				
—end—					

Table 1-2 — LEC0011 New and Changed Office Parameters

New Office Parameters	Changed Office Parameters
CALL_WAITING_CONFERENCE	ACD_OVERFLOW_BLOCKS
CWT_ON_POTS_IBN_3WC_CONTROLLER	AIN_NUM_00_PARA_EXT_BLKS
LSPI_FORWARD	AIN_NUM_01_00_EXT_BLKS
MAX_NUM_ECM_ICCM	AIN_NUM_EXT_BLK
MAX_NUM_ECM_TPQC	AIN_NUM_PROCESSING_EXT_BLKS
MAX_NUM_MWI_CONTROL	AIN_NUM_TERM_NOTIF_EXT_BLKS
NO_OF_CLONE_TIDS	C7_PDU_ERROR_SLMPR_THRESHOLD
PN_SUPPORTED	C7_SSCOP_CON_SLMPR_THRSHOLD
SIMRING_RES_CONTROL	C7_SSCOP_RETRANS_SLMPR_THRESHOLD
SIMRING_CENTREX_CONTROL	CFD_EXT_BLOCKS
SLU_VARIABLE_LENGTH_DN	CFW_EXT_BLOCKS
SO_ALLOW_REDUNDANT_FEATURE	CFZ_EXT_BLOCKS
SO_ALLOW_REDUNDANT_FEATURE_CHF	CRS_PRU_POOL1_SIZE
SRA_BILLING	CRS_PRU_POOL2_SIZE
SRA_TIMERS	CRS_PRU_POOL3_SIZE
SRA_TREATMENT	CRS_SUBRU_POOL5_SIZE
U3WC_ELAPSED_TIME	CRS_SUBRU_POOL1_SIZE
U3WC_FLASH_ONLY	CRS_SUBRU_POOL2_SIZE
U3WC_POTS_ENABLED	CRS_SUBRU_POOL3_SIZE
XLAPLAN_RATEAREA_SERVORD_ENABLED	CRS_SUBRU_POOL4_SIZE
	EA_MF_SS7_EXT_BLOCK_COUNT
	KSHUNT_EXT_BLOCKS
	MAX_NUM_WIDEBAND_CALLS
	NO_OF_HIS_CONTROL_BLKS
	NUM_IBN_IXLA_EXT_BLOCKS
	NO_LOCAL_COIN_EXT_BLKS
	NUM_OF_CCIS_INWATS_BLOCKS
	NUM_DCR_EXT_BLKS
	NUMBER_OF_DITM_EXTENSION_BLOCKS
	NO_OF_FTR_CONTROL_BLKS
	NO_OF_FTR_XLA_BLKS
	NO_OF_HIS_DATA_BLKS
	NUM_OF_INWATS_EXT_BLOCKS
	NO_OF_LARGE_FTR_DATA_BLKS
	NUM_OF_NSC_EXT_BLK
	NUM_OF_NT_RECORDING_UNITS
—continued—	

Table 1-2 — LEC0011 New and Changed Office Parameters

New Office Parameters	Changed Office Parameters
	NO_OF_ORIG_INFO_EXT_BLKS
	NO_OF_PVN_EXTBLK
	NO_OF_PVN_TERM_EXTBLK
	NUM_OF_RTEB_EXTBLKS
	NO_OF_SC_EXT_BLKS
	NUM_RC_EXT_BLKS
	NUMIBNCQEXTBLK
—end—	

Table 1-3 — LEC0011 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
ATMCONDIR (ATMCON)	*AINTRACEDIR (BACK) deleted*
ATMCONDIR (LISTCON)	*AINTRACEDIR (CLEAR) deleted*
ATMCONDIR (LOOPBK)	AINTRACEDIR (HELP)
ATMCONDIR (POST)	*AINTRACEDIR (OPEN) deleted*
ATMCONDIR (QUERY)	AINTRACEDIR (START)
C7LKS_DIR (CARLOOP)	AINTRACEDIR (STOP)
C7LKS_DIR (QUERYATM)	AINTRACEDIR
C7LKS_DIR (QUERYCAR)	ALARMS (AU3186)
CALLTRAKDIR (EVTRACE)	C7LKS_DIR (QUERYFLT)
CI (PRADLYLG)	C7LKS_DIR (QUERYTRF)
CPDBGCI	CALLTRAKDIR (DISPLAY)
CARRIER (CARRIER SCREEN OVERVIEW)	CI (QDN)
EISPRT (DISABLE)	CI (QDNWRK)
EISPRT (DISPLAY)	CI (QLEN)
EISPRT (ENABLE)	CI (QLENWRK)
EISPRT (RESET)	CI (TRAVER)
EISPRT (SET)	DMSCI (QPHF)
EISPRT (STATUS)	ESADIR (QUERYPM)
IPDIR (BSY)	HLIU (LOOPBK)
IPDIR (LOADPM)	HLIUDIR (QUERYPM)
IPDIR (OFFL)	ISDB (LOADQ)
IPDIR (PMRESET)	ISDB (SUSPECT)
IPDIR (QUERYPM)	ISDB (TROUBLEQS)
IPDIR (RTS)	LCBTOOLDIR (LCBCI)
IPDIR (TRNSL)	LN_LTP_DIR (BSY)
LMUDIR (BSY)	LTP (DIAG)
LMUDIR (CONVERT)	LTP (POST D)
LMUDIR (CSINFO)	LTP (POST DK)
LMUDIR (FRLS)	LTP (POST H)
LMUDIR (HOST)	LTP (POST LT)
LMUDIR (NEXT)	LTP (POST SHOWER)
LMUDIR (OFFL)	LTPLTA (DGTTST)
LMUDIR (QUERYTE)	LTPMAN (JACK)
LMUDIR (QUIT)	LTPMAN (LOSS)
—continued—	

Table 1-3 — LEC0011 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
LMUDIR (RTS)	LTPMAN (LTA)
LMUDIR (TST)	LTPMAN (MONLTA)
PESDIR (DISP)	LTPMAN (NOISE)
PESDIR (DOOR)	LTPMAN (RING)
PESDIR (NEXT)	LTPMAN (RLSCONN)
PESDIR (POST)	LTPMAN (TALKLTA)
PESDIR (QUERYPES)	LTPMAN (TONEGEN)
PRADCH (QRYABN)	PM (LOADPM)
PRADCH (QRYPERF)	PMUPGDIR (SET)
PROGDIR (BLOCKCT)	PROGDIR (DUMP)
PROGDIR (BLOCKMON)	PROGDIR (MTRVER)
PROGDIR (EMSI)	PROGDIR (PRIVCLAS)
PROGDIR (ONPREADY)	PRODIR (QLT)
PROGDIR (QPDN)	PROGDIR (SPMECMON)
PROGDIR (QPDN)	PRODIR (TRAVER)
PROGDIR (SETOCMSM)	PROGDIR (TRAVER AIN AINMQG)
PROGDIR (SPMECMON)	PROGDIR (WHATS)
PROGDIR (TOPBLOCK)	QDN
RLDDIR (QUERYPES)	QGRP
SPMDLCDIR (BSY)	QLEN
SPMDLCDIR (LISTALM)	SERVORD (CHG)
SPMDLCDIR (LOADMOD)	SERVORD (EST)
SPMDLCDIR (NEXT)	SERVORD (NEW)
SPMDLCDIR (OFFL)	SERVORD (NEWDN)
SPMDLCDIR (PROT)	SLU_CIDIR (SLUADD)
SPMDLCDIR (QUERYMOD)	SLU_CIDIR (SLUDEL)
SPMDLCDIR (RTS)	SLU_CIDIR (SLUDUMP)
SPMDLCDIR (TST)	SLU_CIDIR (SLUFINDI)
SPMDLCDIR (SELECT)	SLU_CIDIR (SLUFINDO)
SWUPGDIR (SWUPGRADE CMMOCK)	SLU_CIDIR (OMSHOW)
TOPSDEVDIR (RTS)	SOCDIR (ASSIGN)
TSTQUERYDIR (PREFIX)	SOCDIR (REMOVE)
TTP (PHTTP)	SOCDIR (SELECT)
UREMDIR (PES)	SOCDIR (VALIDATE)
USE9KDIR (BSY)	SPERFORM
USE9KDIR (OFFL)	SPMDIR (QUERYPM)
—continued—	

Table 1-3 — LEC0011 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
USE9KDIR (QUERYPM)	SPMACT
USE9KDIR (RTS)	SPUSAGE (START)
USE9KDIR (TST)	STRMDIR (POST)
X75TTP (LOOPBK)	STRMDIR (QUERY)
	SYSDIR (PASSWORD)
	TABAUDIT
	TRACE CI
	TRAVER
	TRAVER (AU33215)
	TSTEQUIPDIR (POST)
	TSTQUERYDIR (APPLICATIONERRORSTRING)
	TSTQUERYDIR (CLRPARM)
	TSTQUERYDIR (LISTPARM)
	TSTQUERYDIR (SEEPARM)
	TSTQUERYDIR (SEND)
	TSTQUERYDIR (SETMSG)
	TSTQUERYDIR (TRIGGERCRITERIATYPE)
	TTP (CKTLOC)
	TTP (LEVEL)
	TTP (TST)
	TTP (X75TTP)
	UCDQUERY (GROUPINFO)
	X75TTP (LOOPBK)
—end—	

Table 1-4 — LEC0012 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
FANISCR	ACDGRP	ARN	DSPRMAN	ARN600	<u>AMREPORT</u>
NPRESERV	ACRTE	IWBM	ECANRMAN	ARN601	AUDT612
XAFWLOAD	AMATKOPT	RTESVCS	HPCBASIC	CARR630	AUDT616
	AUTOTAB	SPMCMR	SCAISRV4	CARR631	AUDT620
	C7GATEPC	TCW	SCAISRV4	CARR640	AUDT621
	C7GATERS	UNBCDC		CARR641	AUDT622
	C7LINK	UNBMISC		DFIL318	AUDT624
	CARRMTC			ISDN311	CARR300
	CTRTE			ISDN312	CARR310
	CUSTHEAD			IWBM800	CARR500
	CUSTSTN			NCAS100	CARR501
	DART			PRSM303	CARR510
	DESTDATA			SCAI103	CARR511
	DNINV			SOS400	CARR512
	DNROUTE			SOS410	CCS101
	E911OFC			SOS411	CCS102
	ENINV			SOS412	CCS103
	FARTE			SPM350	CCS104
	<u>FNPACONT (RTEREF)</u>			TCW600	CCS105
	<u>FNPACONT (FNPASTS(RTEREF))</u>			TCW601	CCS106
	FTRTE			XAC330	CCS107
	<u>HNPACONT (RTEREF)</u>			XAC333	CCS156
	HUNTGRP			XAC628	CCS157
	HUNTMEM			XAC630	CCS158
	IBNFEAT			XAC631	CCS159
	IBNLINES			XAC632	CCS160
	IBNRT2			XAC633	CCS161
	IBNRT3				CCS162
	IBNRT4				CCS163
	IBNRTE				CCS164
					CCS165
					CCS173
					CCS176
—continued—					

Table 1-4 — LEC0012 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	IMGSCHED				CCS190
	IPINV				CCS400
	ISDNVAR				CCS401
	KSETFEAT				CCS402
	KSETINV				CCS403
	L3ABNLOG				CM179
	LCCOPT				NWM107
	LCMDRINV				PM
	LCMINV				PM128
	LENFEAT				PM179
	LINEATTR				PM180
	LIUINV				SPM660
	LNINV				SPM661
	LTCINV				SPRF670
	LTCPSINV				SPRF671
	LTDATA				TCAP100
	LTDEF				TCAP101
	LTMAP				UNB300
	MNCKTPAC				XAC400
	MNCKTPAK				
	MNHSCARR				
	MNNODE				
	MNPRTGRP				
	MNSHELF				
	MPCFASTA				
	MPCLINK				
	MPCLSET				
	MSRTAB				
	NIUINV				
	NSCRTE				
	OFCRTE				
	OFR2				
	OFR3				
	OFR4				
—continued—					

Table 1-4 — LEC0012 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	OFRT				
	OPTOPT				
	PODPATTR				
	PREFHUNT				
	PRSUDATA				
	PXRTE				
	RDTINV				
	SCAICOMS				
	SCAISSRV				
	SETDEFS				
	SELDEFS				
	SPINFO				
	SUSHELF				
	TRIGITM				
	TRKGRP				
	TRKMEM				
	TRKOPTS				
	TRKSGRP				
	V5SIG				
	XACINV				
	XESAINV				
—end—					

Table 1-5 — LEC0012 New and Changed Office Parameters

New Office Parameters	Changed Office Parameters
AR_WITH_NAME_ENABLED	ACTIVE_DN_SYSTEM
BRI_CND_OFFICE	XLAPLAN_RATEAREA_SERVORD_ENABLED
ECHO_STAT_BILL_PARM	
EADAS_CIC_STATUS	
HPC_EGRESS_QUEUING	
L3_SVC_DSRPT_CTRL	
L3_SVC_DSRPT_THLD	
MS_HW_SHELF_CONFIG	
MS_HW_SHELF_CONFIG_KNOWN	
POLL_SCHEDULER	
PRICFIBSFL	
SO_MAX_OPTIONS_ALLOWED	
TCW_OFFERED_ON_SCWID_DSCWID	
XA_COMPONENT_INSTALL_STATE	
—end—	

Table 1-6 — LEC0012 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
CARRUTIL (DUMPHIST)	
CARRPROT (FORCE)	
CARRPROT (MANUAL)	
CARRIER (PROTGRP)	
CARRPROT (QUIT)	
CI (NCASCI)	
CI (QPIN)	
CI (QRYCFIBC)	
CM (MTCTST)	
CMIC (LOADFW)	
CMIC (UNEQ)	
COMPRSCI (COMPRESS)	
DISK (UNEQ)	
DNINVCI (EXPAND)	
DNINVCI (EXPAND)	
—continued—	

Table 1-6 — LEC0012 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
ECHOCI (ADD)	AINTITT (CREATE)
ECHOCI (MOD)	BSY (PRADCH)
ECHOCI (REM)	BSY (TTP)
ESA (LOADFW)	C7LKS (Deact)
IO (LOADFW)	C7LKS (QueryRes)
IO (UNEQ)	CARRIER (DETAIL)
NCASCI (HELP)	CARRUTIL (HELP)
NCASCI (QUIT)	CARRUTIL (LiSTHIST)
NCASCI (RELEASE_NCAS)	CARRIER (POST)
NCASCI (STATUS_NCAS)	CARRUTIL (SETCARR)
PE (LOADFW)	MAPCI (APPLY)
PE (UNEQ)	MAPCI (BSY LINK)
PM (XPE)	CI (EDIT)
PMDEBUG (HELP)	MAPCI (LIST)
PROGDIR (Pollschd)	CI (PHRRCI)
RFWLOAD (QUIT)	CI (POST)
RFWLOAD (upgradefw)	CI (QCUST)
RMACT	CI (QDN)
RTIF (UNEQ)	CI (QDN)
SM (UNEQ)	CI (QDN)
SO (LLCI)	CI (QDNWRK)
SPMDIR (POSTCLS)	CI (QDNWRK)
TAPE (UNEQ)	CI (QDNWRK)
UENDIR (SWLD)	CI (QLEN)
	CI (QLEN)
	CI (QLEN)
	CI (QLENWRK)
	CI (QLENWRK)
	CI (QLENWRK)
	CI (QLT)
	CI (QPHF)
	MAPCI (QUERYPM FLT)
	CI (QUERY)
	MAPCI (REMOVE)
	CI (SOC)
	MAPCI (TRNSL)
—continued—	

Table 1-6 — LEC0012 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
	CM (REXTST)
	CONNECT (PRADCH)
	CONT (PRADCH)
	DLOGDIR (EXCLUDE)
	DLOGDIR (INCLUDE)
	DNINVCI (EXPAND)
	EQUIP (PRADCH)
	ESA (QueryPM)
	KEYCHG (CHANGE)
	LINKDIR (SELECT)
	LINKDIR (STATUS)
	LIUDIR (Loopbk)
	LOOPBK (PRADCH)
	LTP (POST)
	LTP (POST)
	LTPISDN (L3LOGCTL)
	LTPISDN (QLAYER)
	LTPISDN (RLAYER)
	PMUPGDIR (SET)
	PROGDIR (DUMP)
	PROGDIR (POLL)
	PROGDIR (QDN)
	PROGDIR (QDNWRK)
	PROGDIR (QLEN)
	PROGDIR (QLENWRK)
	PROGDIR (SPMECMON)
	PRSM (ASSIGN)
	PRSM (REPORT)
	PRSM (SELECT)
	QCALL (SLRN)
	QRYABN (PRADCH)
	QRYPERF (PRADCH)
	RLDCARR (DISOPT)
	RLDCARR (POST)
	(RSDT)
	RTS (PM)
—continued—	

Table 1-6 — LEC0012 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
	RTS (PRADCH)
	RTS (TTP)
	SE (AINTRACE)
	SE (TSTQUERY)
	SIEZE (TTP)
	SPERFORM
	SPMDIR (LISTALM)
	SPMDIR (LISTRES)
	SPMDIR (QUERYPM)
	SPMDIR (SELECT)
	SPMDIR (SPERFORM)
	SPMDIR (TRNSL)
	SPMDIR (UPGRADE)
	TABAUDIT (AUTO)
	TFAN (QUERYTS)
	TQMISTDIR (MISCHILD)
	(TRACECI)
	CI (TRAVER)
	TST (TTP)
	TTP (POST)
	UENDIR (LOADPM)
	UENDIR (QUERYPM)
	UENDIR (RTS)
	(UNPERMIT)
—end—	

Table 1-7 — LEC0012 Deleted Command Interface Elements

CI name	Feature name
DNINVCI SETPOOL	Table DNINV Expansion
DNINVCI QTOFCNAME	Table DNINV Expansion
DNINVCI QPOOL	Table DNINV Expansion
DNINVCI DISTRIBUTE	Table DNINV Expansion
—end—	

Table 1-8 — LEC0012 New Alarms

Alarm
FWvers
FWSOAK
ISTB
—end—

Table 1-9 — LEC0012 Deleted Alarm Elements

Alarm element name	Feature name
MAJOR	USNBD Miscellaneous Enhancements
—end—	

Table 1-10 — LEC0013 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
CFIBDATA	ACCODE	CALLRDT	AIN	CRT600	AINT700
DNDMSB	AMAOPTS	CTFP	AINICOFF	CTFP600	DFIL802
DPLNSCRN	AMATKOPT	RTESVCS	XACORE	EAD1101	IBN122
EDGERTE	C7LINK	WC		EAD111	PM181
ETANDRTE	CTCODE			EAD112	SPM334
ETERMRTE	CUSTSTN			EAD113	XAC400
FLEXCB	DNROUTE			EAD114	*SPM301 deleted*
ISPTDATA	FACODE			ENET311	*SPM332 deleted*
ISPTMSG	<u>FNPACONT$RTEREF</u>			ISDN404	
ISPTPARM	FTCODE			SPM336	
XAFWLOAD	HOMELRN			SPM337	
XAMDILNK	HUNTGRP			SPM338	
	IBNLINES			SPM339	
	IBNFEAT			SPM510	
	IBNLINES			SPM637	
	IBNRT2			SPM638	
	IBNRT3			TRK921	
	IBNRT4			WHC60	
	IBNRTE			WHC60	
	IBNSC			XAC309	
	IBNXLA			XAC330	
	KSETFEAT			XAC333	
	KSETLINE			XAC335	
	LCCOPT			XAC609	
	LENFEAT			XAC628	
	LIDINFO			XAC630	
	LIUINV			XAC631	
	LNPOPTS			XAC632	
	LTDEF			XAC633	
	LTMAP			XAC634	
	MNHSCARR			XAC635	
	MNNODE				
	NPDIGMAP				

—continued—

Table 1-10 — LEC0013 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	NSCCODE				
	OFCCODE				
	OFRT				
	OFRT2				
	OFRT3				
	OFRT4				
	OKPARMS				
	OPTOPT				
	PVCINFO				
	PXCODE				
	RESOFC				
	SCAICOMS				
	SCAISSRV				
	SERVINFO				
	SPAPAPPL				
	SPAPINV				
	SPINFO				
	STDPRTCT:STDPRT				
	SVRCKT				
	SYNCLK				
	TMTCNTL				
	TOFCNAME				
	TRIGGRP				
	TRKAIN				
	TRKGRP				
	TRKOPTS				
	TRKSGRP				
	VIRTGRPS				
	XACINV				
—end—					

Table 1-11 — LEC0013 New and Changed Office Parameters

New Office Parameters	Changed Office Parameters
AIN_SWITCH_ID	*AIN00_PODP_ANI_CN_OUTPULSING deleted*
CAMAT901	
CONNECTION_HOLD_TIMER_IN_MINS	
CRT_BILLING	
CSMI_DELETE_STUB_MESSAGE	
CTFP_INFO	
DELAY_FSPAIS_ALARMS	
EADAS_DC_INTERFACE	
EADAS_NM_INTERFACE	
INAP_INTERNAL_SRF_IDGT_TIMERS	
WHOS_CALLING_ENABLED	
XA_COMPONENT_INSTALL_STATE	
—end—	

Table 1-12 — LEC0013 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
(UAR)	(ACBAR)
AMDI (ALARM)	(MMINFO)
AMDI (BSY)	(QDN)
aMDI (Indicat)	(QLEN)
AMDI (Query)	(QLT)
AMDI (QUIT)	(TRAVER)
AMDI (RTS)	AINTRACE (HELP)
AMDI (TST)	AINTRACE (REMOVE)
CEM (PURGE)	AINTRACE (SELECT)
CMIC (loadFW)	AINTRACE (STATUS)
dEBUG (DISPLAY PS PAGE)	CARRIER
IOP (loadFW)	CEM (BSY)
MDNMON (MDNMON)	CEM (OFFL)
PE (loadFW)	CEM (RTS)
PE (Uneq)	CI (OBJMGRCI)
PROGdir (AN)	CI (PHRRCI)
PROGdlr (QRDN)	CI (PVCOBJCI)
SM (Uneq)	CI (QCUST)
XAC (AMDI)	CI (QDN)
	CI (QDNWRK)
	CI (QIT)
	CI (QLEN)
	CI (QLENWRK)
	CI (QLT)
	CI (QPHF)
	CI (XPSCI)
	CLOCK
	dEBUG (DISPLAY)
	dEBUG (DISPLAY PS)
	dEBUG (PRINT)
	LTP (BSY)
	PM
	PROGdlr (QDN)
	PROGdir (QDNSU)
	PROGdlr (QLEN)

—continued—

Table 1-12 — LEC0013 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
	PROGdlr (QPDN)
	SOC (ASSIGN)
—end—	

Table 1-13 — LEC0013 Deleted Command Interface Elements

CI name	Feature name
None in this release	
—end—	

Table 1-14 — LEC0013 New Alarms

Alarm
FWsoak
FWvers
—end—

Table 1-15 — LEC0013 Changed Alarms

Alarm
AMDI
FSPAIS
LINK
PE
SPM DS512
—end—

Table 1-16 — LEC0014 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
BRANDING	C7NETSSN	ATMCONN	AINOGSUB	ALT112	CCS260
FLEXRES	CARRMTC	ATMDEV	FCNF	ALT113	IOD206
FLXCMAP	CFW	BRANDING	XACORE	DRM602	TCCI100
XAMDILNK	CUSTSTN	ECANRMAN	XACSRVC	DRM603	UNB300
	E911OFC		XLIUL3	PM420	
	FNPACONT			SPM350	
	HNPACONT			TRK921	
	IBNRTx			TUPL608	
	IBNXLA			XAC309	
	KSETLINE			XAC329	
	LCMINV			XAC335	
	LIDINFO			XAC609	
	LINEATTR			XAC629	
	LTCINV				
	LTCPSINV				
	LTMAP				
	MNCKTPAK				
	MNNODE				
	MTD				
	OFRx				
	OVRx				
	PVCINFO				
	R2PROT				
	RATEAREA				
	RCFCLI				
	SCAICOMS				
	SCAIPROF				
	SLLNKDEV				
	TRKOPTS				
	XACINV				
	XLAPLAN				
	xRTE				
	xxRTE				

—continued—

Table 1-16 — LEC0014 New & Changed Tables, OM Groups, and Logs

New Tables	Changed Tables	New OM Groups	Changed OM Groups	New Logs	Changed Logs
	DELAYOP deleted				
—end—					

Table 1-17 — LEC0014 New and Changed Office Parameters

New Office Parameters	Changed Office Parameters
ALIT_LOG_GEN_FREQ	SO_ALLOW_REDUNDANT_FEATURE
CHNG_NUM_OF_TGS_FOR_PKT_18_22	SO_ALLOW_REDUNDANT_FEATURE_CHF
CONNECTION_HOLD_TIMER_IN_MINS	*TQMS_MIS_MPC_BUFFS deleted*
DAL_PXFX_ON_SAME_SPM	
MSGPSOC_OM_CONTROL	
SPM_MAX_MSGTRK_CARRIER	
SPM_MAX_PRITRK_CARRIER	
—end—	

Table 1-18 — LEC0014 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
AMDI (Alarm_)	(SPMRESMAN)
AMDI (Bsy_)	AINMQG (AINMQG)
AMDI (Indicat_)	AINTracedir (AINTrace)
AMDI (Query_)	AINTraceDIR (HELP)
AMDI (Quit)	AINTraceDIR (REMOVE)
AMDI (RTS_)	AINTraceDIR (SELECT)
AMDI (Tst_)	AINTraceDIR (STATUS)
(FLEXTAB)	CARrUTIL (SPM_MAX_MSGTRK_CARRIER)
DMSMON (IBNEXPCT)	CARrUTIL (SPM_MAX_PRITRK_CARRIER)
USNBD (UNB_OFCWIDE)	CI (OBJMGRCI)
	CI (OBJMGRCI)
	CI (OMSHOW)
	CI (PHRRCI)
—continued—	

Table 1-18 — LEC0014 New and Changed User Interface Commands

New User Interface Commands	Changed User Interface Commands
	CI (PHRRCI - MOVE)
	CI (PVCOBJCI)
	CI (QBB)
	CI (Qcounts)
	CI (QDN)
	CI (QLT)
	CI (QPHF)
	CI (QPHF)
	CI (QSCONN)
	CI (XPSCI)
	CI (XPSCI)
	COMPRSCI (QUIT)
	dPTMEM (cIC)
	LTPISDN (Termchk)
	SYSDIR (MOUNT)
	TRAVER (TRAVER)
	TstQuery (SETMSG)
	TstQuery (TstQuery)
	UPGRADE (BulkAbtk)
	UPGRADE (BulkLoad)
	UPGRADE (BulkSwact)
	USNBD (SURV)
	USNBD (SURV ADD)
	USNBD (SURV LIST)
	USNBD (SURV LIST)
	USNBD (cCR ADD)
	USNBD (CCR ASSOC)
	XRSECHG (cmd)
—end—	

Table 1-19 — LEC0014 Deleted Command Interface Elements

CI name	Feature name
DISPLAY command	TOPS XA-Core Unblocking 4 (OSSAIN)
—end—	

Table 1-20 — LEC0014 New Alarms

Alarm
ETHR
—end—

Table 1-21 — LEC0014 Deleted Alarm Elements

Alarm element name	Feature name
None in this release	
—end—	

THIS PAGE INTENTIONALLY LEFT BLANK

Preventive Maintenance — General

Preventive maintenance on the DMS-100F switch consists of activities such as: performing routine tasks, manual and automated testing, analyzing OMs, logs, service related reports, and observation of central office equipment. The purpose of preventive maintenance is to prevent and find problems before they become service affecting. This can be labor intensive.

Many preventive maintenance routine tests can be performed by automated features built into the DMS-100F switch. It is the responsibility of the maintenance personnel to activate and routinely use the automated maintenance features in a proactive manner.

Even with today's technology, there are still many manual routine tasks that have to be performed. Even the simplest routine tasks, such as inspecting and cleaning or replacing filters, can result in serious problems if they are not scheduled and completed. Some routines, i.e. taking images, can result in more serious service affecting problems if not done properly.

Scheduling and performing preventive maintenance routines are important for meeting the expected performance requirements of the DMS-100F switch. Not performing the necessary manual routine tasks or taking advantage of the automated maintenance testing features in the DMS-100F switch can result in unnecessary corrective maintenance and labor costs. This neglect also causes unnecessary customer service problems and possibly could lead to outage problems.

> **CAUTION:**
> Fix any alarms before starting any routine procedure. An alarm(s) indicates either service is degraded, or it may become degraded. If there is an alarm, fix the problem causing the alarm first, then complete the routine procedure.

The next subsection, "Routine Tasks," identifies routine tasks for:

— DMS-100F SuperNode Routine Tasks

— XA-Core Routine Tasks

— Proactive Routine Tasks

— Routine Tasks for the RLCM and OPM

— Star Remote system routine maintenance

— Power Plant Routine Tasks

Product specific DMS-100F routine maintenance tasks are described in the supporting documentation for that particular product (e.g., RSC, SMA, AIN, SRU, E911, DMS-300 Gateway). For PCL documents, NTP 297-YYYY-546 provides a list of routine tasks for the specific product layer (YYYY). See the *Office Administration* tab and the "Nortel Networks Documentation" subsection within this manual for a list of product layers.

For a list of Nortel Networks Technical Publications (NTPs) that provide routine task procedures for PCL loads, refer to NTP 297-8991-001, *DMS Product Documentation Directory.* It will serve as an index to the NTP 297-YYYY-546 routine maintenance documents.

This section of the MOM contains instructions and references for setting up and operating resident type test tools such as: automatic trunk testing (ATT), automatic line testing (ALT), killer trunk (KT), focussed maintenance, OM thresholding, network maintenance tools, and carrier maintenance.

Routine activity associated with non-DMS equipment should be accomplished using the manufacturer's maintenance manuals unique to that equipment.

Routine Tasks

DMS-100F switch routine tasks

This subsection contains tables that provide a list of routine tasks, their recommended scheduled time interval, and references to NTPs that contain the task procedure. Also included are exhibits of several routine tasks with procedures.

> **CAUTION:**
> The tables of routine tasks in this subsection represent a MOM recommended minimum requirement and are not an all-inclusive list of routine tasks. For some tasks, the "MOM" recommended time interval has been extended or shortened from what is recommended in the NTP.

NTPs or the manufacturer's manual should be used when performing actual routines since they are more frequently updated and would provide any new procedures and current procedural changes that might take place for the detailed task.

For a list of Nortel Networks Technical Publications (NTPs) that provide routine task procedures for PCL loads, refer to NTP 297-8991-001, *DMS Product Documentation Directory*. It will serve as an index to the NTP 297-YYYY-546 routine maintenance documents.

Other routine maintenance activities that are listed within NTP 297-YYYY-546 publications and other manufacture manuals can be scheduled—as required—to meet your operating company requirements and specific site needs. Many routines listed within NTP 297-YYYY-546 are "as needed" routine procedures and can be scheduled as a regular routine if needed. It is understood that the routine intervals recommended by Nortel Networks are subject to modification by the customer to comply with local procedures and maintenance policies.

NT40 routine tasks are no longer listed in the MOM. If there is a need for NT40 routine procedures, reference your supporting NTPs or see the earlier 1995 MOM for the last issue containing a list of NT40 routine tasks.

DMS-100F SuperNode routine tasks

Table 2-1 contains a combined list of routine tasks for SuperNode DMS-100 Family of switches and includes: the SuperNode SE; SuperNode SE SP/SSP; SuperNode STP; SuperNode STP/SSP Integrated Node; SuperNode SP/SSP; and SuperNode SCP II.

Table 2-1 — DMS-100F SuperNode Routine Tasks

Task	Interval	PCL Procedure Location YYYY = PCL Layer
Replacement of horizontal cooling filter CPC A0351174	3 months or use NTP interval	NTP 297-YYYY-546 Routine Maint.
Replacement of horizontal cooling filter CPC A0377837	3 months or use NTP interval	NTP 297-YYYY-546 Routine Maint.
Replacement of vertical cooling filters CPC A0352802 & A0352805	3 months or use NTP interval	NTP 297-YYYY-546 Routine Maint.
Replacing a cooling unit filter in a 1.07-m (42-in) cabinet (see above filters for this cabinet)	3 months or use NTP interval	NTP 297-YYYY-546 Routine Maint.
Inspect and replacement of A0346842 cooling filter within CRSC/LCM, CRSC/ISDN, GPP, and CEXT frames	3 months or use NTP interval for inspecting and replacement	NTP 297-YYYY-546 Routine Maint.
Replacing a cooling unit filter in a 0.71-m (28-in) cabinet	3 months or use NTP interval	NTP 297-YYYY-546 Routine Maint.
Inspecting, cleaning, and replacement of cooling filters CPC A0344437, P0558302, P0623539 within RSC, SMS, SMU, RSC-SONET A, SMS-R, and OPM frames	3 months or use NTP interval	NTP 297-8221-550 RSC Maint. NTP 297-8231-550 SMS Maint. NTP 297-8241-550 SMU Maint. NTP 297-8261-550 RSC-SONET-A NTP 297-8301-550 SMS-R Maint. NTP 297-8361-550 OPM Maint.
Cleaning the tape drive heads on the SLM	monthly	NTP 297-YYYY-546 Routine Maint.
Scheduling and storing daily, weekly, and monthly office image backups	use NTP procedures according to your company policy	NTP 297-YYYY-546 Routine Maint.
Testing wrist strap grounding cords	3 months	NTP 297-YYYY-546 Routine Maint.
Testing wrist strap grounding cords for SCM-100	3 months	NTP 297-8251-550 Maint. Manual
Replacing cooling unit filters A0346842 in CRSC/LCM, CRSC/ISDN, and CEXT cabinets	3 months	NTP 297-YYYY-546 Routine Maint.
Replacing cooling unit filter for SCM-100	3 months	NTP 297-8251-550 Maint. Manual
Air filter NTLX5015 removal and replacement procedure (SPM)	3 months	NTP 297-8001-546 Routine Maint.
Testing of the dead system alarm	yearly	NTP 297-YYYY-546 Routine Maint.
Testing of the dead system alarm for SCM-100	yearly	NTP 297-YYYY-546 Routine Maint.
Cleaning the magnetic tape drive (MTD)	6 months	NTP 297-YYYY-546 Routine Maint.
—continued—		

Table 2-1 — DMS-100F SuperNode Routine Tasks (continued)		
Task	**Interval**	**PCL Procedure Location** **YYYY = PCL Layer**
Scheduling magnetic tape drive maintenance	3 months	NTP 297-YYYY-546 Routine Maint.
Cleaning the optical sensors on the 14" disk drive unit (DDU)	6 months	NTP 297-YYYY-546 Routine Maint.
Recording an ENET image on an SLM disk	monthly or after each ENET software upgrade or patch application.	NTP 297-YYYY-546 Routine Maint.
Recording an EIU/FRIU/XLIU/APU/VPU image on an SLM disk	monthly or after software upgrade or patch application.	NTP 297-YYYY-546 Routine Maint.
Recording an NIU image on an SLM disk	monthly or after software upgrade or patch application.	NTP 297-YYYY-546 Routine Maint.
Backing up an 800Plus database to a digital audio tape (DAT)	daily	NTP 297-YYYY-546 Routine Maint.
Backing up an FP image file on SLM disk to SLM tape	per your company policy	NTP 297-YYYY-546 Routine Maint.
Cleaning digital audio tape (DAT) heads	when the green LED on the DAT driver flashes or after every 8 hrs.	NTP 297-YYYY-546 Routine Maint.
Cleaning SLM tape drive heads in a DMS SuperNode SE	after first pass of new tape cartridge and after each 8 hours of tape drive use	NTP 297-YYYY-546 Routine Maint.
Cleaning digital audio tape (DAT) drive NTFX32CA in an IOM	see NTP table recommendation	NTP 297-YYYY-546 Routine Maint.
Performing a frame-relay interface unit (FRIU) loopback test	per your company policy or carrier troubleshooting	NTP 297-YYYY-546 Routine Maint.
Replacement of magnetic tapes using DIRP	per your company policy	NTP 297-YYYY-546 Routine Maint.
Deallocating recording volumes using DIRP	per your company policy	NTP 297-YYYY-546 Routine Maint.
Verifying and adjusting the time of day clock	daily	NTP 297-YYYY-546 Routine Maint.
Expanding disk recording file space using DIRP	as needed	NTP 297-YYYY-546 Routine Maint.
—continued—		

Table 2-1 — DMS-100F SuperNode Routine Tasks (continued)		
Task	**Interval**	**PCL Procedure Location** **YYYY = PCL Layer**
Testing power converter voltages	every 6 months	NTP 297-YYYY-546 Routine Maint.
Performing a manual file rotation using DIRP	per your company policy	NTP 297-YYYY-546 Routine Maint.
Preventing dust accumulation in a 42" cabinet	every 6 weeks	NTP 297-YYYY-546 Routine Maint.
Recording a EIU/FRIU/XLIU image on a SLM disk	after each EIU/FRIU/XLIU software upgrade or patch	NTP 297-YYYY-546 Routine Maint.
Recording an FP image on a SLM disk	after each FP software upgrade or patch	NTP 297-YYYY-546 Routine Maint.
Recording a NUI image on a SLM disk	after each NUI software upgrade or patch	NTP 297-YYYY-546 Routine Maint.
Reformatting an IOC- or IOM-based disk drive unit	see NTP	NTP 297-YYYY-546 Routine Maint.
Reformatting a SLM-based disk drive unit	see NTP	NTP 297-YYYY-546 Routine Maint.
Testing F-bus taps on an LPP	daily	NTP 297-YYYY-546 Routine Maint.
Testing F-bus taps on an MS	daily	NTP 297-YYYY-546 Routine Maint.

Routine maintenance schedule for XA-Core

Use Table 2-2 to help you prepare a routine maintenance schedule for your office.

The following procedures are for a DMS SuperNode or SuperNode SE switch that has the eXtended Architecture Core (XA-Core).

The tasks are defined in the "Routine procedures" chapter of *XA-Core Maintenance Manual*, 297-8991-510.

Table 2-2 — XA-Core Routine Tasks

Task	Interval
Backup an XA-Core office image from disk to tape	each week or per office schedule
Change XA-Core REx intensity	when required
Check and adjust the TOD clock of XA-Core	daily
Clean the XA-Core tape drive	after eight hours of operation
Copy all files of an XA-Core disk volume to tape	when required
Create a test volume on XA-Core disks	after installation of new disk in disk drive packlet
Create volumes on XA-Core disks	after installation of new or old disk in disk drive packlet
Perform LED maintenance in XA-Core	every 30 days (monthly)
Record an XA-Core office image on a disk	every day or when required
Replace XA-Core cooling unit filters	every six weeks
Restore an XA-Core office image from tape to disk	when required
Return an XA-Core card, packlet, or assembly to Nortel Networks	when required
Schedule automatic image taking for XA-Core	per office manager
Schedule tape drive maintenance in XA-Core	every 180 days (six months)
Test wrist-strap grounding cords for XA-Core	every 30 days (monthly)

Proactive routine tasks

Table 2-3 provides a list of proactive routine tasks recommended by Nortel Networks and operating companies. Use the list of recommended routines as a general guide for your operating company maintenance strategy needs.

Table 2-3 — Proactive Routine Tasks

Task	Interval	Procedure Location
Use and review Focussed Maintenance for Lines & Trunks and ALT and ATT log reports. Run NetFab, NETINTEG, and IBERT tests.	daily	NTP 297-1001-595 Trunks Maint. NTP 297-1001-594 Lines Maint. NTP 297-1001-591 Network Maint. See subsections within this manual
Review scheduled Maintenance Managers Morning Report, SPMS Reports, and supporting OMs	daily	NTP 297-1001-330 SPMS NTP 297-1001-318 Analysis Guide NTP 297-YYYY-814 OMs See Exhibit B within this subsection
—continued—		

Table 2-3 — Proactive Routine Tasks (continued)		
Task	**Interval**	**Procedure Location**
Setting up and running loopback tests	3 months or as needed	NTP 297-YYYY-546 Routine Maint.
Setting up, scheduling, and verifying REX tests	daily	See Routine Exercise (REX) tests later in this subsection
Testing system grounding	yearly	NTP 297-1001-350 Power Routines NTP 297-1001-156 Ground'n Guide NTP 297-1001-158 Grounding Audit Procedures. See Exhibit D within this subsection
Inspect and refill fuses, test alarm panel (ACD) lamps, and file documentation	6 months	NTP 297-1001-122 Alarm System See Exhibit A within this subsection
Inspect and replace burned out bulbs in the aisle-ends and in the frame supervisory panels	3 months	NTP 279-1001-122 Alarm System
Purge unnecessary SFDEV files using LISTSF and ERASESF commands	monthly	NTP 297-1001-360 Basic Xlations NTP 297-1001-822 Commands Manual
Review Emergency Recovery Warnings and Bulletins	weekly	C-SCAN

RLCM and OPM routine tasks

A combined list of routine tasks for the RLCM and OPM is provided in Table 2-4 on page 2-9.

The remote line concentrating module (RLCM) consists of standard line concentrating module (LCM) components equipped for remote functions.

The outside plant module (OPM) is an RLCM contained in a special weatherproof enclosure, along with a power supply and environmental control equipment. All RLCM features are available with the OPM, including intraswitching and ESA.

The LCM and remote maintenance module (RMM) are maintained in the RLCM and OPM using the LCM, PM, and OPMPES MAP levels. The maintenance and user interface commands are the same for the RLCM and the OPM, with the addition of the Power Environment System (PES). OPM maintenance that includes PES is referred to as OPMPES.

For further information on the RLCM and OPM, including the routine maintenance procedures for the RLCM/OPM routine tasks listed in Table 2-4, see NTP 297-8351-550, *DMS-100F RLCM Maintenance Manual* and NTP 297-8361-550, *DMS-100F OPM Maintenance Manual.*

Table 2-4 — Routine Tasks for the RLCM and OPM

Task	Interval
OPM Battery capacity tests for Yuasa (A037761) or Eagle-Picher (A0386201) batteries in an office equipped with an LTU or MTU	every 6 months when LTU or MTU are within specifications or every 3 months if the LTU or MTU are not within specifications
Battery charging	see important note below
Battery, electrical inspection for OPMs	local policy
Battery, physical inspection for OPMs	every 6 months
Battery replacement for OPMs	installation, maintenance, or adding batteries
Temperature dampers testing for OPMs	local policy
Door alarm testing for OPMs	local policy or each visit to cabinet
Dust removal for OPMs	local policy
Discharge test failure (once a month audit— see PES117 log)	after every discharge test failure
Open-circuit test failure for OPMs (see PES117 log)	after every open-circuit test failure
Failure of post charge test for OPMs (see PES117)	after every post charge test failure
Fan alarms testing for OPMs	local policy or each visit to cabinet
Inspecting, cleaning, and replacement of cooling filters CPC A0344437, P0558302, P0623539 within OPM frames	3 months or use NTP 297-8361-550 interval
Filter replacements for RLCMs	3 months or local policy
Inspecting spare fuse holders for RLCMs	every week
Heaters testing for OPMs	local policy
High temperature alarms testing for OPMs	local policy
Low temperature alarms testing for OPMs	local policy
Rectifier replacement for NT8X01AA, AB, BA, BB for OPMs	as required
Rectifier replacement for NT8X01AC, BC for OPMs	as required
Rectifier voltage adjustment for OPMs with an LTU	3 months
Rectifier voltage check for OPMs	every 3 months
Site tests for battery strings that have failed automatic tests	as needed
Testing wrist strap grounding cords for RLCMs	every 3 months

NOTE: Due to the various types of batteries and the possibility of damage with over charging, it is important to first reference parameters OPM_CHARGE_DURATION and OPM_CHARGE_START_TIME in table OFCSTD. See NTP 297-YYYY-855, *Office Parameters Reference Manual*.

Star Remote system routine maintenance schedule

For a summary of the preventive maintenance tasks for the STAR Remote see Table 2-5, " — Star Remote system routine maintenance." For procedure information see NTP 297-8353-550, *DMS-100 Family Star Remote System Maintenance Manual.*

Table 2-5 — Star Remote system routine maintenance	
Task	**Interval**
Battery inspection and cleaning Star Module	6 months
Battery replacement Star Module	perform this procedure when doing the following: • installing the SRME or SRMO • replacing batteries for maintenance • temporarily removing batteries for cleaning
Fan cleaning and testing SRMO	local policy
Fan replacement SRMO	local policy
GFCI check SRMO	perform this procedure before using the outlet supplied with GFCI in the SRMO cabinet
Heater element replacement SRMO	local policy
Heaters test SRMO	annual
High temperature alarm test SRMO	local policy
Inspecting spare fuse holders STAR	weekly
Low temperature alarm test SRMO	annual
Testing ac/dc rectifier voltages RLD	6 months
Testing power converter voltages STAR	6 months
Testing wrist strap grounding cords STAR	monthly

Power plant routine tasks

Table 2-6 lists power plant routine tasks. All the power and grounding routine tasks can be found in NTP 297-1001-350, *DMS-100F Power and Grounding Routine Procedures* or in NTP 297-1001-158, *DMS-100F Grounding Audit Procedures*. For addi-

tional information related to power and grounding reviews, see "Power and Grounding Evaluation" on page 2-12.

The battery and power plant maintenance information described in NTP 297-1001-350 is generic by necessity, since it references numerous different types of power plants in the field. Evaluate the existing power plant routine maintenance work items against this generic model. Identify any new procedures and consider incorporating them into your power routine schedule. Samples of logs and control records are in the NTP.

Table 2-6 — Power Plant Routine Tasks	
Task	**Interval**
Engine alternator starting system check	1 month
Engine alternator engine run	2 months
Charging plant inspection and test	6 months
Standby power operational test (portable)	1 year
Standby power operational test (stationary)	1 month (2 hr. run) and 1 year (7 hr. run)
Battery plant load test	1 year
Miscellaneous power system checks	1 year
AC surge protectors	1 year (by utility co.)
Pilot cell and emergency cell voltage reading	1 week or with each visit
Individual cell voltage readings	3 months
Battery float voltage reading	1 week or with each visit
Emergency cell specific gravity readings	1 week or with each visit
Pilot cell specific gravity readings	every 6 weeks
Individual cell specific gravity readings	6 months
Clean and inspect batteries	3 months
Average battery float voltage under varying voltage and load conditions, and calibration of power panel volt meter	1 year
Electrolyte level	as required
Water analysis	1 year
Gel cell battery inspection	daily
Cleaning gel cell batteries	1 week
Gel cell battery voltage and charge condition	1 month
Battery connector bolt retorquing	1 year
Voltmeter check	1 year

Power and Grounding Evaluation

NTP 297-1001-350, *DMS-100F Power and Grounding Routine Maintenance Practice* is a comprehensive practice describing battery and power plant maintenance activity. In addition, it provides evaluation procedures and related check lists for power plants and standby power installations and a grounding audit procedure.

These are optional evaluations to be scheduled at the discretion of the operating company. Because of the potential impact on service, the following recommended intervals for the evaluation are being presented for operating company consideration.

Power plant assistance review

The power plant review, described in NTP 297-1001-350, consists of checks and observations that ensure that battery plants, power plants, and standby engine-alternators are meeting performance standards and are at expected levels of reliability. The assistance review also verifies that office power plant records are kept and maintenance routines are completed.

The frequency of power plant reviews is normally based on operating company policy; however, a minimum of one review per year is strongly recommended.

To increase the effectiveness of the power plant review, it is recommended that the review be conducted by management personnel not normally responsible for the power equipment.

Operation standby

Operation standby, described in NTP 297-1001-350, is a simulated failure of the commercial AC power source to verify that all standby power equipment functions normally and that continuity of service is maintained. The exercise is under control of local supervision.

Operation standby provides an opportunity for network maintenance and buildings personnel to:

- increase their familiarity with power plant capabilities and operation
- observe the interaction of the power plant subsystems under controlled conditions
- identify and correct unsatisfactory conditions
- test the coordination and allocation of mobile engine-alternators

Perform operation standby at least annually, preferably following a recently completed power plant review. Several sample forms are provided for use in recording the results of the operation standby. These are suggested forms.

Grounding audit

The "Grounding audit procedures" chapter in NTP 297-1001-158, *DMS-100F Grounding Audit Procedures* provides a grounding audit procedure. Use of this proce-

dure can aid knowledgeable managers in assuring that DMS-100F switches have been engineered, installed, and maintained according to the basic grounding principles developed for DMS-100F switching systems. To facilitate the auditing, an elaborate check list has been developed listing the items to be checked and space for the noted results.

Grounding audit frequency

The frequency of performing the grounding audit procedure is governed by individual office conditions. Review of the grounding audit procedure, either in whole or in part, is recommended under the following circumstances:

- in preparation of the building space for the installation of a DMS-100F switch

- to assess the quality of installation of a newly installed DMS-100F switch

- to ensure no grounding violations have taken place as a result of equipment rearrangements or additions

- whenever service degradation is observed or suspected as a result of nearby lightning strikes

Routine Exercise (REX) tests

The DMS is equipped with resident diagnostic routine tests, called Routine EXercise (REX) tests. REX tests can be initiated either by the system scheduler on a regular basis, or manually through the MAP by posting the XPM and using the TST REX NOW command. SuperNode DMS supports concurrent REX for up to 10 XPMs with the same REX test class (LGC, RCC, SMSR, MSB). For references to documentation describing REX testing, see NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide*.

REX test results should be reviewed daily and, if faults are detected, necessary corrective action initiated. Some types of routine diagnostic tests run are:

- all spare memory cards and routine exercise test (REX)
- CM/MS routine exercise (REX) – DMS SuperNode (see Note 1)
- Data Store (standby spare memory cards)
- Image tests
- System audits
- XPM REX tests (see Note 2)
- LCM REX tests

NOTES:

1. Be aware that the CM maintenance alarms are suppressed—except for ClkFlt, CM Flt, CMTrap, IMAGE, LowMem, and NoTOD—during the CM REX. Any alarms that are present at the completion are reissued for attention at the end of the CM REX test.

2. Verify that these tests are turned on in their respective office tables (see next page). Contact your local technical support representative if changes are required for any of these table entries.

LCM REX test flow

A REX test for an LCM includes the following steps:

1. If both units of the LCM are in service, unit 0 is made SysB. A PM128 state change log is generated with the following reason: REX in progress. The LCM node status is made ISTb, and a minor alarm is generated.

2. InSv diagnostics are run on unit 1 in takeover. If any diagnostics fail, the unit is placed ISTb and a PM181 log is generated.

3. Unit 0 is returned to service. OOS and InSv diagnostics are run. If OOS diagnostics fail, the unit is left SysB, a major alarm is raised, and PM106 is generated. If the unit is returned to service successfully and the InSv diagnostic fails, the unit is placed ISTb and a PM181 log is generated.

4. If unit 0 is returned to service successfully, these steps are repeated for unit 1.

In NA004 the "LCM REX Controller Enhancement" feature was added to move LCM REX testing under control of the system REX (SREX) controller—to eliminate conflict between simultaneous REX testing. With this feature, LCM REX testing will no longer be controlled from the table OFCVAR and the LCDREX_CONTROL office paramenter, but from the NODEREXCONTROL office parameter. After posting an LCM at the PM level, technicians can now perform a COVREX (ring continuity and converter voltage tests) by using the TST COVREX command. Also, the QueryPM command has been updated to display information about the LCM node. For more information on this feature, search for LCM REX Controller Enhancement in NTP 297-YYYY-350, *Translations Guide*.

REX records

The QUERYPM, QUERYPM FLT, TST REX QUERY, and TST REXCOV QUERY commands contain information about the last REX test.

A REX maintenance record is stored for each XPM in a office. This record is accessible after posting the XPM and then using the TST REX QUERY command. Also, the QUERYPM command used after posting an XPM contains a subset of the REX maintenance record. This record does not survive PCL load applications.

A CI level REXTEST command can be used to get information about REX tests on various nodes. The first parameter has four options: SUSPEND, RESUME, QUERY, and HELP. The second parameter is the type/class of REX test. Two new type/class parameters were added in NA004 for LCM REX, they are LCM_REX_TEST and LCMCOV_REX_TEST.

PM131 logs are generated for each state change which occurs as a result of the REX test. PM181 logs are generated to report other events which occur in the XPM, including the successful completion (PASSED) or unsuccessful completion (FAILED) of the test. In the case that the REX test failed, the PM181 log indicates the REX failure reason.

The network assessment graph (NAG) NAG400 log report —controlled by the CI level NAG command—provides REX results and a list of nodes not in-service. The LCM_REX anc LCMCOV_REX_TEST results are separated by a colon. LCMCOV REX tests are performed on LCMs, XLCMs, OPMs, and RLCMs.

Log IOAU112 is output when an RLCM has not been REX'd for seven days. The log now includes the LCM REX and LCMCOV REX test classes.

PM600 log is output if REX fails and includes each step that REX executed, the unit the step impacts, the start time of each step, and the failure reason if the step failed. The log now includes the name of the LCM REX test (LCMCOV REX or LCM REX). The PM600 log is not output if a restart occurs while REX is in progress. The PM600 log provides REX data collection within one log and allows for suppression of existing logs produced during REX that do not report an event requiring craft action. Following is an example of a PM600 log report:

```
  ** PM600 JAN08 01:08 8600 TBL REX FAILED XPM 0

Node:ISTb, Unit 0 Act:InSv, Unit 1 Inact:SysB (Diag Failed)

REX Step     Unit    Start Time   Failure Reason
Tst Inact     0       09:17:33
Bsy Inact     0       09:17:47
RTS Inact     0       09:18:15
Sync Inact    0       09:21:43
Pre-SwAct     0       09:21:51
Warm SwAct    -       09:22:37
Bsy Inact     1       09:22:40
RTS Inact     1       09:23:08
Sync Inact    1       09:25:27
Tst Act       0       09:22:50   REX test failed-InSv tests of active
                                               Unit 0 after Swact
Warm SwAct    -       09:25:28
Bsy Inact     0       09:25:29
Finished      -       01:28:25
Supplemental Data
Diagnostic Failures: UTRDIAG
Site Flr RPos Bay_id Shf Description Slot EqPEC
HOST 01   L15 LTE 00 65  LTC : 000     15   6X92
```

Table REXSCHED

Table Routine Exercise Schedule (REXSCHED) contains the information required to schedule series-3 peripheral modules (PMs), applications, and File Processors (FPs). This table allows operating companies the flexibility to schedule different REX tests depending on the specific characteristics of the switch.

> **CAUTION:**
> Beware of conflicts involving scheduling between the table REX-SCHED, table REXINTEN, and with other activities.

Table REXINTEN

The Routine Exercise Intensity (REXINTEN) table allows portions of message switch (MS) and Link Interface Module (LIM) system REX tests in SuperNodes and SuperNode SE switches to be bypassed on selected days of the week.

Parameter NODEREXCONTROL

This parameter, in table OFCVAR, provides for complete node testing (includes CM, MS, XPMs, LCMs, and ENET etc.) on the DMS SuperNode. For LMs and RLMs, use table LMINV and the REX tuple to control REX testing. Use the PM MAP level to enable the XPMs and to set the XPMs to warm swact. The following is an approximate time for REX testing with various XPMs:

FRAME TYPE	TIME IN MINUTES
LTC, DTC,	10 min (according to lab tests)
LGC, ILTC, IDTC	12 min (according to lab tests)
MSB6	less than 12 min (estimate)
PDTC, ADTC	less than 15 minutes (estimate)

Parameter REMTERMEQP

This SuperNode parameter—REMTERMEQP—found in table OFCENG, should be set to "Y" so that the CM REX test verifies that a terminal is connected to the CM Remote Terminal Interface (RTIF) remote channel.

Exhibit A
General – Alarm Control and Display Panel (ACD) - Lamp Check

Frequency:	Weekly
Equipment Required:	None
Material Required:	Bulbs #387 (if replacements required)
Reference Material:	NTP 297-1001-122, *Alarm System Description*

NOTE: ACDLPTST is the SC scan point

Procedure:

Momentarily depress lamp test switch. All lamps should light momentarily. If not, replace defective lamps.

Exhibit B
General – Review Operational Measurement Reports

Frequency:	Daily
Equipment Required:	Current weekly or daily operational measurement reports or daily SPMS reports
Reference Material:	NTP 297-YYYY-814, Operational Measurements Reference Manual
	See the following "operational Measurements" subsection

NOTE: System OM reports, or SPMS reports, should be reviewed daily and used with system logs to isolate faulty procedures or equipment.

OMs to monitor:

The following OM groups should be monitored regularly as they represent the general purpose tools for prediction and analysis of service problems:

- ATTAMA
- PM
- PMTYPE
- TRMTCM
- TRMTER
- TRMTFR
- TRMTRS

The Treatment (TRM) OMs determine why a call received a particular treatment as a result of call blockage or failure. For example, OM group TRMTRS_TRSNBLH measures the number of call attempts that are blocked in the networks and sent to tone or an announcement.

The measurements PM and PMTYPE indicate equipment failures that may affect grade of service and load service curve impact.

It is suggested you review the "Operational Measurements" subsection within this tab and NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide* for an overview of various OM reports.

Exhibit C
General – Testing Wrist Strap Ground Cord

Frequency: Six months

Equipment Required: Ohmmeter

Material Required: Wrist strap and ground cord

NOTE: Recommend equipping a wrist strap test jig in each office and testing wrist straps before each use.

Reference Material: NTP 297-1001-010, *Electrostatic Discharge Protection*

Procedure: Use this procedure to verify the resistance of wrist strap grounding cords. The resistance must be low enough to allow static electricity to discharge from the human body, but high enough to prevent electrical shock if the equipment develops a short-circuit while the wrist strap is being worn.

1.Detach the grounding cord from the wrist strap and using an ohmmeter, measure the resistance between opposite ends of the grounding cord.

   — If the resistance is between 800K ohms and 1200K ohms, you may use the grounding cord and wrist strap assembly. Reconnect the wrist strap to the grounding cord.

   — If the resistance is not between 800K ohms and 1200K ohms, discard the entire assembly. Do not attempt to use it. Read the following danger and warning notices.

DANGER
Risk of electrocution! Do not use a grounding cord with a resistance less than 800K ohms. A lower resistance exposes you to the risk of electrocution if the equipment short-circuits while you are wearing the wrist strap.

WARNING
Risk of static damage to electronic equipment! Do not use a grounding cord with a resistance greater than 1200K ohms. It is unable to conduct static charges to ground adequately. It will not protect sensitive electronic equipment against buildup of potentially damaging electrostatic discharges.

Exhibit D
General – Testing System Grounding

Frequency: Three months

Equipment Required:

- AC/DC clamp-on ammeter capable of measuring current on a 750 MCM cable (AWS DIGISNAP, Model DSA-2003 or equivalent)
- multimeter (capable of measuring voltage of 100V+ AC/DC and resistance of tenths of an ohm)
- blank cable tags
- screwdriver and torque wrench
- wire brush and nonmetallic bristle brush
- flashlight and note pad (for recording problems)

Material Required:

Use the grounding schematic provided (see next page) and reference documents listed below.

Reference Material:

- NTP 297-1001-350, *DMS-100F Power and Grounding Routine Procedures*
- NTP 297-1001-156, *DMS-100F Power Distribution & Grounding Systems*
- NTP 297-1001-158, *DMS-100F Grounding Audit Procedures*

Procedure:

1. Attach clamp-on ammeter at points shown on grounding schematic.

2. AC or DC current must be 0 at all locations.

3. Report any discrepancies to the switch supervisor

NOTE: Action should be taken by management to clear any discrepancies.

NTP 297-1001-158 Grounding Audit Procedures:

- Site information
- DMS switch equipment
- MAP equipment
- DC power equipment
- AC power equipment
- Building grounding system
- Entrance cables and CEG
- MDF equipment
- Radio/microwave equipment
- DMS TOPS equipment

Figure 2-1 — Grounding Schematic

```
┌─────────────────────────┐
│     DC Power Board       │        From power board framework
│       "Isolated"         │        to rectifier's frame or to AC
│   Battery Return Plate   │        power panel green wire buss
└─────────────────────────┘        supplying power to rectifiers.

  AC or DC current must
  be 0 at this point ▶

┌─────────────────────────┐        From any equipment powered by
│           GW             │        DC isolated power configuration
│  (One per DC Power Source)│        only, such as switch lineup
└─────────────────────────┘        framework FGE, PHG, LRE, and
                                    stand-alone, DSX, other
  AC or DC current must             transmission frames.
  be 0 at this point ▶

┌─────────────────────────┐        Street side water main AC
│   Principal Building     │        building entrance ground any
│        Ground            │        improperly grounded frames.
│  (Master Bldg Gnd Point) │        Other metal frames not isolated.
└─────────────────────────┘

           ⏚
```

NOTES:

1. NEC rules state that none of the grounding conductors are to have any AC or DC current flowing on them except temporary short circuit current and only until the protectors trip open or the system fault is repaired.

2. Cables connected to the GW must have no restrictions such as coils, loops, sharp bends, encircling metal piping or clamps.

Operational Measurements

Introduction

Operational measurements, or more commonly called OMs, are the single most significant information source for performing preventive and corrective maintenance—in addition to identifying provisioning problems. Problem areas—due to such causes as: equipment provisioning, equipment faults, translation errors, network congestion, line, trunk, service circuits, and carrier faults—can be identified when OM data is analyzed in real-time.

Operational measurements (OMs) are common to the total system. Voluminous pegs and usage counts are generated by the DMS software and hardware call related sources and equipment. Over 2500 unique register fields, organized into approximately 225 functional groups, are provided in the DMS system to accumulate OM data (number of groups based upon load type).

This subsection of the MOM will provide the following information concerning OMs:

- OM organization
- OM administration
- OM alarms and logs
- OM commands
- OM tables
- OM parameters
- OM class assignments and reports
- OM thresholding
- OM recommended bogey settings
- OM trouble identifiers

Real-time analysis

Real-time OM analysis for identifying current switch problems requiring corrective action is not a maintenance concept that most operating companies utilize. Historically, OMs have been used to determine switch performance after service impairment.

Real-time analysis should also include other indicators such as: log messages, alarms, customer reports, trunk work order activity, and trunk and line fault indicators from the focused maintenance feature. Record the analysis activity to indicate all-is-well, or the fault indication, including action taken and results, using a simple log form or other local method.

Real-time switch indicators include the analysis of the OM2200 log message and related alarms generated by the OM threshold and ALARMTAB features. If the OM thresholding feature is not provided or is not being used, then analysis of the OMs should be made using a printout of customized OM class reports. Depending upon the time needed to accumulate the data for the OM report, the report may be considered as a *near* real-time report, or possibly a subsequent analysis process as described next.

Once a problem is identified using OM real-time surveillance, standard NTP procedures can be used to perform the required remedial tasks, such as: busy out equipment to remove the fault and related machine or service degradation, selected testing, trouble isolation, substitution, repair, replacement procedures, and return to normal service and configuration.

To minimize the amount of data on OM output reports, consider setting the SUPZERO tuple in table OMPRT to "Y". If all the data in a data line (tuple) is zero, then the data line will be suppressed. This not only saves analysis time, but also saves printer paper.

Subsequent analysis

Subsequent analysis involves the accumulating, scheduling, and printing of key OM indicators for switch, line, trunk, and carrier activity. Daily, weekly, and monthly printouts are required. Subsequent analysis identifies intermittent, constant, or obscure type fault conditions. Some fault conditions may require extensive analysis and depend upon available information and testing to isolate and correct the problems. See "OM organization" next and "OM class assignments & reports" later for a description of this process.

It is suggested that key OM data and related bogeys be posted to a DMS Control Record form. The control record form is used for "visual analysis" and to trend performance indicators. See the *Office Administration* section of this manual for a description and example of the DMS Control Record form.

OM Organization

The OM subsystem organizes the collection of data, manages the OM output reports, and designates the appropriate output device (i.e., printer, tape drive, disc drive, VDU) to meet the various operating and engineering requirements such as:

- Maintenance (switch, trunks, lines, carrier)
- Network management

- Traffic loading
- Service indicators
- Provisioning

Data acquisition

Refer to Figure 2-2 for a schematic of the OM organization. Operational measurements consist of monitoring certain events in the DMS system and entering the results into registers in the DMS data store. The registers are incremented either individually every time an event occurs, or when the state of an item is scanned (sampled) at regular intervals, regardless of the time of occurrence of an event. Scan rates are either 100 seconds or 10 seconds and are identified in the relevant register descriptions.

Single events, measured individually, are referred to as *peg counts*. Sampled measurements (states), used to determine the degree of usage for DMS system hardware and software resources, are called *usage counts*.

Peg and usage counts of OM events are stored in ACTIVE registers, which are updated whenever new data is entered.

Data collection

The OM data in the active registers is useful only if related to the specific time during which it was collected. OM data cannot, therefore, be directly copied from the active groups to an output process (disc, tape, printer, etc.) because counts can occur during the copying process. This can cause the data to be skewed.

To prevent data from skewing it is transferred from active registers to a duplicate set of registers classed as HOLDING registers. Data transfer from active to holding registers occurs at periods controlled by office parameters OMHISTORYON in table OFCOPT and OMXFR in table OFCENG. If parameter OMHISTORYON is set to "Y", then OMXFR is disabled and the transfer period will be 5 minutes. Set to "N", the OMXFR can be set to 15 or 30 minutes.

As previously stated above, the transfer time for OMXFR can be set to either 15 or 30 minutes; however, if the switching unit is equipped with the Engineering Administration Data Acquisition System (EADAS) and option EADAS_SHORT_XFER_ALLOWED in table OFCOPT is set to "N", then the transfer time must be set to X30 (default value).

Copying to output processes is performed from the holding registers with a controlled period on which to base subsequent data manipulation. The holding registers isolate the output processes from the active OM data inputs, lessening the urgency and priority of the copying process. The contents of the holding registers are available for display or distribution via OM system commands until the next scheduled acquisition period—when new data is entered.

The OM Transfer Period and History Enhancements feature allows the operating company the option of defining time intervals of 5, 10, 15, 20, or 30 minutes. Mea-

Figure 2-2 — OM Organization block diagram
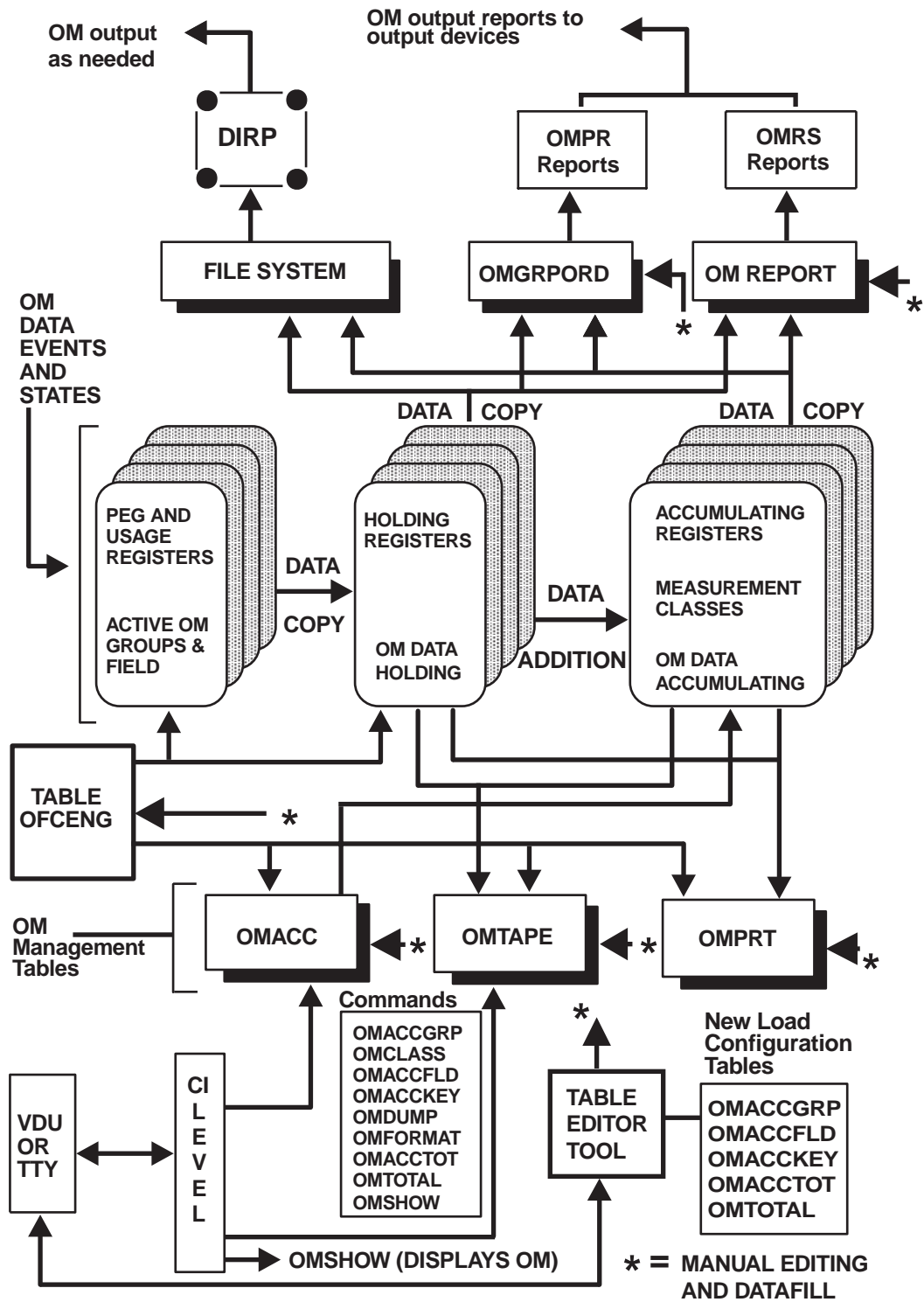
surements from each time interval are placed in a series (maximum 6) of HISTORY registers. The feature cannot be equipped in offices with the EADAS/NM interface—it is automatically removed if equipped.

Data accumulation

For purposes of output reporting of OM data, it is necessary to accumulate the data over longer periods. Additional sets of registers, classed as ACCUMULATING registers, are therefore provided. Each class is associated with a specific start and stop time. The data from the holding registers is copied into the accumulating register at times and for periods scheduled by the OM management tables. Each set of holding or accumulating registers having the same time characteristics is referred to as a measurement class.

The data accumulation process adds the contents of the holding class registers to the accumulating class registers prior to the next data collection. The accumulated data is available until the end of the accumulating period.

At the end of the accumulating period—scheduled by the OM management tables—the total content of the accumulating registers is distributed to selected output devices, such as printers, or to recording devices as an output report to downstream organizations. The first entry of the next period overwrites the final data of the preceding period.

On a reload restart, all OM registers, including accumulating registers, are zeroed. That is, all classes are zeroed.

OM administration

Initial set-up

During the Customer Information (CI) provisioning and planning sessions for the initial switch or subsequent extension, the operating company should request adequate data store for the OM subsystem.

Prepare the OM control tables initial datafill that is included in the software load for new installations. Similar datafill may be required for switch extensions.

Review provisioning and datafill requirements with Nortel Networks at the early job planning sessions.

Each user group should verify that all classes of their OM reports are operational. This check should be completed before the switch goes in service.

Changes involving the addition of OM groups TRK, LMD, DS1CARR, SLU, IBN, and other large groups should be referred to the provisioning primes for verification of memory space, since large amounts of data store may be required.

OM modifications

Requests for modification to the OM system must be strictly controlled by designated primes.

The standard OM reports described within this manual are the minimum requirement and, if warranted, may be supplemented by additional OM registers to meet individual user needs. Each user group is responsible for minor additions of OM registers within their user's class— employing the command OMACCFLD to add or delete registers within OM groups, and command OMACCGRP to add or delete OM groups to the accumulating classes.

The control center (SCC, NOC, NRC etc.) administrator or equivalent, authorizes, activates, and controls modifications to the OM subsystem. This responsibility is very important since this activity may have an impact on the operation and integrity of the OM subsystem, as well as the data store memory capacity.

> **CAUTION**
> Before any changes are made, it is recommended that the OM class with the work activity be turned off in the OMACC and OMPRT tables to avoid corruption of the OM system.

OM procedures

Detailed procedures for administering OMs can be found in NTP 297-1001-300, *DMS-100F Basic Administration Procedures.* The following procedures can be found within this document:

- Specifying OM transfer period from data accumulation
- Designating an accumulating class
- Setting up history registers
- Specifying single or double precision for classes
- Assigning OM groups to an accumulating class
- Deleting OM groups from an accumulating class
- Deleting OM registers from an accumulating class
- Adding OM registers to an accumulating class
- Selecting specified tuples for output
- Specifying output order of OM groups within a class
- Enabling the class
- Scheduling reports
- Routing reports to DIRP
- Assigning a class number to a report
- Setting OM total for all classes
- Setting OM total for a specific group and class
- Specifying reports and the format of the report
- Starting or stopping the device

- Setting up SLU on an individual line
- Setting up SLU on an entire peripheral module
- Stopping the collection of SLU data
- Collecting overflow data using a OM group HUNT

OM table record worksheets

OM table record forms for the DMS-100 Common Local, TOPS, Office Parameters, DMS-200 Toll, and DMS-300 Gateway can be found in the Central Office Data Engineering System (CODES) for PCL loads. These documents have to be special ordered for the administrative groups that use the forms.

Information about use of the table editor—to input the data from the forms—can be found in NTP 297-1001-360, *Basic Translations Tools Guide*.

OM alarms and log messages

OM logs and output reports

OM class device output is controlled by table OMPRT and uses the facilities of the DMS-100F log routing and reporting sub-system. The logging mechanism collects output reports from all parts of the system, which are filed in order by log report number. OMs can be printed out, routed to a storage device (tape or disk), or collected on a mechanized system (e.g., EADAS).

OM reports can be found within logs:

- OMPR (operational measurement print) are reports that contain raw data readings and are associated with table OMPRT.

- OMRS (operational measurement reports system) are the special reports associated with table OMREPORT.

- The OM2 (operational measurement 2) reports when special conditions occur, such as an error, a full buffer, or a restart. An OM2 report is generated when a threshold is reached with the OM threshold feature using table OMTHRESH. Table ALARMTAB also generates an OM2 log when thresholds are reached.

NOTE: Use of the suppress zero option (SUPZERO tuple in table OMPRT) will greatly reduce the volume of the following output reports.

Existing OM threshold alarms

The capability of associating an EXT alarm with OM registers is provided in the ALARMTAB threshold alarms table. This table is write protected and predatafilled by Nortel Networks for the system. Each tuple in the table refers to a specific OM register and provides alarms for software resource overloads. Each register has an alarm level and threshold specified. The threshold represents the amount an OM register is to be incremented during a scan period. Generally one minute is needed to

activate the associated alarm. When a threshold is reached, a log message OM2200 is produced, a visual alarm indication is displayed in the EXT portion of the MAP alarm bar, and the appropriate audible signal is given.

OM threshold alarms

The optional OM Thresholding feature allows switch maintenance personnel to select up to a maximum of 128 OM registers for thresholding. Table OMTHRESH is used to set the register threshold value, scan time, and alarm level. An alarm and log message is generated when an OM register exceeds the threshold and scan time settings. The OMTHRESH and ALARMTAB tables have identical functions, except the OMTHRESH table has flexible scan timing and is for the operating company's use.

Log/OM association

No direct correlation between OM register counts and log message generation is implied, since the OM subsystem and the log subsystem are two separate processes running at different system priorities. However, an indirect correlation exists, and for trouble analysis, related OM and log message data should be considered in the analysis process.

OM commands

The following OM commands are used to add, delete, change, display, and query OM data:

OMSHOW <om group> <class> <active/holding/acc>

Displays all or part of a specified OM group's key structure and part or all of the contents. The output is based upon the parameters specified with the command.

OMDUMP CLASS <OMACC class> <format>

This command is used to display assigned class(es) and their OM groups and OM register fields. See table OMACC for assigned classes.

OMCLASS <class name> <precision/function>

Used to define or change a class for table OMACC. Once defined, a class name cannot be deleted, but it can be renamed. Registers and register groups are added to the class using commands OMACCFLD and OMACCGRP described next.

OMACCFLD [class group ADD/DELETE ALL/FIELD field]

Assigns or deletes individual OM register fields to the accumulating classes in table OMACC.

OMACCGRP

Assigns or deletes OM groups to the accumulating classes that were previously defined by OMCLASS command.

OMFORMAT

Similar to the OMSHOW command, except that only one OM group is displayed based upon the selected OM group.

OMACCKEY

This command, available with feature "OM Group Totals" in feature package OM Selective Output (NTX445AB), allows the operating company to select specific tuples within a named group and class for display or printout. It also eliminates the need to printout the complete group when only a portion is needed for review or analysis. Before selecting specific tuples for output, all the tuples within the group and class must be deleted using the DELETE ALL parameters.

OMTOTAL

This useful command turns the totalling feature on or off for a specified OM group. The purpose of this command, available with the "OM Group Totals" feature, is to allow the operating company to add totals by register for selected OM groups, such as PM, TRK, LCM, and others. The totals appear as an extra tuple for OMPR reports and outputs using the OMSHOW command. The operating company can also threshold the totals tuples using the OM thresholding feature.

OMACCTOT

This command turns the totalling only feature on or off for a specified class and group. The OM group totals feature, using the OMTOTAL command, must be turned ON and the OM class must be designated and command OMACCGRP must be used to assign the group to the class for this capability to work. If turned ON, only the total tuple will be displayed in the OMPR reports.

OMBR

This command—along with parameters: stops, starts, and displays—provides control for buffered OMs. It can be used when problems arise with buffered OM reports.

OMPRDUMP

This command provides the capability to generate operational measurement special reports (OMPRSPEC) for the OM data stored on the tape or disk in the standard recording format (OMTAPE). The reports produced would be in readable form.

OMMASTER

This command, executed on the CM, allows the user to configure a node as the central collector for billing. This is the node (CM, FP2, or the enhanced input/output controller (EIOC)) on which OM accumulation and reporting functions take place.

> **WARNING -** Use of the OMMASTER command causes loss of currently defined accumulation classes and their data. Also, do not "break" (use command HX) from the OMMASTER command.

OMRESET

This command provides for the record count to be reset only on *reload* restarts.

OMREPORT

This command allows the capability to query for a list of all report names in the OMREPORT system and to request an OM report by SCHEDNO in table OMRE-PORT.

Q OMSHOW

Use this command to get a list of the OM groups and classes defined by the OMCLASS command.

CLRINVREG

This command can be used to clear invalid INWATS registers after a restart. Use it before reading or resetting INWATS registers after a restart.

READ

This command is used to query the register content of specified lines and displays the line information.

READPX

This command displays the information for INWATS registers associated with options INW and 2WW for PX trunks.

READRESET

This command queries the register content of specified lines, displays the line information, and resets the register to zero.

READRESETPX

This command displays the information for INWATS registers associated with options INW and 2WW for PX trunks, and resets the registers back to zero.

READVFG

This command displays the information for INWATS VFGs.

READRESETVFG

This command displays the information for INWATS VFGs, and resets the registers back to zero.

SLUADD & SLUDEL

These commands add or delete line identifiers for subscriber line usage (SLU) input tables. New entries are added to the bottom of the table.

SLU_INSTALL

This command looks for errors in the SLU input tables before filling the OM group with new data. Lines not previously installed are set to zero while the installed lines are retained.

SLU_LMINSTALL

For LMs and their associated lines, this command removes all lines from OM group ENG650M1 and creates an OM group ENG640M1. The SLU input table is not affected.

SLU_DEINSTALL

This command stops all OMs on lines in the specified OM group but does not affect the entries in the associated input table.

Q SLU

This command lists all the commands available in the SLU directory.

SLUDUMP

Except for the SLU_DEINSTALL command, the SLUDUMP command lists the commands issued for SLU input tables that have been installed.

SLUFINDI

This command finds and displays the specified line identifier within an input SLU input table. If associated with a hunt group, then all the members are displayed.

SLUFINDO

This command finds and displays the register counts for a specified line identifier within an OM group. This command is more effective if the SLU_DEINSTALL command is used to make the OM group inactive so that the register counts are held.

SLUSET

Establishes a default table for commands SLUADD, SLUDEL, SLUFINDO, and SLUFINDI.

SLU_TABLE_STATUS

This command displays a list of active and inactive tables.

SLU_TEST

This command verifies that the command SLU_INSTALL can be used in the SLU input table with no errors present.

For more detailed information on the OM commands and their parameters, see NTP 297-1001-300, *DMS-100F Basic Administration Procedures.*

OM tables

OM management tables

The data acquired and entered into the OM data tables are managed by four management tables that control the acquisition, collection, accumulation, and distribution functions of the OM system. The OM management tables are OMACC, OMGR-PORD, OMTAPE, OMPRT, OMACCGRP, OMACCFLD, OMACCKEY, OMACC-TOT and OMTOTAL.

The OM configuration file used during the software upgrade is eliminated in BAS06. The data that it contained is moved into tables OMACCGRP, OMACCFLD, OMAC-CKEY, OMACCTOT and OMTOTAL and new fields are added to table OMACC. These tables configure the OM system on the new software load and allow customers to use the table editor instead of using the OM CI commands to configure their accumulating classes

Access to the OM management tables, for purposes of display and/or modification, is via the visual display unit (VDU), or other I/O device such as a TTY. Table editor commands are used to datafill the OM management tables and in modifying some fields.

The following description for each table briefly covers the general principles of operation for the OM management tables.

Table OMACC

The Operational Measurement Accumulation (OMACC) table contains values defining the timing of data copied between holding registers and designated measurement classes of accumulating registers. The commands OMCLASS (defining a new measurement class), OMACCGRP and OMACCFLD (used to add or delete information on a measurement class), and OMDUMP (used to display the groups and fields belonging to a particular class), are used to administer the OMACC table.

Table OMGRPORD

The OM Group Order (OMGRPORD) table provides the customer with the capability to define the order of the OM group output within each OM accumulating class according to their own priority. This is done by datafilling tables OMPRT and OMTAPE. When deleting an accumulating class, delete from table OMGRPORD first.

Table OMTAPE

The Operational Measurement Tape (OMTAPE) table contains values that determine the measurement class, timing, and other parameters. These are required when performing a data copy between a holding, history or accumulating register and a designated recording device. Using the DIRP subsystem, data can be directed to either a tape or disk. The recording device (tape or disk) is determined by datafilling tables DIRPSSYS and DIRPPOOL.

Table OMPRT

The Operational Measurement Printer Table (OMPRT) contains values defining the measurement class, timing and other parameters required when performing a data copy process from a holding, history, or accumulating register to a printer or other similar output device. When the other values (measurement group, class, timing) are entered into OMPRT, the output report is automatically routed—via the routing and reporting subsystem—to the associated device at the scheduled times, triggered by the key reference to the log report number.

Zero data can be selectively suppressed on a device basis if the field SUPZERO in table OMPRT is set to "Y". Only those tuples (keys) containing non-zero data will be output.

Table OMREPORT

The Operational Measurement Report (OMREPORT) table enables special system performance reports to be obtained using the OM data base. Table OMREPORT records which classes are to be reported, the schedule for the reports and the type of counts to be reported. Double precision is supported for accumulating classes. The output report is automatically routed—via the routing and reporting subsystem—to the associated device at the scheduled times, triggered by the key reference to the OMRS log report number. The following are the reports controlled by table OMRE-PORT:

- AMREPORT (Executive Maintenance Morning Report)
- SPMSREP (Switch Performance Monitoring System)
- PRDTKMTC (Periodic Trunk Maintenance)
- ACHGXREP (Attempts per Circuit per Hour Global Exception Report
- ACHREP (Attempts per Circuit per Hour)
- CDSREP (Call Disposition Summary)
- DTDETECT (Unauthorized Digitone Detection Report)
- EATSMS (Equal Access Traffic Analysis Report)
- TFCANA (Traffic Analysis Report)

Table OMDEV

The system uses table Operational Measurements Device Table (OMDEV) to enter dedicated output devices for operational measurements (OM).

Table OMTOTAL

Table Operational Measurements TOTAL (OMTOTAL) holds the operational measurement (OM) configuration data that associates with the OM CI command OMTO-TAL.

Figure 2-3 — OM System information flow
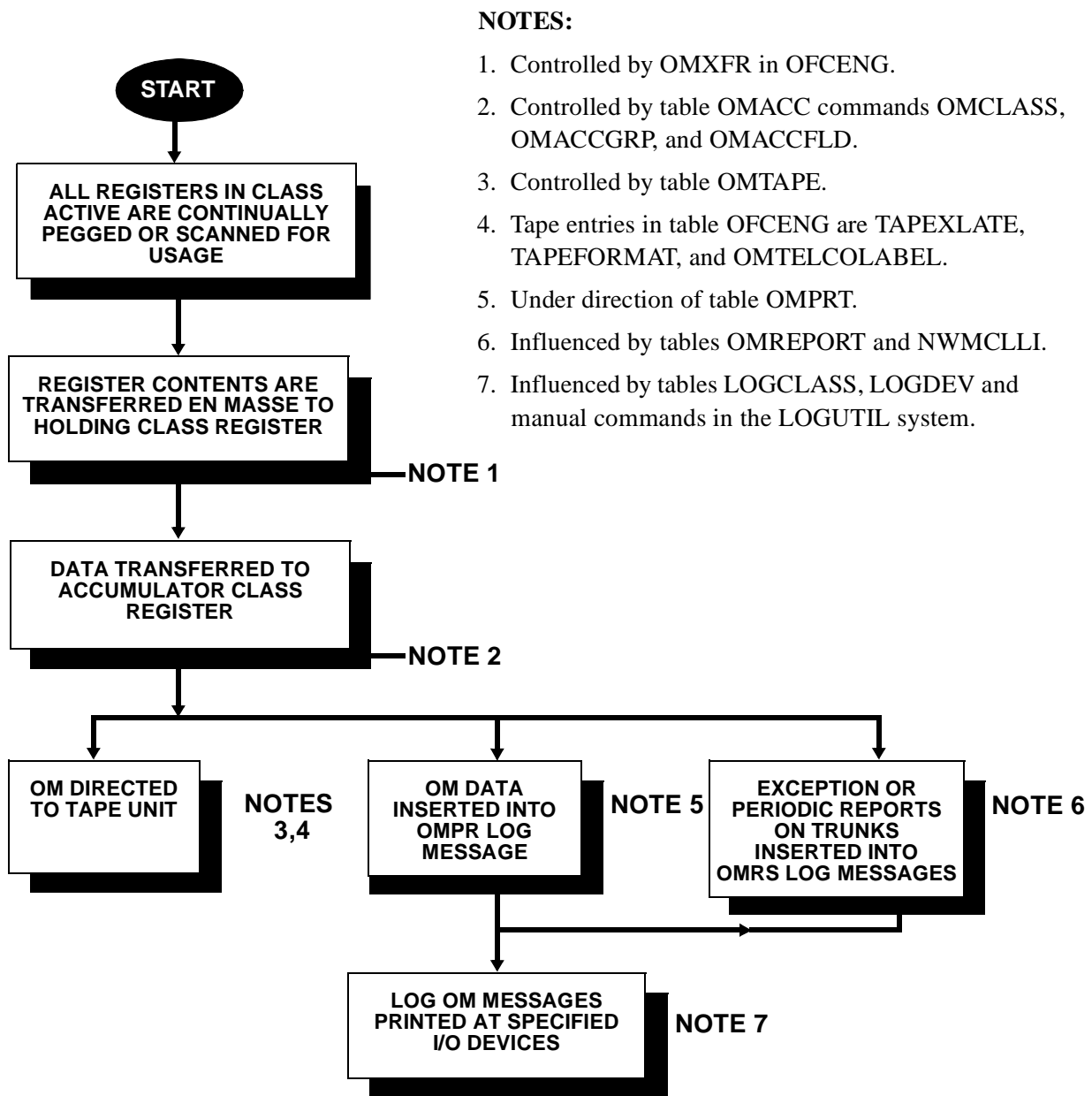
NOTES:

1. Controlled by OMXFR in OFCENG.

2. Controlled by table OMACC commands OMCLASS, OMACCGRP, and OMACCFLD.

3. Controlled by table OMTAPE.

4. Tape entries in table OFCENG are TAPEXLATE, TAPEFORMAT, and OMTELCOLABEL.

5. Under direction of table OMPRT.

6. Influenced by tables OMREPORT and NWMCLLI.

7. Influenced by tables LOGCLASS, LOGDEV and manual commands in the LOGUTIL system.

START

ALL REGISTERS IN CLASS ACTIVE ARE CONTINUALLY PEGGED OR SCANNED FOR USAGE

REGISTER CONTENTS ARE TRANSFERRED EN MASSE TO HOLDING CLASS REGISTER

NOTE 1

DATA TRANSFERRED TO ACCUMULATOR CLASS REGISTER

NOTE 2

OM DIRECTED TO TAPE UNIT — **NOTES 3,4**

OM DATA INSERTED INTO OMPR LOG MESSAGE — **NOTE 5**

EXCEPTION OR PERIODIC REPORTS ON TRUNKS INSERTED INTO OMRS LOG MESSAGES — **NOTE 6**

LOG OM MESSAGES PRINTED AT SPECIFIED I/O DEVICES — **NOTE 7**

Table OMACCGRP

The Operational Measurements Accumulator Groups (OMACCGRP) table holds the operational measurement (OM) configuration data associated with the OM CI command OMACCGRP. Use this table to assign or delete OM groups to or from accumulating classes.

Table OMACCFLD

The Operational Measurements Accumulator Field (OMACCFLD) table holds the operational measurement (OM) configuration data associated with the OM CI command OMACCFLD. Use this table to add or delete an OM field to an accumulating class.

Table OMACCKEY

The Operational Measurements Accumulator Key (OMACCKEY) table holds the operational measurement (OM) configuration data associated with the OM CI command OMACCKEY. The operating company uses this table to select specified tuples in an accumulating group and OM class. The operating company selects these tuples for output to a printing device.

Table OMDEYORD

Table OMKEYORD records the operational measurements (OM) tuple order on the switch. During a One Night Process (ONP), the system transfers the OM tuple order information from OMKEYORD to the new software load. New software loads use the OM tuple order information to order the multiple tuple OM groups for that office.

OM parameters

Table OFCENG

The Office Engineering (OFCENG) table contains the following five parameters for OMs:

- OMXFR
- OMTAPESUPPRESSION
- TAPEXLATE
- OMPRTFORMAT
- OMTELCOLABEL

The office parameter OMXFR contains the basic timing value (OMXFERPERIOD) that determines the periods of data transfer between the ACTIVE and the HOLDING classes of OM registers. OMXFERPERIOD is set to either 15 minutes or 30 minutes, using the table editor procedures. The OMXFERPERIOD is specified by the operating company, but datafilled and controlled by Nortel Networks.

Office parameter OMTAPESUPPRESSION enables or disables the suppression of zero data (unused tuples) from output to OM DIRP. It does not suppress zero data like the 'supzero' field in table OMPRT. Use the OMSHOW command to see valid tuples.

The parameter TAPEXLATE specifies the type of translation to be applied to operational measurement registers as they are written to tape or disk The following types can be applied:

- EBCDIC – character representation in EBCDIC
- ASCII – character representation in ASCII
- ASCII_BINARY – numeric representation in ASCII
- EBCDIC_BINARY – numeric representation in EBCDIC

The OMPRTFORMAT parameter defines the number of registers whose contents are printed on one line of output by the OM printer. One register has eleven characters.

The parameter OMTELCOLABEL is defined by the operating company and specifies the label to be put on the OM tapes.

Table OFCOPT

The Office Options (OFCOPT) table contains the following two parameters for OMs:

- OMHISTORYON
- OMINERLANGS

The parameter OMHISTORYON is part of feature package OM Transfer Period and History Class Enhancements (NTX099AA). It enables the operating company to collect data in a series of user defined time intervals or snapshots that can be 5, 10, 15, 20, or 30 minutes. This permits trend line analysis of short interval information. When OMHISTORYON is set to "Y", parameter OMXFR in table OFCENG is suppressed and a five minute transfer period is put into effect. The feature cannot be equipped in offices with EADAS/NM Interface — it is automatically removed if equipped.

The parameter OMINERLANGS is used for international translations when usage measurements require output to be in erlangs rather than CCS (hundred call seconds).

Table OFCVAR

When the Engineering and Administrative Data Acquisition System (EADAS) feature is added to an office, the EADAS_ENABLED parameter in table OFCVAR should be set to "N" until the operating company has completed all the datafill for EADAS and is ready to send data for polling.

Parameter OM_SOURCE_IDENTIFICATION (Operational Measurements Source Identification) enables or disables the ability to display the source node on which an OM tuple was collected in the OM reports. In the United Kingdom, it is always set to "OFF".

OM class assignments and reports

OM accumulating classes

The OM accumulating classes are provided for customizing the OM output reports for all users. There is a maximum of 32 different measurement classes in a switch. One is *active*, another is *holding*, leaving a maximum of 30 that the operating company can specify as *accumulating* or *history* with different accumulating time periods. Each class may contain from one to all registers, depending on user needs.

Before any management tables can be completed, the accumulating classes must be defined using the OMCLASS command. Corresponding to each class defined, a tuple is automatically assigned in table OMACC. Enabling and disabling of the class is done in table OMACC.

Active and holding classes

Two predefined classes, active and holding, are assigned in table OMCLASS for system use; however, access for printouts is possible through the OMSHOW command. Unassigned OM groups and related fields default to the holding class which has both assigned and unassigned OM groups.

The operating company can assign either a single or double precision status to a class. If a register count is expected to exceed 65,535 (single precision), then a double precision register (4,294,967,295 count) should be assigned. Registers are made double precision when they are in a class assigned as double precision (DPRECISION).

Assigning OM classes

Table OMACC has memory allocated for 30 class entries. Two classes, *active* and *holding*, are not in the table and are preassigned by Nortel Networks. When the switch is commissioned, Nortel Networks establishes the HALFHOUR, OFCB-SYHR, DAY, TRUNKHR, MONTH, TAPE, and SPECIAL 1 through 8 measurement classes. The remainder of the 30 classes, excluding the *active* and *holding*, can be assigned by the operating company. The operating company can also rename the classes that Nortel Networks established. Analysis of these classes can be made from the scheduled printouts or from manually requested printouts at any time. See Table 2-22 for a summary and cross reference to Tables 2-11 through 2-21, and 2-23 through 2-41.

The following classes were developed to meet the switch and trunk maintenance and surveillance requirements. OM groups and registers should be added as needed.

SW_HRLY real-time surveillance

SW_HRLY — key OM data from this class can be used for real-time switch surveillance when the OM thresholding feature has not been supplied. This provides for the capability to perform effective analysis of the OM data for prompt trouble identifica-

tion, isolation, and correction. Class SW_HRLY is programmed to print hourly when maintenance personnel are on hand (daytime M-F 0700-1800 or modify to meet local coverage). See the tables within this subsection for a list of the SW_HRLY OMs to be maintained.

SW_DAY subsequent analysis

SW_DAY — key OM data for next day subsequent analysis. Suggest recording daily key OM data on a control record form for "visual analysis." The "Office Administration" section provides a sample of a control record form and a description of its use. When analyzing the SW_DAY printouts, the 24-hour key MTCE OM totals can disclose constant and marginal conditions, or single events that become identifiable over a longer interval. Realistic bogeys for the 24-hour period are essential for proper analysis of the OM data. See the tables within this subsection for the SW_DAY OMs and the "OM recommended bogey settings" provided later within this subsection.

SW_WKLY subsequent analysis

SW_WKLY — key OM data summarized for 7 days. Summarize and analyze in a similar manner to SW_DAY record OM data on the control record form and develop realistic 7-day bogeys. Using valid bogeys, SW_DAY key OM data identifies the trend for the month end service and performance results. See the tables within this subsection for the SW_DAY OMs to be analyzed, since the SW_WKLY use the same OMs.

SW_MTH subsequent analysis

SW_MTH — key OM data summarized for the month provides input for a service performance results plan. Post on the yearly control record form. Analyze for trends, identify weak areas, set priorities, develop action plans, and implement from the hourly, daily, and weekly control levels. Bogey levels developed for SW_MTH should track month end values recorded in the service results plan, which would earn an acceptable level of performance (96 to 98 index range). See the tables within this subsection for the SW_MTH OMs to be analyzed.

Lines/Trunks/Carrier Days (L/T/C D)

L/T/C D — key OM data for next day subsequent analysis. The system alarms and log messages for trunks and lines provide the necessary information for real-time surveillance. If the focused maintenance feature is provided and used, it can reduce considerably the individual alarms and log message indications by a buffering and threshold technique that sifts out incidental type indicators. Suggest recording the daily key OM data on a control record form for analysis. Analysis of the 24-hour L/T/C D printout helps to identify constant and marginal conditions, or what appears to be isolated events that become identifiable over a longer interval of time. Develop bogeys using trend information for transmission, signaling, and carrier performance criteria. See the tables within this subsection for a list of the L/T/C D OMs to be analyzed.

Lines/Trunks/Carrier Week (L/T/C W)

L/T/C W — key OM line, trunk and carrier data summarized for 7 days. Summarize and analyze in a similar manner to L/T/C D. The weekly L/T/C OMs are the same as the daily and can be found within this subsection.

Lines/Trunks/Carrier Month (L/T/C M)

L/T/C M — key OM line, trunk, and carrier data summarized for the month. Post on a yearly control record form for trend information. Identify weak areas and initiate a corrective program. Again, see the tables for a list of the L/T/C M OMs to be tracked and analyzed.

ISDN classes

Customized class reports are provided within tables of this subsection—they are ISDN_HRLY, ISDN_DAY, and ISDN_MTH.

SPMS classes

The following classes are required when the Switch Performance Monitoring System (SPMS) is used for subsequent analysis and trouble detection. For the SPMS SW_HRLY OM analysis, use the previous description of the SW_HRLY class. The SPMS process is described in the *Performance* section of this manual. Examples of SPMS classes can be found in tables of this subsection.

SPMS_DAY subsequent analysis

SPMS_DAY— back-up key OM data for the SPMS process. This information would be used at times to resolve problems identified by the daily SPMS process — that would require additional analysis using basic OM data collected in the SPMS_DAY class.

SPMS_MTH subsequent analysis

SPMS_MTH — key SPMS OM data summarized for the report month. This information would be used at times to resolve problems identified by the monthly SPMS process — that would require additional analysis using basic OM data collected in the SPMS_MTH class. For trend and historic purposes, post SPMS-MTH raw OM data to the yearly control record form. Analyze for trends, identify weak areas, develop action plans, and monitor results using SPMS_DAY for progress.

SS7 classes

Customized OM class assignments were developed to meet SS7 maintenance and surveillance requirements. Examples of SS7 classes with their assigned OM groups and registers are provided in tables within this subsection. A description of each SS7 table follows:

SSP_HRLY

SSP_HRLY — key OM data can be used at the SP or SSP nodes for real-time SS7 signaling surveillance. SSP_HRLY is scheduled to be printed hourly when maintenance personnel are on hand (daytime M-F 0700 to 1800 or modify to meet local coverage).

SSP_DAY

SSP_DAY — key SSP_DAY OM data is for next-day subsequent SS7 signaling surveillance at SP or SSP nodes. Suggest recording daily key OM data on a control record form for analysis or other computer-assisted method. A control record form for this purpose is described in the *Office Administration* section of the MOM. Where available, combine SSP_DAY analysis with 7_SPMS-D for SP/SSP nodes.

STP_HRLY

STP_HRLY — key STP_HRLY OM data used at an STP node for real-time SuperNode and SS7 signaling surveillance. STP_HRLY is scheduled to be printed hourly when maintenance personnel are on hand (daytime M-F 0700 to 1800 hrs or modify to meet local coverage).

STP_DAY

STP_DAY — key STP_DAY OM data is used for next day subsequent SuperNode and SS7 signaling surveillance at an STP node. Suggest recording daily key OM data on a control record form for analysis or other computer-assisted method. A control record form for this purpose is described in the *Office Administration* section of the MOM. Where available, combine STP_DAY analysis with 7_SPMS_D (for STP).

7_SPMS_D for SP/SSP/STP

7_SPMS_D — SS7 back-up OM data for SP/SSP/STP is used to facilitate in-depth analysis of specific indicators. This information would be used at times to resolve problems— identified by the daily SPMS process—that require the source OM data to be analyzed.

C7SLMPR

The CCS7 Signaling Link Marginal Performance Report (C7SLMPR) provides real-time signaling link surveillance for the identification of signaling link degradation resulting in marginal link performance or trouble. This feature reports faults by individual link when a preset threshold has been reached or exceeded, and features an alarm when programmed. For more information on the SLMPR feature, see the "SS7 Maintenance" subsection and page 4-199 of this manual.

EADAS classes

When the EADAS feature is implemented on the switch, EADAS classes are auto-matically added. The EADAS Data Collection (EADAS/DC) package (NTX218AA) is required and adds the EADAS30M, EADAS60M, and EADAS24H OM classes. An optional EADAS feature, the EADAS Network Management (EADAS/NM) package adds the PREV5M and CURR5M OM classes at loadbuild.

SEAS classes

System Engineering and Administration System (SEAS) — SEAS_30M, SEAS_60M, and SEAS_24H classes support the SEAS/OSS and are derived from the STP OMs. NTP 297-8101-814, *DMS SuperNode STP Operational Measurement Manuals* describe the OM groups and registers needed for SEAS. An example of the SEAS classes for SS7 can be found in Tables 2-24, 25, & 26 within this subsection.

TOPS classes

Tables within this subsection provide suggested TOPS customized operational mea-surements output reports for classes TOPS_HRLY and TOPS_DAY.

Table 2-6

Suggested Customized Operational Measurements Output Report For Class SW_HRLY

CLASS:		SW_HRLY		
ACCUMULATING PERIOD:		HRLY		
OUTPUT SCHEDULE:		DAYTIME MO FR 7 C00 16 C00		
PRECISION:		SINGLE		

See Notes in Table 2-16	GROUP	REGISTERS			
101					
102	MS	MSERR MSLKERR MSLKERR	MSFLT MSPTFLT MSPTFLT	MSCDERR	MSCDFLT
102	CM	CMTRMISM CMSSCFLT	CMTRAP	CMCPUFLT	CMMEMFLT
102	SLM	SLMFLT	SLMSBSU	SLMMBSU	
103	CPU	MTCHINT	TRAPINT SYSCINIT	CPUFLT SYNCLOSS	SYSWINIT
	IOC	IOCERR	IOCLKERR	IOCFLT	
124	EIOC	EIOCFLT	EIOCERR		

Table 2-6   (continued)
Suggested Customized Operational Measurements Output Report For Class SW_HRLY

CLASS: SW_HRLY
ACCUMULATING PERIOD: HRLY
OUTPUT SCHEDULE: DAYTIME MO FR 7 C00 16 C00
PRECISION: SINGLE

See Notes in Table 2-16	GROUP	REGISTERS			
103	CMC	CMCLERR	CMCERR	CMCFLT	
	MTU	MTUERR	MTUFLT		
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL
		NMSPCHFL	NMCFLT		
104	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
105					
104	PMTYP	PMTERR	PMTFLT		
		PMTSCXFR	PMTMCXFR	PMTCCTFL	PMTDRFLT
105		PMTDRERR			
	CP	CCBOVFL	CPTRAP	CPSUIC	ORIGDENY
		WAITDENY	CPLOOVFL	CPLPOVFL	OUTBOVFL
		MULTOVFL	WAKEOVFL	CINITC	WINITC
	EXT	EXTOVFL			
	TRMTER	TERSYFL	TERSSTO	TERRODR	TERSTOB
		TERSTOC			
	TRMTRS	TRSNOSC	TRSNBLH	TRSNBLN	TRSEMR1
		TRSEMR2			
	RCVR	RCVOVFL	RCVQOVFL	RCVQABAN	
	UTR	UTROVFL	UTRQOVFL	UTRQABAN	
	STN	STNOVFL	STNMTCHF		
	CF6P	CF6OVFL	CF6QOVFL		
	DDU	DDUERROR	DDUFAULT		
	AMA	AMAEMTR	AMAROUTE		
	OFZ	INOUT	NIN	OUTMFL	OUTRMFL
		OUTOSF	OUTROSF	INABNM	INABNC
		ORIGOUT	ORIGTRM	NORIG	INTRM
		TRMMFL	TRMBLK	ORIGABDN	

Table 2-6 **(continued)**
Suggested Customized Operational Measurements Output Report For Class SW_HRLY

CLASS:	SW_HRLY
ACCUMULATING PERIOD:	HRLY
OUTPUT SCHEDULE:	DAYTIME MO FR 7 C00 16 C00
PRECISION:	SINGLE

See Notes in Table 2-16	GROUP	REGISTERS			
	CF3P	CNFOVFL	CNFQOVFL		
106	TOPSMTCE	POSD	POSDF	POSTRKDF	POSDMDF
106	TOPSMISC	RONITBL	TMSGLOST	TOPRLOST	
107	AOSS	AOSSQDEF	AOSSOD	AOSSD	AOSSDF

Table 2-7
Suggested Customized Operational Measurements Output Report For Class SW_DAY

CLASS:	SW_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
101					
102	MS	MSERR	MSFLT	MSMBU	MSSBU
		MSCDERR	MSCDFLT	MSCDMBU	MSCDSBU
		MSLKERR	MSPTFLT	MSLKMBU	MSLKSBU
102	CM	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT
102	SLM	SLMFLT	SLMSBSU	SLMMBSY	
103	CPU	MTCHINT	TRAPINT	CPUFLT	SYSWINIT
		SYSCINIT	SYNCLOSS	MSYLOSSU	SSYLOSSU
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU
		IOCLKMBU	IOCSBU	IOCMBU	
124	EIOC	EIOCERR	EIOCFLT	EIOCMBU	EIOCSBU

Table 2-7   (continued)
Suggested Customized Operational Measurements Output Report For Class SW_DAY

CLASS: SW_DAY
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
103	CMC	CMCLERR	CMCERR	CMCFLT	CMCLKSBU
		CMCLKMBU	CMCSBU	CMCMBU	
	MTU	MTUERR	MTUFLT	MTUSBU	MTUMBU
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL
		NMSPCHFL	NMCFLT	NMSBU	NMMBU
		NMPTSBU	NMPTMBU	NMJRSBU	NMJRMBU
		NMSPCHFL	NMCFLT	NMSBU	NMMBU
	SYSPERF	CINTEGFL			
104 105	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
		PM1MBU	PM1SBU		
104 105	PMTYP	PMTERR	PMTFLT		
		PMTSCXFR	PMTMCXFR	PMTCCTFL	PMTUSBY
		PMTUMBU	PMTMSBU	PMTMMBU	PMTSBTCO
		PMTMBTCO	PMTINTEG	PMTDRFLT	PMTDRERR
		PMTDRMBU	PMTDRSBU		
	CP	CCBOVFL	CPTRAP	CPSUIC	ORIGDENY
		WAITDENY	CPLOOVFL	CPLPOVFL	OUTBOVFL
		MULTOVFL	WAKEOVFL	CINITC	WINITC
		INITDENY			
	EXT	EXTOVFL			
	TRMTER	TERSYFL	TERSSTO	TERRODR	TERSTOB
		TERSTOC			
	TRMTRS	TRSNOSC	TRSNBLH	TRSNBLN	TRSEMR1
		TRSEMR2			
	RCVR	RCVOVFL	RCVQOVFL	RCVQABAN	RCVSBU
		RCVMBU			
	UTR	UTROVFL	UTRQOVFL	UTRQABAN	
	STN	STNMTCHF	STNOVFL	STNMBU	STNSBU
	CF6P	CF6OVFL	CF6QOVFL	CF6MBU	CF6SBU

Table 2-7   (continued)
Suggested Customized Operational Measurements Output Report For Class SW_DAY

CLASS:	SW_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDVSBUSY
	AMA	AMAEMTR	AMAROUTE		
	OFZ	INOUT	NIN	OUTMFL	OUTRMFL
		OUTOSF	OUTROSF	INABNM	INABNC
		ORIGOUT	ORIGTRM	NORIG	INTRM
		TRMMFL	TRMBLK	ORIGABDN	
	CF3P	CNFOVFL	CNFQOVFL	CNFMBU	
106	TOPSMTCE	POSD	POSDF	POSTRKDF	POSDMDF
106	TOPSMISC	RONITBL	TMSGLOST	TOPRLOST	
107	AOSS	AOSSQDEF	AOSSOD	AOSSD	AOSSDF

Table 2-8
Suggested Customized Operational Measurements Output Report For Class SW_MTH

CLASS:	SW_MTH
ACCUMULATING PERIOD:	MONTHLY 1 0C00 1 0C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
101					
102	MS	MSERR	MSFLT	MSMBU	MSSBU
		MSCDERR	MSCDFLT	MSCDMBU	MSCDSBU
		MSLKERR	MSPTFLT	MSLKMBU	MSLKSBU
102	CM	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT
		CMTRMISM	CMTRAP	CMCPUFLT	CMMEMFLT
		CMSSCFLT	CMMCSBSY	CMRCPUFL	CMRMEMFL
		CMRSSCFL	CMRMCFL	CMSSMPXU	CMMSMPXU
102	SLM	SLMFLT	SLMSBSU	SLMMBSY	

Table 2-8   (continued)
Suggested Customized Operational Measurements Output Report For Class SW_MTH

CLASS:	SW_MTH
ACCUMULATING PERIOD:	MONTHLY 1 0C00 1 0C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
103	CPU	MTCHINT	TRAPINT	CPUFLT	SYSWINIT
		SYSCINIT	SYNCLOSS	MSYLOSSU	SSYLOSSU
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU
		IOCLKMBU	IOCSBU	IOCMBU	
124	EIOC	EIOCERR	EIOCFLT	EIOCMBU	EIOCSBU
103	CMC	CMCLERR	CMCERR	CMCFLT	CMCLKSBU
		CMCLKMBU	CMCSBU	CMCMBU	
	MTU	MTUERR	MTUFLT	MTUSBU	MTUMBU
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL
		NMSPCHFL	NMCFLT	NMSBU	NMMBU
		NMPTSBU	NMPTMBU	NMJRSBU	NMJRMBU
	SYSPERF	CINTEGFL			
104	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
105		PM1MBU	PM1SBU		
104	PMTYP	PMTERR	PMTFLT		
105		PMTSCXFR	PMTMCXFR	PMTCCTFL	PMTUSBY
		PMTUMBU	PMTMSBU	PMTMMBU	PMTSBTCO
		PMTMBTCO	PMTINTEG	PMTDRFLT	PMTDRERR
		PMTDRMBU	PMTDRSBU		
	CP	CCBOVFL	CPTRAP	CPSUIC	ORIGDENY
		WAITDENY	CPLOOVFL	CPLPOVFL	OUTBOVFL
		MULTOVFL	WAKEOVFL	CINITC	WINITC
		INITDENY			
	EXT	EXTOVFL			
	TRMTER	TERSYFL	TERSSTO	TERRODR	TERSTOB
		TERSTOC			
	TRMTRS	TRSNOSC	TRSMBLH	TRSNBLN	TRSEMR1
		TRSEMR2			
	UTR	UTRQOVFL	UTROVFL	UTRQABAN	

Table 2-8   (continued)
Suggested Customized Operational Measurements Output Report For
Class SW_MTH

CLASS:	SW_MTH
ACCUMULATING PERIOD:	MONTHLY 1 0C00 1 0C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
	STN	STNMTCHF	STNOVFL	STNMBU	STNSBU
	CF6P	CF6OVFL	CF6QOVFL	CF6MBU	CF6SBU
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY
	AMA	AMAEMTR			
	OFZ	INOUT	NIN	OUTMFL	OUTRMFL
		OUTOSF	OUTROSF	INABNM	INABNC
		ORIGOUT	ORIGTRM	NORIG	INTRM
		TRMMFL	TRMBLK	ORIGABDN	
	CF3P	CNFOVFL	CNFQOVFL	CNFMBU	
106	TOPSMTCE	POSD	POSDF	POSTRKDF	POSDMDF
106	TOPSMISC	RONITBL	TMSGLOST	TOPRLOST	
107	AOSS	AOSSQDEF	AOSSOD	AOSSD	AOSSDF

Table 2-9
Suggested Customized Operational Measurements Output Report For
Class L/T/C D

CLASS:	L/T/C D
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
	DS1CARR	DS1LCGA	DS1RCGA	DS1MBU	DS1LOF
		DS1SLP	DS1SBU	DS1ES	DS1PBU
		DS1CBU	DS1BER		DS1SES
		DS1UAS	DS1A1S		

Table 2-9
Suggested Customized Operational Measurements Output Report For Class L/T/C D (continued)

CLASS: L/T/C D
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
	TRK	INCATOT OUTFAIL	INFAIL SBU	NATTMPT MBU	GLARE OUTMTCHF
	LMD	TERMBLK	ORIGFAIL	PERCLFL	STKCOINS
		ORIGBLK	NTERMATT	NORIGATT	
	OFZ2	OFZNCIT OFZNCID OFZNCIM	OFZNCTC OFZNOSC	OFZNCLT OFZNCOT	OFZNCBN OFZNCRT
108	ACSYSTR	ACDMOVFL ACDMFL	ACCF3POV ACCF3PFL	ACEXOVFL ACERR	ACDATAER ACFLT
109	C7LINK1	C7LKFAIL	C7SUER	C7COV	
109	C7LINK2	C7ONSET1	C7ONSET2	C7ONSET3	
109	C7LKSET	C7LSUNAU	C7LSFAIL		
109	C7ROUTE	C7TFR C7TFC3	C7TFP C7FRCRER	C7TFC1	C7TFC2
109	C7RTEST	C7RTUNAU	C7RSUNAU	C7RSFAIL	
110	C7SCCP	C7RTFALL C7RTFSSC	C7RTFNWF	C7RTFNWC	C7RTFSSF
111	ISUPCGRP	ISCKTRAC	ISCKTRAO		
111	ISUPCONN	ISCONBAD	ISCONUCE	ISCONUCC	ISCONCOT
111	ISUPCKTA	ISCKTGBT	ISCKTGBF	ISCKTLBT	ISCKTRBT
112	NSC	NSCTIOVF NSCATMPT	NSCSFLTO	NSCFLICM	NSCFLICS

Table 2-10
Suggested Customized Operational Measurements Output Report For Class L/T/C M

CLASS:	L/T/C M
ACCUMULATING PERIOD:	MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
	DS1CARR	DS1LCGA	DS1RCGA		DS1LOF
		DS1SLP	DS1SBU	DS1MBU	DS1PBU
		DS1CBU	DS1BER	DS1ES	DS1SES
		DS1UAS	DS1A1S		
	TRK	INCATOT	INFAIL	NATTMPT	GLARE
		OUTFAIL	SBU	MBU	OUTMTCHF
	LMD	TERMBLK	ORIGFAIL	PERCLFL	STKCOINS
		ORIGBLK	NTERMATT	NORIGATT	
	OFZ2	OFZNCIT	OFZNCTC	OFZNCLT	OFZNCBN
		OFZNCID	OFZNOSC	OFZNCOT	OFZNCRT
		OFZNCIM			
108	ACSYSTR	ACDMOVFL	ACCF3POV	ACEXOVFL	ACDATAER
		ACDMFL	ACCF3PFL	ACERR	ACFLT
109	C7LINK1	C7LKFAIL	C7SUER	C7COV	
109	C7LINK2	C7ONSET1	C7ONSET2	C7ONSET3	
109	C7LKSET	C7LSUNAU	C7LSFAIL		
109	C7ROUTE	C7TFR	C7TFP	C7TFC1	C7TFC2
		C7TFC3	C7FRCRER		
109	C7RTEST	C7RTUNAU	C7RSUNAU	C7RSFAIL	
110	C7SCCP	C7RTFALL	C7RTFNWF	C7RTFNWC	C7RTFSSF
		C7RTFSSC			
111	ISUPCGRP	ISCKTRAC	ISCKTRAO		
111	ISUPCONN	ISCONBAD	ISCONUCE	ISCONUCC	ISCONCOT
111	ISUPCKTA	ISCKTGBT	ISCKTGBF	ISCKTLBT	ISCKTRBT
112	NSC	NSCTIOVF	NSCSFLTO	NSCFLICM	NSCFLICS
		NSCATMPT			

Table 2-11
Suggested Customized Operational Measurements Output Report For Class ISDN_HRLY

CLASS:	ISDN_HRLY
ACCUMULATING PERIOD:	HRLY
OUTPUT SCHEDULE:	DAYTIME MO FR 7 C00 16 C00
PRECISION:	SINGLE

See Notes Table 2-16	GROUP	REGISTERS			
117	PMTYP *	PMTERR	PMTFLT	PMTSWXFR	PMTSCXFR
		PMTCCTDG	PMCCTFL	PMTPSERR	PMTPSFLT
		PMTSBTCO	PMTCCTOP	PMTINTEG	PMTDRFLT
		PMTDRERR			
117	PMOVLD *	PORGDENY	PTRMDENY		
117	PM1 *	PM1ERR	PM1FLT		
118	ISDNBD	IBDTXDSC	IBDRXDSC	IBDCRC	
	IBNGRP *	NORIGO	DOD	SECINVAL	HLDFRES
		HLDABAN			
118	TRK *	INCATOT	PRERTEAB	INFAIL	NATTMPT
		NOVFLATB	GLARE	OUTFAIL	OUTMTCHF
118	DS1CARR *	DS1LCGA	DS1RCGA	DS1LOF	DS1SLP
		DS1BER	DS1ES	DS1SES	DS1UAS
		DS1AIS			
119	BCAPOF	OFWRNGBC			
119	BCAPCG	CGWRNGBC			
119	ISDNLL	ILLREJTX	ILLREJRX	ILLDISC	ILLLORNR
		ILLRMBSY	ILLNVTE	ILLCRC	ILLPRSBM
119	TRMTCU2	TCUCNAC			
119	LMD *	NTERMATT	NORIGATT	TERMBLK	ORIGFAIL
		PERCLFL	ORIGBLK	ORIGABN	
119	TROUBLEQ	TRBQATT	TRBQOVFL		

* Select ISDN Key Items.

Table 2-12
Suggested Customized Operational Measurements Output Report For Class ISDN_DAY

CLASS:	ISDN_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
117	PMTYP *	PMTERR	PMTFLT	PMTMSBU	PMTUSBU
		PMTMMBU	PMTUMBU	PMTSBP	PMTMBP
		PMTSWXFR	PMTMWXFR	PMTSCXFR	PMTMCXFR
		PMTCCTDG	PMTCCTFL	PMTPSERR	PMTPSFLT
		PMTSBTCO	PMTMBTCO	PMTCCTOP	PMTINTEG
		PMTDRFLT	PMTDRERR	PMTDRMBU	PMTDRSBU
117	PMOVLD *	PORGDENY	PTRMDENY		
117	PM1 *	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
		PM1MBU	PM1SBU		
118	ISDNBD	IBDTXDSC	IBDRXDSC	IBDCRC	
118	IBNGRP *	NORIGO	DOD	SECINVAL	HLDFRES
		HLDABAN			
118	TRK *	INCATOT	PRERTEAB	INFAIL	NATTMPT
		NOVFLATB	GLARE	OUTFAIL	SBU
		MBU	OUTMTCHF		
118	DS1CARR *	DS1LCGA	DS1RCGA	DS1LOF	DS1SLP
		DS1SBU	DS1MBU	DS1PBU	DS1CBU
		DS1BER	DS1ES	DS1SES	DS1UAS
		DS1AIS			
119	BCAPOF	OFWRNGBC			
119	BCAPCG	CGWRNGBC			
119	ISDNLL	ILLREJTX	ILLREJRX	ILLDISC	ILLLORNR
		ILLRMBSY	ILLNVTE	ILLCRC	ILLPRSBM
119	TRMTCU2	TCUCNAC			
119	LMD *	NTERMATT	NORIGATT	TERMBLK	ORIGFAIL
		PERCLFL	ORIGBLK	ORIGABN	
119	TROUBLEQ	TRBQATT	TRBQOVFL		

* Select ISDN Key Items.

Table 2-13
Suggested Customized Operational Measurements Output Report
For Class ISDN_MTH

CLASS:	ISDN_MTH
ACCUMULATING PERIOD:	MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE:	MONTHLY 1 0 C00 1 0 C00
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
117	PMTYP *	PMTERR	PMTFLT	PMTMSBU	PMTUSBU
		PMTMMBU	PMTUMBU	PMTSBP	PMTMBP
		PMTSWXFR	PMTMWXFR	PMTSCXFR	PMTMCXFR
		PMTCCTDG	PMTCCTFL	PMTPSERR	PMTPSFLT
		PMTSBTCO	PMTMBTCO	PMTCCTOP	PMTINTEG
		PMTDRFLT	PMTDRERR	PMTDRMBU	PMTDRSBU
117	PMOVLD *	PORGDENY	PTRMDENY		
117	PM1 *	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
		PM1MBU	PM1SBU		
118	ISDNBD	IBDTXDSC	IBDRXDSC	IBDCRC	
118	IBNGRP *	NORIGO	DOD	SECINVAL	HLDFRES
		HLDABAN			
118	TRK *	INCATOT	PRERTEAB	INFAIL	NATTMPT
		NOVFLATB	GLARE	OUTFAIL	SBU
		MBU	OUTMTCHF		
118	DS1CARR *	DS1LCGA	DS1RCGA	DS1LOF	DS1SLP
		DS1SBU	DS1MBU	DS1PBU	DS1CBU
		DS1BER	DS1ES	DS1SES	DS1UAS
		DS1AIS			
119	BCAPOF	OFWRNGBC			
119	BCAPCG	CGWRNGBC			
119	ISDNLL	ILLREJTX	ILLREJRX	ILLDISC	ILLLORNR
		ILLRMBSY	ILLNVTE	ILLCRC	ILLPRSBM
119	TRMTCU2	TCUCNAC			
119	LMD	NTERMATT	NORIGATT	TERMBLK	ORIGFAIL
	*	PERCLFL	ORIGBLK	ORIGABN	
119	TROUBLEQ	TRBQATT	TRBQOVFL		

* Select ISDN Key Items.

Table 2-14
Suggested Customized Operational Measurements Output Report For Class SPMS_DAY

CLASS:	SPMS_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	CP	CCBSZ	CCBSZ2	CCBOVFL	CPTRAP	CPSUIC
		ORIGDENY	WAITDENY	CPLSZ	CPLSZ2	CPLOOVFL
		CPLPOVFL	OUTBSZ	OUTBOVFL	MULTSZ	MULTOVFL
		WAKESZ	WAKEOVFL	CINITC	WINITC	INITDENY
	EXT	EXTSEIZ	EXTOVFL			
	CP2	ECCBSZ	ECCBOVFL	CPWORKU	INEFDENY	
	DS1CARR	DS1LCGA	DS1RCGA		DS1LOF	DS1SLP
		DS1SBU	DS1MBU	DS1BER	DS1ES	DS1SES
		DS1UAS	DS1A1S			
	PMOVLD	PORGDENY	PTRMDENY			
	CPU	MTCHINT	TRAPINT	CPUFLT	SYSWINIT	SYSCINIT
		MSYLOSSU	SSYLOSSU			
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU	IOCLKMBU
		IOCSBU	IOCMBU			
124	EIOC	EIOCERR	EIOCFLT	EIOCMBU	EIOCSBU	
	CMC	CMCLERR	CMCERR	CMCFLT	CMCLKSBU	CMCLKMBU
		CMCSBU	CMCMBU			
	MTU	MTUERR	MTUFLT	MTUSBU	MTUMBU	
	CSL	CSLERR	CSLSBU	CSLMBU		
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL	NMSPCHFL
		NMCFLT	NMSBU	NMMBU	NMPTSBU	NMPTMBU
		NMJRSBU	NMJRMBU			
	LOGS	SWERRCT	PMSWERCT	PMTRAPCT		
	TS	TS0	TS1	TS2	TS3	TS4
		TS5	TS6	TS7		
	TRMTCU	TCUORSS				
	TRMTCM	TCMATBS				

Table 2-14 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_DAY

CLASS: SPMS_DAY
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	TRMTRS	TSRSNOSC	TRSNBLH	TRSNBLN	TRSEMR1	TRSEMR2
		TRSCQOV	TRSNCRT	TRSNECG	TRSTOVD	TRSEMR3
		TRSNCRT	TRSSORD	TRSGNCT	TRSEMR5	TRSEMR6
		TRSNOSR				
	PMTYP	PMTERR	PMTFLT	PMTMSBU	PMTUSBU	PMTUMBU
		PMTRGFLT	PMTSBTCO	PMMBTCO	PMTCCTOP	PMTINTEG
	PM	PMERR	PMFLT	PMMSBU	PMUSBU	PMUMBU
		PMSBTCO	PMMBTCO	PMCCTOP	PMINTEG	PMRGFLT
	RCVR	RCVSZRS	RCVSZ2	RCVOVFL	RCVQOVFL	RCVQABAN
		RCVSBU	RCVMBU			
	ANN	ANNATT	ANNOVFL	ANNTRU	ANNSBU	ANNMBU
	SVCT	SVCSZRS	SVCSZ2	SVCQOVFL	SVCQABAN	SVCSBU
		SVCMBU				
	STN	STNATTS	STNOVFL	STNMBU	STNSBU	
	ESUP	DESSZRS	DESOVFL	DESTRU	DESSBU	DESMBU
	ONI	ONISBU	ONIMBU			
	FTRQ	FTRQSEIZ	FTRQOVFL			
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY	
	CF6P	CF6SZRS	CF6QOVFL	CF6QABAN	CF6SBU	CF6MBU
	UTR	UTRSZRS	UTRQOVFL	UTRQABAN		
	DTSR	TOTAL	TOTAL_2	DELAY	DELAY_2	
	SITE	LMDT_T	LMDT_D	LCMDP_T	LCMDP_T2	LMDP_T
		LMDP_D	LCMDP_D	LCMDP_D2	LCMDT_T	LCMDT_T2
		LCMDT_D	LCMDT_D2	LCMKS_T	LCMKS_T2	LCMKS_D
		LCMKS_D2	RCTDP_T	RCTDP_T2	RCTDP_D	RCTDP_D2
		RCTDT_T	RCTDT_T2	RCTDT_D	RCTDT_D2	
	TRK	INCATOT	PRERTEAB	INFAIL	NATTMPT	NOVFLATB
		OUTFAIL	SBU	MBU	CONNECT	

Table 2-14 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_DAY

CLASS:	SPMS_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	OFZ	INKLT	INOUT	INOUT2	NIN	NIN2
		OUTNWAT	OUTNWAT2	OUTMFL	OUTRMFL	OUTROSF
		INABNM	INABNC	ORIGLKT	ORIGOUT	ORIGOUT2
		ORIGTRM	ORIGTRM2	NORIG	NORIG2	INTRM
		INTRM2	TRMNWAT	TRMMFL	TRMBLK	ORIGABDN
		TRMNWAT2				
	OFZ2	OFZNCIT	OFZNCTC	OFZNCLT	OFZNCBN	OFZNCID
		OFZNOSC	OFZNCOT	OFZNCRT	OFZNCIM	OFZNCON
		OFZNCOF	PSGM	PDLM		
	OTS	NORG	NORG2	ORGTRM	ORGTRM2	ORGOUT
		ORGOUT2	ORGABDN	ORGLKT	NINC	NINC2
		INCTRM	INCTRM2	INCOUT	INCOUT2	INCABNM
		INCABNC	INCLKT	SYSTRM	SYSOUT	SYSABDN
		SYSLKT				
	SOTS	SOTSPDLM	SOTSPSGM	SOUTNWT	SOUTNWT2	SOUTMFL
		SOUTRMFL	SOUTROSF	STRMNWT	STRMNWT2	STRMMFL
		STRMBLK				
	SYSPERF	TDPCBU	TKBADDG	CINTEGFL	LINPMBU	LINCCTBU
		TRMLNFL	LINBADDG			
	LMD	NTERMATT	NORIGATT	TERMBLK	ORIGFAIL	PERCLFL
		ORIGBLK	ORIGABN			
	CF3P	CNFSZRS	CNFOVFL	CNFQOVFL	CNFQABAN	CNFSBU
		CNFMBU				
	AMA	AMAFREE	AMAROUTE			
	MTERR	LATECHG	BADMDI	METOVFL		
125	ICONF	For International Applications Only				
125	ICWT	For International Applications Only				
125	IFDL	For International Applications Only				
125	IWUC	For International Applications Only				
126	ACSYSTR	ACDMFL	ACCF3PFL	ACERR	ACFLT	
113	CF3P	CNFS2RST	CNFOVFLT	CNFQOVFT	CNFQABNT	CNFSBUT

Table 2-14 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_DAY

CLASS: SPMS_DAY
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
		CNFMBUT	TOPSZRS	TOPSOVFL		
113	TOPSMTCE	POSDF	POSTRKDF	POSDMDF		
113	TOPSUSE	POSMTCE				
113	TOPSVC	UCNMSG				
113	TOPSTRAF	TOPSNIN	TOPSNIN2	TOPSTRK	TOPSTRK2	TOPSCA N
114	AVOFZ	ALORIG	ALORIG2	ALTNWAT	ALTNWAT2	ALTRMMFL
115	AOSS	AOSSOD	AOSSDF			
102	CM	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT	CMTRMISM
		CMTRAP	CMCPUFLT	CMMEMFLT	CMSSCFLT	CMMCSBSY
		CMRCPUFL	CMRMEMFL	CMRSSCFL	CMRMCFL	CMSSMPXU
		CMMSMPXU				
102	MS	MSERR	MSFLT	MSMBU	MSSBU	MSCDERR
		MSCDFLT	MSCDMBU	MSCDSBU	MSPTERR	MSPTFLT
		MSLKMBU	MSLKSBU			
102	SLM	SLMFLT	SLMSBSU	SLMMBSU		
116	SITE2	RCSDP_T	RCSDP_T2	RCSDP_D	RCSDP_D2	RCSDT_T
		RCSDT_T2	RCSDT_D	RCSDT_D2	RCUDP_T	RCUDP_T2
		RCUDP_D	RCUDP_D2	RCUDT_T	RCUDT_T2	RCUDT_D
		RCUDT_D2				
	C7LINK1	CLKFAIL	C7STALFL	C7TLALFL	C7NETCON	C7SLTF L
		C7LKUNAU				
	C7LKSET	C7LSUNAU				
	C7ROUTE	C7TFP	C7FRCRER	C7RTUNAU		
	C7RTESET	C7RSCNGU	C7RSUNAU			
	C7LINK3	C7MSUDSC				
	C7LINK2	C7MSUDC1	C7MSUDC2	C7MSUDC3		

Table 2-14 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_DAY

CLASS: SPMS_DAY
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	C7SCCP	C7RTFALL				
	C7GTWSCR	MSUSCRER				
	ISUPCONN	ISCONUCE	ISCONUCC	ISCONUCA	ISCONUCF	ISCO NCOT
	PM1	PM1FLT	PM1BMU	PM1SBU		
	ENETSYS	ENERR	ENFLT	ENSBU	ENMBU	ENPARU
		ENISCOU				
	ENETMAT	ENCDERR	ENSBCDU	ENPBERR	ENCDFLT	ENMBCDU
		ENPBFLT	ENPBFLT	ENCDPARU	ENCDISOU	ENPBISOU
	ENETPLNK	ENLKERR	ENLKFLT	ENMBLKU	ENLKPARU	
	TENSBLKU	ENLKISOU	ENMPBU			

Table 2-15
Suggested Customized Operational Measurements Output Report For Class SPMS_MTH

CLASS: SPMS_MTH
ACCUMULATING PER   MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	CP	CCBSZ	CCBSZ2	CCBOVFL	CPTRAP	CPSUIC
		ORIGDENY	WAITDENY	CPLSZ	CPLSZ2	CPLOOVFL
		CPLPOVFL	OUTBSZ	OUTBOVFL	MULTSZ	MULTOVFL
		WAKESZ	WAKEOVFL	CINITC	WINITC	INITDENY

Table 2-15 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_MTH

CLASS:	SPMS_MTH
ACCUMULATING PER	MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	EXT	EXTSEIZ	EXTOVFL			
	CP2	ECCBSZ	ECCBOVFL	CPWORKU	INEFDENY	
	DS1CARR	DS1LCGA	DS1RCGA		DS1LOF	D S1SLP
		DS1SBU	DS1MBU	DS1BER	DS1ES	DS1SES
		DS1UAS	DS1A1S			
	PMOVLD	PORGDENY	PTRMDENY			
	CPU	MTCHINT	TRAPINT	CPUFLT	SYSWINIT	SYSCINIT
		MSYLOSSU	SSYLOSSU			
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU	IOCLKMBU
		IOCSBU	IOCMBU			
124	EIOC	EIOCERR	EIOCFLT	EIOCMBU	EIOCSBU	
	CMC	CMCLERR	CMCERR	CMCFLT	CMCLKSBU	CMCLKMBU
		CMCSBU	CMCMBU			
	MTU	MTUERR	MTUFLT	MTUSBU	MTUMBU	
	CSL	CSLERR	CSLSBU	CSLMBU		
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL	NMSPCHFL
		NMCFLT	NMSBU	NMMBU	NMPTSBU	NMPTMBU
		NMJRSBU	NMJRMBU			
	LOGS	SWERRCT	PMSWERC	PMTRAPCT		
	TS	TS0	TS1	TS2	TS3	TS4
		TS5	TS6	TS7		
	TRMTCU	TCUORSS				
	TRMTCM	TCMATBS				
	TRMTRS	TRSNOSC	TRSNBLH	TRSNBLN	TRSEMR1	TRSEMR2
		TRSCQOV	TRSNCRT	TRSNECG	TRSTOVD	TRSEMR3
		TRSNCRT	TRSSORD	TRSGNCT	TRSEMR5	TRSEMR6
		TRSNOSR				
	PMTYP	PMTERR	PMTFLT	PMTMSBU	PMTUSBU	PMTUMBU
		PMTRGFLT	PMTSBTCO	PMMBTCO	PMTCCTOP	PMTINTEG
	PM	PMERR	PMFLT	PMMSBU	PMUSBU	PMUMBU
		PMSBTCO	PMMBTCO	PMCCTOP	PMINTEG	PMRGFLT
	RCVR	RCVSZRS	RCVSZ2	RCVOVFL	RCVQOVFL	RCVQABAN
		RCVSBU	RCVMBU			

Table 2-15 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_MTH

CLASS:	SPMS_MTH
ACCUMULATING PER	MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	ANN	ANNATT	ANNOVFL	ANNTRU	ANNSBU	ANNMBU
	SVCT	SVCSZRS	SVCSZ2	SVCQOVFL	SVCQABAN	SVCSBU
		SVCMBU				
	STN	STNATTS	STNOVFL	STNMBU	STNSBU	
	ESUP	DESSZRS	DESOVFL	DESTRU	DESSBU	DESMBU
	ONI	ONISBU	ONIMBU			
		FTRQ	FTRQSEIZ	FTRQOVFL		
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY	
	CF6P	CF6SZRS	CF6QOVFL	CF6QABAN	CF6SBU	CF6MBU
	UTR	UTRSZRS	UTRQOVFL	UTRQABAN		
	DTSR	TOTAL	TOTAL_2	DELAY	DELAY_2	
	SITE	LMDT_T	LMDT_D	LCMDP_T	LCMDP_T2	LMDP_T
		LMDP_D	LCMDP_D	LCMDP_D2	LCMDT_T	LCMDT_T2
		LCMDT_D	LCMDT_D2	LCMKS_T	LCMKS_T2	LCMKS_D
		LCMKS_D2	RCTDP_T	RCTDP_T2	RCTDP_D	RCTDP_D2
		RCTDT_T	RCTDT_T2	RCTDT_D	RCTDT_D2	
	TRK	INCATOT	PRERTEAB	INFAIL	NATTMPT	NOVFLATB
		OUTFAIL	SBU	MBU	CONNECT	
	OFZ	INKLT	INOUT	INOUT2	NIN	NIN2
		OUTNWAT	OUTNWAT2	OUTMFL	OUTRMFL	OUT ROSF
		INABNM	INABNC	ORIGLKT	ORIGOUT	ORIGOUT2
		ORIGTRM	ORIGTRM2	NORIG	NORIG2	INTRM
		INTRM2	TRMNWAT	TRMMFL	TRMBLK	ORIGABDN
		TRMNWAT2				
	OFZ2	OFZNCIT	OFZNCTC	OFZNCLT	OFZNCBN	OFZNCID
		OFZNOSC	OFZNCOT	OFZNCRT	OFZNCIM	OFZNCON
		OFZNCOF	PSGM	PDLM		
	OTS	NORG	NORG2	ORGTRM	ORGTRM2	ORGOUT
		ORGOUT2	ORGABDN	ORGLKT	NINC	NINC2
		INCTRM	INCTRM2	INCOUT	INCOUT2	INCABNM
		INCABNC	INCLKT	SYSTRM	SYSOUT	SYSABDN
		SYSLKT				
	SOTS	SOTSPDLM	SOTSPSGM	SOUTNWT	SOUTNWT2	SOUTMFL
		SOUTRMFL	SOUTROSF	STRMNWT	STRMNWT2	STRMMFL
		STRMBLK				

Table 2-15 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_MTH

CLASS:	SPMS_MTH
ACCUMULATING PER	MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
	SYSPERF	TDPCBU TRMLNFL	TKBADDG LINBADDG	CINTEGFL	LINPMBU	LINCCTBU
	LMD	NTERMATT ORIGBLK	NORIGATT ORIGABN	TERMBLK	ORIGFAIL	PERCLFL
	CF3P	CNFSZRS CNFMBU	CNFOVFL	CNFQOVFL	CNFQABAN	CNFSBU
	AMA	AMAFREE	AMAROUTE			
	MTERR	LATECHG	BADMDI	METOVFL		
125	ICONF	For International Applications Only				
125	ICWT	For International Applications Only				
125	IFDL	For International Applications Only				
125	IWUC	For International Applications Only				
126	ACSYSTR	ACDMFL	ACCF3PFL	ACERR	ACFLT	
113	CF3P	CNFS2RST CNFMBUT	CNFOVFLT TOPSZRS	CNFQOVFT TOPSOVFL	CNFQABNT	CNFSBUT
113	TOPSMTCE	POSDF	POSTRKDF	POSDMDF	TOPSTRK2	TOPSCA N
113	TOPSUSE	POSMTCE	TOPSNIN2	TOPSTRK		
113	TOPSVC	UCNMSG				
113	TOPSTRAF	TOPSNIN				
114	AVOFZ	ALORIG	ALORIG2	ALTNWAT	ALTNWAT2	ALTRMMFL
115	AOSS	AOSSOD	AOSSDF			
102	CM	CMSWINIT CMTRAP CMRCPUFL CMMSMPXU	CMMWINIT CMCPUFLT CMRMEMFL	CMSCINIT CMMEMFLT CMRSSCFL	CMMCINIT CMSSCFLT CMRMCFL	CMTRMISM CMMCSBSY CMSSMPXU
102	MS	MSERR MSCDFLT MSLKMBU	MSFLT MSCDMBU MSLKSBU	MSMBU MSCDSBU	MSSBU MSLKERR	MSCDERR MSPTFLT
102	SLM	SLMFLT	SLMSBSU	SLMMBSU		

Table 2-15 (continued)
Suggested Customized Operational Measurements Output Report For Class SPMS_MTH

CLASS: SPMS_MTH
ACCUMULATING PER   MONTHLY 1 0 C00 1 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS				
116	SITE2	RCSDP_T	RCSDP_T2	RCSDP_D	RCSDP_D2	RCSDT_T
		RCSDT_T2	RCSDT_D	RCSDT_D2	RCUDP_T	RCUDP_T2
		RCUDP_D	RCUDP_D2	RCUDT_T	RCUDT_T2	RCUDT_D
		RCUDT_D2				
	C7LINK1	CLKFAIL	C7STALFL	C7TLALFL	C7NETCON	C7S LTFL
		C7LKUNAU				
	C7LKSET	C7LSUNAU				
	C7ROUTE	C7TFP	C7FRCRER	C7RTUNAU		
	C7RTESET	C7RSCNGU	C7RSUNAU			
	C7LINK3	C7MSUDSC				
	C7LINK2	C7MSUDC1	C7MSUDC2	C7MSUDC3		
	C7SCCP	C7RTFALL				
	C7GTWSCR	MSUSCRER				
	ISUPCONN	ISCONUCE	ISCONUCC	ISCONUCA	ISCONUCF	ISCO NCOT
	PM1	PM1FLT	PM1BMU	PM1SBU		

Table 2-16
Reference Notes For Table 2-6 through Table 2-32 For Customized Operational Measurement Output Reports

101	Tailor key OM data and classes to meet the needs of individual switch configurations such as: SuperNode, ISDN Service, Meridian Digital Centrex, SS7 Signaling and DMS-STP.
102	When equipped with SuperNode, use MS, CM, and SLM groups.
103	When equipped with standard NT40, use CPU and CMC groups.
104	The following peripheral equipment types are included in the OM groups as follows: PM & PMTYP –ADTC, DCM, LM, TM, CSC, DLM, DTC, IDTC, ILGC, ILTC, IPML, LCM, LGC, LTC, MSB6, MSB7, PDTC, RCC, RCS, RCT, RMSC, SMR, SMS; PM1 –ST6, ST7, DCH, PH1, LIU7
105	Use OMACC key function to select required peripheral equipment listed in note 104.
106	When equipped with TOPS, add groups TOPSMTCE and TOPSMISC.
107	When equipped with AOSS, add group AOSS.
108	MDC consoles – see the *System Products* section of this manual.
109	When equipped with SS7 (MTP [Message Transfer Parts] levels 1, 2 & 3).
110	When equipped with SS7 (SCCP [Signaling Connection Control Part] level 3).
111	When equipped with ISUP (SS7 ISDN User Part [ISUP] level 4).
112	When an SSP (Service Switching Point).
113	When equipped with TOPS.
114	When equipped with AUTOVON.
115	When equipped with AOSS.
116	When equipped with SLC-96 or Subscriber Module Urban (SMU), add group SITE-2.
117	ISDN Peripheral Module Maintenance – Select key ISDN items.
118	ISDN Trunk and Carrier Maintenance – Select key ISDN items.
119	ISDN Loop Maintenance – Select key ISDN items.
120	Specify TM type 2, 4, or 8.
121	Threshold and scan time selected for voice application.
122	Suggest using the OM Threshold feature to alert maintenance personnel of intermittent or persistent T1 carrier problems. Add persistent or intermittent T1 systems to the OMTHRESH table and enable (alarm, scan time, and threshold). A threshold of one and scan time of one second will generate an immediate alarm and log message. Once the problem is corrected, remove from table and replace with the next most chronic T1 carrier system.
123	Avoid any OM register duplication between tables OMTHRESH and ALARMTAB (see "OM thresholding feature" within this subsection for an explanation.
124	When equipped with EIOC, use EIOC OM Group

Table 2-16 (continued)
Reference Notes For Table 2-6 through Table 2-32 For Customized
Operational Measurement Output Reports

125	International switches.
126	Use when attendant consoles are present.
127	See OM group VSNCOM which supersedes AABS group and registers.
128	Directory Assistance Application
129	TMS configuration
130	Monitor TMS peripheral hardware performance using OM group PMTYPE described in another table
131	Tailor OM data to meet the needs of the individual TOPS configuration—such as integrated MP, or optional features such as AABS, ACTS, etc.

Table 2-17
Suggested Maintenance Operational Measurements Class Assignments,
Accumulators, and Output Schedule

See Notes Below	CLASS	ACCUMULATE	OUTPUT	USER	SEE TABLE
1	SSP_HRLY	HRLY C00	AUTO	MTCE	2-21
1	SSP_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-22
1,3	SSP_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	
2	STP_HRLY	HRLY C00	AUTO	MTCE	2-23
2	STP_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-24
2,3	STP_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	
1,2,3	7_SPMS_D	DAILY 0 C00 0 C00	AUTO	MTCE	2-25
2,3	7_SPMS_D	DAILY 0 C00 0 C00	AUTO	MTCE	2-26
1,2,5	C7SLMPR	HRLY C 00	AUTO	MTCE	2-27
4	SEAS_30M	HALFHOURLY C 00	AUTO	SEAS	2-28
4	SEAS_60M	HRLY C00	AUTO	SEAS	2-29
4	SEAS_24H	HALFHOURLY C00	AUTO	SEAS	2-30
	SW_HRLY	HRLY C00	AUTO	MTCE	2-9
	SW_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-10
7	SW_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-11
	L/T/C D	DAILY 0 C00 0 C00	AUTO	MTCE	2-12

Table 2-17 (continued)
Suggested Maintenance Operational Measurements Class Assignments, Accumulators, and Output Schedule

See Notes Below	CLASS	ACCUMULATE	OUTPUT	USER	SEE TABLE
7	L/T/C M	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-13
	ISDN_HRLY	HRLY C00	AUTO	MTCE	2-15
	ISDN_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-14
7	SW_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-15
	L/T/C D	DAILY 0 C00 0 C00	AUTO	MTCE	2-14
7	L/T/C M	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-13
	ISDN_HRLY	HRLY C00	AUTO	MTCE	2-15
	ISDN_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-14
7	ISDN_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-16
7	SPMS_DAY	DAILY 0 C00 0 C00	AUTO	MTCE	2-17
7	SPMS_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	2-18
	TOPS_HRLY	HRLY C00	AUTO	MTCE	Table 2-28
	TOPS_ DAY	DAILY 0 C00 0 C00	AUTO	MTCE	Table 2-29
8	TOPS_MTH	MONTHLY 1 0 C00 1 0 C00	AUTO	MTCE	

NOTES:
1. For SP & SSP nodes. May be incorporated into existing switch class assignments.
2. For STP nodes.
3. Setup for monthly accumulate using day OM register selection.
4. For STP nodes with SEAS application. Set OM history to "Y" in table OFCOPT.
   NTP 297-8101-814, *DMS SuperNode STP Operational Measurement Manuals* describe the OM groups and registers needed for SEAS.
5. Not required when SLMPR feature is operational. See the "SS7 Maintenance" subsection, within the *System Products* section, for a description of the SLMPR feature.
6. C7LINK3 OM Group is reported by individual signaling link.
7. Modify to align with your company's report period.
8. Setup for monthly accumulate using day OM register selection

GENERAL NOTES:
Tailor CLASS and OM data to meet the needs of individual switch configurations, such as: SuperNode, ISDN Service, Meridian Digital Centrex, SS7, and DMS-STP.

For other output times, use the "MONTH" model and change the ACCUMULATE and OUTPUT information to the desired time interval.

SW_DAY, SW_WKLY, SW_MTH classes are not required when SPMS is used.

Use of the suppress zero option will greatly reduce the volume of the output reports.

Table 2-18
Suggested SS7 Customized Operational Measurements Output Report For Class SSP_HRLY

CLASS:	SSP_HRLY
ACCUMULATING PERIOD:	HRLY C00
OUTPUT SCHEDULE:	DAYTIME MO FR 7 C00 16 C00
PRECISION:	SINGLE

See Notes in Table 2-17	GROUP	REGISTERS			
Note 5	C7LINK1	C7SUERR	C7NACKRX	C7AUTOCO	
	C7LINK1	C7LKFAIL C7LINH	C7LKUNAU C7RIHN	C7MANB	C7BSYON
	C7LINK2	C7MSUDSC C7MSURX	C7MSUDC1 C7MSURX2	C7MSUDC2 C7MSUTX	C7MSUDC3 C7MSUTX2
	C7LKSET	C7LSUNAU			
	C7ROUTE	C7RTUNAU			
	C7RTESET	C7RSFAIL			
	C7SCCP	C7RTFAIL			
	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
	PMTYP	PMTERR PMTSCXFR PMTDRERR	PMTFLT PMTMCXFR	PMTCCTFL	PMTDRFLT

Table 2-19
Suggested Additional SS7 Customized Operational Measurements Output Report For Class SSP_DAY

CLASS:	SSP_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
Note 5	C7LINK1	C7LKSYNU C7EXERR C7NACKRX C7NUCFL C7SLTFL C7LPO	C7LKFAIL C7EXCONG C7STALFL C7COV C7BSYON C7RPO	C7ABNRFB C7ALIGNF C7TLALFL C7LKUNAU C7LINH C7AUTOCO	C7EXDLAY C7SUERR C7NETCONN C7MANBY C7RINH

Table 2-19 (continued)
Suggested Additional SS7 Customized Operational Measurements Output Report For Class SSP_DAY

CLASS:	SSP_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
	C7LINK2	C7MSUDSC C7MSURX	C7MSUDC1 C7MSURX2	C7MSUDC2 C7MSUTX	C7MSUDC3 C7MSUTX2
	C7LKSET	C7LSUNAU			
	C7ROUTE	C7RTUNAU			
	C7RTESET	C7RSFAIL	C7RSMANB	C7RSCNGU	
	C7SCCP	C7RTFALL C7RTFNWC C7SYNERR	C7RTFNTN C7RTFSSF	C7RTFNTA C7RTFSSC	C7RTFNWF C7RTFUEQ
	ISUPERRS	ISERRSC ISERRRLC	ISERRGRS ISERRREL	ISERRBLO	ISERRBAD
	TRK	INCATOT OUTFAIL	INFAIL SBU	NATTMPT MBU	GLARE OUTMTCHF
	NSC	NSCORIG	NSCATIN	NSCFPRIQ	
	PM1	PM1ERR PM1MBU	PM1FLT PM1SBU	PM1INITS	PM1LOAD
	PMTYP	PMTERR PMTSCXFR PMTUMBU PMTMBTCO PMTDRMBU	PMTFLT PMTMCXFR PMTMSBU PMTINTEG PMTDRSBU	PMTCCTFL PMTMMBU PMTDRFLT	PMTUSBY PMTSBTCO PMTDRERR

Table 2-20
Suggested Additional SS7 Customized Operational Measurements Output Report For Class STP_HRLY

CLASS: STP_HRLY
ACCUMULATING PERIOD: HRLY C00
OUTPUT SCHEDULE: DAYTIME MO FR 7 C00 16 C00
PRECISION: SINGLE

See Notes in Table 2-17	GROUP	REGISTERS			
	MS	MSERR MSLKERR	MSFLT MSLKFLT	MSCDERR	MSCDFLT
	CM	CMTRMISM CMSSCFLT	CMTRAP	CMCPUFLT	CMMEMFLT
	SLM	SLMFLT	SLMSBSU	SLMMBSU	
	IOC	IOCERR	IOCLKERR	IOCFLT	
	DDU	DDUERROR	DDUFAULT		
	NMC	NMMSGER NMSPCHFL	NMSPCHER NMCFLT	NMCERR	NMMSGFL
	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
	PMTYP	PMTERR	PMTFLT	PMTSCXFR	PMTMCXFR
Note 5	C7LINK1	C7SUERR	C7NACKRX	C7AUTOCO	
	C7LINK1	C7LKFAIL C7LINH	C7LKUNAU C7RIHN	C7MANB	C7BSYON
	C7LINK2	C7MSUDSC C7MSURX C7MSGLOS	C7MSUDC1 C7MSURX2 C7MSGMSQ	C7MSUDC2 C7MSUTX	C7MSUDC3 C7MSUTX2
Note 6	C7LINK3	C7MSOR C7MSTS	C7MSOR2 C7MSTS2	C7MSTE C7MSUBOV	C7MSTE2
	C7LKSET	C7LSUNAU			
	C7MTP	C7MSISIO	C7MSIDPC		
	C7ROUTE	C7RTUNAU			
	C7RTESET	C7RSFAIL			
	C7SCCP	C7RTFALL			
	C7GTWSCR	MSUDSCRD			

Table 2-21
Suggested Customized Operational Measurements Output Report For Class STP_DAY

CLASS:	STP_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
	MS	MSERR	MSFLT	MSMBU	MSSBU
		MSCDERR	MSCDFLT	MSCDMBU	MSCDSBU
		MSLKERR	MSLKFLT	MSLKMBU	MSLKSBU
	CM	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT
		CMTRMISM	CMTRAP	CMCPUFLT	CMMEMFLT
		CMSSCFLT	CMMCSBSY	CMRCPUFL	CMRMEMFL
		CMRSSCFL	CMRMCFL	CMSSMPXU	CMMSMPXU
	SLM	SLMFLT	SLMSBSU	SLMMBSU	
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU
		IOCLKMBU	IOCSBU	IOCMBU	
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL
		NMSPCHFL	NMCFLT	NMSBU	NMMBU
		NMPTSBU	NMPTMBU	NMJRSBU	NMJRMBU
	PM1	PM1ERR	PM1FLT	PM1INITS	PM1LOAD
		PM1MBU	PM1SBU		
	PMTYP	PMTERR	PMTFLT	PMTSCXFR	PMTMCXFR
		PMTUSBY	PMTUMBU	PMTMSBU	PMTMMBU
		PMTSBTCO	PMTMBTCO	PMTINTEG	
Note 5	C7LINK1	C7LKSYNU	C7LKFAIL	C7ABNRFB	C7EXDLAY
		C7EXERR	C7EXCONG	C7ALIGNF	C7SUERR
		C7NACKRX	C7STALFL	C7TLALFL	C7NETCON
		C7NUCFL	C7COV	C7LKUNAU	C7MANBY
		C7SLTFL	C7BSYON	C7LINH	C7RINH
		C7LPO	C7RPO	C7AUTOCO	
	C7LINK2	C7MSUDSC	C7MSUDC1	C7MSUDC2	C7MSUDC3
		C7MSURX	C7MSURX2	C7MSUTX	C7MSUTX2
		C7MSGLOS	C7MSGMSQ		
Note 6	C7LINK3	C7MSOR	C7MSOR2	C7MSTE	C7MSTE2
		C7MSTS	C7MSTS2	C7MSUBOV	
	C7LKSET	C7LSUNAU			

Table 2-21 (continued)
Suggested Customized Operational Measurements Output Report For Class STP_DAY

CLASS:	STP_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
	C7MTP	C7MSISIO	C7MSIDPC		
	C7ROUTE	C7RTUNAU			
	C7RTESET	C7RSFAIL	C7RSMANB	C7RSCNGU	
	C7SCCP	C7RTFALL	C7RTFNTN	C7RTFNTA	C7RTFNWF
		C7RTFNWC	C7RTFSSF	C7RTFSSC	C7RTFUEQ
		C7SYNERR			
	C7GTWSCR	MSUDSCRD			

Table 2-22
Suggested SS7 Customized Operational Measurements Output Report For Class 7_SPMS_D for SP/SSP/STP Offices

CLASS:	7_SPMS_D
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
Note 5	C7LINK1	C7LKFAIL	C7STALFL	C7TLALFL	C7NETCON
		C7SLTFL	C7LKUNAU		
	C7LINK2	C7MSUTX	C7MSUTX2	C7MSURX	C7MSURX2
		C7MSUDSC	C7MSUDC1	C7MSUDC2	C7MSUDC3
	C7LKSET3	C7LSUNAU			
	C7LKSET	C7LSUNAU			
	C7ROUTE	C7RTUNAU	C7TFP	C7FRCRER	
	C7RTESET	C7RSUNAU	C7RSCNGU		
	C7SCCP	C7RTFALL	C7MSGHDL	C7MSGHD2	
	ISUPCONN	ISCONUCE	ISCONUCC	INSCONUCA	ISCONUCF

Table 2-22 (continued)
Suggested SS7 Customized Operational Measurements Output Report For Class 7_SPMS_D for SP/SSP/STP Offices

CLASS: 7_SPMS_D
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS
	NOTE: ISUPCONN applies to SSP nodes only.	

Table 2-23
Suggested Additional SS7 Customized Operational Measurements Output Report For Class 7_SPMS_D for STP Offices Only

CLASS: 7_SPMS_D
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS			
	CM	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT
		CMTRMISM	CMTRAP	CMCPUFLT	CMMEMFLT
		CMSSCFLT	CMMCSBSY	CMRCPUFL	CMRMEMFL
		CMRSSCFL	CMRMCFL	CMSSMPXU	CMMSMPXU
	MS	MSERR	MSFLT	MSMBU	MSSBU
		MSCDERR	MSCDFLT	MSCDMBU	MSCDSBU
		MSLKERR	MSLKFLT	MSLKMBU	MSLKSBU
	IOC	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU
		IOCLKMBU	IOCSBU	IOCMBU	
	NMC	NMMSGER	NMSPCHER	NMCERR	NMMSGFL
		NMSPCHFL	NMCFLT	NMSBU	NMMBU
		NMPTSBU	NMPTMBU	NMJRSBU	NMJRMBU
	DDU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY

Table 2-24
Suggested SS7 Customized Operational Measurements Output Report For Class C7SLMPR

CLASS: C7SLMPR
ACCUMULATING PERIOD: HRLY
OUTPUT SCHEDULE: C00
PRECISION: SINGLE

See Notes in Table 2-17	GROUP	REGISTERS		
	C7LINK1	C7SUERR	C7NACKRX	C7AUTOCO

Table 2-25
Suggested SS7 Customized Operational Measurements Output Report For Class SEAS_30M

CLASS: SEAS_30M
ACCUMULATING PERIOD: HALFHOURLY C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-17	GROUP	REGISTERS		
	C7LINK2	C7MSUOR	C7MSUOR2	C7MSUTE	C7MSUTE2
		C7MSUTS	C7MSUTS2	C7MSUDC1	C7MSUDC2
		C7MSUDC3	C7ONSET1	C7ONSET2	C7ONSET3
		C7MSUTX2	C7MSURX	C7MSURX2	C7BYTTX
		C7BYTTX2	C7BYTRX	C7BYTRX2	C7BYTRT
		C7BYTRT2			
	C7SCCP	C7MSGGT	C7MSGGT2	C7RTFNTN	C7RTFNTA
	C7LKSET	C7LSUNAU			
	C7LINK3	C7MSOR	C7MSOR2	C7MSTE	C7MSTE2
		C7MSTS	C7MSTS2	C7MSUBOV	C7LV1CGU
		C7LV2CGU	C7LV3CGU	C7LPOU	C7RPOU
	C7MTP	C7MSIDPC	C7MSISIO		

Table 2-26
Suggested SS7 Customized Operational Measurements Output Report For Class SEAS_60M

CLASS: SEAS_60M
ACCUMULATING PERIOD: HOURLY C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
Note 5	C7LINK1	C7LKSYNU	C7SUERR	C7NACKRX	C7COV
	C7LINK2	C7BYTRX	C7BYTRX2	C7BYTTX	C7BYTTX2
		C7MSURX	C7MSURX2	C7MSUTX	C7MSUTX2
		C7MSUTE	C7MSUTE2	C7MSUOR	C7MSUOR2
		C7MSUTS	C7MSUTS2		
Note 6	C7LINK3	C7MSOR	C7MSOR2	C7MSTE	C7MSTE2
		C7MSTS	C7MSTS2	C7MSUBOV	C7LV1CGU
		C7LV2CGU	C7LV3CGU	C7LPOU	C7RPOU
	C7MTP	C7MSIDPC	C7MSISIO		

Table 2-27
Suggested SS7 Customized Operational Measurements Output Report For Class SEAS_24H

CLASS: SEAS_24H
ACCUMULATING PERIOD: DAILY 0 C00 0 C00
OUTPUT SCHEDULE: AUTO
PRECISION: DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS			
Note 5	C7LINK1	C7LKSYNU	C7LKUNAU	C7SUERR	C7NACKRX
		C7COV	C7LINH	C7RINH	C7LKFAIL
		C7ABNRFB	C7EXDLAY	C7EXERR	C7EXCONG
	C7LINK2	C7BYTRX	C7BYTRX2	C7BYTTX	C7BYTTX2
		C7BYTRT	C7BYTRT2	C7MSURX	C7MSURX2
		C7MSUTX	C7MSUTX2	C7MSUOR	C7MSUOR2
		C7MSUTE	C7MSUTE2	C7MSUTS	C7MSUTS2
		C7ONSET1	C7ONSET2	C7ONSET3	C7MSUDC1
		C7MSUDC2	C7MSUDC3		
	C7SCCP	C7MSGGT	C7MSGGT2	C7RTFNTN	C7RTFNTA

Table 2-27 (continued)
Suggested SS7 Customized Operational Measurements Output Report For Class SEAS_24H

CLASS:		SEAS_24H		
ACCUMULATING PERIOD:		DAILY 0 C00 0 C00		
OUTPUT SCHEDULE:		AUTO		
PRECISION:		DOUBLE		

See Notes in Table 2-16	GROUP	REGISTERS			
Note 6	C7LINK3	C7MSOR	C7MSOR2	C7MSTE	C7MSTE2
		C7MSTS	C7MSTS2	C7MSUBOV	C7LV1CGU
		C7LV2CGU	C7LV3CGU	C7LPOU	C7RPOU
	C7MTP	C7MSIDPC	C7MSISIO		

Table 2-28
Suggested TOPS Customized Operational Measurements Output Report For Class TOPS_HRLY

CLASS:	TOPS_HRLY
ACCUMULATING PERIOD:	HRLY C00
OUTPUT SCHEDULE:	DAYTIME MO FR 7 C00 16 C00
PRECISION:	SINGLE

See Notes in Table 2-16	GROUP	REGISTERS
	ANN	ANNOVL
	ACCSBNS	BNSACGBL, BNSDBFC, BNSMISCF
	CDACT	ACTSFAIL
	CDMCCS	MCCSFAIL
	CF3P	CNFOVFLT, CNFQOCCT
	CF6P	CF6OVFL, CF6QOVFL
	DALINK	MSGSNDFL, AUTINTFL, INTFLTTO, OHIMPOSE
Note128	MPCBASE	RESETL2, RESETL,3 CONVERR, BDAPPERR
	MPCFASTA	LLNKXFRD
	MPCLINK2	L2PABORT, L2PSYNC, L2PHWERR, L2LACKTO, L2LRXMIT L2MSGLST
	MPCLINK3	L3PABORT, L3PSYNC, L3PHWERR, L3LACKTO, L3LRXMIT L3MSGLST
	RCVR	RCVOVFL, RCVQOVFL

Table 2-28 (continued)
Suggested TOPS Customized Operational Measurements Output Report For Class TOPS_HRLY

CLASS:		TOPS_HRLY
ACCUMULATING PERIOD:		HRLY C00
OUTPUT SCHEDULE:		DAYTIME MO FR 7 C00 16 C00
PRECISION:		SINGLE

See Notes in Table 2-16	GROUP	REGISTERS
	TDCPROT	L1BFOV, L1NIT, L1RXABRT, L1RXCRC, L1RXERR, L1TXERR L2RTX1, L2SETUP
	TDCROUT	DMDICS, IBMDISC
Notes 129 & 130	TOPSMISC	RONITBL
	TOPSMTCE	POSD, POSDF, POSDMDF, POSTRKDF
	TOPSPARS	PARSFAIL
	TOPSVC	MSGLOST, OPRLOST, VCFL
	VSNCOM	VSNDABT, VSNIDFL, VSNIVFL, VSNNOV,L VSNVABI, VSNABT

Table 2-29
Suggested TOPS Customized Operational Measurements Output Report For Class TOPS_DAY

CLASS:		TOPS_DAY
ACCUMULATING PERIOD:		DAILY 0 C00 0 C00
OUTPUT SCHEDULE:		AUTO
PRECISION:		DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS
	ANN	ANNOVL, ANNMBU, ANNSBU
	AABS	
	ACCSBNS	BNSACGBL, BNSDBFC, BNSSPTRA
Note 127	CDACTS	ACTSFAIL, ACTSTEST
	CDMCCS	MCCSFAIL
	CF3P	CNFMBUT, CNFOVFLT, CNFQOCCT, TOPSOVL
	CF6P	CF6MBU, CF6OVFL, CF6QOVFL

Table 2-29 (continued)
Suggested TOPS Customized Operational Measurements Output Report For Class TOPS_DAY

CLASS:	TOPS_DAY
ACCUMULATING PERIOD:	DAILY 0 C00 0 C00
OUTPUT SCHEDULE:	AUTO
PRECISION:	DOUBLE

See Notes in Table 2-16	GROUP	REGISTERS
	DALINK	MSGSNDFL, AUTINTFL, INTFLTTO, OHIMPOSE
	MPCBASE	MPCNSSBU, MPCNSMBU, RESETL2, RESETL3 CONVERR, LOSTMSGS, BDAPPERR
	MPCFASTA	LLNKXFRD, FAOUTFLD
Note 128	MPCLINK2	L2PABORT, L2PSYNC, L2PHWERR, L2LDOWN L2LACKTO, L2LRXMIT, L2LLVIO, L2LRVIO L2MSGLST
	MPCLINK3	L3PABORT, L3PSYNC, L3PHWERR, L3LDOWN L3LACKTO, L3LRXMIT, L3LLVIO, L3LRVIO L3MSGLST
	RCVR	RCVMBU, RCVOVFL, RCVQOVFL, RCVSBU
	TDCPROT	L1BFOV, L1NIT, L1RXABRT, L1RXCRC L1RXERR, L1RXOVRN, L1TXERR, L2FRMRRX L2FRMRTX, L2RTXI, L2SETUP, L2T1TIME L3PDTIME
	TDCROUT	DAVGDBM, DMDISC, IBMDISC
Notes 129 & 130	TOPSMISC	RONITEL, TBLREPORT
	TOPSMTCE	POSD, POSDF, POSDMDF, POSTRKDF
	TOPSPARS	PARSFAIL
	TOPSSUSE	POSMTCE
	TOPSSVC	MSGLOST, OPRLOST, VCDEF, VCFL
Note 127	VSNCOM	VSNDABT, VSNIDFL, VSNIVF,L VSNNOVL VSNVABI, VSNVABT

OM thresholding feature

Introduction

The purpose of OM thresholding is to provide real-time switch surveillance by measuring key OM maintenance registers against pre-set bogeys and a scan time interval. The OM registers, bogeys, scan times, and alarm settings are determined and set by the switch maintenance personnel. Each user group determines the OM data required to manage their job. Groups responsible for service should identify key OMs for real-time surveillance and action. Using the maintenance force as an example, approximately 80 OM fields have been identified as key OMs for real-time switch surveillance and are listed in Table 2-31.

Since the OM thresholding feature is automated, it relieves the technician from manually reviewing OM printouts for the initial fault detection process. OM thresholding can be a very powerful tool for real-time troubleshooting, or when there is a need to be alerted to a potential problem.

Table administration

Two tables are used to control OM thresholding (ALARMTAB and OMTHRESH). Both tables have identical functions, except that ALARMTAB is an existing read-only table and OMTHRESH is a read-write table for the operating company's use. Thresholding may be done for a maximum of 128 selectable OMs in table OMTHRESH, and an equal number in table ALARMTAB.

Avoid any OM register duplication between tables OMTHRESH and ALARMTAB. NTP 297-YYYY-350, *DMS-100F Translation Guides* list the OM registers assigned to ALARMTAB that are pre-datafilled by Nortel Networks. Assigned to table ALARMTAB are OM registers that are to be alarmed if pegged once, such as: CCBOVFL$0, CPLOOVFL$0, CPLPOVFL$0, OUTBOVFL$0, MULTOVFL$0, RCVQOVFL$RCVRDGT, RCVQOVFL$RCVRMF, WAKEOVFL$0, and EXTOVFL$1 to 30.

It is recommended that the following registers related to Common Channel Signaling System 7 (CCS7) be added either to the ALARMTAB or OMTHRESH table:

- E800_TCAP_EXT_BLK
- ISUP_EXTENSION_BLOCK
- ACCS_TCAP_EXT_BLK
- TC_AP_SMALL_EXT
- TC_AP_LARGE_EXT_BLK
- TC_AP_XLARGE_EXT_BLK
- TC_AP_MEDIUM_EXT_BLK
- PVN_TCAP_EXT_BLK

For the registers listed above, see NTP 297-YYYY-814, *DMS-100F Operational Measurements Manuals* for a list of the registers and their index numbers within the EXT OM group. See NTP 297-YYYY-350, *DMS-100F Translation Guides* for a description of tables ALARMTAB and OMTHRESH, and NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System Application Guide* for additional supporting information.

ALARMTAB is a read-only table normally controlled by Nortel Networks. Changes or additions must be arranged through your technical support organization. Assign OM threshold indicators with registers that are unlikely to change (i.e. alarm on one peg) or have special uses (i.e. slow dial tone problems that are detected with registers ORIGABDN$0 and ORIGFAIL$XX). Assign OMs with variable pegs to the OMTHRESH table since it is a read-write table.

OM thresholding logs and alarms

Log OM2200 is generated whenever a specified threshold in table OMTHRESH or ALARMTAB is equalled or exceeded. Visual and audible alarms are also generated with the log message and are based upon the ALMLEVEL field setting in table OMTHRESH or ALARMTAB. The alarm level can be defined as critical, major, minor, or no-alarm. The visual-alarm indicator appears under the EXT status display. The EXT level of the MAP is used to clear visual and audible alarms.

OM2200 log report

The OM thresholding feature generates an OM2200 log report whenever an OM threshold condition stored in table ALARMTAB or OMTHRESH has been equalled or exceeded.

Following is an example of an OM2200 log report:

```
 **  OM2200 JAN2209:50:32 9842 INFO OM THRESHOLD EXCEEDED ON   TMERR$O
      THRESHOLD = 1500        DELTA = 1627          SCANTIME = 8
 (1)                (3)                (4)                    (5)      (2)
```

Report explanation:

1. Alarm level from table OMTHRESH or ALARMTAB

Possible entries:	DMS-100F	SCCS
	= No Alarm	= No Alarm
	* = Minor	* = Minor
	** = Major	** = Major
	*** = Critical	*C = Critical

2. The name of the OM register exceeding its threshold value

3. Threshold value for that OM from table OMTHRESH or ALARMTAB

4. The number of events that have occurred within the last scan interval

5. The scan time value for that OM from table OMTHRESH or ALARMTAB

NOTE: The OM2200 log message is stored in the Logutil system as an OM2 report.

Alarm scanning

The scan time assigned to each OM register is divided into eight time slices of equal value. Whenever a failure occurs, an event count is placed in the time slice the failure occurred in.

After the initial scan time has elapsed, the system activates a moving window scheme in which the oldest time slice is dropped—including the event counts within the time slice—and a new time slice of equal value is added.

The system checks for alarm conditions on a one-minute basis, and compares the current event count to the previous event count from one scan interval earlier.

The following diagram illustrates the alarm scanning process:
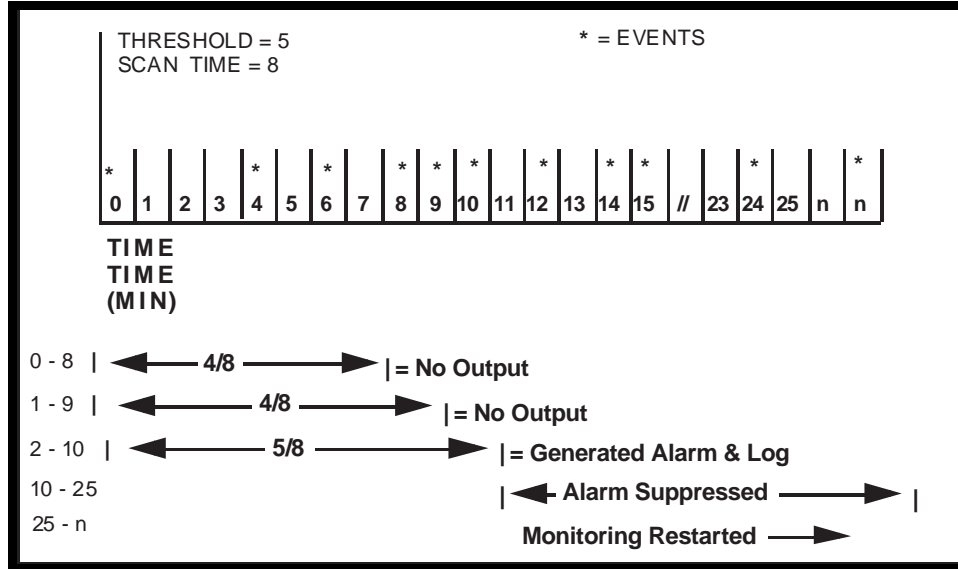
Activating the OM thresholding feature

The OMTHRESH table is a read-write table that allows the switch maintenance personnel to activate the OM thresholding feature by:

- specifying the OM register
- specifying the threshold count
- specifying the scan in minutes
- assigning the alarm level (critical, major, minor, and no-alarm)
- enabling or disabling each assigned register

The register selection for real-time surveillance will remain relatively constant from one switch to another. However, the threshold levels and scan time will vary since some indicators have other dependencies, such as office class, size, and call volume.

See the tables within this subsection for a list of suggested key OM registers, alarm levels, thresholds, and scan times. Also provided are threshold counts and scan times for large, medium, and small office scenarios. Thresholds can be adjusted to meet corporate objectives by using data from current switch performance and company results plan objectives, and from troubleshooting experience.

The OM threshold setting is measured using a moving window time frame and not call processing volume. Therefore, when setting or adjusting a threshold or scan time, consider values suitable for the traffic busy hour. Attempt to use the lowest threshold value and scan time that meet your surveillance criteria.

Access table OMTHRESH and datafill it using the table editor and the selected data for a large, medium, or small office from Table 2-31 within this subsection. Adjust the datafill according to needs.

Make sure the OM2200 log report has a class number assigned in table LOGCLASS. Also, verify that the class number is allowed to be printed to the device you want. If there are any problems receiving the OM2200 log reports after an OM threshold has been reached, see NTP 297-YYYY-350, *DMS-100F Translation Guides* and review the tables LOGCLASS, LOGDEV, and OMTHRESH.

Tables 2-29 and 2-30 record the SS7 OM registers, bogeys, and scan times information for adding SS7 surveillance indicators to OM thresholding. Table 2-30 is for SP/SSP application and includes ISUP trunk thresholding applications that may be used in lieu of other thresholding techniques with a time base.

Table 2-30 — Suggested SS7 Key OM Threshold Settings and Scan Times For SP/SSP						
Key OMs for Real-time Surveillance		**SEE NOTES**	**ENABLED**	**ALARM LEVEL**	**THRESHOLD**	**SCAN TIME**
GROUP	**REGISTER**					
ISUPERRS	ISERRBAD$0	3	Y	MN	15	15
ISUPERRS	ISERRBLO$0	3	Y	MN	10	15
ISUPERRS	ISERRGRS$0	3	Y	MN	15	15
ISUPERRS	ISERRREL$0	3	Y	MN	10	15
ISUPERRS	ISERRRLC$0	3	Y	MN	10	15
ISUPERRS	ISERRRSC$0	3	Y	MN	10	15
CLINK1	C7LKFAIL$0	1	Y	MJ	2	15
C7RTESET	C7RSFAIL$0		Y	MJ	2	15
C7SCCP	C7RTALL$0	2	Y	MJ	40	15

NOTES:

1. See Table 2-23 within this subsection.

2. This OM counts lost message signal units (MSUs) that are load dependent. Start with threshold set at 40 and adjust as required.

3. The OM thresholding feature may be used for surveillance of the SS7 functions such as ISUP errors applicable to ISUP trunking.

Table 2-31 — Suggested SS7 Key OM Threshold Settings and Scan Times For STP						
Key OMs for Real-time Surveillance		SEE NOTES	ENABLED	ALARM LEVEL	THRESHOLD	SCAN TIME
GROUP	REGISTER					
CM	CMTRMISM$0		Y	CR	2	15
CM	CMCPUFLT$0		Y	CR	2	15
MS	MSFLT$0		Y	CR	2	15
MS	MSFLT$1		Y	CR	2	15
MS	MSCDFLT$0		Y	CR	2	15
MS	MSCDFLT$1		Y	CR	2	15
MS	MSLKFLT$0		Y	CR	2	15
MS	MSLKFLT$1		Y	CR	2	15
IOC	IOCERR$0		Y	MN	2	15
IOC	IOCLKERR$0		Y	MN	2	15
IOC	IOCFLT$0		Y	MJ	2	15
DDU	DDUERROR$0		Y	MN	2	15
DDU	DDUFAULT$0		Y	MJ	2	15
NMC	NMCERR$0		Y	MN	2	15
NMC	NMMSGFL$0		Y	MN	2	15
NMC	NMSPCHFL$0		Y	MJ	3	30
NMC	NMMSGFL$0		Y	MJ	2	15
NMC	NMSPCHFL$0		Y	MJ	2	15
NMC	NMCFLT$0		Y	MJ	2	15
PMT	PMTERR$		Y	MN	18	5
PMT	PMTFLT$		Y	MJ	2	15
PM1	PM1ERR$LIUOM		Y	MN	8	30
PM1	PM1FLT$LIUOM		Y	MJ	2	15
C7LINK3	C7MSUBOV$0	2	Y	MJ	**50**	15
C7LINK1	C7LINKFAIL$0	1	Y	MJ	2	15
C7RTESET	C7RSFAIL$0		Y	MJ	2	15
C7SCCP	C7RTFALL$0	2	Y	MJ	**40**	15

NOTES:

1. See Table 2-23 within "OM class assignments and reports" of this subsection.

2. These OMs count lost MSUs that are load dependent. Suggest starting with 50, for C7MSUBOV, and 40, for C7RTFALL, and adjust as required.

Key OM Registers For Real-Time Surveillance	See Notes Table 2-15	ENABLED	ALARM LEVEL	LARGE OFFICE		MEDIUM OFFICE		SMALL OFFICE	
				THRESHOLD	SCAN/T	THRESHOLD	SCAN/T	THRESHOLD	SCAN/T
MTCHINT	103	Y	CR	2	15	2	15	2	15
CPUFLT$0	103	Y	CR	2	15	2	15	2	15
IOCERR$0		Y	MN	2	15	2	15	2	15
IOCLKERR$0		Y	MN	2	15	2	15	2	15
IOCFLT$0		Y	MJ	2	15	2	15	2	15
CMCLERR$0	104	Y	MN	2	15	2	15	2	15
CMCLERR$1	104	Y	MN	2	15	2	15	2	15
CMCERR$0	104	Y	MN	2	15	2	15	2	15
CMCERR$1	104	Y	MN	2	15	2	15	2	15
CMCFLT$0	104	Y	CR	2	15	2	15	2	15
CMCFLT$1	104	Y	CR	2	15	2	15	2	15
MTUERR$0		Y	MN	2	15	2	15	2	15
MTUFLT$0		Y	MJ	2	15	2	15	2	15
DDUERROR$0		Y	MN	2	15	2	15	2	15
DDUFAULT$0		Y	MJ	2	15	2	15	2	15
NMCERR$0		Y	MN	2	15	2	15	2	15
NMMSGER$0		Y	MN	11	26	6	60	2	15
NMSPCHER$0		Y	MN	12	15	8	45	3	30
NMMSGFL$0		Y	MJ	2	15	2	15	2	15
NMSPCHFL$0		Y	MJ	2	15	2	15	2	15
NMCFLT$0		Y	MJ	2	15	2	15	2	15
CPSUIC$0		Y	MJ	6	45	3	30	2	15
AMAEMTR$0		Y	MJ	2	15	2	15	2	15
TRSNBLH$0		Y	MJ	2	15	2	15	2	15
TRSNBLN$0		Y	MJ	9	30	8	90	2	15
TERSSTO$0		Y	MN	12	25	7	60	2	15
TERRODR$0		Y	MN	16	8	13	25	4	60
STNOVFL$0		Y	MN	2	15	2	15	2	15
CNFQOVFL$0		Y	MJ	2	15	2	15	2	15
PMTFLT$LM		Y	MJ	2	15	2	15	2	15
PMTCCTFL$LM		Y	MJ	3	15	3	15	2	15
PMTERR$LM		Y	MN	15	20	9	30	3	30

Table 2-32
Suggested Key OM Register Threshold Settings
and Scan Times for Three Office Sizes

Key OM Registers For Real-Time Surveillance	See Notes Table 2-15	ENABLED	ALARM LEVEL	LARGE OFFICE		MEDIUM OFFICE		SMALL OFFICE	
				THRESHOLD	SCAN/T	THRESHOLD	SCAN/T	THRESHOLD	SCAN/T
PMTERR$TM	120	Y	MN	7	45	6	90	2	15
PMTFLT$TM	120	Y	MJ	2	15	2	15	2	15
PMTCCTFL$TM	120	Y	MJ	3	15	3	15	3	15
PMTERR$DCM		Y	MN	14	10	6	60	3	30
PMTFLT$DCM		Y	MJ	2	15	2	15	2	15
PMTCCTFL$DCM		Y	MJ	3	15	3	15	3	15
PMTERR$LCM		Y	MN	9	30	7	60	3	30
PMTFLT$LCM		Y	MJ	2	15	2	15	2	15
PMTCCTFL$LCM		Y	MJ	3	15	3	15	3	15
PMTERR$LGC		Y	MN	13	30	10	25	5	60
PMTFLT$LGC		Y	MJ	2	15	2	15	2	15
PMTCCTFL$LGC		Y	MJ	3	15	3	15	3	15
PMTERR$LTC		Y	MN	10	30	9	60	3	30
PMTFLT$LTC		Y	MJ	2	15	2	15	2	15
PMTCCTFL$LTC		Y	MJ	3	15	3	15	3	15
PMTERR$DTC		Y	MN	18	5	15	30	7	60
PMTFLT$DTC		Y	MJ	2	15	2	15	2	15
PMTCCTFL$DTC		Y	MJ	3	15	3	15	3	15
PMTERR$MSB7	109	Y	MN	8	30	N/A	N/A	N/A	N/A
PMTFLT$MSB7	109	Y	MJ	2	15	N/A	N/A	N/A	N/A
PMTCCTFL$MSB7	109	Y	MJ	2	15	N/A	N/A	N/A	N/A
PMTDRFLT$DLM	119	Y	MJ	3	15	N/A	N/A	N/A	N/A
PM1ERR$ST7OM	109	Y	MN	8	30	N/A	N/A	N/A	N/A
PM1FLT$ST7OM	109	Y	MJ	2	15	N/A	N/A	N/A	N/A
PM1ERR$DCHOM	117	Y	MN	8	30	N/A	N/A	N/A	N/A
PM1FLT$DCHOM	117	Y	MJ	2	15	N/A	N/A	N/A	N/A
PM1ERR$PHIOM	117	Y	MN	8	30	N/A	N/A	N/A	N/A
PM1FLT$PHIOM	117	Y	MJ	2	15	N/A	N/A	N/A	N/A
CINTEGFL$0	121	Y	MJ	5	30	2	30	2	30
UTRQOVFL$TOTAL	106	Y	MJ	2	15	2	15	2	15
DS1RCGA$TOTAL		Y	MN	1	1	1	1	1	1
DS1LCGA$TOTAL		Y	MN	1	1	1	1	1	1
SWERRCT$0		Y	MN	3	5	3	5	3	5
NSCSFLTO$0		Y	MJ	2	5	2	5	2	5

Table 2-32 (continued)
Suggested Key OM Register Threshold Settings
and Scan Times for Three Office Sizes

Table 2-32 (continued) Suggested Key OM Register Threshold Settings and Scan Times for Three Office Sizes									
Key OM Registers For Real-Time Surveillance	See Notes Table 2-15	ENABLED	ALARM LEVEL	LARGE OFFICE		MEDIUM OFFICE		SMALL OFFICE	
				THRESHOLD	SCAN/T	THRESHOLD	SCAN/T	THRESHOLD	SCAN/T
DS1BER	122	Y	See Note	See Note	See Note	—	—	—	—
DS1LOF$TOTAL	122	Y	See Note	See Note	See Note	—	—	—	—
DS1SLP$TOTAL	122	Y	See Note	See Note	See Note	—	—	—	—
ACERR$0	108	Y	MN	60	15	45	15	30	15
ACFLT$0	108	Y	MJ	30	15	25	15	15	15
ACEXOVL$0	108	Y	MJ	5	15	5	15	15	15
CMTRMISM$0	102	Y	CR	2	15	N/A	N/A	N/A	N/A
CMCPUFLT$0	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSFLT$0	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSFLT$1	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSCDFLT$0	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSCDFLT$1	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSPTFLT$0	102	Y	CR	2	15	N/A	N/A	N/A	N/A
MSPTFLT$1	102	Y	CR	2	15	N/A	N/A	N/A	N/A
C7LKFAIL$CLLInn		Y	MJ	2	15	N/A	N/A	N/A	N/A
C7COV$CLLInn		Y	MN	4	30	N/A	N/A	N/A	N/A
C7LSFAIL$CLLI		Y	MJ	2	15	N/A	N/A	N/A	N/A
C7RTFALL$0		Y	MJ	5	30	N/A	N/A	N/A	N/A
See Note	123								

Bogey settings for key OMs

Key OM data and established performance bogeys form the nucleus of the DMS-100F control and analysis function. This process provides a reliable indicator of service and switch performance, and identifies areas requiring attention for improvement.

The prime tool for maintaining the DMS-100F switch at the designed level of performance, is effective OM management and surveillance of selected key OM registers. Key OMs should be evaluated per site against developed bogeys (anticipated site OM register counts for normal operations). Bogeys that are exceeded indicate areas requiring evaluation and possible corrective action.

Before OMs can be used effectively for real-time or subsequent trouble surveillance and analysis, the expected OM peg count for normal operation must be determined. Since call volume must be considered—to derive a meaningful OM trouble indicator—the ratio of pegs per 10,000 calls is the usual benchmark or bogey. However, many other OMs that track key switch operations will have a zero bogey or minimal trouble occurrence.

Table 2-33 starting on the next page, itemizes suggested factors for developing action level bogeys for switch maintenance activity. It also provides suggested guidelines for setting bogeys with OM groups associated with normal traffic and suggested guidelines for setting bogeys associated with hardware and software provisioning. All the tables provide normal expectancy values that represent customary quality of service and performance. The factors in the tables are intended as a guide, not as a rule. As trend or historical data is developed, adjust bogeys to meet your company objectives or needs.

Table 2-36 lists the key OMs for SS7 surveillance. Provisional bogey settings have been suggested for four indicators. Determine your own initial settings based on current information. As performance improves you may tighten the bogey(s) by decreasing the setting(s). Also provided are registers to determine SS7 signaling message unit volumes and a method for estimating the split between ISUP and PTS trunk calls.

bogeys should be adjusted as needed to meet company performance standards. Where initial OM bogey settings quickly point out potential or serious problems, bogeys should be adjusted—on a gradual basis—until problems are resolved and objectives are met.

Table 2-33
Suggested Action Level Guidelines for Setting Key OM Maintenance Bogeys (Monthly Figures)

GROUP	REGISTER	OM BOGEY
CP	CPSUIC	0.1 x J
	CPTRAP	0.2 x J
NMC	NMMSGFL	1.0 x J
	NMMSGER	3.0 x J
	NMSPCHFL	1.0 x J
	NMSPCHER	1.0 x J
	NMCERR	1.0 x J
CPU (NT40) Note: The equivalent registers for SuperNode are located in the CM group.	MTCHINT	0.05 x J
	TRAPINT	0.10 x J
	CPUFLT	4.60 x #MEXs
	SYSWINIT	0.5
	SYSCINIT	0.5
	SYNCLOSS	0.5
IOC	IOCERR	0.01 x J
	IOCLKERR	0.05 x J
	IOCFLT	1.00 x #IOCs
MTU	MTUERR	0.01 x J
	MTUFLT	1.00 x #MTUs
DDU	DDUERR	0.01 x J
	DDUFLT	1.00 x #DDUs
CMC Note: The equivalent registers for SuperNode are located in the MS group	CMCLERROR	1.00 x J
	CMCERR	0.05 x J
	CMCFAULT	0.5
PMTYP	PMTERR$TM	10 x M x AT
	PMTFLT$TM	0.09 x #TMs
	PMTERR$DCM	1 x M x DT
	PMTFLT$DCM	0.12 x #DCMs
	PMTERR$LM	1.5 x J
	PMTFLT$LM	0.5 x #LMs
	PMTERR$LCM	1.5 x J
	PMTFLT$LCM	0.5 x J
	PMTERR$LGC	3.5 x J
	PMTFLT$LGC	0.5 x J

Table 2-33 (continued)
Suggested Action Level Guidelines for Setting Key OM Maintenance
Bogeys (Monthly Figures)

GROUP	REGISTER	OM BOGEY
PMTYP continued	PMTERR$LTC	1.0 x J
	PMTFLT$LTC	0.5 x J
	PMTERR$DTC	1.5 x J
	PMTFLT$DTC	0.5 x J
	PMTERR$IAC	1.0 x J
	PMTFLT$IAC	0.5 x J
	PMTERR$ISLM	1.5 x J
	PMTFLT$ISLM	0.5 x J
	PMTERR$LMCI	1.5 x J
	PMTFLT$LMCI	0.5 x J
	PMTERR$LGCI	3.5 x J
	PMTFLT$LGCI	0.5 x J

Formula for calculating bogeys using monthly OFZ OM data.

TOTAL NUMBER OF CALLS
$$J = \frac{(NORIG - ORIGABDN) + NIN - (INABNM + INABNC)}{10000}$$

TOTAL TRUNK CALLS
$$M = \frac{INOUT + ORIGOUT + NIN - (INABNM + INABNC)}{10000}$$

ANALOG TRUNKS
$$AT = \frac{TM}{TM + 4 \times DCM}$$

DIGITAL TRUNKS
$$DT = \frac{4 \times DCM}{TM + 4 \times DCM}$$

Table 2-34
Suggested Guidelines for Determining Normal Traffic OM Bogeys (Information Only)

GROUP	REGISTER	NORMAL EXPECTANCY
OFZ	INLKT	The total of INLKT, INTONE, INANN should
OFZ	INTONE	typically be less than 1% of total
OFZ	INANN	incoming traffic (OFZ__NIN)
OFZ	OUTOSF	Typically less than 1% of total outgoing traffic (OFZ__OUTNWAT)
OFZ	OUTROSF	Typically less than .05% of total outgoing traffic (OFZ__OUTNWAT)
OFZ	INABNM	Total of INABNM and INABNC is typically less than 5% of total
OFZ	INABNC	incoming traffic (OFZ__NIN)
OFZ	ORIGLKT	Total of ORIGLKT, ORIGTONE, ORIGANN is
OFZ	ORIGTONE	typically less than 3% of originating traffic
OFZ	ORIGANN	(OFZ__NORIG)
OFZ	ORIGABDN	Typically less than 15% of total originating traffic (OFZ__NORIG)
LMD	ORIGFAIL	Typically less than 1.5% of sum of (LMD__NORIGATT)
LMD	PERCLFL	Typically less than 0.1% of sum of LMD__NTERMATT
TRK	PRERTEAB	Typically less than 5% of sum of TRK__INCATOT
TRK	INFAIL	Typically less than 1% of sum of TRK__INCATOT
TRK	OUTFAIL	Typically less than 0.1% of sum of TRK__NATTMPT
TRK	GLARE	Typically less than 0.1% of sum of TRK__NATTMPT
TRMTRS	TRSNOSC	0
TRMTRS	TRSNOSR	0
TRMTCM	TCMPDIL	The total of PDIL, PSIG, VACT is typically less than 0.5% of total
TRMTCM	TCMPSIG	incoming calls for DMS 200 (OFZ__NIN), or 2% of originating &
TRMTCM	TCMVACT	incoming calls for DMS 100 (OFZ__NIN+NORIG)
TRMTER	TERRODR	Typically less than .05% of total incoming & originating calls (OFZ__NIN+NORIG)
TRMTRS	TRSGNCT	0
TRMTER	TERSSTO	Typically less than .05% of total outgoing traffic (OFZ__OUTNWAT)

Table 2-34 (continued)
Suggested Guidelines for Determining Normal Traffic OM Bogeys
(Information Only)

GROUP	REGISTER	NORMAL EXPECTANCY
TRMTER	TERSYFL	0

NOTE: Traffic related OM registers, such as those in OM groups OFZ, LMD, and TRK, are intended to give a picture of the traffic offered to the office as a whole. It also provides some indication of the quality of service being offered by the office. The above registers can be used to assist in determining switch performance. The percentages given for peg counts are typical and are only intended to be used as a guide.

Table 2-35
Suggested Guidelines For Determining Normal Hardware/Software
Provisioning (Information Only)

GROUP	REGISTER	NORMAL EXPECTANCY
CP	CCBOVFL	0
CP	OUTBOVFL	0
CP	ORIGDENY	0
CP	WAITDENY	0
CP	CPLOOVFL	0
CP	CPLOOFL	0
CP	MULTOVFL	0
EXT	EXTOVFL	0
OFZ	OUTRMFL	1% ABSBH for DMS 100 0.5% 10HDBH for DMS 200
OFZ	TRMMFL	2% ABSBH for DMS 100 only
LMD	TERMBLK	1.9% ABSBH for TOTAL LM or LCM
TRK	OUTMTCHF	1% ABSBH for DMS 100 over all TRK GRPS .5% 10HDBH for DMS 200 over all TRK GRPS
TRK	NOVFLATB	0

Table 2-35 (continued)
Suggested Guidelines For Determining Normal Hardware/Software
Provisioning (Information Only)

GROUP	REGISTER	NORMAL EXPECTANCY
TRMTRS	TRSNBLH	1.0% ABSBH for DMS-100 Outgoing & Terminating Traffic 0.5% 10HDBH for DMS-200 Outgoing Traffic
TRMTRS	TRSNBLN	0.1% ABSBH Terminating Traffic for DMS 100
RCVR	2RCVROVFL	0
RCVR	RCVRQOVFL	0
DTSR	DTSDLYPC	1.5% ABSBH > 3 seconds (LM Only)
DTSR	DELAY	1.5% ABSBH > 3 seconds (LCM)
RADR	RADLDLYP	1.5% ABSHB > 3 Seconds, DMS 100 8% 10HDBH > 3 Seconds, DMS 200
RADR	RADUDLYP	0

NOTE: The registers above are associated with administrative functions as well as provisioning of hardware and software resources. The values given for peg count are typical and do not reflect trouble conditions where equipment may be out of service, or abnormally high traffic.

Table 2-36
Provisional SS7 Maintenance Key OMs and Bogey Settings — Suggested Action Levels

GROUP	REGISTER	OM BOGEY	BASE/NOTE
C7LINK1	C7SUERR	40	Per link per 24H
	C7NACKRX	9	Per link per 24H
	C7AUTOCO	4	Per link per 24H
	C7LKFAIL	1	This register counts in-service link failures
C7LINK2	C7MSUDSC	%	MSU discarded due to congestion
	C7MSGLOS	%	STP – MSU lost through STP
	C7MSGMSQ	%	STP – MSU incorrect sequence
C7LINK3	C7MSUBOV	%	STP – MSU lost - no buffers
C7ROUTE	C7RTUNAU		Route failure in time
C7RTESET	C7RSFAIL		Routeset failure
C7SCCP	C7RTFALL	%	MSU received but couldn't route
C7MTP	C7MSIDPC	%	STP – MSU DPC routing irregularity
	C7MSISIO	%	STP – MSU discarded SIO count read
C7GTWSCR	MSUDSCRD	%	STP – errors in screening

OTHER SS7 KEY INDICATORS	bogey	BASE/NOTE
Signaling link MSU occupancy (normal operation)	0.4 Erlangs	maximum
Link traffic retransmitted	%	

NOTE:

SS7 Message Signaling Unit (MSU) volumes are derived from the following OM groups and registers:

Total for MTP   MSU = (C7LINK2) C7MSUTX + C7MSUTX2 + C7MSURX + C7MSURX2

Total for SCCP   MSU = (C7SCCP) C7MSGHDL + C7MSGHD2

Total for STP   MSU = (C7LINK2) C7MSUTX + C7MSUTX2 + C7MSURX + C7MSURX2

SSP Call volume can be estimated using the ratio of ISUP to PTS trunks as follows:

$$\frac{ISUP}{(ISUP + PTS)} \times 100 = \% \ ISUP \qquad \frac{PTS}{SUP + PTS} \times 100 = \% \ PTS$$

Total Trunk Calls = INOUT + ORIGOUT + NIN - (INABNM + INABNC) (Table OFZ registers)

OM trouble identifiers

DMS-100F switch OMs are a key tool in identifying trouble conditions, service levels, equipment performance, and the need for maintenance activity. When they are evaluated against established OM threshold bogeys, they can quickly point out real-time problems. By utilizing associated log report information and diagnostic tools, problems can be resolved much faster than through other means—such as customer reports.

OM trouble indicators

This part describes the various types of OM trouble indications used for switch maintenance purposes. They are derived from the analysis of the following specific OM register readings :

- ERROR
- FAULT
- INITIALIZATION
- OVERFLOW
- SYSTEM BUSY USAGE
- MANUAL BUSY USAGE
- PEG COUNT

Error OMs

Errors are message or operational problems encountered between equipment modules and may be hardware or software related. Continued abnormal volumes of errors may impede call processing for the equipment units involved. Each error scores an error OM register.

Fault OMs

Faults are detected by system initiated diagnostic and test programs. The circuit failing the test is made *system busy* and periodically retested. Hard faults will remain system busy; however, equipment with intermittent or marginal faults will be returned to service if subsequent diagnostic tests are successful. Each system busy action will score one fault OM.

Initialization OMs

Initialization is a procedure designed to restore a processor to a known starting point. This can be either system or manually initiated. Each initialization will score an initialization OM—calls may be cut off.

Overflow OMs

Overflows are ineffective attempt calls due to a shortage of equipment or software registers. When a queue is provided, the call is placed in the queue to wait for equip-

ment or software registers to become idle to serve the call. When a call finds the queue full, it is routed to overflow and pegged as an ineffective attempt. Shortages of equipment may be the result of too much equipment being busied out manually, by the system, or by unusually heavy traffic conditions.

System busy usage OMs

System busy usage measures the time interval when a piece of equipment has been made busy by the system as a result of a system initiated diagnostic or test failure. The time is measured in hundred second units (CCs)—where 36 CCs is equal to an hour (slow scan). A fast scan rate is used to record some equipment outages resulting in 360 pegs per hour. Fast scan is usually used for equipment that normally has a short holding time, such as transmitters and receivers.

When a unit in a dual unit module is in a system-busy state, the mate unit carries the total load. This may cause some service degradation in heavy traffic. A module system-busy state causes service degradation since both units are out of service. When single unit modules go system-busy, service degradation occurs since the unit is out of service.

Manual busy usage OMs

Manual busy usage measures the time interval when a piece of equipment has been made busy manually. The time is measured the same as system busy usage OMs.

Peg count OMs

Peg count OMs count the number of calls, or the number of times, a piece of equipment is used. The following are some examples of how to use the OMs to determine the type of fault involved:

- Hard fault
  A hard fault will score one error, one fault, and a high amount of system busy usage until manual corrective action is taken. The out-of-service equipment is displayed on the MAP status display with an LED or lamp lit, if equipped.

- Marginal or intermittent fault
  A marginal or intermittent fault will score many errors, many faults, and low system busy usage. The faulty equipment may not be seen on the MAP alarm, and a manually initiated diagnostic may not fail. Circuit packs may have to be replaced in the suspected equipment on a trial and error basis until the source of the problem is found.

- Undetected fault
  An undetected fault will score a high number of errors, but no fault or system busy usage. This is because the system initiated (or manually initiated) diagnostic tests may not be able to detect or test the faulty operation. Circuit packs may have to be replaced in the suspected equipment on a trial and error basis until the source of the problem is found.

Possible trouble causes

The following DMS-100F Trouble Location Charts identify possible sources of troubles when specific OM counters exceed objectives. Use them as a guideline when trying to resolve problems, but other information such as log messages may be needed to find the exact cause of a problem.

It suggested that OMs be reviewed for new OM groups and registers as well as new registers for existing OM groups that are used in the following charts. Add any new or existing OM registers to the blank spaces on the charts that you think would be helpful for problem solving. Other charts could be developed for other products such as ISDN, AIN, TOPS, etc.

DMS-100F Trouble Location Charts

Table 2-37

DMS-100F Trouble Location Chart	RESOURCES — CALL PROCESSES

CALL PROCESSES OM FIELDS (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)

CCBOVFL	ORIGDENY	WAITDENY	CPLOOVFL	CPLPOVFL	OUTBOVFL	MULTOVFL	WAKEOVFL	ECCBOVFL	EXTOVFL	FTRQOVFL	ESPOVRD	ESPDELAY	INEFDENY	NOSR	SYSFL	NOTES	POSSIBLE CAUSE
X												X				1	SHORTAGE OF CALL CONDENSE BLOCKS
	X										X					2	OFFICE OVERLAOD (ORIGINATIONS DENIED)
		X														1	CALLS KILLED DUE TO SHORTAGE OF PROCESSES
			X													1	SHORTAGE OF CP LETTERS
				X											O	1	SHORTAGE OF CP LETTERS
					X										O	1	SHORTAGE OF OUTGOING BUFFERS
						X								O		3	SHORTAGE OF MULTIBLOCK BUFFERS
							X									1	SHORTAGE OF WAKE BLOCKS
								X						O		3	SHORTAGE OF EXTENDED CALL CONTROL BLOCKS
									X					O		4	SHORTAGE OF EXTENSION BLOCKS
										X				O		3	SHORTAGE OF FEATURE QUEUE BLOCKS
													X			1	2ND TRIAL ORIGINATION FAILURES

NOTES:

1. If calls are lost, request traffic to provision more.

2. Calls not necessarily lost.

3. Vertical Service Feature is blocked. Request traffic to provision more.

4. Vertical Service Features and/or non-pots calls are denied. Request traffic to provision more.

Table 2-38

DMS-100F Trouble Location Chart RESOURCES — CALL BUFFERS

CALL BUFFERS OM FIELD (X = EXCEED OBJ. O = MAY EXCEED OBJ.)

CRDOVFL	CFDOVFL	CFBOVFL	CFUOVFL	CWTOVFL	CWOOVFL		CFDAOVFL	CFDFOVFL	CWPTOVFL	CPUFAIL		KSHOVFL	LNRPOVFL	MWTOVFL	CAROVFL	CARDOVFL	CARROVFL	CBQOVFL	OHQOVFL	RTCBQOVF	RTDHQOVF	NOSR	NOTES	POSSIBLE CAUSE
X																						O	1	SHORTAGE OF CALL HOLD EXTENSION BLOCKS (EXTs)
	X																					O	1	SHORTAGE OF CALL FORWARD DON'T ANSWER EXT's
		X																				O	1	SHORTAGE OF CALL FORWARD BUSY EXT's
			X																			O	1	SHORTAGE OF CALL FORWARD UNIVERSAL EXT's
				X																		O	1	SHORTAGE OF CALL WAITING TERM. EXT's
					X																	O	1	SHORTAGE OF CALL WAITING ORIG. EXT's
							X															O	1	SHORTAGE OF POTS CALL FORWARD ACTIVATE EXT's
								X														O	1	SHORTAGE OF POTS CALL FORWARD EXT's
									X													O	1	SHORTAGE OF POTS CALL WAITING EXT's
										X														SHORTAGE OF IBN CALL PICK UP EXT's
												X										O	1	SHORTAGE OF BUSINESS KEY SET HUNT EXT's
													X									O	1	SHORTAGE OF REDIAL EXT's
														X								O	1	SHORTAGE OF MESSAGE WAITING EXT's
															X							O	1	SHORTAGE OF CALL REQUEST EXT's
																X						O	1	SHORTAGE OF DEACTIVATE CALL REQUEST EXT's
																	X					O	1	SHORTAGE OF RETRIEVE CALL REQUEST EXT's
																		X				O	1	SHORTAGE OF CALL BACK QUEUEING EXT's
																			X			O	1	SHORTAGE OF OFF HOOK QUEUEING EXT's
																				X		O	1	SHORTAGE OF CALL BACK QUEUEING EXT's
																					X	O	1	SHORTAGE OF OFF HOOK QUEUEING EXT's

NOTE:

1. See Note in the following Table 2-38 along with remaining call buffer OMs.

Table 2-39

DMS-100F Trouble Location Chart RESOURCES — CALL BUFFERS (continued)																									
CALL BUFFERS CON'T (X = EXCEED OBJ. O = MAY EXCEED OBJ.)																							N O S R	N O T E S	POSSIBLE CAUSE
R C F D F L D	S C P A O V F L	T W C P O V F L																							
X																							O	1	SHORTAGE OF REMOTE CALL FORWARDING EXT's.
	X																						O	1	SHORTAGE OF SPEED CALL EXT's.
		X																					O	1	SHORTAGE OF 3 PORT CONF SPEECH LINKS, CCB's AND/OR PORT_PERM_BLKS. (BUFFERS).

NOTE:

1. Calling features are blocked and NOSR treatment is given.
   In most cases one of the following are scored:
   — ECCBOVFL
   — FTRQOVFL
   — EXTOVFL
   Request traffic to provision more extension blocks as identified.

Table 2-40

DMS-100F Trouble Location Chart   RESOURCES — SERVICE CIRCUITS

SERVICE CIRCUITS OM FIELDS (X = EXCEED OBJ. O = MAY EXCEED OBJ.)

CNFQOVFL	CF6OVFL	CDROVFL	CWTPOVFL	DESOVFL	RCVQOVFL	STNOVFL	SVCQOVFL	TONEOVFL	AMAFREE	CNFMBU	CNFSBU	CF6MBU	CF6SBU	DESMBU	DESSBU	RCVMBU	RCVSBU	STNMBU	STNSBU	SVCMBU	SVCSBU	UTRQOVFL	NOSR	NOTES	POSSIBLE CAUSE
X																							O	1	SHORTAGE OF 3 PORT CONFERENCE CCTS
	X																						O	1	SHORTAGE OF 6 PORT CONFERENCE CCTS
		X																						3	SHORTAGE OF CALL RECORDING RESOURCES
			X																				O	1	SHORTAGE OF CALL WAITING TONE CCTS
				X																			O	1	SHORTAGE OF DIGITAL ECHO SUPPRESSORS
					X																		O	1	SHORTAGE OF RECEIVERS
						X																	O	1	SHORTAGE OF SPECIAL TONE CCTS
							X																O	1	SHORTAGE OF SPECIAL SERVICE CCTS
								X															O	2	SHORTAGE OF TONE CONNECTIONS
										O	O	O	O	O	O	O	O	O	O	O	O			4	EXCESSIVE MTCE BUSY, RETURN TO SERVICE
																						X		1	SHORTAGE OF UNIVERSAL TONE RECEIVERS

NOTES:

1. Calls are given overflow treatment. Request traffic to provision more hardware if maintenance busy is not excessive.

2. Calls are given overflow treatment. Additional connections require additional call processes.

3. May require disk re-allocation.

4. System busy indicates diagnostic failures.

Table 2-41

DMS-100F Trouble Location Chart   HARDWARE — NETWORK MODULE

NMC, SYSPERF OMs (X = EXCEED OBJ. O = MAY EXCEED OBJ.)

NMMSGER	NMSPCHER	NMCERR	NMMSGFL	NMSPCHEL	NMCFLT	NMSBU	NMMBU	NMPTSBU	NMPTMBU	MNJRSBU	NMJRMBU	CINTEGFL											NOTES	POSSIBLE CAUSE
X	O	O	O	O	O	O						O												DEFECTIVE LINKS, PORTS, CONTROLLER CARDS
	X		O				O		O			O											1	DEFECTIVE PORTS, PMs, XPT, FORMATTER CARDS
							O		O		O	O												EXCESSIVE MAINTENANCE ACTIVITY
O	O	O	O	O								X												NETWORK INTEGRITY TROUBLES ON BOTH PLANES

NOTES:

1. Network integrity faults may also cause CPSUIC pegs. network integrities can be caused by loose or crossed patch cords in the speech or digital networking interconnecting frames of JNETs.

2. Network integrities may be caused by the two planes being driven by different system clocks.

3. Use net integ level of MAP to look for patterns that help identify defective card (include formatter cards in XPMs)

4. All net integ counters should have zero counts in a 24 hr. period.

5. Use NETFAB feature tool to routinely test the switch network after hours. See "Network Maintenance" later in this manual.

Table 2-42

																									DMS-100F Trouble Location Chart HARDWARE — LM, TM, DTC, PM1, PM2, and other XPMs
NMC, SYSPERF OMs (X = EXCEED OBJ. O = MAY EXCEED OBJ.)																									
ERR	FLT	CCTDG	CCTFL	MBP	SBP	MBTCO	SBTCO	CCTOP	MSBU	MMBU	USBU	UMBU	SWXFR	MWXFR	SCXFR	MCXFR	PSERR	PSFLT	RGERR	RGFLT	INTEG	PORGDENY	PTRMDENY	NOTES	**POSSIBLE CAUSE**
X	O			O					O	O			O		O		O	O			O				PM PROCESSOR, SPEECH LINK PROBLEMS
		O	X					O																	LINE/TRUNK CARD TROUBLES
O	O			O	O	X	X		O	O	O	O	O	O	O	O	O	O							CALLS CUT-OFF ON PM RELOADS
																			X	X					RING GENERATOR TROUBLES
																					X				SPEECH, NETWORK XPT, FORMATTER TROUBLES
																						X	X		HARDWARE OR TRAFFIC LOADING TROUBLES
		O				O			O		O		O		O										EXCESSIVE MAINTENANCE ACTIVITY

Table 2-43

DMS-100F Trouble Location Chart   HARDWARE — INPUT OUTPUT SYSTEM

NMC, SYSPERF OMs (X = EXCEED OBJ. O = MAY EXCEED OBJ.)

AMAERTR	CSLERR	CSLFLT	CSLSBU	CSLMBU	DDUERROR	DDUFAULT	DDUMBUSY	DDUSBUSY	IOCERR	IOCLKERR	IOCFLT	IOCLKSBU	IOCLKMBU	IOCSBU	IOCMBU	MTUERR	MTUFLT	MTUSBU	MTUMBU	NOTES	POSSIBLE CAUSE
X																					DATA CORRUPTION, DDU, MTU, IOC, IOD TROUBLES
	X	O	O																		IOD, DEVICE TROUBLES
				X	O		O														DISK CONTROLLER, IOD TROUBLES
									X		O			O							IOC CONTROLLER TROUBLES
										X		O									IOC - PERIPHERAL DEVICE TROUBLES
																X	O	O			MAGNETIC TAPE CONTROLLER, IOD TROUBLES
				O			O					O		O					O		EXCESSIVE MAINTENANCE ACTIVITY

Table 2-44

DMS-100F Trouble Location Chart   SuperNode CM (Computing Module)

CM (X = EXCEEDS THRESHOLD) (O = MAY EXCEED THRESHOLD)

CMSSWACT	CMMSWACT	CMRSWACT	CMSWINIT	CMMWINIT	CMSCINIT	CMMCINIT	CMTRMISM	CMDPSYNC	CMTRAP	CMCPUFLT	CMMEMFLT	CMSSCFLT	CMMCSBSY	CMREXFLT	CMRCPUFL	CMREMEMFL	CMRSSCFL	CMRMCFL	CMSSMPXU	CMMSMPXU	CMRSMPXU	NOTES	POSSIBLE CAUSE
X							O		O	O	O	O											HARDWARE OR SOFTWARE FAULT OR ERROR
	X																						MANUAL ACTIVITY SWITCH
		X																			O		REX ACTIVITY SWITCH
			X					O	O														UNRECOVERABLE SOFTWARE OR HARDWARE FAULT
				X																			MANUAL WARM RESTART
					X			O	O														UNRECOVERABLE SOFTWARE OR HARDWARE FAULT
						X																	MANUAL COLD RESTART
							X								O								FAULTY HARDWARE: MEMORY OR MEMORY CONTROLLER
								X											O	O			MANUAL ACTION HARDWARE FAULT
		O		O					X	O								O					SOFTWARE FAULTS OR CORRUPTION
O			O		O			O		X													FAULTY CPU HARDWARE
O						O					X												FAULTY MEMORY HARDWARE: MEMORY OR CONTROLLER
												X					O						FAULTY CLOCK HARDWARE
													X					O					FAULTY MESSAGE CONTROLLER HARDWARE
								O						X									OFFICE OUT OF SYNC OR JAMMED
										O					X								BAD CPU HARDWARE
											O					X							BAD MEMORY HARDWARE: MEMORY OR CONTROLLER
												O					X						BAD SUB-SYSTEM HARDWARE
													O					X					BAD MESSAGE CONTROLLER HARDWARE
							O	O											X				OUT OF SYNC TIME DUE TO SYSTEM ACTION
								O												X			OUT OF SYNC TIME DUE TO MANUAL ACTION
		O												O							X		OUT OF SYNC TIME DUE TO REX TEST

Table 2-45

DMS-100F Trouble Location Chart   SuperNode MS (Message Switch)

CM (X = EXCEEDS THRESHOLD) (O = MAY EXCEED THRESHOLD)

MSERR	MSCDERR	MSLKERR	MSFLT	MSCDFLT	MSPTFLT	MSDIA	MSCDDIA	MSLKDIA	MSDIAF	MSCDDIAF	MSLKDIAF	MSMBP	MSCDMBP	MSLKMBP	MSMBU	MSCDMBU	MSLKMBU	MSSBU	MSCDSBU	MSLKSBU	NOTES	POSSIBLE CAUSE
X			O			O			O													TRANSIENT HARDWARE FAULTS
	X			O			O			O												TRANSIENT HARDWARE FAULTS
		X			O			O			O											TRANSIENT HARDWARE OR MESSAGE FAULTS
O			X			O												O				HARDWARE FAULT — MS SET SYSTEM BUSY
	O			X			O												O			HARDWARE FAULT — MS CARD SET SYSTEM BUSY
		O			X			O												O		HARDWARE OR MESSAGE FAULT — PORT SET SYSTEM BUSY
O			O			X			O													HIGH MS ERRORS OR FAULTS
	O			O			X			O												HIGH MS CARD ERRORS OR FAULTS
		O			O			X			O											HIGH LINK ERRORS OR FAULTS
O			O			O			X									O				BAD HARDWARE — PEGS MS FAULT
	O			O			O			X									O			BAD HARDWARE — PEGS MS CARD FAULT
		O			O			O			X									O		BAD HARDWARE — PEGS MS LINK FAULT
O			O						O			X			O			O				MS SET MANUAL BUSY
	O			O						O			X			O			O			MS CARD SET MANUAL BUSY
		O			O						O			X			O			O		MS LINK SET MANUAL BUSY
												O			X							TIME MS IN MANUAL BUSY
													O			X						TIME MS CARD IN MANUAL BUSY
														O			X					TIME MS LINK IN MANUAL BUSY
O									O									X				TIME MS IN SYSTEM BUSY
	O									O									X			TIME MS CARD IN SYSTEM BUSY
		O									O									X		TIME MS LINK IN SYSTEM BUSY

Table 2-46

DMS-100F Trouble Location Chart   LINES

LMD, OTS, TROUBLE Q. TRMT-OMs (X = EXCEEDS OBJ.) (O = MAY EXCEED OBJ.)

TERMBLK	ORIGFAIL	PERCLFL	STCOINS	ORIGBLK	ORIGABN	ORIGLKT	ORIGABDN	ORIGLKT	LNMBPC	TRBQATT	TRBQOVFL	PMERRS	PMFLTS	RGERR			NBLH	NBLN		SYFL	NOTES	POSSIBLE CAUSE
X			O									O	O				O	O				LINK TROUBLES OR TRAFFIC OVERLOADS
	X			O		O			O	O											1	SET, CA PR TROUBLES, LINE CARD, RECEIVER TROUBLES
		X											O							O		SET, CA PR TROUBLES, RING GENERATOR TROUBLES
			X																			STUCK COIN IN COIN BOX STATION
						X		X										O				LINE LOAD CONTROL, PM PROCESSING ERROR, PM
																						OVERLOAD, LINKS BUSIED OUT
									O	X	X											EXCESSIVE LINE OR LINE CARD DIAGNOSTICS

NOTE:

1. Balance network in line card may not be set right. Perform ALT BALNET 'balance' test. Diagnostic should be run on lines to identify faulty line cards.

Table 2-47

DMS-100F Trouble Location Chart   TRUNKS

ANN, EASHRTRK, OTS, OFZ OMs (X = EXCEEDS OBJ.) (O = MAY EXCEED OBJ.)

ANNSBU	STGOVFL	INCABNM	INCABNC	INCKLT	INLKT	INABNN	INABNC	NCIT	NCTC	NCLT	NCID	NCOT	NCRT	NCIM	NCON	NCOF	PSGM	PDLM	OUTMFL	OUTRMFL	OUTOSF	OUTROSF	NOTES	POSSIBLE CAUSE
X																								DEFECTIVE ANNOUNCEMENT TRUNK
	X																							SHORTAGE EQUAL ACCESS SHARED TRUNKS
		X	O			O	O																1	MAY BE DUE TO DELAYS IN GETTING A RECEIVER
			X	O																			2	INCOMING CALL PROCESS FAILURES
								O	O	O	O	O	O	O	O	O							3	SHORTAGE OF TRUNKS (OR TOO MANY BUSIED OUT)
																	X	X					4	DEFECTIVE TRANSMITTER, TRUNK OR RECEIVER
																			X	O			5	NETWORK LINES/JUNCTORS BUSIED OUT OR OVERLOAD
																					X	O	6	DEFECTIVE TRUNK, OVERLAOD OR TRANSLATION ERROR

NOTES:
See the following TRUNKS (continued) chart for Notes.

Table 2-48

DMS-100F Trouble Location Chart   TRUNKS (continued)

OFZ, TRK, TRMT, PM (X = EXCEEDS OBJ.) (O = MAY EXCEED OBJ.)

PRERTEAB	INFAIL	NOVFLATB	GLARE	OUTFAIL	SBU	MBU	OUTMTCHF	NBLH	RODR	SSTO	SYSFL	STOB	STOC	NOSC	NOSR	VACT	PMERR	PMFLT	CCTDG	CCTFL	XTR	TCO	CCTOP	NOTES	POSSIBLE CAUSE
O																								1	MAY BE DUE TO DELAYS IN GETTING A RECEIVER
	X																							4	DEFECTIVE TRANSMITTER, TRUNK OR RECEIVER
		X		O	O																			3	SHORTAGE OF TRUNKS (OR TOO MANY BUSIED OUT)
			X	O																				7	LOOPED-BACK OR DEFECTIVE TRUNK
				X	O					O		O	O											6	DEFECTIVE TRUNK, OVERLOAD OR TRANSLATION ERROR
						O	O																	5	NETWORK LINKS/JUNCTORS BUSIED OUT OR OVERLOAD
									O		O						O	O	O	O	O	O	O	2	PROCESSING FAILURES
														X										8	OUT OF SERVICE CIRCUITS OR TOO MANY BUSIED OUT
															X									8	OUT OF SOFTWARE RESOURCE OR TOO FEW PROVISIONED
																X									DIGIT RECEPTION TROUBLE OR TRANSLATION ERROR

NOTES:
1. OM registers score together, most often due to customer action.
2. OM registers complement each other.
3. OM registers are similar, may be due to excessive mainte-nance busy.
4. Poor transmission (noise, NL, ERL).
5. OM registers complement each other.
6. OM registers complement each other, translation error in table OFCSTD, TRKGRP, TRKSGRP or poor transmis-sion (noise, NL, ERL).
7. Both offices should not be designated control office for glare treatment.
8. Request traffic to provision more.

Table 2-49

DMS-100F Trouble Location Chart   CARRIER

DS1CARR OMs (X = EXCEEDS OBJ.) (O = MAY EXCEED OBJ.)

L C G A	R C G A	B E R	L O F	S L P	E S	S E S	S B U	M B U	P B U	C B U											N O T E S	POSSIBLE CAUSE
O	O	X	X	X	X	X	O														1	HOST OR REMOTE INTERFACE CARDS, DEFECTIVE REPEATERS, OR INCORRECT SYNCHRONIZATION OPTION
									X	X												DEFECTIVE PM OR NETWORK MODULE
								X														EXCESSIVE MAINTENANCE BUSY USAGE

NOTE:

1. LCGA, RCGA, LOF, SLP, ES, SES, & BER OMs SHOULD BE AT ZERO.

   LCGA   Local Carrier Group Alarm
   RCGA   Remote Carrier Group Alarm
   LOF   Loss of Framing
   SLP   Slip
   ES   Errored Seconds
   SES   Severe Errored Seconds
   BER   Bit Error Rate

Table 2-50

DMS-100F Trouble Location Chart   SELECTED TREATMENT

DS1CARR OMs (X = EXCEEDS OBJ.) (O = MAY EXCEED OBJ.)

TERSYFL	TERSSTO	TERRODR	TERSTOB	TERSTOC	TRSNOSC	TRSNBLH	TRSNBLN	TRSEMR1	TRSEMR2	TRSNOSR	TRSGNCT	TCMPD1L	TCMPSIG	TCUNACK	NOTES	POSSIBLE CAUSE
X																PROCESSING ERRORS
	X															LOOPED BACK OR DEFECTIVE TRUNK
		X														PROCESSING ERRORS
			X													EQUAL ACCESS SIGNALLING TROUBLE
				X												EQUAL ACCESS SIGNALLING TROUBLE
					X											SHORTAGE OF RECEIVERS, TONES, ETC.
						X										SWITCH OVERLOAD
							X									PM OVERLOAD OR PROVISIONING
								X								NETWORK MANAGEMENT CONTROLS
									X							NETWORK MANAGEMENT CONTROLS
										X						SHORTAGE OF SOFTWARE RESOURCES
												X				TIMING PROBLEMS LINES OR TRUNKS
													X			TIMING PROBLEMS LINES OR TRUNKS
											X					ALL TRUNKS BUSY–TRAFFIC OR MANUAL
														X		SHORTAGE OF RESOURCES TO SUPPORT FEATURES

Table 2-51

						DMS-100F Trouble Location Chart													SYSTEM PERFORMANCE						

SYSPERF LOGS CC HUNT TROUBLE Q
(X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)

T K P C B U	T K B A D D G	C I N T E G F L	L I N P M B U	L I N C C T B U	T R M L N F L	L I N B A D D G		S W E R R C T	P M S W E R C T	P M T R A P C T		T R A P I N T		H U N T R H N T		T R B Q A T T	T R B Q O C C	T R B Q O V F L						N O T E S	POSSIBLE CAUSE
X																									USAGE FOR ALL PMB CFL TRUNKS
	X																								INCOMING IMPULSING PROBLEMS
		X																							CUTOFFS DUE TO INTEGRITY PROBLEMS
			X																						USAGE FOR LMB LINES
				X																					USAGE FOR LINES MB, SB, SZD, ETC.
					X																				CALLS FAILING DUE TO HARDWARE FAILURE
						X																			ORIGS FAILING DUE TO DIALING PROBLEMS
								X																	CC SOFTWARE ERRORS–HARDWARE FLTS
									X																PM SOFTWARE ERRORS–HARDWARE FLTS
										X															PM SOFTWARE FLT–HARDWARE FLTS
												X													CC SOFTWARE FLT
														X											DIAG FAILURE FLAG SET
																X									CABLE, SET, PAIR, LINE CARD PROBLEMS
																	X								SLOW MTCE RESPONSE
																		X							CABLE, LCM, TRBL SLOW MTCE RESPONSE

Table 2-52

DMS-100F Trouble Location Chart SS7 SIGNALING ROUTESET AND LINKSET								NOTES	POSSIBLE CAUSE
C7RSUNAU	C7RSFAIL	C7RSMANB	C7RSCNGU	C7RTERR		C7LSUNAU	C7LSFAIL		C7RTESET, C7LKSET (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)
X	O								ROUTESET NOT SUPPORTING TRAFFIC TIME (Associated Logs CCS155 and CCS154)
O	X								NUMBER OF TIMES ROUTESET IS OUT OF SERVICE (Associated Log CCS154)
		X							NUMBER OF TIMES ROUTESET SET MAN BUSY (Associated Log CCS152)
			X	O					TIME ROUTESET IS CONGESTED
O	O		O	X					MESSAGE ROUTING ERRORS
						X	O		TIME LINKSET IS UNABLE TO HANDLE TRAFFIC
						O	X		NUMBER OF LINKSET FAILURES

Table 2-53

DMS-100F Trouble Location Chart   SS7 SIGNALING ROUTE PERFORMANCE AND USAGE

C7RTUNAU	C7TFR	C7TFP	C7TFC1	C7TFC2	C7TFC3	C7FRCRER											NOTES	POSSIBLE CAUSE
X	O																	ROUTE OUT OF SERVICE (measured in 10-second increments).
O	X																	MESSAGE OVERLAOD OR FAULTY SIGNAL LINKS (Associated Log CCS167)
O		X																LINK OR MSB FAILURE (Associated Log CCS168)
			X	O	O													MESSAGE OVERLOAD, DEGRADED SIGNALING LINKS (Associated Log CCS172)
			O	X	O													MESSAGE OVERLOAD, DEGRADED SIGNALING LINKS (Associated Log CCS172)
			O	O	X													MESSAGE OVERLOAD, DEGRADED SIGNALING LINKS (Associated Log CCS172)
						X												MESSAGE OVERLOAD ON ROUTE

C7RTESET, C7LKSET (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)

Table 2-54

DMS-100F Trouble Location Chart — SS7 SIGNALING LINK FAILURES AND RECOVERY

C7LINK1 (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)

C7LKFAIL	C7ABNRFB	C7EXDLAY	C7EXERR	C7EXCONG	C7ALIGNF	C7NACKRX	C7STAFL	C7TLALFL	C7NETCON	C7SLTFL	C7NUCFL	C7COV	C7CBK	C7BSYON	C7BSYOFF	C7LPO	C7RPO	NOTES	POSSIBLE CAUSE
X	O																		NUMBER OF SYNCHRONIZATION FAILURES (Associated Log CCS101)
O	X																		T1 LINK ERRORS (Associated Log CCS101)
O		X																	FAR END CONGESTION (Associated Log CCS101)
O			X																T1 CARRIER ERRORS (Associated Log CCS101)
O				X															FAR END CONGESTION OR MESSAGE OVERLOAD (Assoc. Log CCS101)
O					X														SIGNALING TERMINAL HARDWARE OR CXR JITTER
O						X													FAR END NOT RECEIVING MESSAGES PROPERLY
O							X												SIGNALING TERMINAL TROUBLE NEAR END
O								X											TRANSMISSION LINK IS FAILED OR UNASSIGNED
O									X	O									BLOCKAGE OCCURRED IN THE NETWORK
O										X									SIGNALING LINK TEST FAILURE (Associated Log CCS101)
O									O	X									CHECK MAX. NO. OF PERMITTED NAILED-UP
																			CONNECTIONS (Associated Log CCS108)
O	O	O	O	O	O						X								TRANSMISSION LINK TROUBLE (Associated Log CCS164)
												X							TRANSMISSION LINK TROUBLE CLEARED (Associated Log CCS163)
													X						MESSAGE OVERLOAD OR HIGH RE-TRANSMISSION
														X					CONGESTION CLEARED
															X				NEAR END LOCAL PROCESSOR FAILURE (Associated Log PM102, PM105)
																X			FAR END PROCESSOR TROUBLE (Associated Log CCS104)

Table 2-55

																												POSSIBLE CAUSE

DMS-100F Trouble Location Chart   SS7 SIGNALING LOAD AND OVERLOAD

C7LINK2 (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)

C7BYRT	C7MSUDSC	C7ONSET1	C7ONSET2	C7ONSET3	C7ABATE1	C7ABATE2	C7ABATE3	C7MSUDC1	C7MSUDC2	C7MSUDC3															NOTES	POSSIBLE CAUSE
X																										TRANSMISSION LINK TROUBLES
	X																									HIGH MESSAGE LOAD
		X		O																						EXCESSIVE MESSAGE LOAD (Associated Log CCS173)
			X		O																					EXCESSIVE MESSAGE LOAD (Associated Log CCS173)
				X		O																				EXCESSIVE MESSAGE LOAD
		O			X																					MESSAGE OVERLOAD CLEARED
			O			X																				MESSAGE OVERLOAD REDUCED
				O			X																			MESSAGE OVERLOAD REDUCED
								X																		MSB MESSAGE OVERLOAD
									X																	MSB MESSAGE OVERLOAD
										X																MSB MESSAGE OVERLOAD

Table 2-56

DMS-100F Trouble Location Chart SS7 SIGNALING SCCP STATUS																				
MS (X = EXCEEDS OBJ. O = MAY EXCEED OBJ.)																				
C7RTFALL	C7RTFNTN	C7RTFNTA	C7RTFNTA	C7RTFNWF	C7RTFNWC	C7RTFSSF	C7RTFUEQ	C7UDTSTX	C7UDTSRX	C7SYNERR									NOTES	POSSIBLE CAUSE
X																				ROUTE FAILURE, VARIOUS CLASSES (Associated Logs CCS201, CCS202, CCS203, CCS204, CCS205)
	X																			FAILURE TRANSLATION (Called Party Address) (Associated Log CCS202)
		X																		FAILURE TRANSLATION (Global Title) (Associated Log CCS202)
			X																	NETWORK FAILURE (DPC Prohibited)
				X																NETWORK FAILURE (DPC Restricted)
					X															DESTINATION SUBSYSTEM FAILURE
						X														UNEQUIPPED USER
							X													UNITDATA SVC MESSAGE TX (Could not complete—Returned)
								X												UNITDATA SVC MESSAGE RX (Could not comlete—Returned to Originator)
									X											SYNTAX ERROR MESSAGE RECEIVED (Associated Log CCS202)

Focused Maintenance

General

The Focused Maintenance (FM) feature is a DMS-100F administrative tool that can be used for managing trunk and line log messages. When Focused Maintenance techniques are implemented, trunk and line log message outputs will be reduced significantly.

Focused Maintenance can identify:

- individual line troubles
- line card troubles
- trunk troubles
- peripheral troubles

Focused Maintenance can assist switch maintenance forces in identifying:

- network module problems
- translation problems
- facility problems
- far end equipment problems

Focused Maintenance uses buffers to accumulate data, rather than printing individual log messages per failure. When the quantity of failures reaches or exceeds a pre-set threshold level, a visual alarm indication is registered on the system status display area of the MAP. It also generates log messages FM100 for trunk groups and FM101 for line concentration device (LCD) groups that have reached or exceeded the group threshold setting. Information concerning these failures is obtained by accessing the appropriate MAP level—LNSTRBL for lines or TRKSTRBL for trunk— to view the specifics of the trouble situation causing the alarm.

System components

The following system components are associated with Focused line and trunk maintenance:

- Tables LNSMTCE and TRKMTCE

- Line and trunk trouble buffers

- Attempt and failure counters

- Thresholding system

- LNSTRBL and TRKSTRBL MAP levels

A description of these components follows.

Tables LNSMTCE and TRKMTCE

Table LNSMTCE

This table is used to:

- allocate or de-allocate call processing (CP) trouble buffers for line concentrating devices (LCD).

- assign failure and attempt counters.

- assign CP alarm threshold levels for each LCD.

- establish an attempt count value for each LCD.

Table TRKMTCE

This table is used to:

- allocate or de-allocate CP trouble buffers and/or maintenance processing (MP) trouble buffers for each trunk group in the office.

- assign CP and MP failure counters.

- assign CP attempt counters.

Line trouble buffers

For each LCD entered into table LNSMTCE, a pair of buffers exists to identify lines with trouble conditions. These buffers are known as upper and lower buffers.

Upper buffers may contain a maximum of 10 entries. These entries contain the most recent lines on an LCD with the highest failure count (greater than one). The structure of each entry will contain identification of the LEN (line equipment number), date and time of the last report, count of the troubles on the LEN, and a brief description of the last trouble encountered. The contents of the upper buffer are accessible through the LNSTRBL level of the MAP.

Lower Buffers may contain a maximum of 5 entries. These entries are used to screen out LENs with less than 2 troubles. The contents of the Lower Buffer are not accessible.

Trunk trouble buffers

For each trunk group entered into table TRKMTCE a pair of buffers exists to identify the members of each group with troubles. These buffers are known as upper and lower buffers.

Upper buffers may contain a maximum of 10 entries. These entries contain the most recent members of a trunk group with the highest failure count (greater than one). The structure of each entry will contain the identification of the trunk group and member, date and time of the last trouble, a count of troubles on that member, and a brief description of the last trouble encountered. The contents of the upper buffer are accessible through the TRKSTRBL level of the MAP.

Lower buffers may contain a maximum of 5 entries. These entries are used to screen out trunk group members with less than 2 troubles. The contents of the lower buffer are not accessible.

Attempt counters

One attempt counter is associated with each LCD entered in table LNSMTCE and for each trunk group entered into table TRKMTCE.

Each attempt counter represents the number of call attempts processed by the LCD, or trunk group associated with the counter.

The attempt counter tabulates the number of successful call attempts processed and decrements the failure count by one for every (N) attempts datafilled in tables LNS-MTCE and TRKMTCE. The attempt counters are pegged by the call processing system.

NOTE: Attempt counters are not maintained for trunk maintenance processing failures.

Failure counters

One failure counter is associated with each LCD entered in table LNSMTCE and for each trunk group entered in table TRKMTCE.

The failure counter tabulates the number of troubles that occur on LCDs and trunk groups during call processing activities. The failure counters are pegged by the buffering systems.

Thresholding systemFocused

The thresholding process:

- determines when the failure count of an LCD or trunk group is reached or exceeds the alarm threshold values in tables LNSMTCE and TRKMTCE.

- generates the appropriate MAP alarm indication (minor, major, critical, or no alarm).

- generates the appropriate log messages—FM100 for trunks and FM101 for lines as follows:

        FM100 FEB10   01:01:54   0630   TB3L   FM   TRK   ALARM
               TRK GROUP = OTMF1   ALARM = CR
               ALARM TYPE = CP

        FM101 FEB12   02:23:12   7151   TBL   FM   LNS   ALARM
               LM HOST 00 0
               ALARM = MN

LNSTRBL and TRKSTRBL MAP levelsFocused

The MAP level LNSTRBL has been created to make it possible for maintenance personnel to view line trouble information, control specified trouble types, list and clear alarms, and take appropriate action. The LNSTRBL level is located below the LNS subsystem level (MAPCI;MTC;LNS;LNSTRBL).

The MAP level TRKSTRBL has been created to make it possible for maintenance personnel to view trunk trouble information, control specified trouble types, list and clear alarms, and take appropriate action. The TRKSTRBL level is located below the TRKS subsystem level (MAPCI;MTC;TRKS;TRKSTRBL).

Operating features

AlarmsFocused

The Focused Maintenance feature for lines and trunks generates the appropriate log and alarms (minor, major, critical, or no-alarm) whenever the thresholds in table LNSMTCE or TRKMTCE are met or exceeded.

Visual reporting of alarms is done via the introduction of a top level status display alarm bar (just above the regular out-of-service display bar) for the LNS and TRKS subsystems. The visual status alarm display alternates every 30 seconds between the Focused Maintenance line and trunk maintenance status display and the regular LNS and TRKS MAP status display. See NTP 297-YYYY-543, *Alarm Clearing and Monitoring Procedures* for information on Focused Maintenance alarms.

Buffering by LCD and trunk group

The buffering process places line and trunk trouble information in buffers on a per LCD and trunk group basis. The lines and trunks are identified by the member number within the buffer.

Trouble descriptionFocused

Focused Maintenance provides a brief text description of the most recent trunk or line troubles recorded in the upper buffers. The upper buffer lists the ten worst members with trouble conditions. This is summarized and reported by the LCD or trunk group.

For reference purposes, the following tables in this subsection provide a cross reference between the line and trunk trouble index code description text to the associated log message report(s). This text also may be seen in a buffer entry when displayed at the TRKSTRBL and LNSTRBL MAP levels respectively. Further description of the text codes can be found in NTP 297-1001-594, *DMS-100F Lines Maintenance Guide* or in Table G (Lines and Trunks trouble codes) within NTP 297-YYYY-840, *DMS-100F Logs Reference Manuals.*

Table 2-57 — Focused Maintenance "Trunk" Trouble Index Codes to "TRK" Logs Cross Reference List

Trunk Trouble Number and Description	Suppress (Yes or No)	TRK Log Message
0 NIL Trouble	Yes	Not Applicable
1 Vacant Code Announcement	Yes	111 Outpulsing Trouble
2 No Ckt Available: OG Trk	No	111 Outpulsing Trouble
3 Misdirected CAMA Annc.	Yes	111 Outpulsing Trouble
4 Unauthorized Code Annc.	Yes	111 Outpulsing Trouble
5 Emergency Announcement	No	111 Outpulsing Trouble
6 Inwats Outside Legal Zone	No	111 Outpulsing Trouble
7 Permanent Signal	Yes	183 DGT PSIG Report
8 Partial Dial	Yes	114 DP Reception Trouble
	Yes	116 MF Reception Trouble
	Yes	182 DGT Reception Trouble
9 Extra Pulse	No	114 DP Reception Trouble
10 False Start	No	116 MF Reception Trouble
11 Mutilated Pulse	No	114 DP Reception Trouble
12 Mutilated Digit	No	116 MF Reception Trouble
	No	118 ANI Trouble Reception
	No	120 ONI Trouble
	No	182 DGT Reception Trouble
13 Invalid St Digit Received	No	116 MF Reception Trouble
14 ANI Office Failure	No	118 ANI Trouble Reception
15 ANI Number Failure	No	118 ANI Trouble Reception
16 ANI Timeout	No	118 ANI Trouble Reception
	No	121 Outpulsing Trouble
	No	162 DTMF Outpulsing Trouble
Continued		

Table 2-57 — Focused Maintenance "Trunk" Trouble Index Codes to "TRK" Logs Cross Reference List (continued)

Trunk Trouble Number and Description	Suppress (Yes or No)	TRK Log Message
17 No Start Dial	No	121 Outpulsing Trouble
		162 DTMF Outpulsing Trouble
18 Integrity Failure	No	121 Outpulsing Trouble
	No	113 Trunk Integrity Trouble
	No	122 Integrity Trouble
19 Integrity Lost	No	113 Trunk Integrity Trouble
20 False KP	Yes	116 MF Reception Trouble
21 Reversed Trunk	No	121 Outpulsing Trouble
	No	162 DTMF Outpulsing Trouble
22 Unexpected Stop Dial	No	121 Outpulsing Trouble
	No	162 DTMF Outpulsing Trouble
23 Expected Stop Time Out	No	121 Outpulsing Trouble
		162 DTMF Outpulsing Trouble
23 Expected Stop Time Out	No	162 DTMF Outpulsing Trouble
24 CAMA Position Fault	Yes	120 ONI Trouble
25 CAMA Position Trouble	Yes	120 ONI Trouble
26 ANNC Machine Trouble	No	213 Trunk Trouble
27 Trunk Reset Failed	No	213 Trunk Trouble
28 Trunk Reset	No	213 Trunk Trouble
29 Hit Detected	No	213 Trunk Trouble
30 Pre Route Abandon	Yes	114 DP Reception Trouble
	Yes	116 MF Reception Trouble
	Yes	182 DGT Reception Trouble
31 No5 Signaling Violation	Yes	121 Outpulsing Trouble
32 Digit RCVR Noise High	No	116 MF Reception Trouble
	No	118 ANI Trouble Reception
	No	120 ONI Trouble Reception
	No	182 DGT Reception Trouble
33 Digit RCVR Noise Marginal	No	116 MF Reception Trouble
	No	118 ANI Trouble Reception
	No	120 ONI Trouble Reception
	No	182 DGT Reception Trouble
34 No Interdigit Pause	Yes	114 DP Reception Trouble
35 Large Twist	No	116 MF Reception Trouble
	No	118 ANI Trouble Reception
	No	120 ONI Trouble Reception
	No	182 DGT Reception Trouble
Continued		

Table 2-57 — Focused Maintenance "Trunk" Trouble Index Codes to "TRK" Logs Cross Reference List (continued)

Trunk Trouble Number and Description	Suppress (Yes or No)	TRK Log Message
36 More Than Two Frequencies	No No No No	116 MF Reception Trouble 118 ANI Trouble Reception 120 ONI Trouble Reception 182 DGT Reception Trouble
37 Fluctuation On MF RCVR	No No No	116 MF Reception Trouble 118 ANI Trouble Reception 120 ONI Trouble Reception
38 Ringing Failed	No	113 or 213 Trunk Trouble
39 Coin Collect Failed	No	113 or 213 Trunk Trouble
40 Coin Return Fail	No	113 or 213 Trunk Trouble
41 ANI Test Failed	No	
42 Coin Present Test Failed	No	
43 CP IOMSG Lost	No	113 or 213 Trunk Trouble
44 Bad CP IOMSG	No	113 or 213 Trunk Trouble
45 ANI Failed, ONI Succeeded	Yes	
46 Invalid ANI Request	Yes	121 Outpulsing Trouble
47 Bad Keyset	Yes	113 or 213 Trunk Trouble
48 Line Card Fault	No	
49 Data Unit Sync Lost	Yes	
50 Ground Loop Fail	No	
51 Abandon On RP INC Trk	Yes	113 Trunk Integrity Trouble
52 Overall RP Time-out	Yes	121 Outpulsing Trouble
53 Invalid RP Digit	Yes	121 Outpulsing Trouble
54 Undetermined RP Error	Yes	121 Outpulsing Trouble
55 Excess Digits	No No No No	116 MF Reception Trouble 118 ANI Reception Trouble 120 ONI Reception Trouble 182 DGT Reception Trouble
56 DP Permanent Signal	Yes	115 DP Permanent Signal
57 MF Permanent Signal	Yes	117 MF Permanent Signal
58 DGT Permanent Signal	Yes	183 DGT Permanent Signal
59 DP Reception Trouble	Yes	114 DP Reception Trouble
60 MF Reception Trouble	Yes	116 MF Reception Trouble
61 DGT Reception Trouble	Yes	182 DGT Reception Trouble
62 ANI Reception Trouble	No	119 ANI Reception Trouble
63 ONI Reception Trouble	No	120 ONI Trouble
64 Lockout ON	Yes	110 Lockout ON
65 Lockout OFF	Yes	112 Lockout OFF
Continued		

Table 2-57   — Focused Maintenance "Trunk" Trouble Index Codes to "TRK" Logs Cross Reference List (continued)

Trunk Trouble Number and Description	Suppress (Yes or No)	TRK Log Message
66 Outpulsing Trouble	No	121 Outpulsing Trouble
66 Outpulsing Trouble	No	162 DTMF Trunk Trouble
67 Routing Trouble	No	111 Outpulsing Trouble
68 Bipolar Violation	No	113 or 213 Trunk Trouble
69 PP CC Communication Trouble	No	123 PP CC Communication Trouble
70 thru 76 are Reserved	Yes	
77 Carrier OFFHK Timeout	No	113 Trunk Trouble
78 Wrong Supervisory Signal	No	121 or162 Out Pulsing Trouble
79 Compelled MF Receive Sig. Fail	No	116 MF Reception Trouble
80 R2 Signaling Trouble	Yes	322 Signaling Trouble
81 R2 Outpulsing Trouble	Yes	322 Signaling Trouble
82 R2 Reception Trouble	Yes	322 Signaling Trouble
83 N6 Signaling Violation	Yes	303 Continuity Failed
84 EAOSS_HOLD Trouble	No	
85 and 86 Reserved	Yes	
87 Early DP Digit Detected	No	182 DGT Reception Trouble
88 Wats Threshold Exceeded	No	165 Threshold Exceeded
89 TL105 Test IDs Self Check	No	179, 180, and 223 TL105 Self Check
90 TL105 Fail IDLNR	No	179, 180, and 223 TL105 Self Check
91 TL105 Test IDRSR Shelf Check	No	179, 180, and 223 TL105 Self Check
92 Minor Group Alarm	No	101 Minor Alarm
93 Major Group Alarm	No	102 Major Alarm
94 Critical Group Alarm	No	103 Critical Alarm
95 Trunk Group OK	No	104 Trunk Group OK
96 TRK Diag Failed	No	106 Diagnostic Failed
97 TL100 Test Failed	No	129 TL100 Test Results
98 TRK Treatment	No	138 Trunk Treatment
99 TL105 Test Failed	No	128 TL100 Test Results
100 AIOD Trouble	No	138 Trunk Treatment (AIFL)
101 AUTHCODE Trouble	No	138 Trunk Treatment (INAU, TINV)
102 Database Trouble	No	138 Trunk Treatment (NC8F, N9DF)
103 ATD TRK Trouble	No	108 IBN
104 Invalid Sts	No	138 Trunk Treatment (C7AP)
105 ICN TRK Trouble	No	
106 Wink Of Incorrect Length	No	121 Outpulsing Trouble
107 ANI DB Failed	No	138 Trunk Treatment ADBF()
108 ANI Acct Not Allowed	No	138 Trunk Treatment (ANIA)
Continued		

Table 2-57 — Focused Maintenance "Trunk" Trouble Index Codes to "TRK" Logs Cross Reference List (continued)

Trunk Trouble Number and Description	Suppress (Yes or No)	TRK Log Message
109 ANI Acct Recent Disallow	No	138 Trunk Treatment (ANIA)
110 Calling Card Invalid	No	138 Trunk Treatment (CCNV)
111 Calling Card Timeout	No	138 Trunk Treatment (CCTU)
112 Reorder Treatment	No	138 Trunk Treatment (RODR)
113 Restrict Time And Date	No	138 Trunk Treatment (RSDT)
114 Store Overflow Reorder	No	138 Trunk Treatment (SORD)
115 Start Signal Timeout	No	121 Outpulsing Trouble
116 Vacant Speed Number	No	138 Trunk Treatment (VACS)
117 Vacant Country Code	No	138 Trunk Treatment (VCCT)
118 Trigger Block	Yes	138 Trunk Treatment (DMS-250 Only)

Table 2-58 — Focused Maintenance "Line" Trouble Index Codes to LINE Logs Cross Reference List

Line Trouble Number and Description	Suppress (Yes or No)	LINE Log Message
0 NIL Trouble	Yes	Not Applicable
1 Vacant Code Announcement	Yes	138 Line Treatment (VACT)
2 No Ckt Available: OG Trk	Yes	138 Line Treatment (NCRT)
3 Misdirected CAMA Annc.	Yes	
4 Unauthorized Code Annc.	Yes	
5 Emergency Announcement	Yes	
6 Inwats Outside Valid Zone	Yes	
7 Permanent Signal	Yes	105 Permanent Signal
8 Partial Dial	Yes	106 Line Pulsing Trouble 108 DGT Pulsing Trouble
9 Extra Pulse	No	106 Line Pulsing Trouble
10 False Start	Yes	106 Line Pulsing Trouble
11 Mutilated Pulse	Yes	106 Line Pulsing Trouble
12 Mutilated Digit	Yes	
13 Invalid ST Digit Received	Yes	
14 ANI Office Failure	No	
15 ANI Number Failure	No	
16 ANI Time Out	No	
17 No Start Dial: OG Trk	Yes	109 Line Outgoing Trouble
18 Integrity Failure	No	104 Line Integrity
19 Integrity Lost	No	104 Line Integrity
Continued		

Table 2-58 — Focused Maintenance "Line" Trouble Index Codes to LINE Logs Cross Reference List (continued)

Line Trouble Number and Description	Suppress (Yes or No)	LINE Log Message
20 False KP	Yes	
21 Reversed Trunk: OG Trk	No	109 Line Outgoing Trouble
22 Unexpected Stop Dial: OG Trk	Yes	109 Line Outgoing Trouble
23 Expected Stop Timeout: OG Trk	Yes	109 Line Outgoing Trouble
24 CAMA Position Fault	Yes	
25 CAMA Position Trouble	Yes	
26 Annc Machine Trouble	No	
27 Trunk Reset Failed: OG Trk	No	
28 Trunk Reset: OG Trk	Yes	
29 Hit Detected	No	
30 Pre-route Abandon	No	
31 No5 Sig Violation: OG Trk	Yes	
32 Digit RCVR Noise High	No	108 DGT Pulsing Trouble
33 Digit RCVR Noise Marginal	No	108 DGT Pulsing Trouble
34 No Interdigit Pause	Yes	108 DGT Pulsing Trouble
35 Large Twist	No	108 DGT Pulsing Trouble
36 More Than Two Frequencies	Yes	108 DGT Pulsing Trouble
37 Fluctuation On MF Receiver	Yes	
38 Ringing Failed	Yes	113 Ringing Trouble
39 Coin Collect Failed	No	113 Ringing Trouble
40 Coin Return Failed	No	113 Ringing Trouble
41 ANI Test Failed	No	113 Ringing Trouble
42 Coin Present Test Failed	No	113 Ringing Trouble
43 CP IO Message Lost	No	204 LCM Line Trouble
44 BAD CP IO MSG	No	204 LCM Line Trouble
45 ANI Failed, ONI Succeeded	Yes	
46 Invalid ANI Request	Yes	
47 Bad Keyset	Yes	204 LCM Line Trouble
48 Line Card Fault	No	204 LCM Line Trouble
49 Data Unit Sync Lost	No	204 LCM Line Trouble
50 Ground Loop Fail	Yes	204 LCM Line Trouble
51 Abandon On RP INC Trunk	Yes	
52 Overall RP Timeout	Yes	
53 Invalid RP Digit	Yes	
54 Undetermined RP Error	Yes	
55 Excess Digits	Yes	
56 DP Permanent Signal	Yes	
Continued		

Table 2-58 — Focused Maintenance "Line" Trouble Index Codes to LINE Logs Cross Reference List (continued)		
Line Trouble Number and Description	Suppress (Yes or No)	LINE Log Message
57 MF Permanent Signal	Yes	
58 DGT Permanent Signal	Yes	108 DGT Reception Trouble
59 DP Reception Trouble	Yes	
60 MF Reception Trouble	Yes	
61 DGT Reception Trouble	Yes	108 DGT Reception Trouble
62 ANI Reception Trouble	No	
63 ONI Reception Trouble	No	
64 Lockout ON	Yes	102 Line Lockout ON
65 Lockout OFF	Yes	103 Line Lockout OFF
66 Outpulsing Trouble: OG Trk	Yes	109 Line Outgoing Trouble
67 Routing Trouble	No	
68 Bipolar Violation	No	
69 Foreign EMF Detected	Yes	110 FEMF Detected
70 Foreign EMF Removed	Yes	111 FEMF Removed
71 No 3WC Extension Blocks	No	120 Three Way Call Failure
72 No Perm Extension Blocks	No	120 Three Way Call Failure
73 No Temp Extension Blocks	No	120 Three Way Call Failure
74 No Conference Circuit Available	No	120 Three Way Call Failure
75 No Multiblks Or CCBs Avail	No	120 Three Way Call Failure
76 No Network Conn Available	No	120 Three Way Call Failure
77 thru 79 Reserved	Yes	
80 Invalid Digit Received	Yes	

Implementation

Implementation of the FocusedFocused Maintenance feature requires data additions and changes to some tables. The following parts of this section describe the implementation process. The work operations are:

- Assign privilege classes to the commands for the LNSTRBL and TRKSTRBL MAP levels according to your office security policy. See the *Office Administration* section of this manual concerning office security and NTP 297-1001-129, *DMS-100F Input/Output System Reference Manual,* for the use of the PRIV-CLAS command.

- Datafill tables LNSMTCE and TRKMTCE.

- Suppress specific line & trunk trouble index code messages (see Tables 2-57 & 58) that could fill up the buffers with trivial non-service affecting logs.

- Datafill table LOGCLASS for the FM100 and FM101 log reports.

• Use tables LOGCLASS and LOGDEV to suppress or assign to garbage class the log messages which were replaced by the Focused Maintenance feature (see Tables 2-56 & 57).

Knowledge required

The maintenance personnel activating this feature must be knowledgeable in the following areas:

• Table editor commands in NTP 297-1001-360, *DMS-100F Basic Translations Tools Guide.*

• MAPCI LNS and TRKS subsystem commands listed in NTP 297-1001-594, *DMS-100F Lines Maintenance Guide* and NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide* respectively.

• Datafilling tables using NTP 297-YYYY-350, *DMS-100F Translation Guides.*

• Telephony troubles as listed in Tables 2-56 & 2-57.

• Managing log messages using tables LOGCLASS and LOGDEV.

Activating lines maintenance feature

The following procedures describe the steps for activating Focused Maintenance for lines:

STEPS	ACTION
1	Go to LNSTRBL subsystem level (MAPCI;MTC;LNS;LNSTRBL).
2	Use the SUPPRESS command to suppress selected trouble index code messages such as the examples listed below, and others as suggested in Table 2-57.

TRBL NO.	MESSAGE TEXT	HOW TO SUPPRESS
7	Permanent Signal	Use command SUPPRESS and specify the trouble message number.
8	Partial Dial	
64	Lockout On	Example: >SUPPRESS 7
65	Lockout Off	Response >OK.

NOTES:	1. Trouble code suppression is not retained over a PCL load insertion; therefore, the selected trouble codes must be re-suppressed immediately following a load insertion. If these trouble codes are not suppressed, the trouble buffers will be filled up with trivial trouble data such as permanent signals caused by customer action. Use the QSUP command to list suppressed troubles.
	2. The Line Log Reduction feature, causes the line trouble codes 64 and 65 to disappear. See the "Lines Maintenance" subsection for more information on line log reduction feature.

3	Return to CI level.

Continued

STEPS	ACTION
4	Access tables LMINV and LCMINV and dump the table contents by using table editor commands.
5	Leave tables LMINV and LCMINV.
6	Access table LNSMTCE by using table editor commands.
7	Datafill table LNSMTCE—see "Datafill table LNSMTCE" next.
8	Leave table LNSMTCE.
9	Assign class number to the FM101 log report in table LOGCLASS.

NOTES: 1. All LCD equipment appearing in tables LMINV and LCMINV should be entered into this table.

2. Consider using the SFDEV file and edit process to facilitate the transfer of data from tables LMINV and LCMINV to the LNSMTCE table.

3. Alarms may be received immediately after the feature is activated because the total call attempts per LCD are initially low. As the total call attempts increase, the alarms that are initially generated will disappear if no true faults are present.

Datafill tableFocused LNSMTCE

The following list describes the fields and provides suggested datafill for table LNSMTCE:

FIELD NAME	DESCRIPTION	SUGGESTED DATAFILL
LMNM	LCD identification. This field is made up of three subfields: SITE, FRAME and UNIT.	Enter LCD identification for all frames.
CPMINALM	Call processing troubles minor alarm threshold	5
CPMAJALM	Call processing troubles major alarm threshold	10
CPCRTALM	Call processing troubles critical alarm threshold	15 see note 4
ATMPCNT	Successful attempts required before decrementing failure count	50
CPBUFRQD	Call processing trouble buffer required	Y

NOTES:

1. Buffers may not be de-allocated while a continuous buffer display is in progress in the LNSTRBL subsystem level

2. See NTP 297-YYYY-350, *DMS-100F Translations Guides* and table LNSMTCE for further information on field descriptions.

3. The above alarm and attempt counter thresholds are Nortel Networks suggested datafill for table LNSMTCE. The thresholds are operating company dependent and may change with office requirements.

4. To mask the critical alarm, set the threshold to 101 (not recommended).

Line log suppressionFocused

See Table 2-57 for a list of "LINE" logs to be suppressed or assigned to a class that is not directed to an I/O device (i.e., garbage class). This is done via tables LOGCLASS and LOGDEV.

Activating trunk maintenance feature

The following procedures describe the steps for activating Focused Maintenance for trunks:

STEPS	ACTION
1	Go to TRKSTRBL subsystem level (MAPCI;MTC;TRKS;TRKSTRBL).
2	Use the SUPPRESS command to suppress selected trouble index code messages such as the examples listed below, and others as suggested in Table 2-56.

TRBL NO.	MESSAGE TEXT	HOW TO SUPPRESS
30	Pre-route abandon	Use command SUPPRESS and specify trouble message number.
64	Lockout On	
65	Lockout Off	Example: >Suppress 64 Response >OK.

> **NOTE:** Trouble code suppression is not retained over a PCL load insertion; therefore, the selected trouble codes must be re-suppressed immediately following a load insertion. If these trouble codes are not suppressed, the trouble buffers will be filled up with trivial trouble data—such as permanent signals.

3	Return to CI level.
4	Access table CLLI and dump table contents using table editor commands.
5	Leave table CLLI.
6	Access table TRKMTCE.
7	Datafill table TRKMTCE (see "Datafill table TRKMTCE" next).
8	Leave table TRKMTCE.
9	Assign class number to the FM100 log report in table LOGCLASS.

> **NOTES:**
> 1. Enter all trunk groups appearing in table TRKGRP, except miscellaneous trunk groups (e.g., HSET trunks).
> 2. Consider using the SFDEV file and edit process to facilitate the transfer of data from table CLLI to the TRKMTCE table.
> 3. Alarms may be received immediately after the feature is activated because the total call attempts per trunk group are initially low. As the total call attempts increase, the alarms that are initially generated disappear if no true faults are present.

Table TRKMTCE call processing

The following list describes the fields and provides suggested datafill for table TRK-MTCE as related to call processing:

FIELD NAME	DESCRIPTION AND SUGGESTED DATAFILL
CLLI	Trunk group identification. Enter trk grp CLLI for all trunk groups.
CPBUFRQD	Call Processing trouble buffer required. Enter "Y".
CPCRTALM	Threshold—see note 4

Suggested alarm threshold datafill for call processing trouble alarms: minor, major, and critical.

ALARM		TRUNK GROUP TYPE		
		INCOMING	OUTGOING	TWO-WAY
CPMINALM	Threshold	10	5	5
CPMAJALM	Threshold	15	10	10

NOTES:

1. Buffers may not be de-allocated while a continuous buffer display is in progress in the TRKSTRBL subsystem level.

3. The above alarm and attempt counter thresholds are Nortel Networks suggested datafill for table TRKMTCE. These thresholds are operating company dependent and may change with office requirements.

4. To mask the critical alarm, set the threshold to 101 (not recommended).

Table TRKMTCEFocused maintenance processing datafill

The following list describes the fields and provides suggested datafill for table TRK-MTCE as related to maintenance processing:

FIELD NAME	DESCRIPTION AND SUGGESTED DATAFILL
ATMPCNT	Number of successful attempts required before decrementing failure counter. Enter 50.
MTBUFRQD	For future use—enter "N" at this time. If CP trouble buffer required in the future, then enter "Y".

Suggested alarm threshold datafill for maintenance processing trouble alarms: minor, major, and critical.

ALARM		TRUNK GROUP TYPE		
		INCOMING	OUTGOING	TWO-WAY
MTMINALM	Threshold	10	5	5
MTMAJALM	Threshold	15	10	10
MTCRTALM	Threshold	20	15	15

NOTES:

1. Buffers may not be de-allocated while a continuous buffer display is in progress in the TRKSTRBL subsystem level.

2. The above alarm and attempt counter thresholds are suggested datafill for table TRKMTCE. These thresholds are operating company dependent and may change with office requirements.

3. To mask the critical alarm, set the threshold to 101 (not recommended).

Commands to assist in datafill of table TRKMTCE

Listed below are commands that can be used to assist in the datafill of table TRK-MTCE. The commands have been used in the past and can save considerable time. The commands used the suggested threshold datafill values as default and can be modified for your needs.

The command for incoming trunks:
```
>COMMAND XX (ADD  @1  10  15  20  Y  50  10  15  20  N)
```
The command for outgoing/two–way trunks:
```
>COMMAND YY (ADD  @1  5  10  15  Y  50  5  10  15  N)
```

The following is an example of the incoming command's use:

```
>TABLE TRKMTCE
  EMPTY TABLE
  TABLE:  TRKMTCE

>RAN
   1 CLLICLLI_KEY
   2 CPMINALMUNS IGNEDINT
   3 CPMAJALMUNSIGNEDINT
   4 CPCRTALMUNSI GNEDINT
   5 CPBUFRQDBOOL
   6 ATMPCNTUNSIGNEDINT
   7 MTMINALMUNSIGNEDINT
   8 MTMAJALMUNSIGNEDINT
   9 MTCRTALMUNSIGNEDINT
  10 MTBUFRQDBOOL

LOGICAL TUPLE TYPE;  TRKMTCE_LOG_TUPLE

>XX PTTIN
```

NOTE: PTTIN is the CLLI being added—substitute additional CLLIs as required.

```
TUPLE TO BE ADDED
  PTTIN  10  15  20  Y  50  10  15  20  NP255D

ENTER Y TO CONFIRM, N TO REJECT, OR E TO EDIT
>Y
TUPLE ADDED
```

Trunk log suppressionFocused

See Table 2-56 for a list of "TRK" logs to be suppressed or assigned to a class that is not directed to an I/O device—this is commonly called a garbage class. Perform this step via datafill in tables LOGCLASS and LOGDEV and not by using Logutil.

Focused maintenance operatingFocused recommendations

Initially, the number of line and trunk problems may be so great that implementation of Focused Maintenance creates an overwhelming amount of work. To help eliminate this problem—during implementation of Focused Maintenance—temporarily raise the thresholds and suppress trouble messages. After the troubles become manageable, then lower the thresholds and unsuppress the trouble messages. Focused Maintenance will then—when used on a consistent basis—identify specific lines and trunks requiring attention.

Line Maintenance

General

The DMS-100F system provides both manual and automated resident line maintenance tools. These tools can efficiently identify line card and subscriber loop problems. The automated preventive line maintenance routines can detect subscriber loop problems before they become service affecting and generate customer trouble reports.

Line testing and scheduling for automatic line testing in the DMS-100F switch is performed through the Line Test Position (LTP). The LTP is the human-machine interface between operating personnel and the Line Maintenance Subsystem (LNS). The LTP is a MAP position with a communication module and test jacks. Even though most test circuits are built into the switch, test jacks are provided for external test sets to make impulse noise, return loss, and other special line tests.

MAP access for line testing is first made to the LNS level from the CI level by typing MAPCI;MTC;LNS. From there, the LTP level can be accessed for manual testing, or the ALT level can be accessed for setting up the automatic line tests. The LNS level also provides access to the Focused Maintenance for lines LNSTRBL level.

See Figure 2-4 for the LNS subsystem levels and commands. LTPISDN level commands are accessed off the LTP level and are shown in the *System Products* section under the "ISDN Overview and Maintenance" subsection of this manual.

Line maintenance features

Line maintenance is accomplished with software and hardware features provided within the switch. The following line maintenance features, followed by their descriptions, provide the various line testing facilities for routine and trouble testing, as well as surveillance and monitoring capabilities:

- MAP lines (LNS) alarms and testing
- Line log messages
- Operational measurements (OMs) for lines
- Focused maintenance for lines
- Automatic line testing (ALT)
- ICMOLINE for babbling lines

Figure 2-4 — LNS subsystem MAP levels and commands

LNS
```
0 QUIT_
3 LTP
4 ALT
5 LNSTRBL
```

LTP Level
```
0 Quit
2 Post_
3
4
5 Bsy
6 RTS
7 Diag
8
9 AlmStat
10 CktLoc
11 Hold
12 Next_
13
14
15
16 Prefix
17 LCO_
18 Level_
```

LNSTRBL Level
```
0 Quit
2 Disp_
3 StopDisp
4 ListAlm_
5
6 CreatSet
7
8 Suppress
9 Resume_
10 Qsup
11
12
13
14
15
16 ClrAlm_
17 ClrBuf_
18
```

ALT Level
```
0 Quit
2 Post_
3 ALTInfo
4
5
6
7 SDiag_
8 Diag_
9 LIT
10 Bal
11 CktTst
12
13
14
15
16
17
18
```

ALTLIT Level
```
0 Quit
2 Post_
3 ALTInfo
4 Start
5 Stop
6 Remove
7 Define_
8 Submit
9
10
11 DefMAN
12
13 DefSCHD_
14
15 Status_
16
17 OVRide_
18
```

LTPMan Level
```
0 Quit
2 Post_
3
4 Loss
5 Noise_
6 ToneGen
7 Jack
8 TestRing
9 Bal
10 RlsConn
11 Hold
12 Next
13
14 Ckttst
15 Sustate
16 SetLpBk_
17
18
```

LTPLTA Level
```
0 Quit
2 Post_
3 MonLTA
4 TalkLTA
5 Orig
6 LnTst
7 VDC
8 VAC
9 Res
10 Cap
11 Hold
12 Next
13
14 LTA
15 BalNet
16 Coin_
17 Ring
18 DgtTst
```

LTPData Level
```
0 Quit
2 Post_
3
4 Equip_
5 Connect_
6 Sustate
7 LoopBk_
8 BERT_
9
10 BPVO_
11 Hold
12 Next
13
14
15
16
17
18
```

CSDDS Level
```
0 Quit
2 Post_
3 Seize
4 Cktloc
5 Bsy_
6 RTS_
7 Diagn
8 LoopBk
9 BERT_
10 Rate_
11 Hold
12 Next_
13
14 Reset
15 Turn_
16 Monitor_
17 Select_
18 NextS
```

IBNCON Level
```
0 Quit
2
3 Select_
4 Next
5 Busy
6 RTS
7 Diagnose
8
9
10 Seize
11 Release
12 Clear
13 PrevDM
14
15
16 QConline
17 QCustGrp
18 QSeated
```

NOTES:
1. The following levels are available only with the specified software:
   IBN Console = NTX101   LTPData= NTX250   CSDDS = NTX061
2. The menu of commands for the ALTLIT level is the same as for the other ALT sublevels except that command LITINFO in the ALTLIT level does not appear at any other ALT sublevel.

- World line card (WLC)
- Line card monitoring
- BIC relay testing

MAP lines (LNS) alarms and testing

Function

Line alarms appear under the LNS subsystem header of the MAP. When different classes of LNS alarms exist simultaneously, the MAP displays only the highest priority alarm. When more than one alarm of the same severity exists, an abbreviated version of the alarms may be displayed. When alarms appear under the headers to the left of the LNS header, they should be cleared before the LNS alarms.

Higher level alarms for the Line Module (LM) and Line Concentrating Module (LCM) appear on the PM level of the MAP.

Line maintenance procedures

For references to NTPs that support line maintenance procedures, see NTP 297–1001–594, *DMS-100 Family Lines Maintenance Guide* and any related PCL documents. The following procedures can be found in the NTPs:

- analyzing LNS subsystem alarms
- analyzing line status codes
- diagnosing subscriber complaints
- correcting system diagnostic failures
- replacing faulty line cards (POTS, EBS DATAPATH, and ISDN)

Line alarm status

The ALMSTAT command on the LTP level, when used *without* parameters, interrogates the alarm system of the LNS subsystem and displays the status of line alarms. The command, used with parameters, displays all or selected alarms at specified units in the host or remote sites. The command can also be used to set or change the threshold of the alarm classes in the switch. The following are the default settings and should be adjusted to meet surveillance triggering and the operating company service and performance objectives:

DEFAULT SETTINGS

	MINOR	MAJOR	CRITICAL	NOTE
Long Diagnostic Fail (D)	25	50	100	1
Facility Fault (F)	25	50	100	1
Short Diagnostic (S)	25	50	100	1
Needs Long Diagnostic (N)	25	50	100	1

ICMO Major (I)	5	10	15	1,2
ICMO Minor (i)	5	10	15	1,2
CKTTST Fail Terminal (l)	5	10	15	1,3
CKTTST Fail Line Card (L)	5	10	15	1,3
STATE = PLO (PSPD)	10	20	30	3

NOTES:

1. Adjust alarm settings to meet your "trigger" levels.

2. ICMOLINE line condition setting must be low enough for early
   trouble indication.

3. Dependent on number of lines—must be low enough for early
   trouble indicator—but high enough not to alarm on an average day.

LTP level

Manual testing of lines is performed using the LTP level and its sublevels from the
MAP. The main work operations are

- line card testing, all types and conditions

- subscriber loop testing, all conditions

- console test

- electronic business set testing (IBNCON level)

- Datapath data unit testing

- AIM (Asynchronous Interface Module)

- Bit Error Rate Testing (BERT)

LTP commands programmable feature

The User Programmable LTP Levels feature in software package NTX001AA pro-
vides for the capability of assigning commands within the LTP sublevels and creating
user-defined sublevels that contain a subset of commands. This capability exists
through two tables, LTPDEF and LTPAUX.

The Line Test Position Default Commands (LTPDEF) table contains the LTPMAN,
LTPLTA, LTPDATA, and LTPISDN maintenance sublevels of the LNS subsystem.
The LTPDEF allows for customizing or reorganizing the commands (moving or hid-
ing commands in different menu levels).

The Line Test Position Auxiliary Commands (LTPAUX) table allows the user to cre-
ate sublevels containing commands from other existing sublevels. A maximum of 16
user-defined sublevels can be defined with a maximum of 32 commands per sublevel.

For information on using this feature, see NTP 297-YYYY-350, *DMS-100F Translations Guides* and tables LTPDEF and LTPAUX.

Line log messages

Three types of logs that are directly related to line activity: LINEXXX logs for POTS, EBS, and DataPath lines, LINEXXX and ISDNXXX for ISDN lines, and ALTXXX for automatic line testing. There are also indirectly related line activity logs, such as AUDXXX logs and the SECU127 log that are generated when a START, STOP, REMOVE, or OVERRIDE is used in the ALT MAP levels. See the *System Products* section and the "ISDN Overview and Maintenance" subsection of the manual for further information on ISDN logs.

Line log recommendations

If the Focused Maintenance for lines feature is not available in the switch—to help manage line logs—it is recommended that certain line logs be threshold controlled, or suppressed within table LOGCLASS. Other line logs related to manual activity could also be suppressed. Evaluate the need for the log and its impact on service before suppressing any log. See the "Log System Administration" subsection within the *Office Administration* tab for further information.

It is also recommended that specific LINEXXX logs—such as ISDNXXX logs—be assigned a special class through table LOGCLASS and routed to a printer or other device for analysis.

Line log reduction

The line log reduction feature can help reduce high runner LINE logs. As an example, the LINE102 and LINE103 line lockout logs are no longer generated with this feature; however, they are still available through LOGUTIL. Also, line logs 105, 106, and 108 generated from permanent signal/partial dial (PSPD) calls are not generated or pegged until call treatments (recordings, tones, howler, etc.) have been completed.

This feature should have a significant improvement for line log maintenance by:

- reducing line log volume, including LINE100 & 101 line card diagnostic logs
- preventing customer dialing errors from causing PSPD logs and helping with the analysis of PSPD logs

Focused maintenance feature for lines

This feature focuses on line problems through thresholding, alarm generation, and buffering of line trouble messages. See the previous "Focused Maintenance" subsection for a description and information on the operation and datafill for activation. NT recommends that focused maintenance be used daily.

Use of this feature allows trivial line log messages to be suppressed or routed to garbage class; therefore, providing a significant reduction in logs.

Automatic line testing (ALT)

The Switching Control Center (SCC), or other comparable group responsible for maintenance, should be responsible for ensuring that the preventive maintenance ALT routine is scheduled and log reports are being routed to the proper group for analysis. See the "Routine Tasks" subsection at the beginning of the *Preventive Maintenance* section for recommended scheduling. See Exhibit F (Summary of Automatic Line Testing Recommendations) later for recommendations on scheduling of the following subroutine tests.

The following is a brief description of the automated line card and loop tests:

- **BAL:** The balance (BAL) test automatically sets the balance network in the line card to provide transmission balance between the four-wire side of the switch and the two-wire loop. The BAL test used with ALT is performed as an on-hook balance test. For further information, see "Balance network testing" on page 2-140. Also, see Exhibit A on page 2-145 (Line Card Balance (BAL) Testing Recommendation).

- **LIT:** The Line Insulation Test (LIT) automatic test identifies cable pair faults so they can be cleared before they become service affecting, and before subscribers report hum, grounds, noise, and false ring trip types of trouble. See Exhibit B on page 2-146 (Automatic Line Insulation Testing Recommendation).

- **DIAG:** The Diagnostic (DIAG) test is a comprehensive automatic test that checks virtually all line card circuits for correct operation. It identifies defective line cards and facility faults before they cause customer reports. See Exhibit C on page 2-147 (DIAG: Diagnostic Testing Recommendation).

- **SDIAG:** The Short Diagnostic (SDIAG) performs a subset of tests from the comprehensive DIAG test to ensure that most of the line card circuitry operates correctly. See Exhibit D on page 2-147 (SDIAG: Short Diagnostic Testing Recommendation).

- **CKTTST:** Applies to loops using Electronic Business Sets (EBS), Data Units (DU) associated with Datapath, Asynchronous Interface Modules (AIM) and IBERT line cards. It performs *circuit tests* to confirm the ability of the set and/or line card to transmit and receive messages correctly and adhere to the message protocol. See Exhibit E on page 2-148 (CKTTST; Circuit Testing Recommendation).

ALT routine test outline

A general outline for setting up ALT routine tests follows. For this scenario, the BAL test was selected. In practice, the same scenario would be followed for all the ALT tests: SDIAG; DIAG; LIT; BAL; and CKTTST.

Step	Action/response	MAP Activity (Example Only)
(A)	Advance MAP position to ALT menu.	>CI; MAPCI; LNS; ALT
(B)	Select the desired ALT test to be run.	>BAL
(C)	Menu changes from ALT to TBAL.	
(D)	Create a name for the test.	>DEFSCH <TEST ID>
(E)	Define the test to be run.	>DEFINE (enter data)
	– STARTLEN	
	– ENDLEN	
	– Start and stop times and day	

NOTE: For LIT tests, foreign voltage, leak and ground values are defined.

(F)	Place data in ALTSCHED table for subsequent testing as programmed.	>SUBMIT
(G)	Test ready to run at next schedule time span. Testing commences from the STARTLEN or from last LEN tested + 1.	>START

The ALT routine test schedule is stored in table ALTSCHED. It may be changed using the ALT commands and finishing with the command SUBMIT that updates the tuples in the table. The ALT testing must be stopped before modifying table ALTSCHED. Table control may also be used to modify table ALTSCHED.

Retesting ALT troubles

All identified troubles are retested before the scheduled ALT test time expires. The retesting is performed on completion of the testing for each LCD and at the end of the scheduled test time span. An algorithm determines when to stop routine testing and start retesting troubles based on the quantity of troubles and test time.

If a currently running ALT test is stopped, or overridden from a command, date, or time change that causes the test to be stopped, a retest cycle is not performed.

TTT/TTU equipment allocation

The TTT and TTU test equipment is now allocated between ALT usage and other test requirements. The default value is a 50% split. However, to ensure maximum ALT testing, allocate the highest possible percentage of test equipment for ALT, while still meeting other needs. The allocation of TTTs and TTUs is made in table OFCENG, using parameters ALT_TTT_USAGE_PERCENTAGE and ALT_TTU_USAGE_PERCENTAGE.

ALT references

Reference NTP 297-1001-594, *DMS-100 Lines Maintenance Guide.*

ICMOLINE feature for babbling lines

Incoming message overload line handler (ICMOLINE) is a feature for managing *babbling line* (also known as showering lines) conditions. A babbling line is defined as a line that is reporting excessive on-hook and off-hook transitions. They can degrade and even take down an LCM if not detected and removed from service. Cordless phones have been known to babble a line under various field induced conditions. The main points of this feature are:

- detection of ICMOLINE (babbling line) conditions.

- establishes a new line state "system busy" (SB) to indicate the system has taken the line out of service.

- establishes a separate test queue for ICMOLINE conditions.

- audits the diagnostic process to ensure it is always capable of diagnosing ICMOLINEs.

- audits the ICMOLINEs that have been taken out of service and ensures that the transient ICMOLINE lines are returned to service with continuous ICMOLINE lines remaining disabled (SB).

- establishes a RECIDIVIST queue for repeat offenders. Posting the RECIDIVIST queue provides a record of the 128 most frequent ICMOLINE reports. This queue highlights problem areas requiring investigations.

- allows maintenance personnel to post the ICMOLINE queue to determine current system busy lines. These lines are out of service and should be repaired promptly to avoid a customer trouble report.

Line Card Monitor feature

The Line Card Monitor feature "NC0109" in software package NTXP00AA was developed to indicate that a line hazard—foreign line voltage—has been detected on the line, and that the cut-off relay on the line card has been operated to isolate the line. This feature was formerly called the "Line Card Hazard" feature. The affected line remains out of service until the hazard condition is cleared. This over voltage feature is part of the new World Line Card (WLC).

World line card (WLC)

The world line card (WLC) is a universal type line card introduced to replace the Plain Old (or Ordinary) Telephone Service (POTS) type "A" and "B" domestic and international line cards. In North America, it replaces the NT6X17AA, NT6X18AA & AB Line Cards. The template names for the WLCs are NT6X17BA and NT6X18BA.

Line logs LINE170 and LINE171 provide measured information for WLC diagnostic failures. An optional parameter "D" has been added for the DIAG command to allow the logs to be generated with failures. The intent is to provide the log information as an attachment to the card when it is returned for repair.

For a description of the WLC, see PLN-8991-104, *DMS-100F Provisioning*. Further description of the NT6X17BA and NT6X18BA WLCs can be found in NTP 297-8991-805, *DMS-100F Hardware Description Manuals.*

Hazard line logs

To alert personnel to this important problem, a critical alarm LINE132 log is generated whenever a line is confirmed as being hazardous. The following is an example of that log:

```
*** LINE132 AUG01 10:15:57 2356 TBL
        LEN HOST 15 1 9 27    DN 3511005
        REASON = Line Hazard Condition Found
        INFO =      0 VAC    839 Ohms     76 VDC
        ACTION TAKEN = Cut-off Relay Operated
        ACTION REQUIRED = Check Facility
         CARD CODE = 6X17AA
```

Another line log, LINE133 with no alarm, is generated whenever the cut-off relay is released and the line is no longer isolated.

Hazard OMs

A new OM group, LINEHAZ, provides a count of the number of detected line hazard conditions, a 100 second peg count for all the line hazards in effect at that moment, and a count of the number of line hazards cleared. See registers, HAZDET, HAZSCAN, and HAZCLR in NTP 297-YYYY-814, *DMS-100F Operational Measurements* for further information.

Hazard line parameter

The hazard line feature is enabled and disabled for the entire office with the LINE_CARD_MONITOR parameter in table OFCVAR.

Hazard line options

The no hazard test (NHT) option is used in tables LENLINES and IBNLINES to prevent line hazard testing on specific lines as needed.

LCM talk battery audit

Previously, loss of talk battery to an LCM shelf was not reported unless the talk battery fuse blew. The unreported loss of talk battery meant that operating company personnel were not alerted that LCM subscriber lines were unable to draw dial tone. The Talk Battery Alarm feature, AF5912, addresses this problem by adding new computing module (CM) and LCM maintenance software that periodically audits each LCM shelf for the presence of talk battery.

If the audit fails to detect talk battery, a critical alarm log report (PM179) is generated.

To be capable of supporting this feature, each LCM shelf must be provisioned with at least one world line card (WLC). The WLC used for the talk battery audit can also be

used by a subscriber for call processing. A minor alarm log report (PM179) is generated if no WLCs are available to perform the audit when the feature is ON.

NOTE: This feature supports all WLC types, and there are no restrictions where the WLC is assigned in the LCM shelf.

BIC relay testing

One relay on the NT6X54AA Bus Interface Card (BIC) is a reversal relay that is used to apply ringing for multiparty ringing with a NT6X17AA Line Card, and tip-side ringing on a NT6X19AA Message Waiting Card. For the BIC reversal relay to be used for this purpose, the ALLOW_RINGING_ON_TIP_SIDE parameter in table OFCENG has to be set to "YES" (Y). To detect any BIC reversal relay problems, a feature was developed to test the BIC reversal relay—it is called the BICRELAY test.

The BIC relay test (BRT) feature provides the capability to schedule automatic BIC relay testing throughout the office on an LCM basis. It should only be used where multiparty ringing on a NT6X17AA Line Card and NT6X19AA Message Waiting Cards are used.

The BICRELAY command at the CI level turns the BIC relay test on or off, restarts the test, queries the status of the test, queries the number of LCM level tests in progress, and queries the next LCM to be scheduled in the system. Turning the BRT off does not affect the use of the manual command from the LCM menu MAP level,

In table LCMINV is a field called "BICTST" that has to be set to "Y" for the automatic test to be run for any XPM equipped with BIC relays. In table OFCVAR are two parms that control the scheduling of the automatic BIC relay test—parameters POS_BICRELAY_XLCM_TEST_SCHEDULE and POS_BICRELAY_NUM_SIMUL_TESTS.

For procedures on how to set up BIC relay testing, see NTP 297-YYYY-546. Reference NTP 297-1001-822, *DMS-100F Commands Reference Manual* for a description of the BICRELAY command and subcommands.

Balance network testing

Balance (BAL) network testing (BALNET) of a subscriber loop measures the transhybrid loss by sending a short burst of tones over the loop. This determines whether the loop is loaded, non-loaded, and if necessary adds padding for echo return loss requirements. Balance network pads are provided on the line cards to match the impedance of loaded and non-loaded loops. The test should not be run on lines with loop electronics since tests would not be valid.

It is very important to understand the need for running on-hook and off-hook tests for subscriber loops. It can help minimize subscriber reports of: noise, echo, garbled, hollow, hum, too loud, and can't be heard. It can also indicate other outside plant problems that need correcting.

The LTPLTA level BALNET test can be run for both on-hook and off-hook. For the LTPMAN level, the BAL test is used for on-hook testing only. The ALT level for automatic line testing uses the BAL test for on-hook testing.

Real-time off-hook testing

For BCS35 and earlier, balance network testing in the off-hook state requires that the technician: use the LTPLTA level of the MAP, contact the subscriber, and perform the BALNET test with the subscriber on the line. Even though the off-hook test is more accurate than the on-hook test, it requires time and field assistance.

In BCS35, an optional feature called "Off-Hook Testing" provides an off-hook balance test on an originating call basis. The test is performed after the last digit is collected with the following conditions:

- the line is a NT6X17 or NT6X18
- the feature is enabled in table LNADMIN
- the CC occupancy is below the level set in table LNADMIN
- the field TEST_TYPE is enabled in table LNBNV
- the line has not already been tested
- a TTU is available according to the requirement in table LNADMIN

Besides the loaded and non-loaded tests, the new off-hook balance test can determine whether a 900+2 balance network would be a better choice for maintaining echo at a minimum.

Tables LNADMIN and LNBNV have been added to support the off-hook testing capability. Logs LINE220, 221, and 222 have been added to provide test failure and changes in BNV values for lines. The CI level QBNV command has been added to display a range of specified LENs and their off-hook test status.

For further information on this feature, see the NC0495 "Off-Hook Testing" feature in the NTX901AA software package within the TAM-1001-005 ISS35, *BCS35 Maintenance Synopsis* and the *BCS35 Release Doc*.

SET_TO_UNBALANCE parameter

This OFCENG table parameter—when set to "Y" (Yes)—informs the automatic line testing (ALT) feature that a balance test must be performed on all new POTS lines that have the table LNINV manual override (MNO) field set to "N", and a padgroup setting of STDLN.

When this parameter is set to "Y" and a service order on a POTS line is activated using SERVORD, the padgroup in table LNINV is changed to UNBAL and a BAL test is scheduled for the line.

Remember, this parameter is always set to "N" with a new load or a restart.

Dialable test line features

Test line features that are accessed through dialing a number are primarily used by outside plant repairman to diagnose facility and customer premises equipment (CPE) problems. Other than the 101 communication test line—used only by inside plant personnel—the following dialable loop and station type tests can be performed by installers or repair personnel at the customer's site or other loop facility access locations:

- 101 communication test line
- 108 test line for ISDN BRI lines
- Dialable cable pair locator (Feature package NTX277AA02)
- Dialable short circuit (Feature package NTX277AA02)
- Silent switchman test (SSMAN) (Feature package NTX053AA04)
- Station ringer tests (SRT) (Various feature packages)

101 communications test line

The 101 communication test line uses a 5X30AA card mounted in a Trunk Module (TM). It interfaces the Network Module (NM) and the LTP, and is used at the communications module to originate voice contact with a subscriber or a far-end office while performing tests. The test line is activated when the LTPLTA level is accessed and the TALKLTA command invoked.

It is possible to remote the 101 communication test line when the LTP is located remotely from the switch. Interconnecting digital facilities can be tied directly to the test line through a line card; however, where analog facilities are used, the test line might require a dial long line circuit and voice amplification.

108 test line for ISDN BRI lines

The 108 test line for ISDN Basic Rate Interface (BRI) was introduced in BCS35. This feature provides the capability for the 108 test line to be dialed up from the customer premises. When it is dialed up, a B-channel loopback will be applied at the line card toward the customer end. BERT testing can then be preformed from the customer's end. For further information on this feature, see the *System Products* section and the "ISDN Overview and Maintenance" subsection in this manual. Also see the trunk side 108 test line in the following "Trunk Maintenance" subsection.

Dialable cable locator

The dialable cable locator (DCL) tone feature places a tone from an external generator on the line under test for identifying the physical plant by the installer/repair technician. This is achieved by the technician first dialing a security access code for the DCL test feature and then dialing the line number under test. The switch connects the tone by way of a MAINT type trunk that is datafilled in table TRKGRP. The technician then uses a special probe, designed to accept the frequency of the applied tone,

and locates the desired cable pair. The tone remains on the line for a specified interval, up to 600 seconds (10 minutes), then the line returns to normal. Operating companies establish the access code for the DLC feature by datafilling table STDPRT. The tone time-out value is set with the parameter CABLE_LOCATE_TIMEOUT in table OFCENG.

Dialable short circuit

The dialable short circuit (DSCKT) feature places a short circuit across the tip and ring of the cable pair at the switch end by using the metallic test access (MTA) feature. This action is taken by the installer/repair technician during some line trouble locating procedures. The DSCKT test is executed by the technician dialing the access code on the line under test or another line. The shorted loop remains in effect for the interval set by the operating company (range 0 to 600 seconds). Operating companies establish the access code and timing by datafilling tables MTATRK, CLLI, STDPRTCT and setting parameter CABLE_SHORT_TIMEOUT in table OFCENG.

Silent switchman test

Silent switchman test (SSMAN) feature opens the tip and ring of the cable pair at the cut-off relay on the line card. This action is taken by the installer/repair technician during some outside plant trouble locating procedure. The SSMAN test is executed by the repair person dialing a three digit code from the customer station being tested. When the code is dialed, ten seconds of interrupted tone is received, and the line is cut-off for a period of up to 225 seconds (to allow testing on the open circuit). See parameters INTL_SILENT_SWITCHMAN_TIMEOUT and SILENT_SWITCHMAN_TIMEOUT in table OFCENG for setting the time-out.

Station ringer test

The station ringer test (SRT) consists of tests performed on the station equipment—usually a residential telephone (POTS, EBS) or coin station—by a technician at that station. In some cases the customer can perform the tests. SRT features have been developed for the following types of stations:

- DP & DGT (POTS and COIN service)
- Electronic Business Sets (EBSs—various types)
- Data sets

The technician can access the SRT by dialing the access digits. Some of the tests that can be performed are:

- DP or DGT dial test
- off-hook ground test
- on-hook ground test
- party identification

- coin return control mechanism test for coin stations.

See the "MDC Overview and Maintenance" subsection within the *System Products* section for additional information on the EBS SRT feature.

Exhibits

The following exhibits provide a quick reference to the line maintenance tools previously described in this subsection.

Exhibit A — Line card balance (BAL) testing recommendation

Exhibit B — ALT line insulation testing (LIT) recommendation

Exhibit C — Extended diagnostic (DIAG) testing recommendation

Exhibit D — Short diagnostic (SDIAG) testing recommendation

Exhibit E — Circuit testing (CKTTST) recommendation

Exhibit F — Summary of automatic line testing recommendations

Exhibit G — Focused maintenance for subscriber line CP failures

Exhibit H — Restoring lines in the diagnostic failure state

Exhibit A

Line card balance (BAL) testing recommendation

Purpose:

Balance line circuit networks as required to prevent customer reports of noise, hum, static, echos, too loud, etc. Problems can show up when customers from different subscriber carrier systems call each other, or from outside cable problems. See "Network balance testing" within this subsection for more information.

Recommended Operation:

ALT BAL testing should be operated seven days a week to assure that all subscriber lines will be balanced in the event recent work activity—line transfers, cable transfers, service orders and the replacement of line card equipment—has ocurred on the line.

M T W T F S S   2101   2300

- - - - - - - - - - -

Y Y Y Y Y Y Y

Also, recommend setting SET_TO_UNBALANCE parameter to "Y" in table OFCENG.

Activation:

The recommended testing frequency should be activated as soon after cutover as possible. The basic scenario for setting up and activating ALT testing is described on page 2-136.

Note:

The frame containing the line card must be isolated from the old office to get a correct test result. Running time is approximately 5 seconds per line card.

Exhibit B

ALT line insulation testing (LIT) recommendation

Purpose:

ALT Line Insulation Testing identifies line faults so they can be cleared before they become service affecting, and cause subscriber reports (i.e., hum, grounds, noise, and false ring trips). Analysis of ALT10x—LIT log messages is normally performed by the operating company group responsible for outside facility problems. It may be the Local Test Desk, Repair Service Bureau, or Predictor Group. Testing time is approximately 15 seconds per line.

Recommended Operation:

M T W T F S S   05:01 to 07:00 (Time slot determined by Predictor, LTD, RSB.)

- - - - - - - - - -

Y Y Y Y Y Y Y

Log failure messages produced:

ALT102 — LIT Incomplete

ALT103 — LIT Volts

ALT104 — LIT Resistance

ALT106 — LIT Capacities

It is recommended that log failure messages be routed to the Local Test Desk, or Repair Service Bureau, or Predictor Group.

Activation:

The recommended testing frequency should be activated as soon after cutover as possible. The basic scenario for setting up and activating ALT testing is described on page 2-136.

Notes:

1. Customer lines equipped with long-haul equipment and PBX terminations that place battery or ground conditions on the loops towards the DMS-100F switch will cause the ALT to report a trouble condition. Therefore, these types of lines should be excluded from the ALT test schedule by adding No Line Test (NLT) line option.

2. The group responsible for outside facility problems should determine fault detection values commensurate with outside plant conditions.

3. See "EBS testing" within the "MDC Overview and Maintenance" subsection for a description of the feature required to prevent resetting EBS telephone set volume level when running ALT.

4. Once LIT is setup, operations personnel responsible for the DMS-100 switch should periodically verify that LIT is being used.

Exhibit C

> # Extended diagnostic (DIAG) testing recommendation
>
> **Purpose:**
> DIAG is a comprehensive test of virtually all of the line card circuits for correct operation. Identification of the line card trouble and facility faults before they become service affecting. ALT101 log messages are produced with failures.
>
> **Recommended Operation:**
> M T W T F S S   23:01 to 05:00
>
> - - - - - - - - - -
>
> Y N Y N Y Y Y
>
> **Activation:**
> The recommended testing frequency should be activated as soon after cutover as possible.
>
> **Notes:**
> 1. Testing time is approximately 60 seconds per line card. If translations for ground start does not match line card settings, this test will fail. Check table LNINV for translations.
> 2. See "EBS testing" within the "MDC Overview and Maintenance" subsection for a description of the feature required to prevent resetting EBS telephone set volume level when running the DIAG test.

Exhibit D

> # Short diagnostic (SDIAG) testing recommendation
>
> **Purpose:**
> Performs a subset of tests from the extended DIAG. To ensure that most of the line card circuitry operates correctly. ALT100 log messages are produced with failures.
>
> **Recommended Operation:**
> M T W T F S S   23:01 to 05:00
>
> - - - - - - - - - -
>
> N Y N Y N N N
>
> **Activation:**
> The recommended testing frequency should be activated as soon after cutover as possible. The basic scenario for setting up and activating ALT testing is described on page 2-136
>
> **Note:**
> Testing time is approximately 15 seconds per line card.

Exhibit E

Circuit testing (CKTTST) recommendation

Purpose:
Performs "circuit tests" for the Electronic Business Set (EBS), Data Unit (DU), Asychronous Interface Module (AIM), and Integrated Bit Error Rate Test (IBERT) type services to confirm the ability of the set or line card to transmit and receive messages correctly and adhere to the message protocol. The test path includes the line card, cable pair and station set. ALT101 log messages are produced with failures.

Recommended Operation:
M T W T F S S   19:00 to 21:00

- - - - - - - - - - -

Y Y Y Y Y Y Y

Activation:
The recommended testing frequency should be activated as soon after cutover as possible. The basic scenario for setting up and activating ALT testing is described on page 2-136.

Notes:
1. The LCM generates and transmits the test messages, and when received back, validates the accuracy of the messages. For this feature to function, the PM loads must include the "keyset option."

2. The test time is dependent upon the number of messages sent (ten messages – approximately thirty seconds).

Exhibit F

Summary of automatic line testing recommendations													
SUB ROUTINES	**APPROX TIME for ONE TEST**	**DAY SCHEDULE**							**HOURLY SCHEDULES**				**NOTES**
		M	**T**	**W**	**T**	**F**	**S**	**S**	**1900 to 2100**	**2101 to 2300**	**2301 to 0500**	**0501 to 0700**	
BALANCE (BAL) TEST	APPROX 5 SECONDS	X	X	X	X	X	X	X		X			1
LINE INSULATION (LIT)	APPROX 15 SECONDS	X	X	X	X	X	X	X				X	1
LINE CARD DIAG. (DIAG)	APPROX 60 SECONDS	X		X		X	X	X			X		1
SHORT LINE CARD DIAG (SDIAG)	APPROX 15 SECONDS		X		X						X		1
CKTTST	APPROX 10 SECONDS	X	X	X	X	X	X	X	X				1,2

NOTES:

1. Adjust scheduling to meet local conditions. Strive to maximize test intervals and frequency.

2. CKTTST applies to the EBS, DU, AIM and IBERT services.

Exhibit G

Focused maintenance for subscriber line CP failures

Purpose:

Manages line call processing (CP) failure messages utilizing a system of buffers, thresholds and alarms. This is an efficient and effective alternative to the existing log system which outputs all line log messages for manual analysis.

Recommended Operation:

Implement Focused Maintenance procedures for lines when Feature Package NTX272AA F3830 has been provided.

Take corrective action for failures exceeding the threshold by responding to the visual alarm indication in the MAP system status display area under LNS.

Note: Focused Maintenance CP alarms are displayed in the system status display area under the MAP header LNS. The CP alarm displays at 30-second intervals, alternating the display position with any other LNS alarm.

Access the LNSTRBL level of the MAP and post the line concentrating device exceeding the threshold. Displayed are the 10 worst line cards which caused the threshold alarm. The details describing the last fault is recorded.

At CI level enter:

MAPCI;MTC;LNS;LNSTRBL

Once the fault has been identified, move to the LNS testing level of the MAP. Proceed with the necessary testing and verification to isolate and repair the fault.

Review (daily) and clear the worst failures recorded for the various LCDs.

Activation:

The recommended testing frequency should be activated as soon after cutover as possible. See the previous "Focused Maintenance" subsection for a description of the feature, and for specific steps to implement and activate Focused Maintenance for lines.

Exhibit H

Restoring lines in the diagnostic failure state

Purpose:
> To restore lines in a diagnostic failure state—MB, CUT, SB etc.— to a working state.

Recommended Operation:
> Every morning these service affecting conditions should be checked and resolved *immediately*.
>
> Action Commands Required: MAPCI;MTC;LNS;LTP
>
> Post S PLO
>
> Post S CUT
>
> Post S SB
>
> Post S MB
>
> **Note:** MB state should be checked last because force releasing (FRLS) any line would place it in a (MB) maintenance busy state.

> **CAUTION**
>
> Do not use a REPEAT "XX" command (Send) since this procedure could tie up receivers.

Examples:

> Restoring PLO Failures
> > MAPCI;MTC;LNS;LTP
> > Post S PLO
> > FRLS;RTS;SLEEP 10;NEXTP
>
> Restoring MB Failures
> > MAPCI;MTC;LNS;LTP
> > Post S MB
> > RTS;NEXTP
>
> Restoring CUT Failures
> > MAPCI;MTC;LNS;LTP
> > Post S Cut
> > LCO REL;NEXTP
>
> Restoring SB Lines
> > MAPCI;MTC;LNS;LTP
> > Post S SB
> > RTS;NEXTP

Trunk Maintenance

General

The DMS-100F system provides a variety of internal maintenance tools to quickly and efficiently identify trunk problems before they become service affecting. This subsection provides a description of those tools, their purpose, associated commands, and reference documents where more detail is provided. A proactive approach toward trunk maintenance would improve service and help reduce customer reported troubles.

Most trunk testing and troubleshooting can be performed from a trunk test position (TTP). The TTP is a MAP equipped with hardware components used for trunk testing. Except for dedicated hardware, up to 64 detached TTPs can be assigned with all the software capabilities of a regular TTP. Specifically, the TTP hardware includes the jack fields—for external test equipment—and the voice communication facility with the headset jack.

Trunk maintenance includes preventive maintenance testing—manual and automatic—for trunk integrity, and corrective maintenance to clear any existing trunk problems. Testing and control capabilities for trunk testing is provided from the TRKS subsystem level of the TTP. By using the commands on the TTP and other subsystem levels, a technician can control, test, and do repetitive tests on:

- all types of trunks
- all digital carrier trunks connected to the switch
- various types of common service circuits such as:

    —multifrequency and digitone receivers
    —special tone and announcement circuits
    —conference circuits
    —test lines
    —test circuits

Information for maintenance on carrier systems can be found in the "Carrier Maintenance" subsection at the end of this section.

Figure 2-5 on page 2-155 provides the commands starting with the TRKS subsystem. Repetitive testing is done using the hidden REPEAT command (e.g., REPEAT 5 TST). For details on the use of all the TRKS subsystem commands and their parame-

ters, as well as hidden commands, see NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide.*

Analog trunks

This basic circuit facility design consists of analog equipment from end to end; however, it may have digital carrier facilities. The trunks terminate on circuit packs within the Trunk Modules (TMs) in the DMS-100F switch and are usually connected to analog switches at the far end.

In this design:

- all trunks must be tested individually.
- voice grade transmission tests should be routinely performed.
- operation and signaling tests should be routinely performed.
- if the trunk is two-wire at any point, then Echo Return Loss (ERL) should be performed. (Loss [E] command at the TTP manual level).

Hybrid trunks

The basic design consists of a digital termination at the DMS-100F and with analog equipment somewhere in the circuit design, either in the facility or at the far end.

In this design:

- all the same tests are required as for analog trunks described above.
- normally a trouble condition in the DMS will affect all trunks in the same digroup.

Digital trunks

This basic design consists entirely of digital equipment (no analog circuitry used anywhere). The trunk originates and terminates in four-wire digital switches and uses digital carrier facilities end to end. In this design:

- all transmission tests are generally measured on one trunk in each DS1 facility.
- operation tests normally need to be done on only one trunk in the digroup.
- echo return loss (ERL) is not required.
- troubleshooting can normally be done on a trunk per digroup basis—except for transmission troubles.

Trunk maintenance features

Trunk maintenance can be accomplished with software and hardware features provided within the switch, and by connecting external test equipment for various tests such as:

- phase jitter
- singing point
- absolute delay distortion
- Echo Return Loss (ERL)
- envelope delay distortion
- foldover distortion
- frequency attenuation distortion
- harmonic distortion
- level tracking distortion
- longitudinal balance

The following trunk maintenance features (followed by their descriptions) provide the various trunk testing facilities for routines and troubles, and surveillance and monitoring capabilities:

- MAP trunks (TRKS) level alarms and testing
- Trunk log messages
- Focused maintenance feature for trunks
- Automatic trunk testing (ATT)
- Dialed loopback on trunks (TKLPBK) feature
- Killer trunk (KT) feature
- Carrier (CARRIER) level
- Trunk group status (STAT TKGRP) level
- Trunk status (STAT TRKS) level
- TTP level and stuck sender (STKSDR) command
- Period trunk maintenance (PRDTKMTC) report
- Translation verification (TRNSLVF) feature
- Diagnostic signaling test (SIGTST) feature

MAP trunks (TRKS) level alarms and testing

Alarms for trunks appear under the TRKS subsystem header of the MAP. Alarms are displayed by priority and can be cleared by following NTP alarm clearing procedures. The following trunk testing descriptions and network settings can be found in NTP

Figure 2-5 — TRKS subsystem MAP levels and commands
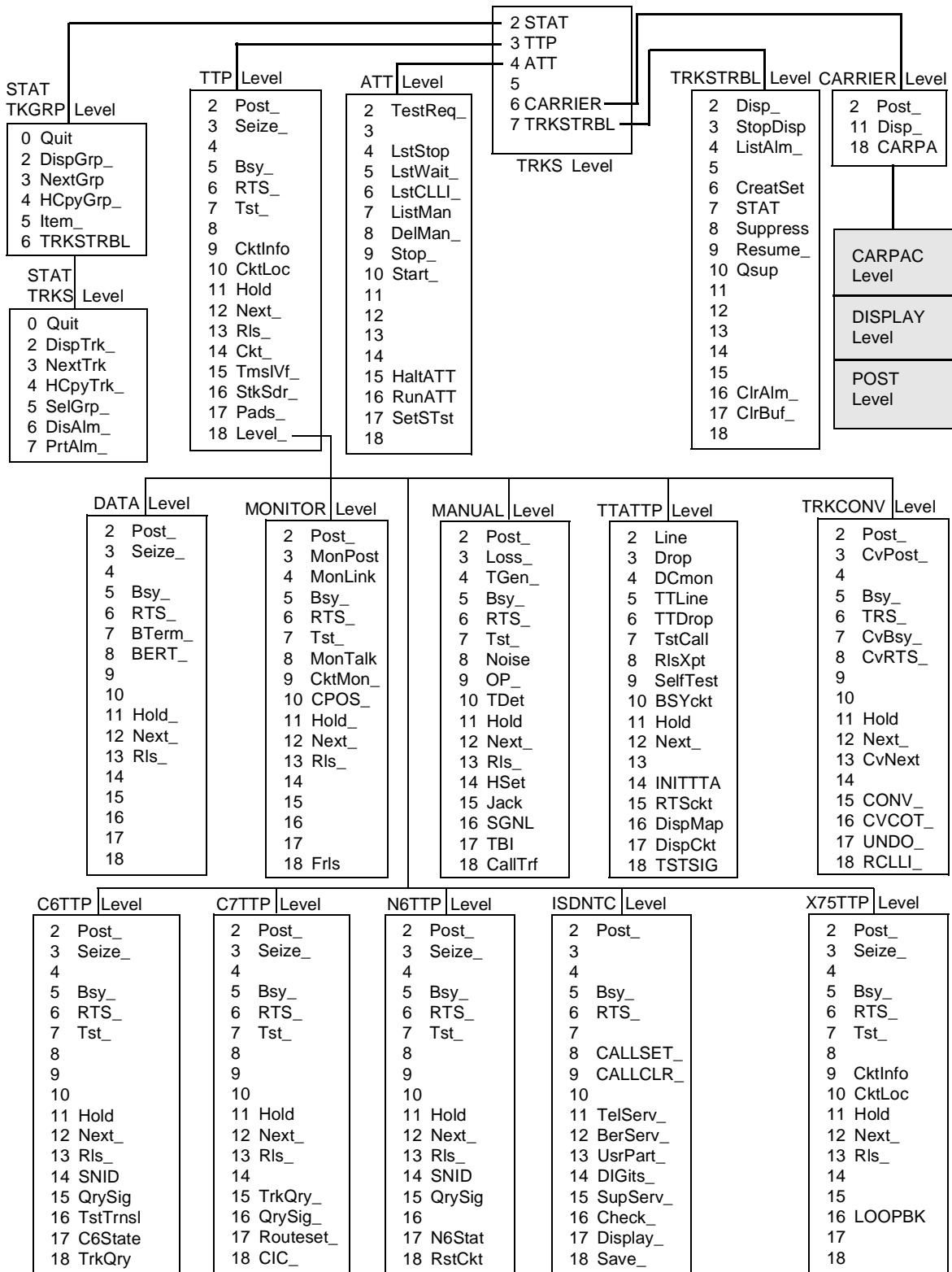
297-1001-595, *DMS-100F Trunks Maintenance Guide* and NTP 297-8991-805, *DMS-100F Hardware Reference Manual*:

- receiver diagnostic test
- test line test
- diagnostic test of trunk test equipment
- level meter test
- noise measurement
- monitoring an in-use trunk
- echo return loss and singing point test
- far-end to near-end loss test
- near-end to far-end loss test
- NT2X80 precision balance network settings
- NT2X77 compromise balance network settings

Trunk log messages

Trunk log messages provide detailed information on trunk failures detected during call processing. Prior to CCS7, the primary trunk log messages were the TRKXXX type. After trunks are converted to CCS7, attention has to be given to specific C7UPXXX logs for analysis of CCS7 trunk problems. For example, since the method of signaling is totally different for trunks after converting to CCS7, log message TRK121 is no longer valid for sender time-out problems as senders are not used for CCS7. C7UP107 and C7UP111 log messages are CCS7 trunk continuity (COT) problems. They present a different maintenance strategy for problem resolution than the sender time-out related TRK121 log messages.

For detailed information on trunk TRK and C7UP log messages, see the NTP 297-YYYY-840, *Log Reference Manuals*. The *Corrective Maintenance* section has more on handling sender and COT failures for CCS7 trunks (more commonly know as ISUP trunks). Also, the "SS7 Overview and Maintenance" subsection in the *System Products* section provides more on ISUP trunk related problems.

Trunk troubles can be identified using the focused maintenance for trunks feature and OM thresholding feature. Other problems can be identified using the ATT, KT, stuck senders, and signaling tests that are described within this subsection. It is recommended that log messages be used to provide further detailed information to correct troubles that have been identified using focused maintenance for trunks, ATT, KT, OMs, and the various TTP testing levels.

TRK138 trunk treatment logs can be used to identify treatment problems. They should be controlled within the TMTCNTL table and the TRKGRP related subtables when they are not needed for analysis.

Focused maintenance feature for trunks

This feature focuses on trunk problems through thresholding, alarm generation, and buffering of trunk trouble messages. See the previous "Focused Maintenance" sub-section for a description and information on the operation and datafill for activation. Nortel Networks recommends that focused maintenance be used daily.

Use of this feature allows trivial trunk log messages to be suppressed or routed to garbage class; therefore, providing a significant reduction in logs.

Automatic trunk testing (ATT)

Automatic trunk testing (ATT) in feature package NTX051AA allows the scheduling of specific trunk maintenance tests—on one-way outgoing (OG) and two-way (2W) trunks, and their facilities—to be run by the system automatically. Automatic testing can test trunks for proper operation (call through tests) and proper transmission (net loss, noise, and BER). ATT should be scheduled to <u>test all trunks at weekly intervals</u> (recommended) . The supporting document for ATT is NTP 297-1001-121, *DMS-100F Automatic Trunk Testing*.

Access to ATT (MAPCI;MTC;TRKS;ATT) allows tests to be scheduled, initiated, monitored, or stopped. Up to fifteen tests can be run simultaneously. The various ATT level commands are described in NTP 297-1001-121.

Functional and diagnostic tests are run by ATT. The functional tests are set up to test circuits in distant offices. These test the signaling integrity and transmission requirements. Diagnostic tests check the trunk hardware within the office.

Activation

To activate ATT, the following tables and subtables must be properly datafilled:

- Table ATTOPTNS (Automatic Trunk Test Sequence Options)
- Table ATTSCHED (Automatic Trunk Test Schedule)
- Table TSTLCONT (Test Line Control)
- Subtable TSTLCONT.TLNOS (Test Line Number)
- Table CLLIMTCE (CLLI Maintenance)
- Subtable DIAGDATA (CLLI Maintenance Diagnostic Data)
- Table MWDATA (Milliwatt Data)

ATT log reports

ATT log reports are generated to provide information on test failures, results, skipped trunks, and summary of test results information on trunk groups. If there is a need to transfer the ATT results to a Device Independent Recording Device (DIRP) file, then parameter TTR_SELECTION_OPTION in table OFCVAR must be set.

ATT recommendation

It is recommended that tests be scheduled during low traffic periods and not interfere with line balance testing (see the previous "Line Maintenance" subsection). Keep ATT tables updated with trunk groups as they are added. Include the three and six-port conference circuits—and other service circuits—in the routine tests. It is also recommended that BERT test be setup on ATT. See the next subsection "Network Maintenance" for BERT setup, and the next paragraphs "Dialed loopback on trunks (TKLPBK) feature" for further information on BERT testing for trunks.

Dialed Loopback on Trunks (TKLPBK) feature

The capability to loopback the T1 carrier (DS1/24 channels) using the CARRIER MAP level commands and manual methods has existed for some time. However, the capability to provide a dialable loopback for an individual DS0 trunk was not available until BCS27 introduced the Datapath feature. Initially, the capability to provide a dialable loopback was developed for data units (DUs) with the Datapath feature (NTX250AA).

A feature in software package NTX001AA provides a dialable loopback capability for trunks on an individual channel (DS0). The loopback is provided within the Network Module (NM) through call processing for local and toll networks. The dialable loopback feature is known as the 108 test line. Various tables define the test line number access codes as described next.

108 test line for trunks

The 108 test line for trunks can be used to isolate trunk troubles and to measure net loss, noise, and run BERT for trunks at the DS0 rate. The 108 test line for trunks as presently described in the Installation Manuals (IMs) and NTPs is for an echo suppressor test line—this is not correct. In 1986 the *American National Standards Institute* (ANSI) and Bellcore's TR-TSY-000476, *Network Maintenance*: *Access and Testing* defined the 108 test line as a *digital circuit test line*. The 108 test line—as defined under these requirements—is the dialable method for accessing the dialed loopback on trunks feature.

For further information on the use of the 108 test line for bit error rate testing, see "BERT for trunks" within the "Network Maintenance" subsection.

108 test line activation

Until the Installation Manual (IM-925), Section 410, implementing the requirements for the 108 test line for trunks is revised, use the following as a general guideline for activation:

- Datafill the following tables and subtables using current translation NTPs:

    — assign CLLI in table CLLI

    — assign a route in table OFRT

— define access code and route in table DN (Bellcore's TR-TSY-000476 recommends 959-1080—verify this within your company before assigning)

— assign the 108 toll access digits in subtable STDPRTCT.STDPRT

— assign the test line numbers TB08 & TB18 (ATT) in subtable TSTLCONT.TLNOS

— set the parameter TRKLPBK_TIMEOUT_IN_MINUTES in table OFCVAR. (Recommend 10 minutes)

Killer trunk (KT) reporting feature

The killer trunk reporting feature (NTX053AA) identifies trunks with short holding time, always idle, always busy, and slow release or disconnect time. Long holding times may indicate improper release conditions. Some of the characteristics are further defined as follows:

KILLER TRUNK — A trunk that has a high number of seizures due to a problem. The problems generally cause the subscriber to drop the connection and attempt the call again. Killer trunks have a high attempt rate with a lower than average holding time. For example, excessive or short duration holding could indicate:

- no transmission on analog, digital, or ISUP trunk (watch for COT failures)
- transmission static or noise
- reaching wrong numbers due to signaling problems
- sleepy trunks
- cutoffs soon after the connection is made
- the lack of a start signal for non-ISUP trunks

ALWAYS IDLE — A trunk that has a usage of 0 CCS and zero attempts. Improper network management controls, over-engineering, and equipment malfunctions are all causes of this condition.

ALWAYS BUSY TRUNK — A trunk that has a usage of 36 CCS and zero attempts. Under-engineering, normal high usage, facility, and equipment malfunctions are among the causes of this condition.

SLOW RELEASE TRUNK — A trunk that indicates a low attempt rate with a fairly high usage. Malfunctioning supervisory and facility equipment is typically the cause of this problem.

Operating modes

The killer trunk feature provides the following three modes of operation:

AUTO — Trunks are instrumented on a rotational basis as specified in table TRKGRP. When the next interval begins, the next set of 2048 trunks is instrumented.

MANUAL — Trunks are instrumented in order of the groups declared in table KTGROUP. When the next interval begins, the next set of 2048 trunks is instrumented.

SEMI-AUTO — Trunks are instrumented in order of the groups (2048 max trunks & 350 max trunk groups) defined in table KTGROUP and are instrumented on a rotational basis.

KT reports

KT reports can be received through the KTPARMS table GENKTLOG field, or manually through the KTREPORT command at the CI level of the MAP.

KTRK100 LOG REPORT — This log is generated at the end of every interval if the GENKTLOG field in table KTPARMS is set to "ON". Based upon other settings in the KTPARMS table, the log report will list trunk groups that exhibit any of the killer trunk properties. If needed, the last log generated is stored in holding registers and can be accessed by using the LOGUTIL OPEN command.

Following is an example of a KTRK100 log report:

```
KTRK100    mmmdd    hh:mm:ss    ssdd    INFO  KTRK_REPORT
_____
EXCEPTIONS
KTPARMS  CRITERIA:          PEG            HT            TROUBLE
                     > ktpegmin  <  kthtmax    KILLER  TRUNK
                                 >  srhtmin    SLOW  RELEASE
_____
GROUP      MEMBER      PEG      USAGE      HT      TROUBLE
clli       ext_trk      n1       n2        n3       trbl

ACCUMULATION  TIME:  n  n
```

KTREPORT — This command and its parameters generates one of the following three types of outputs:

- ACTIVE — Displays all the trunk groups currently under KT observation.
- FILEDIR — Lists all KT raw data files from DIRP.
- ANALYSIS — Analyzes raw data files to develop lists of trunks with KT properties.

The following are examples of ACTIVE and FILEDIR outputs:

KTREPORT ACTIVE command sample report:

```
KILLER  TRUNK  REPORT: Active  Trunk  Groups
Report  Time:   yy/mm/dd    hh:mm:ss
_____
CLLI1
CLLI2

          Continued  on  next  page
```

```
CLLIn
TOTAL  TRUNK  GROUPS  INSTRUMENTED    =  yyyy
TOTAL  TRUNKS  INSTRUMENTED     =  xxx
```

KTREPORT FILEDIR command sample report:

```
KILLER  TRUNK  REPORT: Directory  of  file  XXXXX
Report  Time:   yy/mm/dd    hh:mm:ss
_____
Report  Interval: xx  Hrs  xx  Min

REPORT     INTERVAL
NO         START
1          hhmm   .  .    yy/mm/dd
2          hhmm   .  .    yy/mm/dd
.
.
.
n          hhmm   ..  yy/mm/dd
```

KT data storage

KT raw data can be stored in the DIRP subsystem. Tables DIRPOOL and DIPRSSYS must be datafilled if the KTRK stream is to be retained for all restarts and BCS applications. The command KTRBIND is used before and after datafilling table DIRPSSYS to bind DIRP to the KTRK subsystem.

Where the customer data change (CDC) feature exists in a switch and the customer desires to have access to KT data, then the KT_SELECTION_OPTION parameter in table OFCVAR must be datafilled. Also, table DATAOWNR, which determines whether the operating company or the customer owns the trunk, must be datafilled.

If DIRP is no longer to be used to record KT data, then the KT volumes should be removed using DIRP, and command KTRUNBND should be used to unbind the KTRK stream from DIRP. Use the DIRP AUDIT command to remove any KTRK alarms from the MAP.

KT activation and verification

To activate the KT reporting feature, the following steps are suggested:

1. In the Killer Trunk Parameters (KTPARMS) table, set the ENABLE field to "OFF" and datafill with the desired values for:

— scan rate

— start and stop times

— report interval

— peg counts and holding times to be used as default values during the report generation

— mode of operation

— GENKTLOG "ON" or "OFF" as desired for the KTRK100 log

2. Datafill Killer Trunk Group (KTGROUP) table with the valid CLLIs that are already defined in table TRKGRP and are supported by the KT feature.

3. Datafill table KTMINMAX with peg count and holding time criteria for specific supported trunk groups. The CLLIs within this table must have been previously defined in table TRKGRP. The datafill in table KEMINMAX is necessary for the KTMINMAX parameter and the use of the KTREPORT ANALYZE command.

4. Set the ENABLE field in table KTPARMS to "ON" to activate the schedule function. The trunk groups are instrumented within ten seconds after the ENABLE field is set to "ON".

5. To verify that the KT feature is active, type in the KTREPORT ACTIVE command and you should receive a list of the trunks that are instrumented for the KT feature. If not, then check the ENABLE field in the KTPARMS table to be sure it is on.

KT recommendations

It is recommended that the KT program be run continuously during busy hours. Adjust the KTPARMS peg counts and holding time fields to focus on obvious trunk problems first and to eliminate a long list of potential trunk problems that might discourage any analysis effort.

KT reference

The best single source reference is NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*.

Trunk group status (STAT TKGRP) level

Function

The STAT TKGRP level is accessed off the TRK level of the MAP —see Figure 2-5 on page 2-155. At the CI level, type MAPCI;MTC;TRK;STAT to get to the STAT TKGRP level. The commands at this level are used to monitor and maintain outgoing, incoming, two-way, and miscellaneous trunk groups—including test trunks and receivers. The ITEM command is used to display data on individual circuits within a group that has been displayed using the DISPGRP command, and to access the STAT TRKS level. The TRKSTRBL command for the focused maintenance feature (previously described) for trunks is off this level.

Trunk status (STAT TRKS) level

Function

Once the STAT TRKS level is reached through the ITEM command on the STAT TKGRP level, it provides status information and maintenance functions for individual

trunks or circuits within a group. An example of the individual trunks for a two-way trunk group is provided in Figure 2-6 on page 2-163 in the STAT TRKS level.

Figure 2-6 — STAT TRKS level example

```
 CM      MS            IOD    Net    PM     CCS    Lns    Trks   Ext    APPL
 .       .             .      .      .      .      .      2GC    .      .
                                                          *C*

  STATTRKS  /                  TWOWY      ITG     OTG                   MISC
 0 Quit     /                  2GC         .       .              .
 2 DispTrk_ /
 3 NextTrk  /          ITEM  TYPE A     COMLANG        TOT SB MB EX %OS
 4 HCpyTrk_ /            2    2W    GC  OTWAON2301T2    3   0  3  0  100
 5 SelGrp_  /
 6 DisAlm_  / PM  NO TRMNL  CKTNO STATE PM  NO TRMNL CKTNO STATE
 7 PrtAlm_  / TM8 1     3      1     INB TM8 0    24    2     INB
 8          / TM8 2     1      3     INB
 9          /
10          /
11          /
12          /
13          /
14          /
15          /
16          /
17          /
18          /
     User ID
      hh:mm
```

TTP level and stuck sender (STKSDR) command

Function

Stuck senders occur on non-CCS7 type calls when no start dial signal is received from the far end office, or an unexpected stop dial signal is received while outpulsing. The Stuck Sender feature in the DMS-100F switch uses the TTP level STKSDR command and its variables to assist in managing stuck sender problems. This feature can be used to detect and hold a stuck sender (for tracing the call to the problem area in electro-mechanical offices).

Periodic trunk maintenance (PRDTKMTC) report

The PRDTKMTC provides a summary report of the failures for both incoming and outgoing trunk groups. Trunk groups to be reported are datafilled in table NWM-CLLI. Scheduling options such as report frequency, reporting period, and report start time are datafilled in table OMREPORT. Datafill in table OMREPORT determines whether the PRDTKMTC report is generated through scheduling or when thresholds are exceeded. The report is output in an OMRSXXX log format and its output is defined in tables LOGCLASS and LOGDEV. Following is an example of the PRDT-KMTC report:

```
          OMRS001 JAN1  00:30:00:  6304 INF  OM PERIODIC REPORT

 REPORT  NAME:  PRDTKMTC      REASON   SCHEDULED (See Note 1)

 CLASS: HOLDING
 START: 1995/01/01 00:00:00  SUN: STOP
 SLOWSAMPLES:        16; FASTSAMPLES:        164;
 ELAPSED  TIME:  00/00 00:30:0

 DATA:  L_LEN            = L           (See Note 2)
        U_UNIT            = CC
 =======================================================
              # CF  TOTAL   TOTAL   TOTAL   TOTAL   TOTAL
 CLLINAME     TRK  INCATOT  INFAIL   ABAN  NATTEMPT OUTFAIL
 TERM1000     128     0       0       0       0       0
                   TOTAL  #  TRK    % TRK
                  MTC USG MTC BS   MTC BS
                     0       0       0
                    END  OF  REPORT
```

NOTES:

1. This PRDTKMTC is a normal report scheduled to be output every half hour, giving data for eight fields of a group of 128 trunks.
2. Due to space limitations, this report is shown as having two rows of field headers. In an actual report, when L_LEN=L, the printout is a single row up to 132 characters in length.

PRDTKMTC report recommendation

It is recommended that the PRDTKMTC report be run periodically during busy traffic periods to identify faulty trunk groups. Analyze trunk group data to identify problem groups requiring further maintenance activity. Utilize features such as focused maintenance, killer trunk, and stuck sender to find specific trunk problems.

Translation verification (TRNSLVF) feature

The TTP MAP level TRNSLVF command is part of the TTP - digit verification and the translation verification (TRNSLVF) features. This command is similar to the TRAVER command except that it only supports trunk originations from a posted trunk. The TRNSLVF command does not set up any network connections.

The TRNSLVF command on the TTP level assists in identifying trunk translation problems by performing the following three functions:

*   verifies the translation and routing data
*   traces the data used to translate the incoming digits into a route
*   displays the digits to be outpulsed on the posted circuit for a given test line code

TRNSLVF command recommendation

If the translation verification fails, or the results are unexpected, then it is recommended that the command TRNSLVF be re-entered with the parameter "T". This

parameter traces the translation and screening tables that were used to arrive at the TRNSLVF results. The displayed data is the same as the data that is displayed by the TRAVER command.

If a data related problem occurs during the trace, the trace is aborted so that the user can tell which table is at fault. Whenever a tuple is missing and there is a default value, the default value will be displayed.

Diagnostic signaling test (SIGTST) feature

This feature is helpful in identifying PTS trunks that would cause transmitter time-outs (stuck senders). It is performed after a diagnostic test either from system maintenance, automatic trunk tests, or manually from the TTP level of the MAP. The actual test verifies that the far end can return a *Start Dial* or *Wink Start* from the distant office. When a trunk fails the test, the trunk is made System Busy (SBSY) and displayed on the MAP under the TRKS alarm system. Also, register PMCCTOP in PM OM group is pegged and log TRK106 or TRK144 is generated.

SIGTST activation

The following two steps have to be taken to activate this feature:

1. Parameter SIG_TST in table OFCVAR has to be set to "Y".

2. For each outgoing or two-way trunk group that uses *Delay Dial* or *Wink Start* signaling, the feature can be activated by setting the SIGTST field in table CLLIMTCE to "Y" for each trunk group CLLI.

SIGTST recommendation

PTS two-way trunks (Cama and TOPS) using E&M lead signaling, and two-way trunks using loop signaling should have the option for Remote Make Busy (REMBSY) set to "Y" in the TRKSGRP table. This allows for the trunk to be made busy when the trunk fails a diagnostic test, and prevents the possibility of the far end office from hitting the trunk and getting a transmitter time-out. If the REMBSY is not set to "Y", then any manual testing should be done quickly and the far end contacted to manually busy out their trunk.

Exhibits

The following exhibits provide a quick reference to the trunk maintenance tools previously described in this subsection.

Exhibit A — Automatic trunk testing (ATT)

Exhibit B — Killer trunk (KT)

Exhibit C — Trunk group alarms

Exhibit D — Focused maintenance for trunks

Exhibit E — Signaling test (SIGTST)

Exhibit F — Stuck sender (STKSDR) maintenance

Exhibit G — Periodic trunk maintenance report (PRDTKMTC)

Exhibit H — Dialed loopback on trunk (TKLPBK)

Exhibit A

Automatic trunk testing (ATT)

Purpose:
Automatically performs routine trunk tests which have been pre-scheduled on outgoing 1W and 2W trunk groups

Type of Transmission Tests Performed:
Net Loss

Noise

Tone Detection

Bit Error Rate (BER)

Operational (call-through and signaling)

Recommended Operation:
Set it up to run during low traffic periods.

Schedule it not to interfere with line balance (BAL) test setup in ALT since line balance test and transmission test use the same test equipment.

All outgoing trunks should be tested weekly for net loss and proper signaling operation. All trunks capable of carrying Datapath service should be tested weekly or as often as testing resources permit.

The ATT test "TE&M" (Test E & M) checks that the trunk is able to return a "Start Dial" signal. This test can be done on all outgoing trunks, including DID and PBX trunks. It is recommended that the test "TR2S" (Repeat Test Twice - Short Timing) be combined with "TE&M". This will verify that the trunk circuitry releases properly from the first test and operates properly on the second test.

Activation:
Commands:

   MAPCI;MTC;TRKS;ATT

Verify that ATT is activated by datafilling the following tables and sub-tables:

- CLLIMTCE
- DIAGDATA (subtable of CLLIMTCE)
- TSTLCONT
- TLNOS (subtable of TSTLCONT)
- ATTOPTNS
- ATTSCHED
- MQLIMITS

Continued on next page

Automatic trunk testing (ATT) (continued)

References:
- NTP 297-1001-121, *DMS-100F Automatic Trunk Testing*
- See "BERT for trunks" within the "Network Maintenance" subsection.

NOTES:
1. Use exception reporting for surveillance purposes.
2. Since ATT is table driven, update tables to coincide with trunk work order activity.
3. Add service circuits—including 3/6 port conference circuits—in the ATT routine test schedule to ensure early detection of faulty units.
4. Trunks may be tested manually for trouble investigation using the command TESTREQ in the ATT menu.

Exhibit B

Killer trunk (KT)

Purpose:
Identifies trunks with short holding time (Killer Trunk), always idle, always busy and long disconnect time. Excessive or short duration holding times may be an indication of static, noise, reaching wrong numbers, sleepy trunks, or the lack of a start signal. Long holding times may indicate improper release conditions.

Recommended Operation:
Run continuously during normal business day period in Auto mode. Review KT reports frequently for problem trunks and groups.

The operating modes are:
AUTO — Trunks instrumented on a rotational basis as specified in table TRKGRP. When the next interval begins, the next set of 2048 trunks are instrumented.

MANUAL — Trunks instrumented in order of the groups declared in table KTGROUP (2048 maximum). Repeatedly instrumented for each report interval.

SEMI-AUTO — Trunks instrumented in order of the groups defined in table KT-GROUP and instrumented on a rotational basis.

A CI increment command called KTREPORT generates three types of outputs as follows:
ACTIVE — Displays all trunk groups currently under KT observation.

FILE DIR — Lists all KT data files available from DIRP.

ANALYSIS — Analyzes raw data files to develop lists of trunks with KT properties.

KTRK100 log report generation, at the end of every report interval, must be specified in KTPARMS (GENKTLOG ON).

Continued on next page

Killer trunk (KT) (continued)

Activation:

Tables affected: KTPARMS, KTGROUP, KTMINMAX & DIRPSSYS

Suggested datafill for table KTPARMS:

```
ENABLE  ON
SCANRATEFAST
START   0600
STOP    1800
REPORT 400
KTPEGMIN5
KTHTMAX15
SRHTMIN300
RETYPE  EXCEPTION
NTRUNKS2047
MODE    AUTO
GENKTLOG0N
```

NOTES:

1. Before adding or deleting KTPARMS data, turn ENABLE "OFF"—when finished, turn ENABLE"ON".

2. KTGROUP table specifies the trunk groups to be instrumented when in the MANUAL or SEMI-AUTO mode.

3. KTMINMAX table permits unique parameters to be set for each trunk group instead of the global criteria defined in table KTPARMS.

4. Suggested datafill for table DIRPSSYS to support KT archives:

```
FILEDATE          CLOSED
   NUMFILES        1
   MINFILES        0
```

5. Recommended that no manual or scheduled rotates or closures be done.

6. KTACTIVE table has been cancelled. This function replaced by the new CI level command KTREPORT

Exhibit C

Trunk group alarms

Purpose:

The STAT TRKS level of the MAP checks alarm status of all trunk groups which includes test trunks, receivers, etc.

Recommended Operation:

Perform daily.

At the CI level enter:

MAPCI;MTC;TRK;STAT (to access STAT TRKS level)

DISPGRP (TWOWY, ITG, OTG, MISC)

DISPTRK (from STAT TRKS level)

NOTE: Also check all trunks for INB and INI state

At the CI level enter:

MAPCI;MTC;TRKS;TTP; Post A (INB and INI — individually)

Activation:

Analyze each individual trunk and take appropriate action.

Utilize STAT TRKS level commands to check alarm status.

References:

- See NTP 297-1001-595, *DSM-100F Trunks Maintenance Guide* and NTP 297-1001-822, *DMS-100F Commands Reference Manual.*

- See Figure 2-5 on page 2-155 and Figure 2-6 on page 2-163 within this subsection.

- See "Trunk group status (STAT TKGRP) level" and "Trunk status (STAT TRKS) level" on page 2-162 within this subsection.

Exhibit D

Focused maintenance for trunks

Purpose:

To manage software identified trunk trouble messages utilizing a system of buffers, thresholds and alarms. This is an efficient and effective alternative to the existing log system which outputs all trunk log messages for manual attention.

Recommended Operation:

Implement focused maintenance procedures for trunks feature when software package NTX272AA has been provided.

Take corrective action for failures exceeding the thresholds by responding to the visual alarm indication in the system status display area under TRKS.

NOTE: The trunk alarm status display for Focused Maintenance alternates at thirty second intervals with any other trunk status alarm indication.

Access the TRKSTRBL level of the MAP, post the CLLI trunk group exceeding the threshold; displayed are the 10 worst members which have caused the threshold alarm. These troubles are listed by trunk group and member. The details describing the last trouble is also recorded.

At the CI level enter: MAPCI;MTC;TRKS;TRKSTRBL

Once the trouble has been identified, move to the TRKS testing level of the MAP. Proceed with the necessary testing and verification to isolate and repair the trouble.

Review periodically (daily) the worst failures recorded by the various trunk groups, for in-depth analysis, control and repair activity.

Activation:

The "Focused Maintenance" subsection within this tab of the manual describes, in detail, the specific steps to implement and activate Focused Maintenance for Trunks—including suggested datafill information.

References:

- See the "Focused Maintenance" subsection within this tab.

Exhibit E

Signaling test (SIGTST)

Purpose:

To identify non-SS7 trunks causing "Stuck Senders" (Transmitter Time-outs) by performing an automatic signaling test for *Start Dial* or *Wink Start* from the far office.

Recommended Operation:

This test is recommended for:

- All non-SS7 one-way out and two-way trunk groups terminating into DP, MF, UTR, or DGT receivers.
- All types of trunk groups, such as: Intertoll, Toll Connecting, Interoffice, Local, Tie Trunks, and PBX trunks, where *Delay Dial* or *Wink Start* signaling is used.

Activation:

1. Verify that the "Signaling Test" feature is activated in the office engineering table OFCVAR and parameter SIG_TST is set to "Y". If set to "N", request your control center or regional support group to set SIG_TEST to "Y".

2. Activate "Signaling Test" feature for each required trunk group in table CLLIMTCE by entering a "Y" in Field SIGTST for each CLLI trunk group using *Delay Dial* or *Wink Start* signaling.

The signaling test is performed after the trunk diagnostic test initiated by the system or from a TTP request and is an excellent way of identifying trunks that are causing stuck senders.

The trunk failing the system initiated diagnostic and signaling test will be made system busy (SB) and the status will be displayed on the MAP under the TRKS alarm level.

Two-way trunk groups should be optioned for remote make-busy (RMB). When a two-way trunk fails a diagnostic test, the RMB option will remove the trunk from service at both ends in real time without human intervention. The RMB option is set in table TRKGRP. If the RMB option is not used, the two-way trunk should be manually tested quickly and busied out at the far-end in order to prevent stuck sender failures at the far end office.

Each initiated failure will score one peg in field PMCCTOP of OM Groups PM and PM-TYP, and also generates TRKI06 and/or TRK144 logs.

Exhibit F

Stuck sender (STKSDR) maintenance

Purpose:

To manage stuck senders —transmitter time-outs— by utilizing available DMS-100F features for detection and correction.

Introduction:

A stuck sender occurs on a call when the DMS-100F switch fails to complete outpulsing on an outgoing trunk. This may be due to not receiving a *Start Dial* signal from the far-end office or an unexpected *Stop Dial* signal is received from the far-end office.

The DMS-100F has a form of "Sender Retrial" feature that automatically tries another idle outgoing trunk after the first no *Start Dial* time out. The call could complete or if the second trial times out, then the call is sent to TERSSTO (Stuck Sender Time Out) reorder treatment.

Log message TRK121 provides real time information on trunks experiencing stuck senders—outpulsing trouble. The log message is printed for first and second trial failures, including the notation "first or second trial" in the text as appropriate. Since this log message identifies the incoming trunk, the outgoing trunk and the called number, it is useful in identifying far-end office troubles, overload conditions, and mass calling telephone numbers. This log message is a good candidate for log thresholding. The hourly bogey calculation (see "Recommended Operation" below) developed below— divided by 6—would be a reasonable threshold for a 10 minute interval.

The first and second trial failures score the following OM registers as indicated:

OFZ Group

OUTOSF Register (First trial failures only)

OFZ Group

OUTROSF Register (Second trial failures only)

TRMTER Group

TERSSTO Register (Second trial failures only)

TRK Group

OUTFAIL Register (First and second trial failures for the trunk group)

The "STKSDR" (Stuck Sender) level of the TTP provides real time "Hold" and "Trace" on outgoing trunks that are causing stuck senders (see Note 1). Up to four trunk groups (maximum per office) can be posted and each TTP can hold up to 2 trunks that are causing stuck senders. Suspected trunk groups are identified by high "OUTFAIL" registrations which is summarized in report PRDTRKMTC. The trunks that are held can be traced to the far-end office in order to verify the signaling status on the trunk at various equipment locations, or the trunk can be released and tested for proper overall operation.

"Focused Maintenance" (optional feature NTX272AA) monitors trunk troubles in real-time and it will identify trunks experiencing high quantities of stuck senders and other types of troubles. The trunks in trouble are identified at the TTP "TRKSTRBL" (Trunk Trouble) level.

Continued on next page

Stuck sender (STKSDR) maintenance (continued)

Recommended Operation:

Review weekly, daily, and hourly OM printouts and determine that respective bogies are met as follows:

This calculation can be used to determine the weekly, daily and hourly failure rates by using the respective OM data. However, it is simpler to calculate the acceptable monthly quantity of Stuck Senders as follows:

$$\text{Quantity} = \frac{5 \,(\text{OUTNWAT} + \text{OUTNWAT2})}{10{,}000}$$

This quantity is then divided by 4, 30, and 300 (assumes 10 busy hours for each day) to arrive at weekly, daily and hourly "bogies". The hourly bogey may require some adjustment depending on the office load distribution. Stuck sender problems can be identified in one or more of the following ways:

- Monthly results for stuck sender component not meeting index.
- Weekly, Daily, Hourly OUTROSF (or SSTO) bogey exceeding limits.
- Real-time TTP TRKSTRBL level, OM OUTROSF threshold or log TRK121 threshold is exceeded.

Identify the trunk groups that are causing stuck senders. This can be done in one or more of the following ways:

- Enter the TTP TRKSTRBL level.
- Analyze the log TRK 121 messages.
- Calculate the percent failure rate for each trunk group as follows (Objective is less than 0.1%)

$$\% \text{ Failure Rate} = \frac{\text{OUTFAIL}}{\text{NATTMPT}} \times 100$$

- All the registers are in the TRK OM group. Use "OMSHOW" command to obtain current hard copy of "ACTIVE", "HOLDING" or "Daily" (OMCLASS) registers for TRK OM group.

Analyze log TRK121 or focused maintenance data, test the trunks from the TTP, and check various translation tables for possible trouble conditions such as:

- far-end office overload
- mass calling to a specific number
- defective carrier
- defective trunks

Recommended Operation:

Check trunk group translation for errors or values outside the norm:

- Outgoing Start Dial Signal (OSTARTSG)
- Trunk Guard Timing (TRKGRDTM)
- Yield to Glare (GLAREYD)
- Number of Stop/Goes (NUMSTOPS)

Review the following office parameters for inconsistent values among offices:

- REC_PRE_WK_TIME
- REC_MIN_WK_TIME

Continued on next page

Stuck sender (STKSDR) maintenance (continued)

- REC_MAX_WK_TIME
- REC_PRE_DD_TIME
- REC_MIN_WK_TIME
- REC_MAX_WK_TIME
- CHECK EQUAL ACCESS WK TIME and 2nd WK TIME

Preventive Maintenance:

Verify that the diagnostic signaling test (SIGTST) is activated. Ensure that reported trunk failures are investigated for trouble—including stuck sender problems. See Exhibit E "Signaling test (SIGTST)" for information on scheduling the diagnostic signaling tests.

Verify that automatic trunk test (ATT) is programmed and test TE&M combined with TR2S is part of the testing program. Run a minimum of once every seven days. See the previous "Automatic trunk testing" Exhibit A.

Verify daily the carrier system maintenance performance summary since it also affects the quantity of stuck senders. See the "Carrier maintenance" exhibit within the "Carrier Maintenance" subsection for obtaining carrier system performance information.

> **NOTE:** The Hold and Trace testing procedure works best when the call terminates on a trunk into an electro-mechanical office. Hold and Trace is not a viable test for calls terminating on trunks into a digital office.

Recommended Routine Interval: Monthly

Exhibit G

Periodic trunk maintenance report (PRDTKMTC)

Purpose:

Provides a summary report by trunk group of the failures, both incoming and outgoing, in addition to the system busy and manual busy data for the report period.

Recommended Operation:

Run periodically, particularly during busy traffic periods, to identify faulty trunk groups.

Activation:

Datafill tables as shown for appropriate output and routing:

Table OMACC

Table OMREPORT

Table LOGDEV

Table LOGCLASS

NOTES:

1. Since PRDTKMTC is a system preformatted OM report output. It is only necessary that the required group and registers accumulating the OM data be collected in table OMACC—use either an existing class or a class can be established for this purpose. The data should be available hourly during the business day.

2. Analyze trunk group data to identify problem groups requiring further maintenance activity and the specific trunk(s) at fault—by utilizing features such as focused maintenance, killer trunk, and stuck sender (STKSDR).

3. For easier readability, consider using the optional long line length (132 column) printout setting.

Exhibit H

Dialed loopback on trunk (TKLPBK)

Purpose:
Provides a transmission path loopback on an individual trunk when the trunk is seized and the loopback number is dialed. The loopback takes place in the network module. The loopback is removed on disconnect, or after reaching a time-out period defined in office parameters.

Recommended Operation:
Perform to isolate trunk transmission troubles and bit errors. Can be used with net loss, noise, and bit error rate testing.

Activation:
Datafill table OFCVAR tuple TRKLPBK_TIMOUT_IN_MINUTES to 10 (minutes). This can be increased if required. See NTP 297-YYYY-855, *DMS-100F Office Parameter Reference Manual.*

Datafill the following tables and sub-tables:

CLLI

DN

OFRT

STDPRTCT

STDPRT

NOTES:

1. See "BERT for Trunks" within the "Network Maintenance" subsection for a description of manual and automatic BER testing using TKLPBK.

Network Maintenance

General

The purpose of this subsection is to identify switch resident tools for the maintenance of DMS-100F switch networks, and to describe the maintenance terms and processes needed to maintain switch networks. Most of the tools described in this subsection are used to maintain the *Bit Error Ratio* (BER) requirements for the DMS-100F switch as well as the trunking facilities between offices. The tools identified will be for the junctored network (JNET) as well as the enhanced network (ENET). Network tools were first developed for the NT40 JNET. The same tools are used for the SuperNode ENET with some differences in operation and response outputs. If equipped with ENET, then see the "ENET Overview and Maintenance" subsection within the *System Products* section of this manual for ENET maintenance tools.

This subsection provides the following information as related to network maintenance:

- DMS-100F switch BER
- DMS-100F LBER process
- Digital switch BER performance criteria
- BER performance (BERP)
- Integrated BER testing (IBERT)
- Network maintenance tools
- Maintenance tools and work activity application notes
- Integrity
- Integrity monitoring
- Integrity logs
- Causes of integrity failures
- Integrity troubleshooting
- BER testing (BERT) guidelines

References

For a primary source of network maintenance information, see NTP 297-1001-591, *DMS-100F Network Maintenance Guide.*

DMS-100F switch BER

The bit error ratio (BER)—sometimes called bit error rate—is the fraction of errored bits relative to total bits received in the transmitted digital stream. The BER requirement for *high speed data* transmission within the DMS-100F switch is to have no more than one bit errored in 1×10^{-9} bits (one in a billion), or one errored call in 48 ten-minute calls. This sometimes is expressed as low-bit error ratio (LBER)—*it is used within this manual as indicating a process to meet low BER threshold requirements*. When expressed in observed or analyzed maintenance terms, it means no more than one NET102 log per 2800 calls. This figure is based on a parity threshold setting of one in the switch. The *voice grade* parity error criteria is less than one NET102 log message per 10,000 calls at a parity threshold setting of 20. Parity settings are described later.

It should be noted here that the BER requirement for the SuperNode Enhanced Network (ENET) is one bit errored in 1×10^{-12} even though the overall switch is tested for one bit errored in 1×10^{-9}. This is because ENET is designed to support services requiring bandwidths greater than 64 Kbps.

Prior to the implementation of high speed data features, DMS-100F switches were installed and set to run at voice grade service. Since the implementation of Datapath, ISDN, and other high speed data features, DMS-100F switches are installed and set to run for high speed data. Those not performing at the high speed data level are required to be groomed prior to the implementation of high speed data services. It is then up to the operating company to maintain those requirements for good service.

BER end-to-end requirements

An objective for end-to-end connections through the network is that the BER should be less than 1×10^{-7} on at least 95% of the connections. To help meet those objectives, it is important that bit error rate test (BERT) be performed over digital trunking facilities between offices. Therefore, it is recommended that BERT be set up and scheduled within automatic trunk test (ATT) on a daily basis—see "BERT for trunks" later within this subsection. If ATT is not used, then BERT should be performed using manual or another mechanized system.

DMS-100F LBER process

The purpose of meeting the switch low-bit error rate (LBER) requirement is to reduce the network parity errors from the current voice grade levels to meet high speed data requirements.

Reducing the parity threshold will cause the quantity of network errors—NET102 logs—to increase. If the network errors become excessive, return the parity setting

back to a higher level so that they become more manageable. As the troubles are cleared out of the networks and XPMs—by using the NET102 logs and other data—progressively reduce the parity threshold, and clear all network problems until the desired high speed data requirement is met.

The first step in the LBER process is to ensure the network and XPMs are meeting the current voice grade parity requirements—one NET102 log message per 10K call at a parity of 20—using the test tool features that are described later within this subsection.

The second step in the LBER process is the changing of the parity threshold from voice grade to high speed data grade—by changing the parity setting from 20 to one respectively—while clearing troubles out of the networks and XPMs using the network maintenance test tools.

The third step for LBER is for ongoing maintenance to sustain the network and XPMs at the high speed data criteria—less than one NET102 log message per 10,000 calls at a parity threshold of one. Once the network is manageable at a threshold setting of one, the following routines are recommended to help maintain that parity level:

- BERP — run daily to determine bit error rate performance
- NETFAB — run daily to exercise paths through the network to identify faults
- XBERT — run monthly on all DTCs

LBER benefits

Previously, LBER was implemented only in offices that had one or more of the following features: Datapath, DialLan, and ISDN. There are, however, some immediate benefits that can be obtained if LBER levels are maintained in switches that have not implemented one of the above features.

The benefits that can be achieved with LBER are:

- 30% average reduction in customer trouble reports (codes five, seven, & eight)
- same day resolution of network/XPM parity/integrity faults
- no external test equipment required
- automation of loopback points
- reduction in average work time to identify and replace faulty packs
- a reduction in no-fault-found (NFF) circuit packs

Digital switch BER performance criteria

The following provides transmission performance objectives for a digital switch forming part of a digital communications network. The objectives can satisfy the service needs of both voice band and digital data services.

The switch objectives have been derived from previously developed network level performance objectives by allocation. Some adjustment of methodology has been needed to adapt to the differences between switches and transmission facilities. The main difference is that a switch has multiple transmission paths and a sample of the possible paths must be taken when demonstrating specification compliance.

The performance objectives are presented in the following pages for: network model, network objectives, allocation, and switch objectives. These are followed by test setup criteria.

Digital network transmission facility objectives and digital switch objectives have evolved independently in the past. Service based network transmission objectives usually one error in 1×10^{-9} bits. However, with the development of broad-band and wideband requirements, it became evident that both of these practices need to be changed. Also, performance objectives related to end-to-end network objectives must be used to derive those for digital switches, and should be specified with similar methodology.

Definitions

Errored Call — any call in which either no sync is found or the number of bit errors is greater than zero.

Bit Error Ratio — BER, a measure of the number of bits that are in error in the transmission of data or PCM voice. Usually BER is expressed in terms of $n \times 10^{-y}$ (where n=number of errors and y=exponent) for example, 5×10^{-7} means 5 errors in 10,000,000 bits transmitted). A 10 minute call has 10x60x64,000 = 38,400,000 bits transmitted (for a 64-Kbps data rate). If this call has a BER of 5×10^{-7}, then we expect to see $(38.4 \times 10^5) \times (5 \times 10^{-7})$ = 19.2 errors.

Errored Seconds — ES, a call is divided into one-second time intervals. Therefore, a 10-minute call will have 600 one-second intervals. A second is marked as an errored second if it has one or more errors during that one particular second. A call could have none, one, or many errored seconds. Errored seconds do not equate to errors in a call. Derivatives of ES are error-free seconds (EFS) and percent error-free seconds (PEFS).

Severe Errored Seconds — SES, the number of seconds during which a carrier was in a state of severe failure. Frames were not being exchanged during periods of severe failure.

Performance specifications

Network model

For purposes of digital performance planning, a digital network is represented by a hypothetical reference connection (HRX). The HRX considered represents a near worst-case connection with the existing hierarchical structure, and contains six switches.

A high-performance routing (HPR) environment at the early stages of implementation, and during busy hours, requires additional tandeming of trunks. The near worst-case of switches in a connection in this environment may be assumed to be eight.

In the United States, the architecture evolving between the exchange and inter - exchange carriers also employs eight switches in the near worst-case.

Switch performance model

The BER performance characteristics of a digital switch may be expected to differ from transmission system behavior. While transmission systems exhibit time varying error statistics, switch performance can be relatively time invariant, but differs from path-to-path. Therefore, in characterizing switch performance, it is necessary to take a composite view of many paths.

Transmission performance parameters

The transmission performance objectives for a digital switch—similar to those of a transmission facility—shall be specified in terms of:

- bit error ratio (BER)

- percent error-free seconds (PERS)

NOTE: at the DS0 rate, short interruption performance is controlled by PEFS performance specified for digital data services.

Digital transmission performance is time dependent (nonstationary). For each parameter, measured intervals are classified as quiescent or degraded, and are defined as follows:

- Quiescent Performance — This is defined as that performance level when a system or network component exceeds 95% of the available time. It is specified to minimize the probability that the end-to-end performance of a connection can exceed the degraded level, when the individual components of the connection are operating in the satisfactory performance category. In addition, it may be used by equipment designers and as a reference for specifying circuit order limits.

- Degraded Performance — The performance is defined as degraded if one or more of the parameters exceeds the degraded threshold. Degraded performance is the performance level at which the users of some services may experience less than satisfactory performance. Degraded performance should be limited to a percentage of the total available time.

For each performance parameter, thresholds defining these categories are established, and the allowed percentage of measurement intervals falling in each impairment category is determined.

Allocation methodology

The objectives of the individual components of a digital network are derived by allocating the end-to-end objectives among them. The rules are to:

- divide the allowed percent of time for degraded objectives.
- divide the performance threshold for quiescent objectives.

The switches of the connection are allocated 10% for the allowed end-to-end impairment and are divided equally among a maximum number of eight switches.

Transmission performance objectives

- Network End-to-End Objectives — The following objectives for the degraded level of performance have been specified to satisfy voice band, digital data, and ISDN services:

  — BER less than 5% of one-minute intervals worse than BER 1×10^{-6}

  — PEFS less than 5% of one-hour intervals worse than 99.5% PEFS

Reference quiescent thresholds of 7.8×10^{-8} for BER and 99.5% for PEFS are established. Network components are to meet an allocated quiescent threshold for 95% of the time.

- Service Specific Performance Objectives — To accommodate a preference for service specific objectives, switch specifications have been derived separately for voice band service and high-speed digital data service. Voice-grade objectives may be expressed by BER. An objective that 85% of connections should meet a user data BER of 1×10^{-5} may be applied.

Performance specification

The switch objectives are defined at two levels to satisfy the requirements of voice grade, and alternatively, those of high-speed digital data. The high speed data specification would not normally be applied alone, since it is unlikely that an end office switch would be dedicated to such a service. In order for this specification to apply to a switch in a remote environment, the interconnecting facility must be essentially error free.

- Voice-Grade — BER

  — no more than 1 in 1600 calls should exceed 3 errored seconds

  — no more than 1 in 70 calls should be errored

  (see following the confidence level table)

- High-Speed Digital Data — PEFS

  — no more than 1 in 533 calls should exceed 38 errors (1×10^{-8} BER)

  — no more than 1 in 10 calls should be errored

  (see the following confidence level table)

- Test Setup Criteria — A switch can be evaluated by measuring a number of test calls made through the switch. Define an appropriate test plan in terms of:

  — test call duration

  — sample size

— and sample distribution in space and time

- Test Call Duration — Test call duration is 10 minutes, since it provides a near-true performance of a path and represents a relatively long average call.

- Sample Size — The sample size should be selected to demonstrate meeting the specification with a confident level of at least 80%. A table of sample size for the 80% confidence level is provided in the following Confidence Level table.

- Sample Distribution — Test calls shall be evenly distributed among and include all line and trunk terminating equipment modules. The testing shall be distributed over an entire day or include one busiest hour in every three-hour testing period.

Table 2-59 — Confidence Level				
NO. OF CALLS NOT MEETING THRESHOLD	p=1/10	p=1/70	p=1/533	p=1/1600
0	15	111	857	2574
=< 1	28	208	1595	4789
=< 2	41	298	2281	6845
=< 3	53	384	2940	8822
=< 4	65	469	3583	10751
=< 5	77	551	4215	12647
=< 6	89	633	4838	
=< 7	100	714	5455	
=< 8	112	794	6067	
=< 9	123	874	6674	
=< 10	124	953	7278	

BER performance (BERP)

The BERP setup and testing procedures from the MAP are described in detail in NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing*. MAP displays, output files, and illustrations of line and trunk configurations for BERP testing are provided in this document. For additional guidance in setting up and performing BERP testing, see "BER testing (BERT) guidelines" later within this sub-section.

BERP provides a means to measure how the switch is performing in terms of bit error rate. A bit error rate is a measure of the number of bit errors in a transmission stream. This bit error rate is sometimes expressed as an absolute ratio (i.e., 1×10^{-9}). This ratio implies that out of 1 billion bits sent, 1 was in error. This is perfectly valid when one is measuring the transmission quality of one single link. Given the complexity of a DMS switch, with the multitude of different permutations of paths one can have, measuring the bit error ratio on every permutation of every path that a call could take through the DMS and its associated peripheral devices is time consuming.

Given that it is not feasible to test all the paths within a DMS, other methods must be used. To measure the bit error rate performance of the switch, a random sample of test calls must be made. Based on the performance of these test calls, one can estimate the

overall performance of the switch. Since it is not feasible to set up test calls to transmit over a billion bits of data each, another method for measuring the bit error performance of each call must be used. This is generally done by measuring the number of error-free seconds (EFS) in a test call of at least 10 minutes in duration. The percentage of error free seconds in a call is then used to estimate the true performance of the data call. The number of error-free seconds in the overall test plus the number of error-free calls made can be used to generate a statistical confidence level for the true bit error rate performance of the switch. Once a desired confidence level has been determined, the criteria for a successful test will also follow (i.e., number of error-free calls or number of error-free seconds in a test).

It is up to each operating company to determine for themselves what confidence level they wish to achieve and therefore, the criteria for a successful test. See the "Digital switch BER performance criteria" previously described, which reviews the criteria for establishing BER performance (BERP) requirements. The purpose of this feature is to make random data calls of a predetermined duration, and to measure the key factors relating to transmission quality of those calls. Namely, the factors include: the number of bits transmitted; the number of bits in error; the length of the call in seconds; and the number of seconds that contain any bit errors. It is then up to each operating company to take the statistics generated and determine whether their switch is performing up to their standards or not. In the case of a switch that is not performing up to its desired standards, the following section describes how this feature can help to correct the problem and get the switch to meet its standard.

BERP uses resident software and hardware of the DMS and has knowledge of the end-to-end path being taken. By providing a detailed breakdown of all the paths that were involved in errored calls, faulty links can be identified and corrected using the Datapath resident test tools.

A test from the BERP level is composed of many individual bit error rate tests (BERTs). A single BERT consists of connecting an integrated bit error rate (IBERT) or Digital Test Unit (DTU) testing circuit pack to the designated line subgroup looparound point and transmitting a known bit pattern. The known bit pattern is reflected back to the testing circuit pack where it is compared to what was sent. Any errors found in the returned bit stream are recorded. The results of all the individual BERTs comprise the BERP test.

The statistics gathered during a BERP test are a summation of the results of each of the individual BERTs. The statistics kept include:

- number of calls made
- number of error free calls
- number of errored calls
- number of errored calls with a bit error rate worse than a user specified value
- number of errored calls with more than a user specified number of errored seconds

- number of call setup failures
- number of seize failures

A call is considered as having been made if the IBERT circuit card was successfully connected to an endpoint and had begun a test. Note that this does not imply that any data was passed. The first stage of a call of this type is to achieve sync. This is done through an internal protocol that allows both ends to identify their operating parameters and to decide which set of parameters to use in the test. The IBERT can adapt to the other end's protocol. If for some reason this protocol fails, no data will be passed. This is represented as a no sync call. It is considered an errored call since it represents a condition so severely errored that no data could be passed. An errored call is any call in which either no sync was found or the number of bit errors was greater than zero.

BERP capabilities

Initially, BERP was limited to testing data line cards (DLCs) or looping back to an IBERT card. Later, the capability to provide a loopback within the scan cards located on the bus interface cards (BICs) of the LCM was added (see the following illustration). This eliminated the need to have IBERT cards in every line subgroup. By making use of the line subgroup looparounds, three advantages are gained as follows:

- Any line card may be used for the purposes of connecting to an IBERT card
- Additional test coverage, since all line subgroups in an LCM/LCMI can be included in a BERP test

Fewer IBERT cards are required. Now, one IBERT card can sequentially cover all the line subgroups in many LCMs without even being located in the LCMs it is testing. Simultaneous IBERT tests may be scheduled to reduce the total testing time interval.

BERP testing includes Line Modules (LMs). LMs do not have the drawer looparounds which are available in an LCM. The only looparounds that are available on an LM are the channel 16 looparounds on the links connecting an LM to the network. These looparounds are located at the interface to the LM of these links. No hardware on the LM, other than the channel 16 looparound in the interface to the network links, is included in the BERP test. Due to an internal hardware restriction, the messaging link cannot be included in a BERP test.

Before any BERP tests can be started, the IBERT and DTU test cards must be assigned according to the IBERT Resource Management guidelines. See "IBERT" following BERP and the "IBERT resource management" subheading.

A BERP routine test may be interrupted so that the IBERT or DTU test card may be used and reassigned to a demand LTP/TTP test function. When interrupted, the BERP test in progress is aborted, and the test result data is excluded from the BERP statistics.

BERP routine test recommendation

It is recommended that the bit error rate performance testing program be run daily to determine the switch BER performance and identification of network and XPM faults. Avoid running during PM REX testing. Also, develop a schedule for assigning and controlling BERP testing at the LCM and LM levels.

BERP assessment criteria

The following recommendations for assessing the BER performance of a DMS-100F switch have been set forth. There are two assessment guidelines, one for a switch that is used for high speed data applications, and one for voice grade applications. It is highly recommended, for overall switch performance, that all switches be assessed and maintained for high speed data. The following specifications are based on a set of test calls which are 10 minutes in duration with a transmit speed of 64 Kbps:

The specification for high-speed (64 or 56 Kbps) data performance is:

- no more than 1 call in 1600 test calls made can exceed 3 errored seconds
- no more than 1 test call in 70 can be errored

The specification for voice band data is:

- no more than 1 call in 533 test calls at a Bit Error Ratio of 1×10^{-6}
- no more than 1 test call in 10 can be errored

BERP MAP level and commands

COMMAND	EXPLANATION
BERP	enters the BERP level of the >MAPCI;MTC;BERP or >MAPCI;MTC;OFCINTEG;BERP
QUIT	exits the BERP level of the MAP.
REVIEW	reviews all relevant test setup information about a BERP test. Also provides the number of interrupted test calls, including IBERT and circuit identification. This shows if all calls or errored calls are traced.
SUMMARY	displays the last known test results, including link loopback failures—if any.
SELECT	selects IBERTs as testers, which can be any combination of DTUs and ILCs.
DEFINE	defines the circuit and links for testing, including loopbacks **continued on next page**
CALLSET	Used to set up the call parameters for a test. These parameters include the length of each test call, the delay between calls, the number of calls to be made in the test and whether ALLCALLS or just ERRORED calls are traced by BERP.
DEFTIME	Sets the start and/or stop time of the test. It can also be used to clear either or both the start and stop times.

CHECK	Checks the consistency of all data entered. If all data is valid, a test may be started. Error messages are output to identify irregularities.
START	Starts up the tests either right away or at the specified start time.
STOP	Stops a currently running test right away. Any calls that were active at the time are taken down. These calls are not considered as part of the test and are not included in the test statistics.
OUTPUT	Specifies the output file to be used or to clear the previous definition of the output file.
RESET	Resets all statistical counters to 0.
PARMSET	Used to set the BER exponent parameter and the error free seconds parameter of the test.
SORTKEY	Used to determine the path components to be included in the sorting of path information by the PROCESS command. It can include or remove a specified node and/or sortkey (component) for processing.
PROCESS	Process a BERP result file and produce a report file based on the path data.
LOOPBK	Selects the loopback points to be used for all types of testing. Not applicable when testing to LSG since it is the loop point.

Integrated BER testing (IBERT)

Figure 2-7 — BERP MAP level display

```
   CM      MS      IOD     Net      PM      CCS      Lns      Trks     Ext      APPL
   .       .       .       .       2 IDT    .        .        C       1 Min     .


 BERP
  0 Quit        Test Status : Unchecked
  2
  3 Review     Calls : 0            Errored Calls : 0            Ratio  0/0
  4 Summary
  5 Select_    Calls with BER > 10E- 7          : 0            Ratio  0/0
  6 Define_
  7 Callset_   Calls with > 3   errored seconds : 0            Ratio  0/0
  8 Deftime_
  9 Check      MTC:
 10 Start      BERP:
 11 Stop
 12 Output_
 13 Reset
 14 Parmset_
 15 Sortkey_
 16 Process_
 17 Loopbk_
 18
   ITAS
Time  17:04  >
```

IBERT can stand for "integrated bit error rate testing" when referenced as the feature, or "integrated bit error rate tester" when referenced as hardware (e.g., IBERT line

card). IBERT consists of both software and hardware. Both internal and external test equipment are supported for maximum testing flexibility.

IBERT is designed to test the subscriber's data path, including ISDN lines. The commands for seizing and testing the loop are accessed through the LTPDATA level of the MAP. Testing capabilities include: error injection, loop backs, BERT, ISDN line test, and modem testing. When starting BERT tests at the LTPDATA level, the user is informed of any failures to start BERT tests with a particular IBERT, and is also informed of what IBERTs were obtained. The QBERT command provides information about IBERT's usage and status.

IBERT test equipment includes the NT6X23 Digital Test Unit (DTU) located in the MTM and the NT6X99 IBERT Line Card (ILC).

DTUs may be used in place of ILCs at the LTPDATA level. The DTU has the same LTP BERT test features as the ILC, including the ability to perform maintenance diagnostics on Datapath DPX cards. For this flexibility, the DTUs must be datafilled in table FMRESINV with command sets that enable them to be used at the LTP.

The following applications make use of IBERT hardware and software:

- BERP (Bit error rate performance testing)
- LTP (BERT command at the LTPDATA sublevel)
- TTP (BERT command at the DATA sublevel)
- ATT (Automatic trunk testing)

Figure 2-8 on the next page provides a view of how the IBERT card can be used to test from one LCM location to another and utilize the loopback capability of the BIC card to perform the test.

For more information on IBERT, see NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing*.

IBERT resource management

The BERP application typically uses a large quantity of IBERT hardware for long intervals of time, making many consecutive tests with the same IBERTs. Without a resource allocation scheme, an application such as BERP could potentially tie up all IBERT hardware in an office, leaving none for such applications as the LTP or TTP. Through table control, it is possible to reserve IBERT hardware for a particular application, or to share the test resources.

This feature allows a *foreground* IBERT user, such as the line test position (LTP) or trunk test position (TTP), to interrupt and seize an IBERT from a *background* user, such as at the bit error rate performance (BERP) level. The IBERT being claimed must be assigned in the tables for use by both BERP and LTP/TTP use.

Figure 2-8 — Typical IBERT to LSG loopback configuration
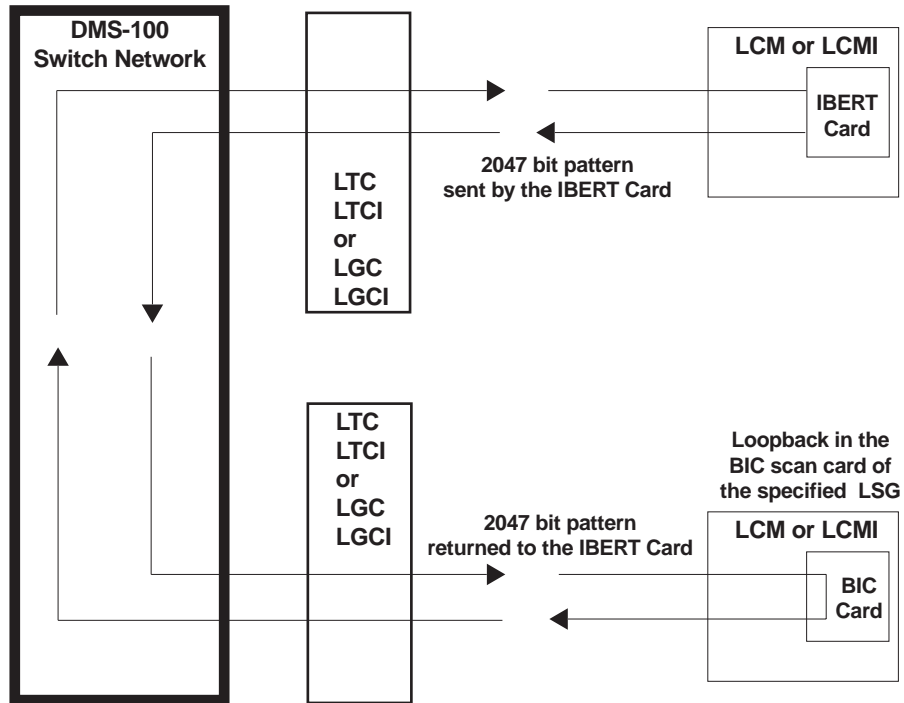
Control of this interrupt ability is provided by an optional interrupt parameter "I" on the BERT START command at the LTPDATA level of the MAP. This interrupt aborts the specific BERP test in progress and excludes the data from the statistics. The number of "I" interrupts is also recorded.

The overall impact on BERP because of this interrupt capability should be minimal, provided BERP is making a large number of calls and interruptions are occurring only occasionally. If this is not the case, then it is advisable that a number of IBERT hardware be datafilled explicitly for LTP/TTP use.

All IBERT hardware—DTUs and ILCs—*must* be datafilled in table FMRESINV for them to be used as an IBERT by *any* test application. A maximum of 128 IBERTs— which can include ILCs and DTUs—can be datafilled in FMRESINV. Also, a companion table FMRESUSE, that associates the test application with the designated IBERT test equipment, should be datafilled. The default value for table FMRESUSE is ALL.

IBERT assignment strategy

Because there are many ways to datafill the FMRESINV and FMRESUSE tables, the following datafill strategy may be useful:

1.Assign the applications command sets first, via table FMRESUSE. It is perhaps simplest to assign each application a command set containing a single distinct class. Afterwards, datafill table FMRESINV according to desired usage.

2.Group the IBERTs into a number of different categories according to some characteristic (i.e., ILCs at host and remote sites, and a separate category for DTUs). Datafill table FMRESINV with a distinct command set for each category. Datafill table FMRESUSE according to how the applications are to make use of these categories.

The demand for IBERT testers (ILCs and DTUs) is staggered to some degree, since some BERP and ATT trunk testing is scheduled during off-normal hours (light load) and the demand for service testing activity from the LTP/TPP position is during the business day. If this prevails, try shared IBERT assignments.

BERT log reports

A BERT100 log is output when a failure is encountered trying to get an IBERT to start a BERT test. The log is also used to indicate failures to query IBERTs. The log identifies the IBERT's LEN or CLLI, the IBERT number, and the fault encountered. The log is output only when the suspect status of the IBERT changes from BERT OK to BERT SUSPECT.

At the time the BERT100 log is output, an attempt is made to put the IBERT on the appropriate shower queue for a diagnostic. When the IBERT is diagnosed, a diagnostic log is output indicating the results of the diagnostic. An ILC diagnostic results in a LINE100 (pass) or LINE101 (fail), and a DTU diagnostic in a TRK107 (pass) or TRK106 (fail).

A BERT101 is a log generated to inform the tester of the test results for Wideband BERT, or the reason for an aborted test.

Network maintenance tools

Besides the existing NETINTEG analysis tool that is traditionally used, other resident DMS-100F tools can be used to meet BER requirements. They can also be used for maintenance and troubleshooting via the MAP. These tools are required for the initial grooming of the networks and XPMs, and can be used for ongoing maintenance to maintain the networks/XPMs at the required BER level—for high speed data services.

The new tools are designed to work on in-service equipment during light traffic periods. Safeguards have been incorporated into some tests to prevent service degradation during heavy traffic periods.

The features of the maintenance tools may be enhanced when used as a maintenance package, since some of the functions have a complementary interaction.

The following network maintenance tools will be described within this subsection:

- NETINTEG (Network integrity analysis tool)
- NETPATH (Network path fault isolation)
- ICTS (Integrity check traffic simulator)
- XBERT (XPM bit error rate test)
- NETFAB (Network fabric testing)
- Switch bit error rate indicator for trunks
- BERT for trunks
- ATT BERT for trunks

NETINTEG

The Network Integrity (NETINTEG) Analysis feature (NTX053AA04) is an original network maintenance tool that is used to identify errors on speech links between PMs and the switch JNET or ENET networks. In the past, NETINTEG was the only tool available to analyze network problems. The process to resolve problems was laborious and required trial and error methods for resolving network problems. NETINTEG can now be used with other tools, such as NETPATH described next, to isolate and verify problem pack(s) without having to change out suspected pack(s) on a trial basis. The NETINTEG level of the MAP is set up to handle two distinct types of problems, software and hardware. The hardware problems are of interest for the office clean-up. The hardware faults are distinguished from faults in the logs and the NETINTEG level by the string *parity*. The software faults have *integrity* as the reason and should not be considered here.

If you have ENET, see the "ENET Overview and Maintenance" subsection within the *System Products* section of this manual for a description of the INTEG level. There are significant differences in commands and displays between the JNET and ENET for this level.

The NETINTEG level of the MAP can be entered from the CI as follows:

>**MAPCI;MTC;NET;INTEG**

Upon entering that level from an office with JNET, the status of a number of parameters is printed in the display area and includes:

- pegging mode of the counters
- log types to be stored in a local buffer
- status of the automatic clearing

The function of each of these is contained within the descriptions of the commands, which follows.

JNET NETINTEG level commands

The following is a brief description of some of the commands available to the user once the NETINTEG level is entered:

MODE	This command allows for three possible choices: INTRA, INTER, and SPECIFIC. The INTER mode is the normal mode where every parity fault results in a count being pegged against the hardware involved in the call. The INTRA mode restricts the pegging to those calls that are confined to a single pair (INTRA pair calls). This mode is useful, as it prevents a faulty card on another NM from causing high counts on other NMs. With the SPECIFIC mode, a particular pair of NMs may be selected and only faults that occur between the selected pairs are pegged.
BUFFSEL	This command controls the contents of a 100 entry circular log buffer (LOGBUFF). The buffer contains the last 100 logs of the type specified by the BUFFSEL command. A combination of the NET 101 and NET 102 logs may be selected. The contents of the LOGBUFF are displayed with the DISP command described later.
POST	This command posts a specific plane and pair. The posted plane and pair then become the targets of certain subsequent commands.
SETLOG	This command is used to switch the NET101 and NET102 logs of the posted set on and off. It does not affect the storage of the logs in the LOGBUFF. This command is seldom used.
TRNSL	Gives the location of a specified card type and card number. The plane and pair of the specified card are defined by the POST command.
RSTI	Resets ISTB conditions for the plane and pair posted and displayed by the ANALYZE command. It also clears the counters that have reached their threshold. Command "RSTI ALL" resets failure counter for all the planes and pairs.
TIMER	When enabled, all counters are zeroed at 0800 local time. Counts that accumulate too slowly may be cleared by the daily reset (before it can be investigated to determine what card is most likely at fault). By disabling the timer, the counts will eventually reach the threshold. The counts that approach the threshold most rapidly are most likely at fault. The *Office Administration* section in this manual describes a store file (SF) work-a-round for altering the automatic daily clearing time

The DISP command, when input with other parameters, has some of the following forms:

DISP MASTER	Shows the total of the card counts for all planes and pairs of the posted NM.
DISP LOGBUFF	Displays the contents on the circular net log buffer. Only the logs of the posted NM are displayed. If qualified with the string ALL, the entire buffer will be displayed.
DISP CLEAR LOGBUFF	Clears the contents of the logbuff.
DISP COUNTS	Displays the counts pegged against the cards of the posted NM.
DISP CLEAR COUNTS	Clears the counters of the posted NM. It may be qualified with the string ALL to clear all the counters on the LOGBUFF.
PMS	Shows total integrity faults on a PM basis. Also lists faults on a per link basis for the 20 worst PMs in the office.

Besides the various operational measurement (OM) registers in the OM NMC group that are helpful in pointing out network problems, the following commands within the INTEG MAP level help provide an indication of network problems:

ANALYZE COUNTS	Displays the 10 cards of each card type that have the highest counts. This is done for the posted NM.
ANALYZE PM	Displays the 10 PM/ports with the highest counts on the posted NM.
ANALYZE JUNCTORS	Displays the 10 junctors (both ends) with highest counts on the posted NM.

The following are NETINTEG level hidden commands.

UPTH	Changes the thresholds for the failure counters upon which the command DISP COUNTS relies. When the threshold specified here is reached, the network is set ISTB.
RETH	Restores the thresholds of the counter back to the default 250. The NET142 log is generated whenever the NETINTEG counter is cleared or the counter thresholds are changed.
TRLNK	This hidden command translates the information of the pair, port, or channel of the network in order to determine the corresponding circuit(s) of the PM that is connected to it. This command should be used by maintenance support personnel.
FILTER	The FILTER command is a hidden command off the NETINTEG level of the MAP. It is used to *query* the integrity and parity threshold values or *alter* the parity threshold level throttling for each XPM. This throttling level determines the number of errors (faults) that are required in a ten second interval to invoke corrective activity by the PM (e.g., transfer to the other network plane and initiate diagnostics).
	For more information on the use of this command and its relationship to the XPM_PARITY_THRESHOLD parameter, see the "FILTER command" later within "Integrity" within this subsection. Also, for ENET, more information can be found on the FILTER command in the "ENET Overview and Maintenance" subsection with the *System Products* tab of this manual.
CHKLNK	CHKLNK is an unlisted command accessed from the NET level of the MAP. It is used to alter (increase) the sensitivity of message links to errors. CHKLNK may be used on all junctor networks—except NT0X48—to aid in locating constant or intermittent messaging problems that have eluded the normal menu tests.

The tool checks all message links not actively sending messages for correct idle conditions. Values other than those listed below indicate a messaging error:

30	IDLE	(Idle)
32	HIDLE	(High Idle)
34	MIS	(May-I-Send)
36	SEND	(Send)
38	SOM	(Start of Message)
3A	PACK	(Positive Acknowledgment)
3C	NACK	(Negative Acknowledgment)
3E	IWS	(I-Will-Send)
3F	WAI	(Who-Am-I)

> **CAUTION**
> The CHKLNK command may cause calls in progress to drop and links with problems to be set system busy. These may be identified from the MAP or through log reports. Since links are removed from service, the tests must be supervised and limited to testing one network and one plane at a time. This procedure can help minimize outages and service degradation.

NETPATH

The network path (NETPATH) diagnostic is one of four features in the Switch Path Diagnostics software package (NTX885AA). It is a test tool used for fault isolation and verification testing in the networks (except the NT0X48 type network). NETPATH (Pathtest for ENET) is accessed from the NET level of the MAP. NETPATH allows the technician to perform fault isolation and verification on the network components of a speech path by selecting the speech path in question, or the path segment through the network, and initiating tests to be run on the selected path in question. NETPATH complements the troubleshooting process since the failures detected by NETINTEG, NETFAB, ICTS, and BERP are placed in the *Path Fault Buffer* and are used as the path to be tested using NETPATH.

The NETPATH test tool assists in speech path maintenance by providing the user with these capabilities:

- identifies faulty components causing integrity failures
- confirms suspected components are faulty before replacement
- verifies that replacing the components has corrected the fault(s)

When a problem is detected during a call (or simulated call), indication of the problem is presented to the network maintenance system. In response to the problem, a log report is generated (the most recent 100 are saved), counters for each network component involved in the call are incremented, and finally, a diagnostic is run on the path to see if the location of the problem can be determined. In many cases, the diagnostic does not locate the source of the problem. The reason for this is that many problems are intermittent and may not occur during the diagnostic.

When using the NETINTEG analysis without NETPATH, only an educated estimate of the hardware at fault can be made. At this point the *suspect* hardware is changed and the correlation is again observed to see if the problem is resolved. NETPATH provides a means of testing a *suspicious path* without changing the hardware.

NETPATH supports the following network types: NT5X13, NT7X27, NT7X40, and NT8X11, but not NT0X48 network (due to hardware restrictions). NETPATH tests can be run on PMs directly connected to a network.

NETPATH fault isolation

NETPATH is a means of performing fault isolation. The fault isolation may be performed manually by specifying a series of tests with different insert and extract locations, different path components, or a combination of the two comparing the results of the tests. NETPATH can run automatically as well as manually. NETPATH run in the AUTO mode changes its own insertion, extraction, and test when a failure is encountered. NETPATH provides the ability to perform a scheduled NETPATH testing. Test data, passing from ICTS (integrity check traffic simulator), NETFAB (network fabric test), NETINTEG (network integrity analysis), and BERP (bit error rate performance) are extracted from the path buffers and submitted to the NETPATH test automatically. This eliminates the efforts of manual testing. A summary report is generated at the end of the test.

Since ICTS can test in-service trunks associated with XPMs, NETPATH was provided the capability to test in-service trunks as well.

The scheduled NETPATH test runs at the user specified time period of a daily schedule. It takes paths from a new path buffer—named INPUT—and performs path test on the problem paths automatically. The scheduled test, invoked from the MAP, sets up the path tests based on the severity and frequency of the problems. Multiple scheduled tests are allowed to run simultaneously. Test results are printed in logs and a status report is generated at 8:00 a.m. every morning. All failed paths, identified by a scheduled test, are placed in a *fault* buffer for maintenance actions.

It is not necessary for the user to provide all of this information if certain components of the path are not of interest. The user is provided with a template of the complete path and fills in the components of interest—the system will then select the rest.

It should be noted that NETPATH allows the user to specify and submit more than one test on the same path at the same time. Under these conditions, the tests will form a queue and run sequentially.

As already mentioned, the user has a number of sources to obtain the information needed to specify the path. The required information is available from:

- NET102 logs
- integrity level counters and buffers
- error reports generated by the various BER tests
- path fault buffer (NETFAB and ICTS)

NETPATH level and commands

The NETPATH level is accessed by the commands: MAPCI;MTC;NET;PATH. The NETPATH level display and some of its commands follow, along with a brief explanation.

Figure 2-9 — NETPATH MAP level display

```
   CM      MS      IOD     Net     PM     CCS     Lns     Trks     Ext    APPL
   ●       ●       ●       ●       ●       ●       ●       ●       ●       ●

 NETPATH      NET                 11111 11111 22222 22222    33
 0 Quit       Plane  01234 56789 01234 56789 01234 56789 01
 2 Post       0        .
 3 DefPath
 4 AltPath    1        .
 5 CpyPath
 6 BufPath    Queued:  nn  Running:  nn  Finished:  nn  Aborted:  nn
 7 VerPath    Test Type:  type       User:  mapid   Source:  where
 8 DefTest    Record:  name              State:  state
 9 AltTest    ASide: Net p-pa  port pt-ch  Xpt pt-ch  Jctr pt-ch  PM:
10 AltType    BSide: Net p-pa  port pt-ch  Xpt pt-ch  Jctr pt-ch  PM:
11 Disp       <               Test_Info                          >
12 Next       <               Result_Info                        >
13 Start      <               Abort_Info                         >
14 Reset
15 Clear
16 Stop
17 Info
18 Cardlst

 TIME 14 : 40  >
```

NETPATH commands:

QUIT	Leave the NETPATH MAP level and return to the NET MAP level.
POST	This command has two functions. The first is to create a new test record and provide the necessary commands to define and submit a test. The second is to specify a test record or set of records to be displayed in the status area of the MAP.
STOP	This command aborts the manual test or a scheduled test temporarily or permanently.
CLEAR	This command is used to free a test record. If a test is running on the test record, it is aborted before it is freed.
CardLst	CardLst is a command that displays the location of all cards in the posted path after the test path has been defined. It displays all the cards between the user–defined insertion and extraction locations for the AUTO test. With the fault parameter, the faulty card list can be displayed. A full path card list is displayed for the HOLD and ICTS tests.
DISP	This command displays a test or AUTO record, or a group of records in the conversation area of the MAP.
DEFPATH	This command specifies the initial path information for a newly posted test record. If this command is issued on posted test record with a path already defined, the previously defined path data is cleared and the new data added. The record must be posted and in the *Path Data Input* state to use this command.

Continued on next page

DEFTEST	This command defines the test data for the record. The record must be posted and the *Data Input* state to use this command. The DEFTEST command is used to define the START time, STOP time, and the option of testing INSV trunks of a scheduled test.
ALTTEST	This command alters the test data for the record. The record must be posted and in the *Test Data Input* state to use this command. The ALT-TEST command is used to define the START time, STOP time, and the option of testing INSF trunks of a scheduled test.
ALTPATH	This command alters a portion of the path definition without changing the rest of the path. The record must be posted and in the *Path Data Input* state to use this command.
CPYPATH	This command copies the path data from an existing record to the posted record. The posted record must be in the *Path Data Input* state to use this command.
VERPATH	This command verifies that the path entered is valid. (It checks to see if the data describes a legitimate path through the network.) The posted record must be in the *Path Data Input* state to use this command.
DEFTEST	This command defines the test data for the record. The record must be posted and in the *Data Input* state to use this command.
ALTTEST	This command alters the test data for the record. The record must be posted and in the *Test Data Input* state to use this command.
SET	SET is a hidden command that is used to set the threshold of the failure count for the NETPATH tests. This threshold can only be set when no NETPATH test is running. It is also used to turn off the NETPATH logs in the AUTO mode.
RESET	When a test has finished or been aborted, this command may be used to return it to the input state so that the data may be modified, the test re-submitted or both. The record must be posted and in the *Finished* or *Aborted* state to use this command.
START	When a test has been newly defined or reset, this command is used to start the test. The record must be posted and in the *Test Data Input* state to use this command.
NEXT	Post the next element in the post set. If there are no more elements in the post set, the current element is left posted.
ALTTYPE	This command alters the test type. Any existing test data is reset if this command is issued. The record must be posted and in the *Path Data Input* state to use this command.
BUFPATH	This command controls access claiming and releasing of the paths in the NETPATH fault buffer.

ICTS

Integrity check traffic simulator (ICTS) is another feature in the Switch Path Diagnostics software package (NTX885AA). Tests are initiated from the CI level by using the ICTS command. It is completely software driven; no external hardware is required. ICTS simulates high volume calling, which exercises potentially every network link and channel to every XPM in the office. ICTS is a resident software tool for testing the integrity of network connections by setting up a number of connections and monitoring them through the peripherals. ICTS is designed to aid in network and PM speech path clean up by identifying hardware marginal conditions that result in integrity failures. The feature allows for focusing on specific network components by

selecting appropriate XPMs for the testing end points. The tests and scheduling are determined by a technician who runs the tests. For a description of EICTS (ENET ICTS) for ENET, see the "ENET Overview and Maintenance" subsection in this manual.

ICTS is usually performed for the following reasons:

- routine maintenance

- monitoring of the integrity logs or network fabric (NETFAB) maintenance shows that the PM, slot, link or other hardware has recurring problems and you want to confirm the problem

- the manual ICTS tests allow for more control when testing the system (i.e., testing can be limited to specific hardware, or a specific time)

- to simulate an overload situation which should be performed jointly by Nortel Networks and the operating company

ICTS has the following features:

- exercises in parallel, potentially every network link and channel to every PM in an office

- allows long duration (multiple minute) connections which are continuously monitored for integrity/parity failures, by the PM

- software driven package requiring no external hardware test sets

- can be used in both in-service and precutover offices (for in-service offices, safeguards are implemented to ensure there is no resource competition with normal call processing)

- provides pinpoint troubleshooting capability by allowing the user to specify the network links and PMs on which connections are to be established (as well, the same connections can be reestablished after suspect hardware has been changed)

- very quickly highlights marginal hardware paths by retaining the PM's integrity and parity checking on the original plane which encountered the fault (does not switch to other plane). Since the ICTS connection constantly exercises the same hardware, it can cause the integrity counts to accelerate when faulty hardware is involved in the path

How ICTS works

The links involved with ICTS connections are set up by the user. These links are marked as available for ICTS use. ICTS works by scanning the set of ICTS links for two available channels. Once the two channels are found, a network connection is made, PCM is established, and integrity is enabled.

Messages are sent to the PMs involved to request the start of integrity scanning. If an integrity or a parity failure occurs, the connection continues scanning on the original plane and generates a NET102 log. A field in the NET102 log indicates that the connection was owned by ICTS. The NETINTEG level of the MAP can be used to pat-

tern and find the ICTS failures. A hard integrity failure causes numerous integrity faults in a short time frame. ICTS turns off the integrity scanning in the PMs if the number of integrity failures per minute has exceeded the integrity threshold. The integrity threshold is set by the user as one of the IOPTION commands.

If a PM that has ICTS connections does a warm swact, a burst of integrity faults can occur for the ICTS connections (also applies to NETFAB).

The connections are left established until a command is performed to take down the connection or the connection does not pass the checks made by the audit process.

The audit process reevaluates the current traffic situation. If any ICTS link or junctor has exceeded the traffic limitations, the audit can clear the ICTS connections on the link/junctor until the number of ICTS connections are within the limits.

Every half hour, the audit process produces an ICTS101 log. The log contains a connection summary that includes the number of ICTS connections that successfully refreshed the integrity and the number of connections that were cleared due to traffic limit problems. The audit status can also be accessed through the IQUERY command.

ICTS channel selection for PMs & XPMs

ICTS includes testing to the LM peripheral. Phantom TIDs (terminal identifiers) have been developed to facilitate the LM test connection. A normal TID is a node number and a terminal number assigned to a physical device. A phantom TID is assigned to a virtual device. Every line has a TID assigned to it, starting from 1 to 640. TIDs over 640 are called phantom TIDs. Using a phantom TID in making connections, no physical line is taken, and thus, no service is affected. The phantom TID is designed on a many-to-one basis so that many C-side channels can use the same phantom TID, which simplifies the setup problems. A new LM peripheral load will be required.

For DCMs, TMs, TMBs, and MTMs, a search is made for an INB trunk. If one is available, the channel and link associated with the trunk becomes an endpoint in the ICTS connection.

For LGCs, SMUs, SMRs, a search is made for a free channel. If the channel is found and the channel limits for the link have not been exceeded, the channel is taken for the ICTS connection. The channel cannot be used for call processing unless ICTS releases the connection. The limits used for the link within an in-service office are:

- MIN. number of free channels = 7
- MAX. number of channels on the link used by ICTS = 7

For DTCs, the first search involves looking for a non-reserved channel—one that does not have a trunk datafilled against it. If a non-reserved channel is found, the channel and link can be used in an ICTS connection.

If all the channels are allocated, the second search looks for a trunk that is in the INB state. If an INB trunk is found, channel and link will be used for ICTS connections. The DTC does not have any traffic limitations, since all the channels involved are not

available to call processing. IDL trunks can be selected using the IOPTION and XPM variable commands.

For LTCs, a combination of the DTC and LGC channel searches is used. The LTC's link has a combination of line and trunk channels on it. The link is scanned for line channels that are free. If a free channel is found, another check is done to analyze the traffic and number of ICTS connections on all the line channels on the link. The channels reserved for lines must not exceed the limits for an in-service office as follows:

- MIN. number of free line channels = 25%
- MAX. number of line channels used by ICTS = 25%

If a free channel that is within the traffic limits cannot be found, the link is searched for an INB trunk. If an INB trunk is found, the channel is used for ICTS connections. There is no traffic check required for the INB channel, since the channel was not available to call processing.

Regardless of the PM type involved in the connection, the junctor involved in the connection avoids blockage by remaining within the limits shown below:

- MIN. number of free channels = 7
- MAX. number of channels on the junctor used by ICTS = 7

To enter the ICTS subsystem, simply input ICTS at the CI level. ICTS does not require a dedicated terminal. The user can leave (LEAVE command) the ICTS increment, ICTS continues working and leaves the terminal available for other uses.

It is highly recommended that NTP 297-1001-591, *DMS-100F Network Maintenance Guide* and NTP 297-1001-822, *DMS-100F Commands Reference Manual* be referenced when using ICTS or EICTS commands. Serious problems can occur in an in-service office if ICTS is not used properly.

The following is a brief description of some commands available to the user once ICTS is entered:

>ICONFIG: Indicates the mode and the links to be used in ICTS connections for PMs and LMs.
>ISETUP: Makes the connections on the configured links, and start integrity scanning.
>ICLEAR: Clears all ICTS connections.
>IQUERY: Outputs information relevant to ICTS connections.
>IOPTION: Alters the conditions under which ICTS operates (i.e., in-service or not-in-service office).
>IREFRESH: Reinitiates the integrity scanning for the ICTS connections, whether or not the scanning has changed planes due to an integrity fault. This ensures that the connections are monitored on the original plane.
>ITRNSL: Translates a channel on a network link to the corresponding PM circuit, channel, and calling line identification number.

XBERT

XPM bit error rate testing (XBERT) is another feature in the Switch Path Diagnostics software package (NTX885AA). Tests are initiated from the CI level by using the XBERT command. XBERT is designed to detect bit errors in the XPM configurations. XBERT supports six separate tests for testing the various hardware components in the peripheral speech or Datapath. The tests and scheduling are determined by a technician. In addition to the XBERT software feature package, XPMs require a NT6X69AA or NT6X69AB message card and a NT6X79 tone card for the XBERT test feature to operate.

XBERT is designed to detect bit errors in the transmission of high speed data in XPM circuit packs. In addition, XBERT provides a facility for commissioning DS1 or PCM30 links and trunks that have been physically looped back at the remote end without the use of a remote node. XBERT can be supported by the following XPM types:

- LTC, LGC, DTC, RCC, MSB7, STC, LCM, CSC, SMR, SMS, SMU, ESA, IDTC, RMM, DLM, ADTC, PDTC.

All peripheral types listed above must be equipped with a 6X69AA message card or an NT6X69AB message card and a NT6X79 tone card to use XBERT.

While XBERT tests a variety of XPMs, there are some limitations. For example, XBERT tests the Remote Cluster Controller (RCC) and its C-side node independently, but it does not test the link between the RCC and its C-side node. With the Subscriber Module—Rural (SMR), three of the five XBERT tests, described later, are available for use (XPMINT, XPMPSL, XPMHLP).

With the Subscriber Module—Urban (SMU), only the XPMINT and XPMPSL commands are available to support business sets and ISDN features for the DMS-1 Remote Carrier Urban (RCU).

XBERT tests

The XBERT diagnostics supports six separate tests that are capable of testing different hardware components in the peripheral speech and data paths. The tests and their corresponding cards are as follows:

1. XPMINT test – 6X41 6X42 6X69 6X44 6X48
2. XPMPSL test – 6X69 6X44 6X48
3. XPMDCC test – 6X69 6X44 6X48 6X52
4. XPMBIC test – 6X69 6X44 6X48 6X52 6X54
5. XPMHLP test – 6X69 6X44 6X50/6X27 and associated carrier
6. ISOLATE tests

The ISOLATE test mentioned above provides a facility for automatic fault isolation. If this function is requested, XBERT automatically runs the appropriate subtests (XPMPSL XPMDCC XPMBIC) to detect and isolate a fault to a particular set of cir-

cuit packs. The number of cards in a card list isolated in this manner can vary between one and three cards, depending on the individual test results.

Also, XBERT provides the capability for the user to request that several XPM P-side ports be tested sequentially without any further user intervention. Similarly, the user can request that several LCM Bus Interface Cards (BICs) be tested sequentially without any further user intervention.

In each of the above tests, if the XPM P-side port being tested is a DS1 port instead of a DS30A port, then the NT6X50 DS1 Interface Card is tested in place of the NT6X48 DS30A Peripheral Interface Card. Also, for the XPMDCC and XPMBIC tests, if the node on the P-side of the XPM is an RLCM instead of an LCM, then the NT6X73 Link Control Card and 6X50 cards on the RLCM Host Interface Shelf are tested.

For accurate fault detection tests, each of the above tests must be run on an active in-service XPM unit. In addition, for the XPMDCC and XPMBIC tests, at least one unit of the LCM/RLCM must be in-service.

XBERT is designed to be a fault detection and isolation tool. It must be emphasized that XBERT *should not* be used as a tool for providing accurate bit error ratio assessments. It does not use the CCITT standard test patterns in its test procedure. Instead, it uses XPM tone PCM to provide the 64-Kbps test bit stream.

XBERT commands

The commands associated with XBERT follow, along with a brief explanation:

> **WARNING:** After entering XBERT, it is <u>highly recommended</u> that you enter a carriage return (CR) before entering any command.

XBERT This command may be invoked from any MAP level. The user can gain access to the XBERT main menu by entering the XBERT command and **then a carriage return (CR) to prevent potential problems.** After access has been gained to XBERT, the user can enter any of the commands provided by the XBERT main monitor commands.

To test Digital Trunk Controller 1 at the CI MAP level, enter command: XBERT DTC 1. The response should be XBERT - CONNECTING TO PM. These commands can be requested by either typing the entire command name or by typing the initial letter(s) of the command.

The XBERT main menu provides the following commands:

INITIATE This command allows the user to start up one of the XBERT tests. The INITIATE
I(nitiate) command requires several parameters. Many of the parameters are not used with the tests.

STOP S(top) This command stops the current test before its specified time duration has expired. Once the test has been stopped, the results of the test are displayed in a manner similar to that of the DISPLAY command.

RESET R(eset)	This command is used to reset the bit error rate counters of a currently running test. The effect of the command is to reset the number of bits tested counter and the number of bit errors counter to 0. Also, the elapsed time counter is reset to 0.
DISPLAY D(isplay)	This command is used to display the current statistics of a running test.
QUERY Q(uery)	This command allows the user to identify those XPM P-side ports and LCM BICs on which XBERT tests have been run.
PREVIOUS P(revious)	This command displays the statistics for the last completed test. The information provided is similar to that provided by the DISPLAY command except that the ELAPSED TIME field is not present and the DURATION field specifies the actual length of time for which the test ran.
PORT INFO PO(rtinfo)	This command displays the statistics for all the tests requested with the multiple ports (MP) option. It displays which port(s) have already been tested, which port is currently being tested, and which port(s) have yet to be tested. It is possible to display the results of one or all ports that have been tested with the multiple ports option. Also, this command displays the statistics for the tests requested using the multiple BICs test facility.
HELP H(elp)	This command displays information about the syntax and use of the XBERT commands.

XBERT references

See NTP 297-1001-592, *DMS-100F Peripheral Module Maintenance Guide* and NTP 297-1001-822, *DMS-100F Commands Reference Manual* when using XBERT.

NETFAB

The network fabric (NETFAB) test feature is part of the Switch Path Diagnostics software package (NTX885AA). The network fabric refers to the call paths through the network modules of the switch. NETFAB is accessed from the CI level through the ICTS command. It is completely software driven; no external hardware is required. NETFAB is an automated routine testing procedure that uses the ICTS test features to identify network problems. It is essentially a scheduled test that exercises call paths during low traffic periods, and without the need for manual intervention. The NETFAB feature uses the ICTS software to set up groups of ICTS connections—in a controlled manner—to test all the call paths in the network.

NETFAB is essentially a scheduled version of the ICTS package. For ENETFAB testing of the ENET, see the "ENET Overview and Maintenance" subsection within the *System Products* tab of this manual.

NETFAB test feature

The NETFAB feature provides the ability to perform a scheduled test of the DMS-100F switch network fabric. All links and junctors are scheduled to be tested for four hours each night—provided they map into peripherals supported by the ICTS package. Faulty paths are stored in the path fault buffer. If a port appears in more than one errored path, each subsequent errored path—involving the same port—overwrites the previous path entry. Testing starts over when all the link and junctor channels have been exercised.

NETFAB test features include LM peripherals and the testing of in-service trunk channels associated with XPMs. All channels are tested on the supported links if they are not being used or required by call processing during the test.

Although the NETFAB test is essentially a scheduled test, it can be suspended to run a manual ICTS test, and resumed when the manual test has been completed. The NETFAB test can also be manually started and stopped.

How NETFAB works

NETFAB, using ICTS software, allows the user to establish a series of connections through the Network Modules (NMs) to perform integrity and parity checking. If an integrity failure is detected on one of these connections, integrity checking is reestablished on the same network plane to focus testing on the problem. In a normal call, if integrity checking failed, it would switch to the other plane.

Using the ICTS software, the NETFAB feature sets up a connection on each junctor in the office. The end points for each connection are distributed to each link in the office. For each connection, NETFAB:

- establishes integrity and parity checking on one plane
- maintains a count of the quantity of integrity faults detected on each connection
  - If more than ten failures are detected on a given connection, NETFAB stops integrity checking on that connection
- reports each failure to the NETINTEG feature, which correlates the integrity failures according to the hardware in the connection
- switches integrity and parity checking—after ten minutes—to the other plane and again monitors the failures
- analyzes the results of the testing—after another ten minutes—and stores the results in the path fault buffer
- selects new links and channels as end points for the connections and repeats the steps above. Selecting new channels on each link as new end points ensures that all link channels are tested

When all link and junctor channels have been tested, the test starts again.

To be included in NETFAB testing, links must map into PMs that are supported by the ICTS package. All channels on the links that map into one of these PMs are tested if they are not required for call processing during the test. Most PMs are as follows:

ADTC	IDTC	OAU	TM
ALGC	ILGC	PDTC	TMA
ATM	ILTC	PTM	TM2
DCM	LGC	SMR	TM4
DES	LM	SMS	TM8
DSM	LTC	SMU	T8A
DTC	MTM	STM	

NETFAB tests cannot be run at the same time as manual ICTS tests. However, NET-FAB testing can be suspended (to allow an ICTS test to run) and resumed after the ICTS tests are complete.

Integration with other test tools

The NETFAB feature integrates into the network maintenance system by interacting with current features in the following manner:

- The network integrity (NETINTEG) analysis feature monitors and correlates the integrity failures generated by NETFAB testing

- The network path (NETPATH) test tool tests the paths that are identified as faulty by NETFAB testing

NETFAB commands

For references to NETFAB commands, see NTP 297-1001-591, *DMS-100F Network Maintenance Guide* and NTP 297-1001-822, *DMS-100F Commands Reference Manual*.

The commands by which NETFAB testing is manipulated are described as follows:

SUSPEND	Suspends scheduled testing for the following intervals:
	If scheduled testing is running when the command SUSPEND is issued, the test is suspended for the remainder of the test interval. It automatically resumes at the start of the next interval.
	If scheduled testing is *not running* when the command SUSPEND is issued, the next scheduled interval is missed, and testing automatically resumes in the subsequent interval.
RESUME	Resumes a scheduled NETFAB test. Testing resumes in a few minutes (if the RESUME command is issued during a scheduled test period) or at the start of the next scheduled period. Testing starts from the point where it stopped when the SUSPEND command was executed.
START	Initiates a manual NETFAB test. The test starts immediately and runs until it has attempted to exercise all the components of the network. The manual NETFAB test can also be stopped by issuing the command STOP.
STOP	Stops a manual NETFAB test.
STATUS	Displays the history of the current or last run NETFAB test—scheduled or manual.
QUIT	Exits from the NETFAB increment.

NOTE: As with scheduled NETFAB testing, manual NETFAB testing should only be run during periods of low traffic.

NETFAB logs

The NETFAB feature generates the following ICTS logs:

- Log ICTS105 — The NETFAB feature generates log ICTS105 each morning at 8:00 a.m. The log report informs the user of the results of the NETFAB testing run the previous night

- Log ICTS106 — The NETFAB feature generates log ICTS106 whenever a NET-FAB test is completed — that is, when all the channels on all the links and junctors in the network have been tested

---

NOTE: These logs are intended for information purposes only. They contain records of the paths on which integrity failures were detected during NETFAB testing. To locate the hardware failures, use the NETPATH test tool that is described next.

NETFAB status

The status of NETFAB testing can be displayed at any time using the STATUS command. The parameters of this command are as follows:

- PERIOD — displays the status of the current test
- PREVIOUS — displays the results of the last completed test

NETFAB scheduling

Two office parameters in table OFCVAR control the activation and scheduling of NETFAB.

NETFAB_SCHEDULE_ENABLE — This parameter tells the machine that the feature is enabled or disabled. The recommended default value "Y" enables the test. Any change to this value takes effect immediately.

NETFAB_SCHEDULE_TIME — This parameter establishes the start time for the four-hour network fabric test. The default value is 0200 (2:00 a.m.), meaning the test runs from 0200 to 0600 daily (2:00 a.m. to 6:00 a.m.). Changes to this value are effective immediately.

Switch bit error rate indicator for trunks

The switch bit error rate (BER) indicator for trunks testing procedure is described in NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing*. The switch BER indicator for trunks feature can be found in the NTX881AC software package for local switches and NTX882AA for DMS-200 switches. For the local switch, the feature tests the bit error rate (BER) on trunks by using either or both of the NT4X23AA Digital Test Unit (DTU) cards located in the MTM shelf, or the NT6X99 IBERT cards in the LCM. The DMS-200 uses only the DTUs for testing.

Trunks can be tested several different ways:

- loopback (any channel) at the NT6X48 DS30 card
- global loopback (full loopback all channels) at the NT6X50 DS1 card (XPMs)
- looped back at some external point (no DS30 or DS1 loopback)

When testing individual circuits, trunks are always tested using the DS30 loopback.

Most trunks only support 56 Kbps because of zero-suppression used on the DS1 links. When a trunk is looped back for testing, it must be placed in the off-hook state

(bit "A"= 1) so that the effects of zero-suppression do not affect the results of the BERP (similar scenario for AB bit signaling).

When running BERP testing without the DS30 or DS1 loopback, ensure the trunk is in the off-hook state for the same reasons stated above.

For additional information on setting up and performing BERP testing of trunks, see "BER testing (BERT) guidelines" later within this subsection.

BERT for trunks

The NTX883AA BERT For Trunks feature provides for *DS0* bit error rate testing (BERT) on digital outgoing and two-way trunks to another digital switching office. The trunk tests can be originated manually from the DATA level of the MAP, or automatically using the automatic trunk test (ATT) level of the MAP. The DATA level is accessed through the DATATTP hidden command off the TTP level of the MAP.

The automatic trunk BERT tests are set up to the far-end office "Dialed Loopback on Trunks" 108 testline connection, which loops the transmit and receive paths of the trunk under test. The 108 testline loop is provided in the network through software action. Further information on the 108 testline and BERT testing for trunks can be found in the previous "Trunks Maintenance" subsection.

Testing is performed from the TTP and ATT by:

- manual BERT test functions from the TTP DATA level
- automatic BERT test functions — BERTL from the ATT

The toll or tandem office originating the tests requires a NT4X23AA Digital Test Unit (DTU) card to perform BERT on the trunk circuits. The DTU is located on the MTM. The existing NT6X99 IBERT card can also be used as test equipment, but it is only provided in offices that support LCMs. The test equipment selection is for a DTU first and then IBERT card.

For the automatic testing of trunks for BERT at the *DS0* level, the far-end office must be equipped with a 108 testline. The 108 testline software provides loopback for incoming trunk(s). It must be datafilled in table OFCVAR, including the (new) testline numbers to be dialed for the far-end loop around access. See the previous "Trunks Maintenance" subsection for information on the implementation of the 108 testline.

The bit error rate test speeds are 56Kbps and 64Kbps and the bit error rate test patterns are 2047 and 51.

NOTE: The 64-Kbps test speed is used for *clear* type trunk facilities, such as ISDN and SS7 type trunks.

NOTE: The ATT test uses only the 2047 pattern. The test is run synchronous.

The results from the manual tests are stored in a table. A maximum of 500 test results can be stored at any one time. When the test results for a circuit are to be stored and the table is full, it overwrites the oldest test result stored. For the circuits whose test results are already in the table, the previous test results are overwritten with the new test results. On request, the test results can be displayed on screen. When the circuit under BERT test is placed in the control position of the TTP DATA level, the test results are displayed on the screen and updated continuously. The ATT test results are not stored in the table—they are formatted into a log message and sent to the log system.

BERT trunk testing description

BERT trunk testing is initiated from the TTP DATA level manually by command, or from the ATT automatically on a scheduled basis. A test connection is established upon a request from the TTP or ATT—usually to the distant office 108 testline connection.

The 108 testline software at the distant office loops back the transmit to the receive path in the network for the circuit being tested and returns answer supervision. The test equipment at the originating office is connected to the circuit under test and sets it up for bit error rate testing. The test equipment at the originating end transmits the test pattern on the trunk circuit transmit path and checks it on the receive path. Any deviation between the transmitted and the received bit pattern is recorded. At the end of the test the test results are recorded, connections released, and the circuits idled. If call setup troubles are encountered while establishing the connection or testing time, the test is aborted and the condition indicated.

TTP BERT testing

The TTP provides the control access functions for BERT testing on selected trunks and the display of the test results. The testing is performed by a separate process in the background. The TTP is not held up by the BERT testing. It is needed only for the duration while the requests are executed. Afterwards, it is available for other operations.

The test setup information is validated before starting the BERT test. The test is rejected if the circuit under test is not a digital circuit. A warning is displayed if the speed is 64 Kbps. A warning is also displayed if the test connection is set up without any termination. Normally, the test time is the time indicated by the command BERTTIME. If a terminating testline is specified, the test time is indicated by the maintenance Q-Limits test data. It overwrites the BERTTIME.

When the BERT test starts, the test results are displayed and updated on the screen as the test progresses. The test results are updated as long as the BERT test is running and the circuit remains in the control position of the data level. When the circuit is removed from the control position or the level is exited, the updating is stopped and the displayed information is erased (the test is not stopped). Whenever a circuit is placed in the control position of the DATA level and it has BERT test running on it, the test results are displayed and updated.

The number of trunks that can be BERT tested at any one time is equal to the number of IBERT test cards (NT6X99 or NT4X23) available in the office, up to a maximum of 128. Limiting factors include IBERT resource management and the availability of far-end terminating testlines.

DATA level commands

The BERT trunk testing DATA level is accessed by the commands: MAPCI;MTC;TRKS;TTP;DATA. Following is a list of DATA level commands and descriptions:

BTERM	Registers the type of termination to be set up for the BERT test. This information is used when the BERT command is executed. The information cannot be changed after the test has started. Related parameters are:
TL	Set up termination to the 108 terminating testline.
DIG	Set up termination to the number indicated.
RESET	Reset the termination registered.
QUERY	Display termination registered.
BERT	Provides the manual BERT test control functions. Related parameters are:
START	Start BERT with 56 Kbps or 64 Kbps speed and a pattern of 2047 or 511.
STOP	Stop BERT test.
INJECT	Inject bit errors indicated in the test pattern.
RESET	Reset the BERT test results.
QUERY	Display the test results for the circuit in control position. Display all active BERT tests. Display all test results. Display test results for the CLLI.
BERTTIME (Non-Menu Command)	Provides the BERT test time. The time is only registered. If the time is not specified, it defaults to BERT test time of 100 hours. Related parameters are:
SET	Time Units Type of time units (minutes or hours).
QUERY	Query the time set.

ATT BERT for trunks

The automatic trunk test (ATT) BERT for trunks test functions are provided by the bit error rate testlines (BERTL) TB08 for 56 Kbps or TB18 for 64 Kbps.

ATT functions

The ATT is modified to allow BERTL tests to be performed in a way similar to how it is done for other testlines—that is:

- store test request
- initiate BERT test
- request TEST process to perform the test
- wait for test results
- format the test results into a log message (test or connect fail log)
- return the circuit to service or remove from service (test data dependent)

ATT BERTL TB08 & TB18

The ATT test data provides information on how the test is to be performed on a particular group of circuits. This information is preset for each test request. The BERTL requires new information—that is, the BERT maintenance Q-Limits. The ATT test information is modified to include an index for the maintenance Q-Limits in the Maintenance Q-Limits (MQLIMITS) table.

BERTL test description

The ATT initiates the BERTL test, but it does not control it. The test is performed by the test process. The ATT requests the test and waits for the results. It formats the test results in a log message and sends them to the log system as an ATTXXX log—see "ATT logs" later.

On a request from ATT, the BERTL establishes the connection to the distant office 108 terminating testline by outpulsing the assigned testline number. The terminating office connects the incoming trunk transmit path to the receive path and returns an answer message. The originating office connects the test equipment to the circuit under test and sets it up for bit error rate testing. A specified bit pattern—at indicated speed—is sent on the trunk transmit path and checked on its receive path (returned from the far-end office). Any deviation in the received bit pattern, to that of the transmitted, is recorded. The test is run for the specified duration of the time (1 to 15300 minutes). At the end of the test, the connections in both offices are released and the circuits idled, except the circuit under test. On test failure, the idling of the circuit is test data dependent. The test results are compared with the indicated maintenance Q-Limits to determine the test Q-Limit.

If any trouble is encountered during the connection setup or during the test interval, the test is aborted and the condition indicated.

While the test is in progress, it cannot be stopped or queried for test results.

ATT commands

ATT level command TESTREQ has parameter BQINDEX (index number to point to the maintenance Q-Limits in the MQLIMITS table).

ATT log messages

The following log reports are generated when BERTL tests are run by the ATT:

ATT109   An existing log that has additional fields added to include BERTL information. This log is generated at the start of every trunk group test by the ATT

ATT121   A log generated when the ATT performs a BERTL test on a trunk. This log records the test results.

ATT122   A log generated when the ATT performs a BERTL test on a trunk and encounters a call setup or connection failure (no test results).

Table MQLIMITS

A Maintenance Q-Limits (MQLIMITS) table is provided for storing the maintenance Q-Limits for the BERTL and its test time. The information provided is:

- BERQ — bit error rate Q-Limit (default = 3)
- ERSQ — errored seconds Q-Limit (default = 8)
- SLIPSQ — number of slips Q-Limit (default = 3)
- TLTIME — test time in minutes (default = 15)

This table provides 10 sets of values that can be preset by the operating company to their requirements. It is modifiable by the standard table control.

The values within the MQLIMITS table are needed when using the TTP and ATT levels to get the required maintenance Q-Limits and the test time. The TTP uses the Q-Limits from position zero and the ATT from the other positions.

A new field, MQIDX, is added to ATTOPTNS table. This indexes into table MQLIMITS to obtain the test requirements for the automatic BERT testing. The default value setting is one.

Maintenance tools and work activity application notes

Following is a table providing a summary of the network maintenance tools previously described. This table provides a view of the tools and the associated work activities they support. Following the table are the A1 through J1 notes that provide a description of the work activity as related to the maintenance tool.

Table 2-60 — Network Maintenance Tools and Work Activity Application

TOOLS -----> WORK ACTIVITY	I B E R T	I C T S	B E R P	X B E R T	NET P A T H	NET F A B	NET I N T E G	SWITCH BER FOR TRUNKS	BERT FOR TRUNKS	T K L P B K
NETWORK GROOMING **A**		See Note **A1**	See Note **A6**	See Note **A4**	See Note **A3**	See Note **A5**	See Note **A2**			
ROUTINE PREVENTIVE MAINTENANCE **B**				See Note **B2**		See Note **B1**			See Note **B3**	See Note **B3**
BER PERFORMANCE (SWITCH) **C**			See Note **C1**							
SWITCH BER ANALYSIS **D**			See Note **D1**		See Note **D1**		See Note **D1**			
NETWORK TROUBLESHOOTING **E**		See Note **E2**	See Note **E1**		See Note **E2**		See Note **E1**			
PM/XPM TROUBLESHOOTING **F**			See Note **F1**	See Note **F2**			See Note **F1**	See Note **F3**		
LINE TESTING (LOOP/STN/LC) **G**	See Note **G1**			See Note **G2**						
NETWORK END-TO-END PERFORMANCE **H**									See Note **H1**	
TRUNK BER TROUBLESHOOTING **J**								See Note **J1**	See Note **J1**	See Note **B3**

NOTE: See the following work application notes and their relationship to the various tools

BER Maintenance Tools and Work Activity Application Notes

A. NETWORK GROOMING

A1. ICTS — testing is programmed systematically by the tester—in workable segments—to identify BER faults in the network path. The fault information is stored in NETPATH and NETINTEG for isolation and correction (steps A2 & A3). The ICTS testing is continued systematically until all the networks in the office are cleared of faults.

A2. NETINTEG — summarizes the faults detected during ICTS testing and call processing (step A1). NETFAB summarizes faults identified by ICTS testing only. It determines the worst faults detected from ICTS testing summaries, and proceeds to NETPATH for trouble isolation.

A3. NETPATH — sectionalizes the fault to the defective circuit pack. The fault path information identified in step A2 is handed off to NETPATH, which reestablishes the faulty path for testing. Repeated NETPATH testing using different insert and extract points sectionalizes the fault to the defective card. It repeats steps A1 and A2, and verifies that the fault is corrected.

A4. XBERT — testing is designed to detect bit errors in the XPM, LCM, and RLCM speech and data transmission paths. The tester systematically programs the XBERT testing to cover all the XPMs. Bit error-rate failures are accumulated in the XBERT MAP menu against specific cards, between one and three. Trouble isolation and clearing involves replacing the suspected card and retesting. XBERT testing is continued systematically until all the XPMs are cleared of faults.

A5. NETFAB — essentially a scheduled automated version of the ICTS test. Once high speed data grooming for the office is complete, run (schedule) NETFAB to confirm network performance and detect faults. Correct any detected faults using steps A2 and A3.

A6. BERP — a statistical measurement for evaluating the overall BER performance of the office. BERP is indicative of the user's high speed data service. Run BERP to determine the BER for the office. See the previous "Digital Switch Bit Error Criteria" which describes the criteria and statistical sample size for valid results. Ongoing, BERP is run continuously to determine current office BER performance.

B. ROUTINE PREVENTIVE MAINTENANCE

B1. NETFAB — an automated routine testing procedure that uses the ICTS test features to identify BER faults. It is a resident tool accessed from the CI, MAPCI, or MAP level using the ICTS command and then the NETFAB command. From the NETFAB menu, NETFAB testing can be set to *enabled*. It can also be controlled from table OFCVAR using parameters NETFAB_SCHEDULE_ENABLED, NETFAB_SCHEDULE_TIME, and NETFAB_DAILY_DURATION. The default run time is from 2:00 a.m. to 6:00 a.m. Log message ICTS105 records the results from the previous night's fabric testing. Log message ICTS106 records the results for the last complete NETFAB test for the total network. Correct faults identified using steps E1 and E2 (NETWORK TROUBLESHOOTING).

B2. XBERT — it is recommended that XBERT testing be done on a periodic routine schedule (monthly) for all XPMs. Bit error rate failures are accumulated in the XBERT MAP menu against specific cards. Trouble clearing involves replacing the suspected cards and retesting.

B3. BERT FOR TRUNKS — feature provides manual MAP testing from the TTP level and automatic testing from the ATT level. The far-end office (terminating trunk end) must be equipped with the Trunk Loopback (TKLPBK) feature (108 Testline). Manual test results are stored in a table containing 500 entries; the ATT test results are formatted into a log report. Correct faults identified using step J1 (TRUNK BER TROUBLESHOOTING).

Continued on next page

C. BER PERFORMANCE (SWITCH)

C1. BIT ERROR RATE PERFORMANCE (BERP) — a tool used by the operating company to measure their switch performance in bit error rate terms. BERP is a statistical sampling type measurement. For example, a one week window for high speed data testing, at a confidence level of 80%, requires 4789 test calls, at ten minutes each. Completing this test schedule in a one week window requires 5 ILCs or DTUs running 24 hours a day for 7 days. Analyze the results, and correct faults following steps D, E, and F, as required.

D. SWITCH BER ANALYSIS

D1. Analyze accumulated fault indicators resulting from NETPATH routine testing, call processing and NETINTEG diagnostics using the NETINTEG and NETPATH buffers. Also review the summary of fault indicators resulting from BERP testing. Faults detected by BERP, and not identified by NETPATH testing, indicate an XPM fault condition. Determine the troubleshooting priority, and initiate action per steps E or F.

E. NETWORK TROUBLESHOOTING

E1. NETINTEG — summarizes the faults detected during NETFAB routine testing and normal call processing. BERP summarizes faults detected during overall BER assessment of the switch. Analyze the fault data to determine the problem areas requiring troubleshooting.

E2. NETPATH — sectionalizes the fault condition to the defective circuit pack. The NETINTEG fault path information selected in step E1 is handed off to NETPATH, which reestablishes the fault path for testing. Repeated NETPATH testing using different insert and extract points sectionalizes the fault to the desired card. Replace the suspect card and retest using NETPATH. Retest any repaired paths using ICTS to verify all is well.

F. PM AND XPM TROUBLESHOOTING.

F1. Determine if the problem is in the XPM by analyzing the BERP results and cross-checking the NETINTEG fault buffers for related equipment. If NETINTEG does not indicate a fault condition for the equipment being analyzed, but BERP data does, this indicates a potential XPM fault.

F2. XBERT — program the suspected faulty XPM for XBERT testing as described in the previous step A4.

F3. SWITCH BER for TRUNKS — tests suspected digital trunks to the C-side of the DS30 link on a per channel basis (the remaining 23 channels remain in-service), or at the P-side of the DS1 link, all 24 channels are looped back (all 24 circuits must be removed from service). The loopbacks are set and removed using the BERP level of the MAP. SWITCH BER for TRUNK testing applies to all DMS-100F and DMS-200 type offices. For DMS-200 offices, only digital test units (DTUs) can be used.

G. LINE TESTING (loop, station, and line card)

G1. IBERT — the loop testing tool for maintaining the subscriber's loop data path. Access is via the LTP, LTPMAN, LTPLTA, and LTPDATA level menus. Testing features include: error injection, loopbacks, bit error rate testing, and modem testing. Other tests from the LTP include diagnostic tests on the data line card (DLC) and data unit (DU) monitoring. Other tests from the station end include: looparound tests into the DMS-100 switch, silent switchman tests, and a data unit station ringer test. The trigger for IBERT line testing is generally a customer trouble report. Using the IBERT loop testing features, verify the trouble condition, sectionalize using looping techniques, and isolate to a repairable unit. In some cases, the trouble may prove back into the switch, trunk network, far-end switch, or called number.

G2. When the trouble tests back into the switch, run a series of XBERT tests on the XPM in question to determine XPM performance.

H. NETWORK END-TO-END PERFORMANCE

H1. NETWORK END-TO-END PERFORMANCE — The "Digital Switch Bit Error Performance Criteria" previously described in this section provides guidelines for end-to-end BER performance requirements. This is the overall service the data user sees, plus the loop and station at the near and far-end of the call setup. Utilize the BER test function associated with the ATT feature described in B3. Within the ATT guidelines multiple BER tests may be set up simultaneously. Identify any trunks not meeting the BER performance criteria, rank them in order of severity, and correct them using step J1.

J. TRUNK BER TROUBLESHOOTING

J1. TRUNK BER TROUBLESHOOTING — Analyze the ATT BER results to determine if any association of equipment or facilities exists that might be a common cause for the trouble. Rank the problem trunks by severity and investigate the worst faults first. In some instances, remove the trunks with bad BER counts from service. Sectionalize the fault using one or more of the following test procedures. When the fault is sectionalized, initiate the necessary corrective action. Retest the BER upon completion of repairs to verify fault is corrected. Test procedures to consider are:

1. From the TTP DATA level, establish a manual BER test connection on the faulty circuit and reaffirm that the fault condition is active. Factors causing the fault may be load related or intermittent; therefore, the BER test connection may require monitoring over a period of time.

2. Determine BER readings for the DS1 facility using the CARRIER level of the MAP at the home and distant offices, assuming that both are DMS-100F offices.

3. Verify NETPATH and XBERT routine test results for the equipment in question are clean for both the home office and distant office.

4. If the fault has not been sectionalized and corrected using the above steps, proceed to looping the facilities associated with the faulty trunk. Coordinate and integrate the testing with the far-end office.

5. Remove from service the trunks working on the DS1 facility to be tested.

6. Using the Switch BER for Trunks feature, establish test calls and proceed to loop the DS1 using global loopbacks, and if required, external loopbacks at the DSX bay. Faults sectionalized into the office are identified using NETPATH and XBERT (home office or distant office). Faults sectionalized into the DS1 facility are investigated and corrected by carrier maintenance personnel.

REFERENCES

The Switch Bit Error Rate (BER) Indicator for Trunks testing procedure is described in NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing.* Also, see NTP 297-1001-591, *DMS-100F Network Maintenance Guide.*

Integrity

This subsection describes what integrity means in and the possible causes of integrity failures within the DMS-100F switching system networks. Troubleshooting guidelines and approaches to correcting integrity failures for junctor networks are also provided. The terminology used for presenting integrity for junctor networks is basically the same for the SuperNode Enhanced Network (ENET), except for the difference in hardware.

NOTE: Throughout this subsection, references to junctor network equipment code NT5X13 also refers to the NT7X27, unless explicitly stated otherwise, since the NT7X27 is a repackaged variation of the NT5X13.

The network menu permits access to the network integrity (NETINTEG) program. NETINTEG provides a tool for identifying faulty network cards that are causing problems. NETINTEG does this by enhancing the information contained in NETINTEG failure logs NET101 and NET102.

What is integrity?

Integrity is used to verify the sanity of the speech path between two Peripheral Modules (PM). Integrity is checked by the PM in two ways: *first*, by comparing a randomly selected 8-bit code against a stored integrity value, and *second*, by checking for channel parity errors. If a mismatch or error is detected, the PM reports it to the NT40 Central Controller (CC) or SuperNode Message Switch (MS), which initiates an analysis of the speech path.

Every PM has numerous communication speech links available to other PMs—via the network, and every PM constantly monitors the integrity of links connected for calls. To do this, the PM exchanges pulse code modulation (PCM) samples, pertaining to the call in progress, and channel supervision messages (CSM). See Figure 2-10 on the following page, for DS30 speech and message data format. See Figure 2-11 on a following page, for DS30 CSM data format.

A PCM sample is 8 bits long and one is exchanged every 125 µs. CSM synchronization consists of 16 bits and takes 5 ms to transmit because the CSM is sent one bit at a time, rather than as a whole like the PCM sample. As each PCM sample is sent, one bit from the CSM is appended to it and sent along with it. This bit is called the channel supervision bit (CSB). There are 40 PCM samples and one CSM exchanged over every communication link every 5 ms. Every PCM sample has one bit appended to carry the CSM and 24 bits remain for transmitting the synchronization pattern (40-16=24).

To detect faults in the transmission of the 9-bit PCM and CSB code, a parity bit is added, which the PM uses to check for channel parity. Thus there is a 10-bit channel between the PMs—8 bits for the PCM, 1 bit for the CSB, and 1 bit for parity.

Figure 2-10 — DS30 speech and message data format

```
                 |<----------1 Frame-time (125 us)----------->|
              _ _ _                                                          _ _ _
           _|    |      |     |     |                        |     |     |     |      |_
    * *   | 31 |  0  |  1  |  2  | * * * * * * * * * * * | 30 | 31 |  0  | * * *
          |_    |      |     |     |                        |     |     |     |      |_
              _ _ _|    |                                                    _ _ _
                   |    |
                   | _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _|
                                                                          1 Bit
                 |<-------1 Channel-time (3.9 us)------->|<--|<--|(390 ns)

          | * * * * | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 9 | 8 | * * * * |
                                                          ↑   ↑
Speech                                                                 Parity Bit
Channel     <----------PCM or Data-------->
                                                                 Channel Super-
                                                                 vision Bit

Message                                                   ↑   ↑
Channel     <---------Message Data-------->                      Frame Synchro-
                                                                 nizing
                                                                 (Chan. 0 only)

                                                                 Spare (not used)

                              Increasing Time
          |------------------------------------------------------------------>
```
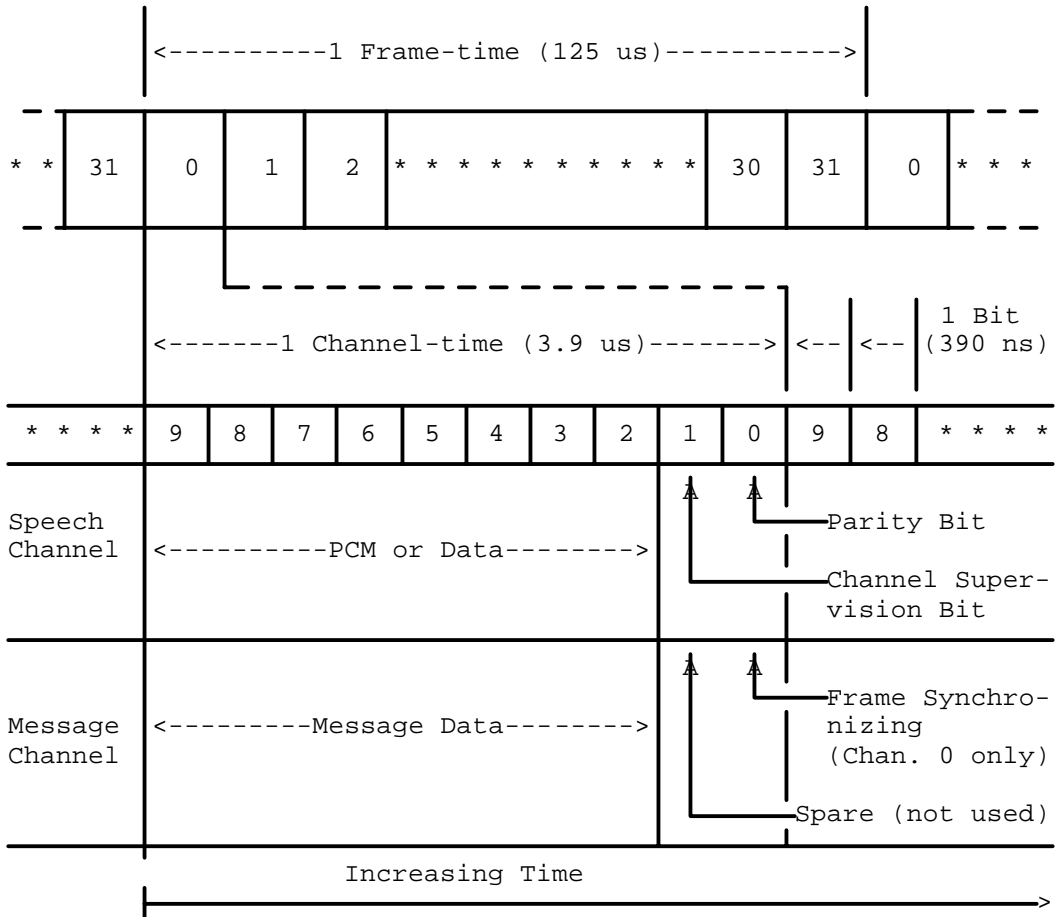
Figure 2-11   —   DS30 CSM data format

```
Frame No.
┌──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┬──┐
│0 │1 │2 │* │* │13│14│15│16│* │* │* │23│24│* │* │31│32│* │* │39│
└──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┴──┘
                                :           :           :           :
 ◄───────────── 5 milliseconds (40x125 u sec) ──────────────►
                                :           :           :           :
CSM──Channel 31                 :           :           :           :
┌────────────────────┬──┬───────────────┬───────────────┬────────────┐
│ CSM Sync. 16 Bits  │0 │ Con. Data Byte│ Integ. Byte   │ Sync 8 bits│
└────────────────────┴──┴───────────────┴───────────────┴────────────┘

CSM──Channel 2
┌────────────────────┬──┬───────────────┬───────────────┬────────────┐
│     all ones       │0 │ Con. Data Byte│ Integ. Byte   │  all one   │
└────────────────────┴──┴───────────────┴───────────────┴────────────┘

        ◄──────────Frame-0  125 u sec──────────►◄────Frame-1────►

         Channel No.
┌──┬──┬──┬──┬──┬──┬─ ─ ─ ─ ─ ─ ─┬──┬──┬──┬──┐
│30│31│0 │1 │2 │3 │             │31│0 │1 │2 │
└──┴──┴──┴──┴──┴──┴─ ─ ─ ─ ─ ─ ─┴──┴──┴──┴──┘

                                             ┌──┐
                                             │1 │
                                             └──┘
        Bit No.                               Bit
 9 8 7 6 5 4 3 2 │1│ 0

                 390
                 ns

 ◄──PCM Speech──►│ └──Channel Supervision Bit
       Bits

 ◄──────3.9 u sec────►
```
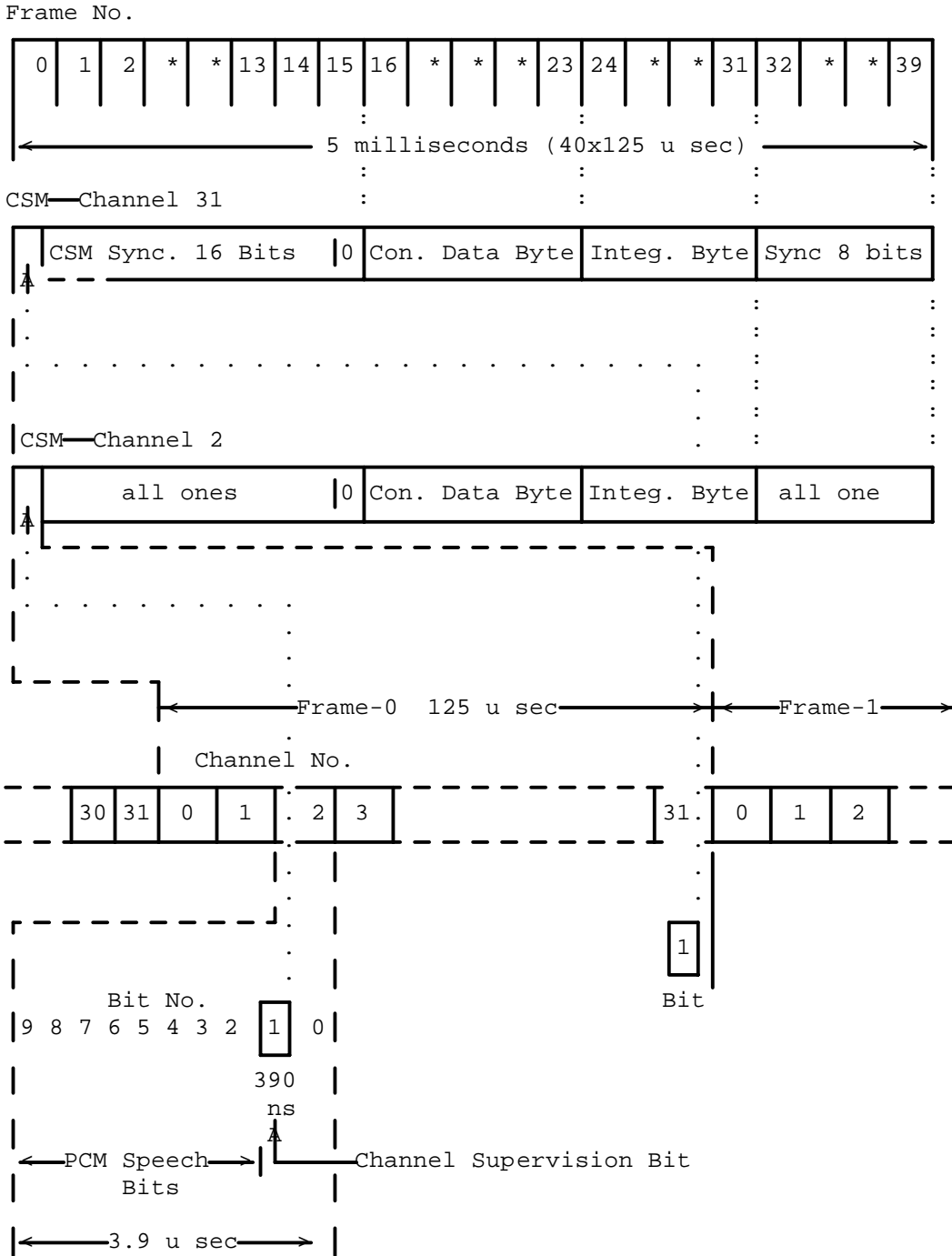
Figure 2-12 — Network Planes
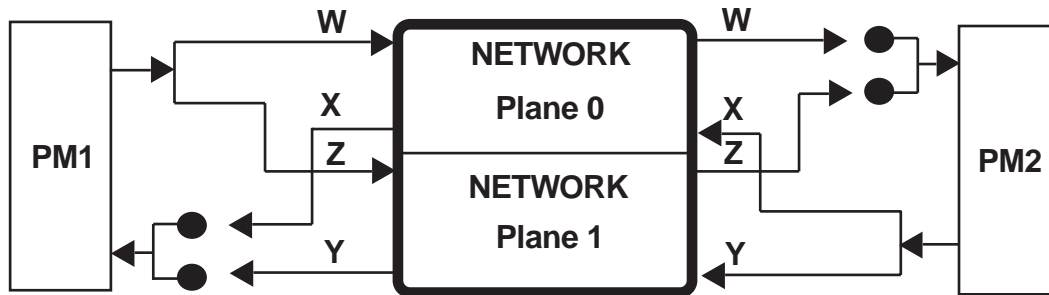
When the network has both planes in-service, there are four speech paths set up (W, X, Y, Z). Each PM transmits the 10-bit code simultaneously over both planes. Each PM receives on one plane only. PM1 in the diagram receives on plane 1 and PM2 receives on plane 0. The above setup for receiving on alternate planes is typical when both network planes are in-service.

The mismatch in integrity is always detected by the receiving PM. If PM1 detects an integrity mismatch, the path that is suspect is path Y. PM1 switches to receive from plane 0, path X, and then reports that it had problems receiving from plane 1. The network CC code then attempts to freeze the connection and run speech diagnostics on path Y.

If the speech connection has been disconnected between PM1 and PM2 before the network has a chance to freeze the connection for diagnostic purposes, a NET101 log should be generated. The NET101 (single-ended integrity) contains the information about the PM that reported the problem. The other end information, however, is lost.

If the speech connection still exists, the network CC code attempts to freeze the connection by setting a *maintenance hold* flag against the connection in the CC software maps. A diagnostic is then run on path Y. When the network CC code freezes a connection, the connection remains set up—even if the parties go on hook—until the diagnostic has been completed. Once the diagnostic has been completed, a NET102 log is produced with the call path information.

If the call terminates normally and call processing attempts to free the connection, the maintenance hold flag should keep the connection up. If, during the integrity diagnostic, the call is terminated and a new call attempts to set up another connection to one of the endpoints, it will be blocked and a NET132 log indicating "Double Connection Attempts" is generated. There are a few points to note here:

    1.The network integrity diagnostic duration depends upon office traffic conditions. During this time, new connection attempts to the endpoints involved in the integrity diagnostic are blocked.

2. If the path end involved in the integrity diagnostic maps into a heavily used trunk or line channel, a number of NET130, NET131, or NET132 logs may be encountered during an integrity failure. The logs related to an integrity failure are identifiable by comparing their log information and the NET102 log information.

3. The maintenance hold flag is used only for integrity diagnostics. Should the flag be erroneous, or left set after the integrity diagnostic is complete, the background network connection audit should recover the path. This may take minutes or hours depending upon office traffic conditions.

If the network has only one plane in-service at the time the connection was established, the plane that was out-of-service will not have the hardware setup. Therefore, if an integrity mismatch occurs, the PM will attempt to verify integrity on the alternate plane and fail. At this point the *call will be dropped*. The same holds true if there is bad hardware on the alternate plane—even if the plane is in-service. Any time integrity is lost on one plane, and the attempt to switch planes fails because integrity cannot be re-established, the *call is lost* and the CPSUIC OM register is scored.

Integrity monitoring

LGC/DTC integrity monitoring
The Line Group Controller (LGC) and Digital Trunk Controller (DTC) NT6X42 Channel Supervision Message (CSM) Card performs all the functions required for channel supervision messaging between peripherals. It can accommodate 16 network ports or 512 channels. Any channel connection between two peripherals establishes a duplex path that transmits a 10-bit byte in each direction every frame time. The parity bit of the CSM maintains odd parity for all bytes transmitted. The CSM bit provides a 3.2-Kbps message link between the connected peripherals on a per path setup basis. The channel data byte (CDM) transmits the connection data required to set up, maintain, and terminate a call. The value of the 8-bit integrity byte is given by central control for every path setup. It ensures the correctness of a pulse code modulation (PCM) path setup from one peripheral, to another. It also provides a means to measure the quality of the speech path throughout the connection.

CSM bit extraction from network channels
When a sync pattern is detected, the frame counter circuit records this and waits for the channel supervision message CDB and integrity byte. The parity bit is processed by the circuitry. The received integrity value is then compared with the expected integrity value. If there is an integrity match (IM) and no parity error has occurred for this channel within the last 40 frames, then the received CDB is updated into a CDB RAM for the signaling processor (SP). Results of the IM and a parity check are stored in and error report RAM for the SP

Integrity and parity error reporting
The results of the IM and parity check are stored in a set of RAMs as flags. RAMs are 16 bits wide and each location represents a network channel, for example, 16 ports. The IM bit is updated only at the end every 40 frames. The IM bit is set to zero when

there is no IM. The IM bit is set to 0 when there is no IM. A loss of sync signal is gated with the IM bit and this sets the IM bit to 0 when a loss of sync occurs.

Channel parity checking and generation of integrity messages due to parity failures is performed as a firmware background task. Firmware then monitors for parity interrupts for 10 ms. If a channel on one of sixteen ports has twenty or more parity errors during this 10 ms period, an integrity failure message is generated.

Integrity byte matching is started on a software request after a connection has been set up. Firmware loads the integrity check hardware with the integrity value to be monitored and enables matching (post an interrupt on integrity mismatch). The LGC/DTC allows up to 2.5 seconds for integrity to be detected, during the look-for-integrity (LFINTEG) mode. Once an integrity byte match has been established and present for 480 ms, the LGC/DTC switches to the check-integrity (CHKINTEG) mode.

If an integrity failure occurs, the integrity match hardware posts an interrupt to firmware. Hardware is then requested to generate an interrupt on integrity match, and firmware goes into a timing loop. If an interrupt is received within 480 ms—indicating the integrity byte has been re-detected—the original integrity failure is ignored. The timing loop is exited, and the integrity hardware is requested to post interrupts when the integrity byte mismatches again.

If integrity is lost and then found again within the timing period, the timer is reset. A subsequent loss starts the timer over. If integrity is not re-established, the PM switches network planes. The integrity failure regarding this previous plane is reported to the CC, and the PM enters LFINTEG mode on the new plane.

If integrity is not found on the new link, the message to the call process is sent, to take down the call. This message to the call process results in a LINE104 or TRK113 log message. No message is sent to maintenance in this case, and no NET log is generated for the second plane failure. The CPSUIC OM register is scored.

The initial integrity failure may be logged as a NET101 or a NET102 depending upon resource availability and call processing load.

Integrity monitoring for other PMs and XPMs

This order of reporting integrity failures is consistent on all existing PM and XPM types using network integrity, except that different timing filters are used. Following are some examples of timing filters:

DCM integrity monitoring filter
DCM FILTER VALUES

look for integrity (CHKINTEG) 15*80 ms = 1.2 sec
check integrity (CHKINTEG) 7*80 ms = 560 ms
parity filter 8 in 80 ms per channel

Figure 2-13 — Network Integrity Failures (Junctor Network Logs Listed)
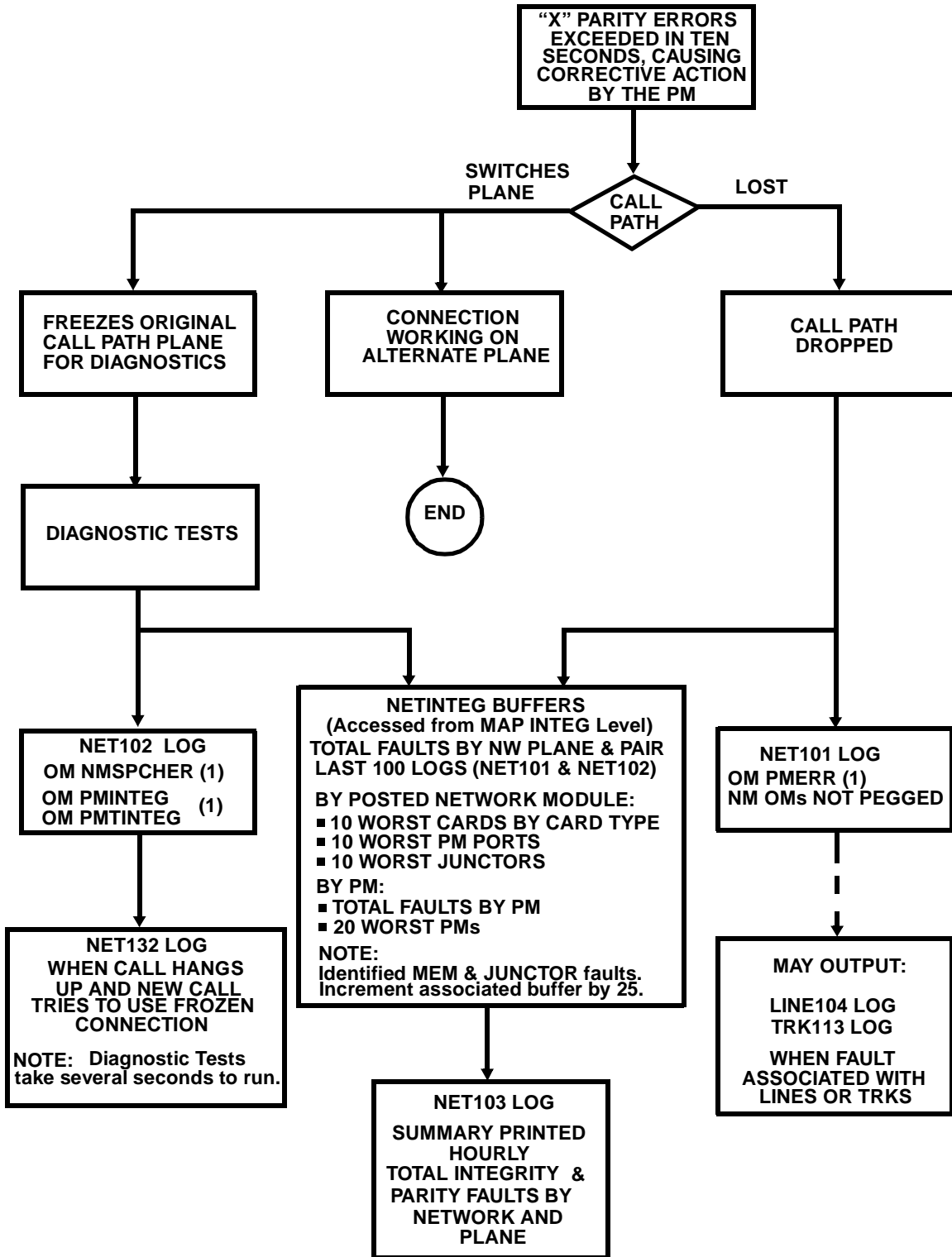
TM integrity monitoring filter
The firmware implementation and threshold values for the TM are similar to the DCM, but a different circuit pack is used for integrity detection.

TM FILTER VALUES
look for integrity (LFINTEG) 15*80 ms = 1.2 sec
check integrity (CHKINTEG) 7*80 ms = 560 ms
parity filter 8 in 80 ms per channel

LM integrity monitoring filter
The LM uses the same circuit pack for integrity detection as the DCM, but the firmware implementation and threshold values are different.

FILTER VALUES
look for integrity (LFINTEG) 127*10 ms = 1.27 sec
check integrity (CHKINTEG) 12*10 ms = 120 ms
parity filter 175 in 160 ms per channel

LTC/DTC/LGC integrity monitoring filter
FILTER VALUES
look for integrity (LFINTEG) 2.5 sec
check integrity (CHKINTEG) 480 ms
parity filter 20 in 10 ms per channel

Integrity logs

NET101 and NET102 logs
Network logs that report integrity information are NET101 and NET102. A NET101 log is generated when an integrity failure occurs and the network path is no longer defined (connected). NET101 log records the following information:

- indicates a problem with PM firmware or hardware
- indicates which unit was active when the fault occurred—if relevant to the PM type
- indicates a problem with CC software if both network planes were in-service at the time of the failure

Example of a NET101 log
```
NET101 DEC01 23:24:05 5595 EXC INTEGRITY LTC 0
FAILURE, CALL WAS SET UP,
PATH INSERVICE NET 1-0, PORT 40, CH 4
```

No NMC OM is pegged on a NET101, since the problem is probably not a network problem. However, PM OM errors are pegged for the PM reporting the integrity failure, since at the time the integrity failure is reported, it has not yet been determined that the path is gone. This type of log generally indicates a PM firmware or hardware

problem—or a CC software problem—of both network planes that were in-service at the time of the failure.

If this log is accompanied by a LINE104 or TRK113 log message indicating INTEGRITY LOST, a call has terminated abnormally, and the problem may be service affecting. If no LINE or TRK log accompanies the NET101, the problem may simply be due to a PM being slow on call takedown, and the network path being reused before the PM has stopped looking for integrity. This would not be service affecting, since it occurs on call takedown and does not affect any calls being set up.

A NET102 log is generated when an integrity failure occurs and the network path is still defined. NET102 log records the following information:

- the one or two PMs involved in the integrity failure

- indicates which unit was active when the fault occurred—if relevant to the PM type

- the reason for the failure

- the call state 9 being set up (in progress)

- the link numbers between the one or two PMs and the Network

- the source of the failure (call processing, ICTS, NETFAB)

Example of a NET102 log

```
NET 102 NOV19 01:00:53 0536 EXC INTEGRITY
DCM 2, DTC 10 Unit 0
INTEGRITY FAILURE, CALL WAS NOT SET UP, CALL PROCESSING
ASide: Net 0-22, PORT 21-17, Xpt 1-22, Jct 44-11
BSide: Net 0-11, PORT 13-22, Xpt 9-18, Jct 11-28
```

The format of the network logs may vary, depending upon the type of network cards.

The NMC OM group NMSPCHER register is pegged for each occurrence of the NET102 log. PM OM errors are also pegged for the PM reporting the integrity failure.

NET103 log

The NET103 log is generated by the network (NET) subsystem and summarizes the integrity and parity faults in the switch. The summary by network and plane is the total number of faults attributed to all cards on the indicated network.

For example, a single integrity or parity fault involves four different hardware cards, thus, the NET103 log counter will be incremented by four.

This report is generated one hour following a restart, and every hour after then. The counters for integrity and parity faults are reset to zero every day at 0800 or on all restarts.

Following is an example of a NET103 log (hourly summary report).

```
NET103 NOV03 09:03:34 2500 INFO INTEGRITY SUMMARY
Parity & Integrity - Consult the NETINTEG Level for
Details
```

Pair	0	Plane 1	Pair	0	Plane 1	Pair	0	Plane 1
10	0	0	11	140	0	22	–	–
11	0	0	12	–	–	23	–	–
12	124	124	13	–	–	24	–	–
13	10	12	14	–	–	25	–	–
14	0	0	15	–	–	26	–	–
15	8	8	16	–	–	27	–	–
16	0	0	17	–	–	28	–	–
17	0	0	18	–	–	29	–	–
18	64	14	19	–	–	30	–	–
19	0	0	20	–	–	31	–	–
10	0	0	21	–	–			

Causes of integrity failures

Integrity failures can be caused by hardware, CC software, PM software, or manual office activity.

Hardware induced integrity failures

Hardware induced integrity failures may be caused by hardware problems anywhere along the integrity transmit or receive path, in either of the two peripheral modules involved in the call, or in the network or networks, involved in the call.

There are three basic vintages of junctor type networks, and the card codes involved in each are different for an equivalent path. Descriptions of each of these networks are available in the NTP listed as references. The NETINTEG level of the MAP also provides card code and circuit locations of network cards involved in integrity failures. The most common network cards involved in integrity failures, and not detected by other diagnostics, are the network-to-PM interface cards. The most common type of junctor network in the field is the NT5X13 and its repackaged variant the NT7X27. The peripheral interface card for this network type is the NT3X72.

There are four basic PM types that interface directly to the network and can be involved in integrity failures. Card lists for the PM are not currently output in the NETINTEG MAP level integrity card list. Following is a description of those PMs and the circuit cards that support integrity and parity functions:

1. Trunk Modules (TM) — variants are TM8, TM4, TM8A, ATM, STM, MTM.

2. Digital Carrier Modules (DCM) — variants are DCM, DES.

3. Line Modules (LM) — the only North American variant is the LM.

4. Line Trunk Controller (LTC) — variants are LTC, LGC, and DTC.

CSM TM cards

-   NT2X45 — Network Interface Card. The Interface Card provides two, 2-way interfaces between the two transmission paths from each network plane and the TM. It contains message registers, bit and channel timing, parity checking, and data reformatting circuitry.

-   NT2X53 — Control Card. The Control Card contains three controllers that handle trunk, network, and integrity messages. It communicates with the Processor and Memory card via data and address buses and provides enable signals to the 30 individual trunk interface circuits.

-   NT0X70 — Processor Card. The Processor and Memory Card contains a microprocessor driven by read-only-memory (ROM) firmware and two random-access-memory (RAM); one for program storage and the other for operational use. The latter contains connection information concerning PCM channel-to-trunk assignments. This card also performs clock generation, parity checking, and synchronization.

-   NT4X65 — On the cost-reduced TM, the three cards listed above are combined on a single card, the NT4X65.

CSM DCM cards

-   NT2X36 — Network Interface Card. This card contains eight bi-phase modulators and demodulators, assigned to four ports in each of two planes. A per channel looparound circuit loops the eight speech bits back towards the network for test purposes. Parity generation for signals transmitted to the network is also provided.

-   NT2X34 — Supervision Card. This card contains a hardwired sequencer for transmitting and receiving channel supervision messages to and from the network, as well as parity detection circuits for checking incoming speech signals. All circuits are shared over 120 channels. The card also contains a processor bus interface with interrupt capability.

-   NT2X33 — Control Card. This card contains ROM-controlled message handling circuits that interface with the CC. The circuits include a message buffer, reset message detection code firmware and a sanity timer responsible for DCM sanity. The card also contains a phase-locked loop that extracts a 10.24 MHz clock from the network speech data.

CSM LM cards

-   NT2X36 — Network Interface Card. This card contains eight bi-phase modulators and demodulators, assigned per channel looparound circuit, loops the eight

speech bits back towards the network for maintenance purposes. It also generates parity check bits for signals on the transmit path to the network.

- NT2X23 — Receive Multiplexer (MUX) Card. This card contains the receive multiplexer circuit that performs the connections between four network receive buses and 20 terminal receive buses. A separate bus provides a looparound path to the transmit MUX.

- NT2X22 — Connection Memory and Transmit MUX Card. This card contains the RAM for the connection memory and the transmit multiplexer circuit that performs the connections between 20 terminal transmit buses and four network transmit buses. A separate bus provides a looparound path to the receive MUX.

- NT2X34 — Peripheral Processor (PP) Message Processor Card. This card provides integrity checking and channel supervision messages for each PCM channel connection to the LM from the Network, under control of the Master Processor.

- NT2X33 — CC Message Processor Card. This card controls the handling and routing of CC (channel 00) messages to and from the CC in the DMS-100 Digital Processor Control. It also contains the LM clock pulse generator.

CSM LTC cards
The cards that would most likely be involved in integrity failures in the LTC or its variants are:

- NT6X40AA or NT6X40AB — PM-to-Network DS30 Interface Card. There are four NT6X40AA cards, or two NT6X40AB cards per LTC. The PM interface cards to network plane 0 are located on LTC unit 0, and the plane 1 interface cards are located on LTC unit 1.

NOTE: There are 16 ports per NT6X40AB card. In the case of the NT6X40AA, the ports alternate between the two cards as follows:

	CARD 0	CARD 1
	0,1	2,3
Ports	4,5	6,7
	8,9	10,11
	12,13	14,15
	(Card Slot 22)	(Card Slot 23)

- NT6X41 — Formatter Card. The 6X41 formatter card is situated between the NT6X40 I/F DS30 card and the NT6X42 CSM card. It consists of two main sections, the formatting section and the clock section. The clock section generates the 10.24 MHz shelf clock and a number of other signals used by various parts of the shelf.

    The formatting section of the card handles 16 DS30 ports in both directions; the main features are:

        a. Parallel to serial (P/S) conversion of the transmit pulse code modulation

(XPCM) data.

    b.   Serial to parallel (S/P) conversion of the receive pulse code modulation (RPCM) data.

    c.   Network plane selection.

    d.   CSM looparound.

    e.   Network looparound.

    f.   Parity error generation.

    g.   Raw T1 clock generation.

- NT6X42 — CSM Card. The NT6X42 CSM card performs all the required functions for CSM messaging between peripherals. It can accommodate 16 network ports or 512 channels. On the network side of the card, it interfaces to the NT6X41 Formatter card. On the PM side, it originates the 8-bit parallel RPCM speech bus and terminates the XPCM speech bus.

The main functions of the CSM card are:

    a.   Extraction of the CSM bit from 512 network channels.

    b.   Assembly of received channel data byte (CDB) for all channels.

    c.   Parity checking on all bytes.

    d.   Integrity checking.

    e.   Insertion of transmit synchronization pattern and CSM into PCM path.

    f.   Parity generation.

The oscillator on this board is phased-locked by PM resident software to a clock signal derived from the DS30 signal incoming from the network links.

Problems with either the oscillator or the phase-lock-loop software can result in integrity failures, and in extreme circumstances, PM messaging failures as well.

Other network cards

Some additional network cards are listed here because these cards are not part of the card list generated at the NETINTEG level of the MAP. These cards are common to multiple paths, and in practice, are not *high runners* in terms of contributing to office integrity failures.

- NT3X73 — Serial to Parallel formatter
- NT3X86 — Parallel to Serial formatter
- NT3X74 — Network C-side Processor

NT5X13 Network Junctor port assignments

The junctors in the NT5X13 Network Module have been distributed over the NT3X72AB Junctor Interface Cards to give more balanced loading and to minimize the blocking.

The junctor ports are distributed as follows:

NT5X13 Junctor Ports

Slot	Card	Junctors			
8	0	0,1	16,17	32,33	48,49
7	1	2,3	18,19	34,35	50,51
6	2	4,5	20,21	36,37	52,53
5	3	6,7	22,23	38,39	54,55
4	4	8,9	24,25	40,41	56,57
3	5	10,11	26,27	42,43	58,59
2	6	12,13	28,29	44,45	60,61
1	7	14,15	30,31	46,47	62,63

CMC fault

A fault in the NT40 Central Message Controller (CMC) that prevents the DUPLEX message transmission mechanism from functioning could result in integrity failures. This mechanism is checked frequently by a background CMC audit and should be readily identifiable by CMC diagnostics. Duplex messages are currently used exclusively during network connection setup, so that the CC only needs to dispatch a single network connection message. CMC hardware then takes over to send the connection message to both network planes to set up the identical path in both planes of the network. Loss of one of these messages would result in no connection set up in the affected network plane.

Software induced integrity failures

CC Integrity failures

CC software problems can induce integrity failures if correct protocols are not followed. The result can be either of two integrity logs. A few possible scenarios are described below, but they are not the only possible ones.

- A call is set up between callers A and B. A call transfer from A to C is attempted. When caller C is connected to caller A, the network connection from caller A to caller B is broken. The normal sequence would be to tell callers A and B to stop looking for integrity. The connection between A and C would be set up. A and C would be given their new integrity values to transmit, and then both would be requested to start looking for integrity. If caller B was not told to stop looking for integrity, it would report an integrity failure when the A to C connection was set up.

- A call is set up between callers A and B. During a call setup between C and D, part of the network path between A and B is reassigned for use by C and D. When the C to D network connection is set up, A and B will experience integrity failures on both network planes, and the A to B call will be taken down.

- As part of the network junctor or link diagnostics, connections are set up and test code transmitted over the network path. During the development on one BCS, a software problem was introduced that occasionally resulted in part of an active network path being overwritten during a junctor diagnostic. The result was a network integrity failure on one plane only, and a NET102 log being generated indicating a connection memory problem.

- Messages to a PM that are lost during call setup or take-down could result in integrity failures. Since the commands to transmit a particular integrity value, or start looking for integrity, are generally bundled with other call setup functions, a lost message would probably result in other aspects of the call setup failing as well. However, the main symptom in the logs might be an integrity failure accompanied with a LINE or TRK log indicating INTEGRITY LOST.

- Integrity failures are not necessarily reported on the call that originally set up the network path and integrity parameters. Suppose a call between A and B is set up and then, at the termination of the call, B is not requested to stop looking for integrity. When the network connections are freed in the CC software maps, the actual network hardware connection is not released. The previous connection is still set up in the network hardware, so the CSM from the previous call is still intact. Depending upon office traffic, it may be some time until either one of the network path ends, or some other part of the previous network path, is reused for another call or for some diagnostic. When a new network connection is established, the CSM from the previous call is disrupted. If neither of the old endpoints are involved in the new call, the result is a NET101 log, since there is no connection to the PM port and channel reporting the integrity failure. If one of the old endpoints is involved in the new call, the result could be a NET102 log.

When the integrity failure is reported, the new connection would be found in the CC software maps, and this report would be treated like a normal, legitimate, integrity failure.

PM integrity failures
PM software problems can induce integrity failures. The result can be either of two integrity logs. A few possible scenarios are described below, but they are not the only possible ones.

- Call processing messages from the CC to a PM are generally in the form of a "primitive" command with data for that primitive. When the PM receives the message, it processes it sequentially from first byte to last during message processing. Certain protocol checking is done on the data in the message to confirm the validity of the message (a range check of the channel to be assigned to a terminal). If an error is detected, the PM reports a command protocol violation (CPV) to the CC. The log generated and actions taken may vary from PM to PM, but in most current cases, the PM suspends further processing of that message since the message validity is now in question. If the remainder of the message is

the part that specifies the integrity byte data to be transmitted during a call setup, an integrity failure would follow.

- A failure mode, which results in NET101 logs, is due to slow mapping of the CSM supervision to one end of a call. Consider a call from caller A to B. When caller A goes on-hook, the PM reports a message to the CC indicating the on-hook condition. The PM also changes the CSM supervision bit to inform caller B that the call terminated and to stop looking for integrity. With this process, the CC is relieved of sending a separate message to caller B to stop integrity search. When the CC receives the "on-hook" message, it frees up the network connections during the call take-down process. With the connection free, it is available for reuse by another call. In some PMs under some traffic conditions, the "on-hook" message to the CC may be sent and processed, and the old network connection refused, before the PM has changed the supervision bit to inform caller B to stop looking for integrity. If another call reuses part of the original network connection, call B detects and reports an integrity failure.

- During a call setup from caller A to B, which may be on separate PMs, the PM is told to transmit a particular integrity value. Depending upon the traffic and messaging loads on the particular PM, there may be delays within the CC, the network, or the PM, or in the processing of these messages. If the delays are long enough, one PM may be looking for integrity before the second PM has started transmitting the new integrity value. This could result in one of two types of integrity logs.

- Depending upon the PM, various background diagnostics and audit tasks are being executed. PM software implementation errors could potentially result in integrity failures due to operation of maintenance facilities at an inappropriate time.

Manual activity integrity failures

When a network is set out-of-service, either manually or by the system, calls that were in progress still continue to be monitored for integrity. Due to the potential number of calls up on a particular network, no attempt is made to message all the PMs involved, or to inform each terminal that the network or link or junctor, is out-of-service. As long as no further actions are done on the out-of-service network, the original calls will experience no problems. All new calls are requested to look for integrity on the remaining in-service network plane.

If further maintenance action is taken on the out-of-service network (i.e., removal of power, removal of circuit packs, or performing an out-of-service diagnostic), then all calls that were in progress at the time the network was set out-of-service may experience integrity failures on this plane. This also includes calls that are still in progress and are being monitored for integrity on this network plane. This could result in a large number of integrity failures being reported to the CC in the space of a few seconds. For this reason, during the periods of relatively high traffic, it is suggested that after setting a network plane out-of-service, a period of at least 30 minutes elapse before any further maintenance activity be performed on that network. This allows for

calls in progress at the time of the out-of-service operation to be completed. The return-to-service (RTS) operation is not included in this restriction because it does not induce integrity failures.

The out-of-service network diagnostic may induce integrity failures because the connection memories are changed as part of the diagnostic. A MAP message warning of this is output at the time such a diagnostic is requested.

Integrity troubleshooting facilities

Diagnostics

For all networks other than the NT0X48 network, there are two types of out-of-service diagnostics. One is completely controlled by CC software and performs a basic overall test of the network. This is invoked from the Net level of the MAP by the TST command when the network to be tested is out-of-service. The second is a firmware driven self-diagnostic which provides a much more comprehensive test of the XPT cards and connection memories.

This test is invoked only from the Net XPts sublevel of the Net level of the MAP, and may take up to one hour to complete, depending upon the network type and office configuration.

There are four basic types of link diagnostics. The diagnostic varies depending upon the PM type, and whether the link is a combined message and speech link or a speech only link. The four types of link diagnostics are described below.

- On message links, a message is sent from the CC and is looped back by the PM to the CC.

- On speech links of the TM, DCM, and LM a looparound connection is set up in the network and a channel (trunk or line) in the PM is requested to transmit a specific integrity value. The PM looks for this integrity value being looped back through the network. The particular channel being tested on the link depends upon the datafill of the PM. C-side channels of certain service circuits and trunks cannot be seized. The MAP response indicates if this test was run on a speech link. The PM must be in-service to run these link diagnostics, but the network link may be in or out-of-service.

- On speech links to an LTC or its variants, a looparound is set up in the PM. The network sends *test code* through the PM looparound and checks for reception of this test code. Channel 16 is used for this diagnostic because this channel is only used for Inter-Peripheral Message Links (IPML) in Common Channel Signaling 7 (CCS7) equipped offices, and the diagnostic is not likely to be blocked due to trunk datafill or trunk states. This test, however, does not fully exercise the complete CSM path.

- At one time, a more comprehensive link diagnostic was added to the LTC to fully exercise the complete CSM path. It is similar to the integrity looparound diagnostic described above for TM, but tests all channels on the link. However, it

requires that the link pair (both planes) be set *manual busy* to run the test. If a link diagnostic is performed and the link pair is out-of-service, this diagnostic automatically runs instead of the test code looparound.

PCM diagnostic enhancements

BCS34 and BCS35 provided improvements in the hardware detection on the C-side interface of the PCM stream for the first level XPMs. A new diagnostic and enhancement to the existing NETDIAG diagnostic will test the complete channel supervision message (CSM).

This is accomplished by providing a network path loopback to the NT6X42 CSM Card in the XPM and performing the following tests:

- integrity and parity checking
- plane selection verification
- channel data byte (CDB) pattern test

For diagnostic failures, the following logs are generated:

- NETM120 for JNET
- ENET311 for ENET

Integrity analysis package

The integrity analysis (NETINTEG) sublevel off the Net level of the MAP provides tools oriented towards integrity troubleshooting. Depending upon the state of a particular office, and the integrity failure mode and its location, integrity logs may or may not immediately show some correlation. The general manual mode of analysis is to review all integrity logs for some period of time and look for some pattern in the network paths and PM involved. Once a pattern is noted, the appropriate network or PM cards involved are determined and changed. More traffic is run and a check is made to see that some improvement is shown. This is a tedious process and open to inconsistency.

To assist this process, the NETINTEG sublevel of the MAP provides the following facilities:

1. A 100-message circular buffer that saves certain information from the network integrity log reports.

2. Failure counts associated with network cards are pegged as a result of integrity failures. As an integrity or parity failure is reported, the count associated with each card found in the log report is incremented. Exceptions to this are found in incrementing counts on NET102 log reports.

3. When the diagnostics identify a HIT condition, then the cards on both the A-side and B-side will have their counts incremented.

4. When the diagnostics identify a MEM fault on one or more XPT cards, the only counts affected are the associated cards. Those XPT cards will have their counts incremented by 25.

5. When the diagnostics identify a fault condition on the junctor, that junctor count on the A-side will be incremented by 25.

6. Failure counters associated against each PM port, to help in the correlation of the PM involved.

7. An integrity analysis audit that monitors all the failure counts is run approximately every 60 seconds. If the XPT card has its threshold set, an in-service trouble (ISTB) condition is set for that network module. If a link or junctor card is set at the threshold, an in-service diagnostic is run on all ports associated with that card. If the test passes, an ISTB condition is set for that network module. If the test fails, that link or junctor is set "System Busy."

Integrity log buffers

When an integrity or parity failure occurs, the failure counters associated with the network cards displayed in NET101 and NET102 logs are pegged.

The network integrity diagnostic associated with NET102 does the following three things:

- Verifies that the connection memory coincides with the software maps.
- Verifies that the PCM is sane when traveling through the network.
- Requests a diagnostic on the network-to-PM link involved.

When no faults are found, the diagnostic is flagged as a HIT.

When the connection memory has a mismatch with the expected software contents, the software is considered to contain the correct value. An attempt is made to alter the faulty connection memory location. If the change to the connection memory is successful, the fault is considered transient and flagged as a HIT (correctable memory fault). If the location cannot be changed, the fault is considered hard and flagged as a fault. In both cases, the XPT card that had the connection memory problem is flagged.

For troubleshooting and analyzing network faults, use the fault data that has been sorted and accumulated in the following NETINTEG buffers:

- SPMS
  — Record of the total integrity faults on a PM basis
  — Record of the faults on a per-link basis for the worst 20 PMs.

- ANALYZE COUNTS
  — Record of the ten cards with the highest count of faults per each card type in the posted NM.

- ANALYZE PM
    — Record of the ten PM ports with the highest fault counts on the posted NM.

- ANALYZE JUNCTORS
    — Record of the ten junctors (both ends) with the highest fault counts on the posted NM.

- DISP LOGBUFF
    — Record of the logs NET101 & NET102 for the posted NM.
    — When qualified with ALL, the entire buffer is displayed (maximum of 100 logs).

- DISP MASTER
    — Record of the total card fault counts for all planes and pairs.

- DISP COUNTS
    — Record of the card fault counts by card for the posted NM.

The NETINTEG program triggers an integrity check when the threshold level is reached in the buffer. When the threshold of either the link, the junctor, or the cross-point is reached, the NM is set ISTB. The existence of an ISTB state is displayed under the subsystem status header Net, and in more detail by the command QTST at the Net level. When counts for the port of a link or junctor reaches the threshold, the port is automatically tested and made system busy if it fails.

Threshold values are changed by the NETINTEG MAP level, non-menu commands UPTH and RETH. The default threshold setting is 250.

A non-menu command RDBUFF off the Net level of the MAP can be used to read up to 48 bytes of a NM memory buffer. This command is recommended for use by maintenance support personnel that are familiar with DMS software.

Fault sectionalization

The following tools are used for identifying and correcting network faults:

- Network fabric (NETFAB)
- Network path (NETPATH)

NETFAB is a resident tool that simulates high volume calling for routine network testing. It performs an *automated* method of integrity and parity checking between the two ends of the simulated network connections. The integrity check traffic simulator (ICTS) feature is a manual method that can be set to test selected paths for pinpointing faulty conditions.

The faulty paths identified using NETFAB or ICTS testing are recorded in the NETINTEG buffers as was previously described. Repeated path faults on a given path test terminate the testing, and the faulty path is recorded in the path fault buffers associated with NETPATH. When NETFAB/ICTS tests identify a faulty path, testing is sustained on the same (faulty) plane (no switch to the other plane) and increments the fault counters in the NETINTEG buffers, thus highlighting the problem with the high count.

Network path (NETPATH) is a resident tool for fault isolation and verification testing in the networks. NETPATH complements the NETINTEG, NETFAB, ICTS trouble-shooting process. The faulty path information stored in NETINTEG log buffer and NETPATH path fault buffer is selected by the NETPATH test process to set up the same path as the fault for troubleshooting.

The NETPATH test pattern inserting and extracting technique is used to isolate the faulty component. After the component is replaced, the test is rerun to verify the fault is corrected.

NETFAB, ICTS, and NETPATH are further described within this subsection.

Network error counters

Various network error counters that are supported by network firmware are useful in the analysis of problems, especially transient or intermittent type problems. The counters that are available for access from the Net level of the MAP with the DISP command are listed below with a brief explanation of the use of each. Relating these counts to specific network problems can require detailed knowledge of network operation and is beyond the scope of this document. In general, these counters all display error conditions and should display zero during normal errorless operation.

C-Side Counter 0X48 Network

WFSND wait for send time-out
WFACK wait for acknowledgment
WSOM wait for start of message time-out
NACK1 single NACKs received
NACK2 double NACKs received
NACKS NACKs sent to CMC
OPCOOR opcode out of range
RMKILL return message killed
BUFFULL buffer full counter
INCDEL incoming message delayed

C-Side Counters 5X13/7X27/8X11 Network

WFSND wait for send time-out
WFACK wait for acknowledgment
WSOM wait for start of message time-out
NACK1 single NACKs received
NACK2 double NACKs received
NACKS NACKs sent to CMC
OPCOOR opcode out of range
RMKILL return message killed
BUFFULL buffer full counter
INCDEL incoming message delayed
RETRY retry counter on writes to connection memory

P-Side Counters

```
WFSND  wait for send time-out
WFACK  wait for acknowledgment
WSOM   wait for send time-out
NACK1  single NACKs received
NACK2  double NACKs received
NACKS  NACKs sent to CMC
MSGIGN messages ignored
BUFERR buffer errors
ERRLOG error log. Data is port and error index. The error is a
       number from 1 to 8 corresponding to one of the
       counters above.
```

Counters explanation

WFSND — Wait for send time-out. The standard DS30 protocol for message transfer between nodes is for the sending node to transmit a "MAY-I-SEND" (MIS) to the receiving node, and then to wait for a period of time—varies with node type—for a "SEND" signal from the receiving node. If the WFSND time-out period expires, the network pegs the WFSND time-out counter for the CMC or P-side link as appropriate.

WFACK — Wait for acknowledgment. After the sending node has transmitted the message to the receiving node, the receiver confirms that the *checksum* calculated over the message bytes matches the checksum byte appended to the message. If the checksum matches, a POSITIVE ACKNOWLEDGEMENT (PACK) is transmitted to the sender. If the checksum does not match, a "NEGATIVE ACKNOWLEDGE-MENT" (NACK) is transmitted to the sender. The sender waits for the WFACK time-out period for either a PACK or a NACK to be sent. If neither is received, the WFACK counter is pegged.

WSOM — Wait for start-of-message time-out. After the receiver detects the MIS from the sender, it transmits a "SEND" signal. If the sender does not start transmitting the message within the WSOM time-out period, the WSOM time-out counter is pegged by the receiver.

NACK1 — Single NACKs received. If a message is received with an incorrect checksum, the receiver replies with a NACK to the sender. The sender pegs this in the NACK1 counter and attempts to send the message a second time.

NACK2 — Double NACKs received. If, on the second attempt to transmit the message, another NACK is received, no further attempt is made to transmit that message, and the NACK2 counter is pegged.

NACKS — NACKs sent. This is a count of the number of times the network was the receiver, detected message checksum problems, and sent NACK signals to the CMC or PM as appropriate.

OPCOOR — Opcode out-of-range. An out-of-range network operation code was encountered during message processing.

RMKILL — Return message killed. A reply message from a network operation that could not be sent to a PM, or a message that could not be sent to the CC via the CMC. This counter is pegged and the message is discarded.

BUFFULL — Buffer full counter. When the CMC attempts to send a message to the network, the network checks that a message buffer is available to store the received message, before it replies with the SEND signal. If all buffers are full, the network delays the SEND to the CMC until a buffer becomes available, but pegs a counter to flag that this delay has occurred. The message time-out periods between the CMC and the network and the PM are set such that a buffer becomes available before the CMC can time-out on a WFSND.

Depending upon the distribution of PM over the networks, as well as traffic and messaging loads, some buffer full pegs are normal. But a consistently high, uneven distribution over networks may indicate fault conditions or incorrect traffic engineering of PM over the networks. There is some effect on CMC messaging throughout when the BUFFULL conditions are encountered, and ideally, this count should always be zero.

MSGIGN — Messages ignored. The only normal check on an incoming message during message reception is on the message length. If a message with a length less than 10 bytes or greater than 64 bytes— as defined by the length byte— is encountered, the network immediately stops further processing of the message, pegs the MSGIGN counter, and proceeds to scan other ports. The PM times-out on a WFACK and reports a trouble to the CC.

A second condition this counter is pegged occurs with the network *sensitivity* flag turned on. The MSGIGN counter is pegged each time a link is closed due to protocol violations.

Network firmware link "Sensitivity" monitor

The network firmware of the NT5X13, NT7X27, and NT8X11 contains additional message link protocol checking that is not normally turned on. This function may be activated by invoking a non-menu Net level MAP command CHKLNK. As PM ports are scanned, or message transactions occur, the firmware checks to see that normal DS30 link protocols are followed. If protocol is violated, special actions are taken. If a message transfer is affected, the CC is informed, and appropriate maintenance action is taken. This may result in network links being set system busy. This firmware maintenance action is part of the normal maintenance functions. An additional check is made on links that are enabled for messaging, but are not currently involved in a message transfer. The normal signal on such a link should be an IDLE code being transmitted from the PM to the network. This additional network check is to ensure that an IDLE code 30 is being received on all enabled network-to-PM links that are not currently involved in a message transfer.

Detection of a non-idle code may indicate PM link problems. Such problems may be of a transient nature and normally would only be detected if they occurred during a message transfer sequence. Thus, in some respect, this check sensitizes the link to potential link problems that could result in sporadic messaging problems.

When such a problem is detected on any enabled port of the network, the *illegal* data seen is stored in a firmware location. Since a single location is used, it is an indication only of the data seen of the last faulty port. The port number in question is not stored, so the data may only be used to indicate the presence of a faulty port on the network. This data location may be initialized to a known good value and monitored for changes by options to the CHKLNK command.

CHKLNK ALL command

The CHKLNK command is intended to be used *only* by support personnel with DMS software knowledge. Use of this command may cause links to go system busy.

An option to the CHKLNK command— which should be used with caution on an in-service switch— allows setting the network link to system busy when such a protocol problem is encountered. The port that had the problem is then quite obvious from the MAP and logs. Once enabled, this option stays enabled until it is disabled by a command, and the network is set busy until manually returned-to-service, or a system restart occurs.

Although primarily useful in tracing messaging problems, this facility may also be useful in clearing integrity failures.

FILTER command

Switched data service requires a very clean network to meet customer data transmission requirements. Another maintenance feature used to clean the network is the FILTER command, which can assist the operating companies in reducing network parity errors — one of the causes of data transmission service complaints.

The FILTER command is a hidden command off the NETINTEG level of the MAP for junctor networks. For ENET, the FILTER command is not hidden but is located off the NETINTEG level of the MAP. It is used to *query* the integrity and parity threshold values or *alter* the parity. This throttling level determines the number of errors (faults) that are required in a ten second interval to invoke corrective activity by the PM (e.g., transfer to the other network plane and initiate diagnostics). Reducing the threshold value increases the trouble identification sensitivity, stimulating the need for trouble repair activity. As the parity error faults are cleared out of the networks and associated equipment, the NET logs should reduce and service improve. It is recommended to continue throttling the parity threshold level until the lowest parity error rate is achieved, possibly one. Guidelines for performing this process can be found in the "BER testing (BERT) guidelines" later within this subsection.

Field experience in the past has proven that changing the integrity value was of no help for improving networks, and in some cases when it was changed, caused unnecessary problems. Therefore, integrity is being set to a fixed value of 12 (previous default value for XPM_INTEGRITY_FILTER parameter). The XPM_INTEGRITY_FILTER parameter in the OFCSTD table was removed in BCS33. The capability to change the integrity value using the FILTER command was also removed in BCS33.

Parity value settings, as described next, will continue to be used for high speed data certification and should be used by operating companies to keep networks clear of problems.

The normal office table default setting for parity errors is 20 errors in 10 seconds, that is satisfactory for voice service. However, data service requirements are much more stringent (the parity threshold value is lowered). Once a satisfactory parity error threshold is reached through using the FILTER command, then that value should be placed in the XPM_PARITY_THRESHOLD parameter of the OFCSTD table.

Nortel Networks suggests that changes to the parity threshold values using the FILTER command or the XPM_PARITY_THRESHOLD parameter be controlled by a Tier II control center or maintenance group.

Integrity troubleshooting execs

Pre-test considerations

Samples of some CI execs that are useful for NT40 network troubleshooting are provided below. Before beginning any extensive network troubleshooting, it is suggested and helpful to perform a manual test of all network controllers, network junctors, and network links. Manual tests of the PMs and XPMs are useful. In general, manual out-of-service tests on a particular piece of hardware provides the most comprehensive test.

Testing network junctors

This exec is entered as TSTJCTR in SFDEV and is executed by command READ TSTJCTR. It tests all network junctors.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
0 -> X
MAPCI NODISP;MTC;NET
% TEST ALL JUNCTORS
REPEAT NUMNM (JCTRS X;0 -> JCT;+
REPEAT 64 (PRINT 'NETWORK' X 'JUNCTOR' JCT;TST 0 JCT; +
TST 1 JCT; JCT+1 -> JCT);X+1 -> X)
PRINT 'JUNCTOR TESTS DONE. CHECK LOGS AND MAP FOR FAULTS'
```

This exec is entered as BRTSJCTR in SFDEV and is executed by command READ BRTSJCTR. It will test (TST), busy (BSY), and return-to-service (RTS) all network junctors. All faulty junctors stay manual (MAN) busy.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
0 -> X
MAPCI NODISP;MTC;NET
% TEST ALL JUNCTORS
```

```
REPEAT NUMNM (JCTRS X;0 -> JCT;+
REPEAT 64 (PRINT 'NETWORK' X 'JUNCTOR' JCT;BSY 0 JCT;+
RTS 0 JCT: BSY 1 JCT;RTS 1 JCT;+
JCT+1 -> JCT);X+1 -> X)
PRINT 'JUNCTOR BSY/RTS DONE. CHECK LOGS AND MAP FOR FAULTS'
```

Testing network links

This exec is entered as TSTLINK in SFDEV and is executed by command READ
TSTLINK. It tests all network links.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
0 -> X
MAPCI NODISP;MTC;NET
% TEST ALL LINKS
REPEAT NUMNM (LINKS X;0 -> LNK;+
REPEAT 64 (PRINT 'NETWORK' X 'LINK' LNK;TST 0 LNK;+
TST1 LNK;LNK+1 -> LNK);X+1 -> X)
PRINT 'LINK TESTS DONE. CHECK LOGS AND MAP FOR FAULTS'
```

Clear (zero) network counters

This exec is entered as CNTCLR in SFDEV and is executed by command READ
CNTCLRP. It initializes pertinent switch data useful in the correlation of network
integrity failures.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
0 -> X
MAPCI NODISP;MTC;NET
% CLEAR NM CSIDE AND PSIDE COUNTERS
REPEAT NUMNM (DISP CLEAR 0 X;DISP CLEAR 1 X;X+1 -> X)
% DISPLAY NETWORK INTEGRITY COUNTERS
INTEG
DISP CLEAR COUNTS ALL
YES
DISP CLEAR INTG
YES
QUIT ALL
```

Display P-side buffer locations

This exec is entered as CHKBUF in SFDEV and is executed by command READ
CHKBUF. It displays various network P-side buffer locations that have been set to
#AA after an out-of-service network diagnostic, and which retain this value. Any non
#AA values are symptomatic of faulty NT3X74 cards in NT5X13 and NT8X11 junc-
tor type networks.

This exec is only meaningful on NT5X13 and NT8X11 junctor type networks or their
variants.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
PRINT 'THIS EXEC IS NOT MEANINGFUL ON NT0X48 NETWORKS'
DATE
0 -> X
#641B1
#671B2
#6B1197B3
MAPCI NODISP;MTC;NET
% DISPLAY PSIDE BUFFERS #641 - #670, #671-#6A0, #6B1-#6E0
REPEAT NUMNM (+
RDBUFF 0 X B1 #30;RDBUFF 0 X B2 #30; RDBUFF 0 X B3 #30;+
RDBUFF 1 X B1 #30;RDBUFF 1 X B2 #30; RDBUFF 1 X B3 #30;+
X+1 -> X)
QUIT ALL
```

Display C-side and P-side counters

This exec is entered as CNTDISPC in SFDEV and is executed by command READ
CNTDISPC. It displays the network C-side and P-side counters for all networks that
are useful in the correlation of network integrity failures. See Exhibit "A" for an
example of EXEC "CNTDISPC" output.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
0 -> X
MAPCI NODISP;MTC;NET
% DISPLAY NM CSIDE AND PSIDE COUNTERS
REPEAT NUMNM (DISP COUNT C 0 X;DISP COUNT P 0 X;+
  DISP COUNT C 1 X;DISP COUNT P 1 X;X+1 -> X)
QUIT ALL
```

Display integrity counts and analyze for patterns

This exec is entered as CNTDISPI in SFDEV and is executed by command READ
CNTDISPI. It displays the network integrity counters for all networks, and is useful
in the correlation of network integrity failures. See Exhibit "B" for an example of
EXEC "CNTDISPI" output.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
MAPCI NODISP;MTC;NET
% DISPLAY NETWORK INTEGRITY COUNTERS
INTEG
0 -> X
REPEAT NUMNM (POST 0 X;PRINT X;DISP COUNTS;+
ANALYZE COUNTS;ANALYZE PM;ANALYZE JCTRS;+X+1 -> X);+
REPEAT NUMNM (POST 1 X;PRINT X;DISP COUNTS;+
ANALYZE COUNTS;ANALYZE PM;ANALYZE JCTRS;X+1 -> X)
QUIT ALL
```

Display NMC, PM, and OFZ active OMs

This exec should be entered as CNTDISPO in SFDEV and may be executed by command READ CNTDISPO. It displays pertinent OM data useful in the correlation of network integrity failures. See Exhibit "C" for an example of EXEC "CNTDISPO" output. For more detailed display of PMs, use OMSHOW PM ACTIVE.

```
% DISPLAY OMS RELATED TO INTEGRITY ANALYSIS
OMSHOW NMC ACTIVE
OMSHOW PMTYP ACTIVE
OMSHOW OFZ ACTIVE
```

Display network clocks

This exec is entered as CLKDISP in SFDEV and is executed by command READ CLKDISP. It displays the CMC clock that is providing the synchronization timing signal to the networks. All networks should be driven by the same CMC clock. See Exhibit "X" for an example of the "CLKDISP" output.

```
TABLE NETWORK
COUNT -> NUMNM
NUMNM/2 -> NUMNM
QUIT
DATE
R0 -> X
MAPCI NODISP;MTC;NET;INTEG
% DISPLAY NETWORK SYNC CLOCK BUFFERS
PRINT '*** NETWORKS PLANE 0 ***'
REPEAT NUMNM (RDBUFF 0 X #64 1;X+1 -> X)
0 -> X
PRINT '*** NETWORKS PLANE 1 ***'
REPEAT NUMNM (RDBUFF 1 X #64 1;X+1 -> X)
QUIT ALL
```

Exhibit A — Example of EXEC "CNTDISPC" Output

In this example, network 0 is an NT0X48, network 1 is an NT5X13, and network 2 is an NT8X11.
Time is: 17:17:42
MAPCI:
MTC:
NET
NM 0-0

```
                              COUNTERS

                        CMC0    CMC1
            WFSND       0000    0000
            WFACK       0000    0000
            WSOM        0000    0000
            NACK1       0000    0000
            NACK2       0000    0000
            NACKS       0000    0000
            OPCOOR      0000    0000
            RMKILL      0000    0000
            BUFFULL     0000
            INCDEL      0000
            NM 0-0      COUNTERS
            1-WFSND     0000
            2-WFACK     0000
            3-WSOM      0000
            4-NACK1     0000
            5-NACK2     0000
            6-NACKS     0000
            7-MSGIGN    0000
            8-BUFERR    0000

            ERRLOG  0000  0000  0000  0000  0000  0000  0000  0000
                    0000  0000  0000  0000  0000  0000  0000  0000

            NM 1-0      COUNTERS

                        CMC0    CMC1
            WFSND       0000    0000
            WFACK       0000    0000
            WSOM        0000    0000
            NACK1       0000    0000
            NACK2       0000    0000
            NACKS       0000    0000
            OPCOOR      0000    0000
            RMKILL      0000    0000
            BUFFULL     0000
            INCDEL      0000
            NM 1-0      COUNTERS
            1-WFSND     0000
            2-WFACK     0000
            3-WSOM      0000
            4-NACK1     0000
            5-NACK2     0000
```

Continued on next page

Exhibit A   —   Example of EXEC "CNTDISPC" Output (continued)

```
                         6-NACKS        0000
                         7-MSGIGN       0000
                         8-BUFERR       0000

                         ERRLOG  0000  0000  0000  0000  0000  0000  0000  0000
                                 0000  0000  0000  0000  0000  0000  0000  0000

                         NM 0-1         COUNTERS

                                        CMC0    CMC1
                         WFSND          0000    0000
                         WFACK          0000    0000
                         WSOM           0000    0000
                         NACK1          0000    0000
                         NACK2          0000    0000
                         NACKS          0000    0000
                         OPCOOR         0000    0000
                         RMKILL         0000    0000
                         BUFFULL        0000
                         INCDEL         0000
                         RETRY  0000  0000  0000  0000  0000  0000  0000  0000
                         NM 0-1         COUNTERS
                         1-WFSND        0001
                         2-WFACK        0000
                         3-WSOM         0002
                         4-NACK1        0000
                         5-NACK2        0000
                         6-NACKS        0000
                         7-MSGIGN       0000
                         8-BUFERR       0000

                         ERRLOG  0000  0403  0401  0403  0000  0000  0000  0000
                                 0000  0000  0000  0000  0000  0000  0000  0000

                         NM 1-1         COUNTERS

                                        CMC0    CMC1
                         WFSND          0000    0000
                         WFACK          0000    0000
                         WSOM           0000    0000
                         NACK1          0000    0000
                         NACK2          0000    0000
                         NACKS          0000    0000
                         OPCOOR         0000    0000
                         RMKILL         0000    0000
                         BUFFULL        0000
                         INCDEL         0000
                         RETRY  0000  0000  0000  0000  0000  0000  0000  0000
                         NM 1-1         COUNTERS
                         1-WFSND        0000
                         2-WFACK        0000
                         3-WSOM         0000
                         4-NACK1        0000
                         5-NACK2        0000
                         6-NACKS        0000
```

Continued on next page

Exhibit A — Example of EXEC "CNTDISPC" Output (continued)

```
                        7-MSGIGN      0000
                        8-BUFERR      0000
                        ERRLOG  0000  0000  0000  0000  0000  0000  0000  0000
                                0000  0000  0000  0000  0000  0000  0000  0000
                        NM 0-2        COUNTERS
                                      CMC0   CMC1
                        WFSND         0000   0000
                        WFACK         0000   0000
                        WSOM          0000   0000
                        NACK1         0000   0000
                        NACK2         0000   0000
                        NACKS         0000   0000
                        OPCOOR        0000   0000
                        RMKILL        0000   0000
                        BUFFULL       0000
                        INCDEL        0000
                        RETRY  0000   0000  0000  0000  0000  0000  0000  0000
                        1-WFSND       0000
                        2-WFACK       0000
                        3-WSOM        0000
                        4-NACK1       0000
                        5-NACK2       0000
                        6-NACKS       0000
                        7-MSGIGN      0000
                        8-BUFERR      0000
                        ERRLOG  0000  0000  0000  0000  0000  0000  0000  0000
                                0000  0000  0000  0000  0000  0000  0000  0000
                        NM 1-2        COUNTERS
                                      CMC0   CMC1
                        WFSND         0000   0000
                        WFACK         0000   0000
                        WSOM          0000   0000
                        NACK1         0000   0000
                        NACK2         0000   0000
                        NACKS         0000   0000
                        OPCOOR        0000   0000
                        RMKILL        0000   0000
                        BUFFULL       0000
                        INCDEL        0000
                        RETRY  0000   0000  0000  0000  0000  0000  0000  0000
                        NM 1-2        COUNTERS
                        1-WFSND       0000
                        2-WFACK       0000
                        3-WSOM        0000
                        4-NACK1       0000
                        5-NACK2       0000
                        6-NACKS       0000
                        7-MSGIGN      0000
                        8-BUFERR      0000
                        ERRLOG  0000  0000  0000  0000  0000  0000  0000  0000
                                0000  0000  0000  0000  0000  0000  0000  0000
```

Exhibit B — Example of EXEC "CNTDISPI" Output

In this example, network 0 is an NT0X48, network 1 is an NT5X13, and network 2 is an NT8X11.

Time is 17:17:42
MAPCI:
MTC:
NET:
INTEG:
OK net selected
0
NM 0-0 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 0-0 Buffer last cleared Mar24 16:31:03
Request failed - all counts zero
NM 0-0 Buffer last cleared Mar24 16:31:03

CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0			0	0			0
9	0			0	0			0
10	0			0	0			0
11	0			0	0			0
CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
12	0			0	0			0
13	0			0	0			0
14	0			0	0			0
15	0			0	0			0

Continued on next page

Exhibit B — Example of EXEC "CNTDISPI" Output (continued)

```
OK net selected
NM 1-0 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 1-0 Buffer last cleared Mar24 16:31:03
Request failed - all counts zero
NM 1-0 Buffer last cleared Mar24 16:31:03
```

CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0			0	0			0
9	0			0	0			0
10	0			0	0			0
11	0			0	0			0
CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
12	0			0	0			0
13	0			0	0			0
14	0			0	0			0
15	0			0	0			0

```
OK net selected
1
NM 0-1 Buffer last cleared Mar24 16:31:03
ILNK 3X72 Shelf 65 pos 20 Count = 1
OLNK 3X72 Shelf 65 pos 20 Count = 1
AJCT 3X72 Shelf 65 pos 4 Count = 1
BJCT 3X72 Shelf 65 pos 8 Count = 1
AIXP 3X70 Shelf 51 pos 4 Count = 1
AOXP 3X70 Shelf 51 pos 4 Count = 1
BIXP 3X70 Shelf 51 pos 9 Count = 1
BOXP 3X70 Shelf 51 pos 8 Count = 1
NM 0-1 Buffer last cleared Mar24 16:31:03
PM - MTM 0 port 0 Count = 2
NM 0-1 Buffer last cleared Mar24 16:31:03
```

CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
0	0	0	0	0	1	1	0	0
1	0	1	1	0	0	0	1	0
2	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	1
4	0			1	0			0
5	0			0	0			0
6	0			0	0			0
7	0			0	0			0

Continued on next page

Exhibit B — Example of EXEC "CNTDISPI" Output (continued)

```
OK net selected
NM 1-1 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 1-1 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 1-1 Buffer last cleared Mar24 16:31:03
```

CARDILNK	AIXP	AOXP	AJCT	BJCT	BIXP	BOXP	OLNK
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0			0	0			0
5	0			0	0			0
6	0			0	0			0
7	0			0	0			0

```
OK net selected
2
NM 0-2 Buffer last cleared Mar24 16:31:03
ILNK 8X12 Shelf 51 pos 17 Count + 1
OLNK 8X12 Shelf 51 pos 17 Count + 1
AJCT 8X12 Shelf 51 pos 1 Count + 1
BJCT 8X12 Shelf 51 pos 1 Count + 1
AXPT 8X13 Shelf 51 pos 12 Count + 1
BXPT 8X13 Shelf 51 pos 5 Count + 1
NM 0-2 Buffer last cleared Mar24 16:31:03
PM - DCM 2 port 2 Count + 2
NM 0-2 Buffer last cleared Mar24 16:31:03
```

CARDILNK	AXPT	AJCT	BJCT	BXPT	OLNK
0	1	1	1	1	1	1
1	0	0	0	0	0	0
2	0		0	0		0
3	0		0	0		0

```
OK net selected
NM 1-2 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 1-2 Buffer last cleared Mar24 16:31:03
Request failed - All counts zero
NM 1-2 Buffer last cleared Mar24 16:31:03
```

CARDILNK	AXPT	AJCT	BJCT	BXPT	OLNK
0	0	0	0	0	0	0
1	0	0	0	0	0	0
2	0		0	0		0
3	0		00			0

Exhibit C — Example of EXEC "CNTDISPO" Output

```
Time is 17:17:42
CI:

NMC

CLASS: ACTIVE
START:1996/01/01 00:01:00 MON; STOP: 1996/01/01 12:18:02 MON;
SLOWSAMPLES:   10 ; FASTSAMPLES    107 ;


              NMMSGER     NMSPCHER    NMCERR      NMMSGFL
              NMSPCHFL    NMCFLT      NMSBU       NMMBU
              NMPTSBU     NMPTMBU     NMJRSBU     NMJRMBU
  0           0           0           0           0
              0           0           0           0
              30          0           0           3120

DCM

CLASS: ACTIVE
START:1996/01/01 17:00:00 MON; STOP: 1996/01/01 17:18:03 MON;
SLOWSAMPLES    10 ; FASTSAMPLES     107 ;


              DCMERR      DCMFLT      DCMSBU      DCMMBU
              DCMCCTDG    DCMCCTFL    DCMMBP      DCMSBP
              DCMMBTCO    DCMSBTCO    DCMCCTOP
  0           3           0           0           0
              0           0           0           0
              0           0           0

TM

CLASS: ACTIVE
START:1996/01/10 17:00:00 MON; STOP: 1996/01/01 17:18:04 MON;
SLOWSAMPLES:   10 ; FASTSAMPLES     107 ;

              TMERR       TMFLT       TMSBU       TMMBU
              TMCCTDG     TMCCTFL     TMMBP       TMSBP
              TMMBTCO     TMSBTCO     TMCCTOP
  0           0           0           0           0
              0           0           0           0
              0           0           0

LM

CLASS: ACTIVESAT
START:1996/10/10 17:00:00 MON; STOP: 1996/01/01 17:18:05 MON;
SLOWSAMPLES:   10 ; FASTSAMPLES     107 ;

              LMERR       LMFLT       LMSBU       LMMBU
              LMCCTDG     LMCCTFL     LMMBP       LMSBP
              LMMBTCO     LMSBTCO     LMCCTOP
  0           0           0           20          0
              0           0           0           0
              0           0           0
```

Continued on next page

Exhibit C — Example of EXEC "CNTDISPO" Output (continued)

```
   PM2

CLASS: ACTIVE
START:1996/01/01 17:00:00 MON; STOP: 1996/01/01 17:18:06 MON;
SLOWSAMPLES:    10 ; FASTSAMPLES    107 ;

   KEY (PM2 - OMTYPE)
INFO (PM2 - OMINFO)

                    PM2ERR       PM2FLT       PM2INITS     PM2LOAD
                    PM2USBU      PM2UMBU      PM2MSBU      PM2MMBU
                    PM2CXFR      PM2ECXFR     PM2CCTSB     PM2CCTMB
                    PM2CCTFL     PM2CCTER

      0 LCMOM
      4             3            0            0            0
                    0            0            0            0
                    0            0            0            0
                    0            0

      1LGCOM        0            0            0            0
                    0            0            0            0
                    2            0            0
                    0            0

      2 LTCOM
                    2            0            0            0
                    0            0            0            0
                    0            0            0            0
                    0            0

      3 DTCOM
                    1            0            0            0
                    0            0            0            0
                    0            0
   OFZ

CLASS: ACTIVE
START:1996/01/01 17:00:00 MON; STOP: 1996/01/01 17:18:09 MON;
SLOWSAMPLES:    10 ; FASTSAMPLES    107 ;

                    INANN        INLKT        INOUT        INOUT2
                    INTONE       NIN          NIN2         OUTNWAT
                    OUTNWAT2     OUTMFL       OUTRMFL      OUTOSF
                    OUTROSF      INABNM       INABNC       ORIGANN
                    ORIGLKT      ORIGOUT      ORIGOUT2     ORIGTRM
                    ORIGTRM2     ORIGTONE     NORIG        NORIG 2
                    INTRM        INTRM2       TRMNWAT      TRMN
                    TRMMFL       TRMBLK       LNMBPC       ORIGABDN
      0             0            0            763          0
                    0            763          0            796
                    0            33           16           0
                    0            0            0            6
                    0            0            0            0
                    0            0            6            0
                    0            0            0            0
                    0            0            0            0
```

Exhibit D — Example of EXEC "CLKDISP" Output

```
DATE IS FRI. 01/JAN/1999 08:45:00
* * * NETWORKS PLANE 0 * * *
ADDRESS: 0064-DATA: 00C1
ADDRESS: 0064-DATA: 00C1
ADDRESS: 0064-DATA: 00C1
* * * NETWORKS PLANE 1 * * *
ADDRESS: 0064-DATA: 00C1
```

BER testing (BERT) guidelines

Purpose

The purpose of the following information is to provide assistance and guidance in setting up and performing BERT testing for networks, lines, and trunks.

> **CAUTION:**
> The following procedural guidelines *are not* to replace any existing procedures in other documents. They should only be used for reference and guidance when using procedures within other Nortel Networks documents.

References

The following documents should be referenced for procedures and use of commands when performing BERT, BERP, XBERT, ICTS, NETFAB, or NETPATH testing:

- SAM 6584, *High Speed Data Certification*
- IM926, *NETIBERT Bit Error Rate Performance*
- IM926, Section 0008, *BERP/XBERT User Guide*
- IM926, Section 0017, *ICTS/NETPATH User Guide*
- IM926, Section 0019, *Network Troubleshooting Manual*
- NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing*
- NTP 297-1001-591, *DMS-100F Network Maintenance Guide*
- NTP 297-1001-822, *DMS-100F Commands Reference Manual*

Preliminary recommendations

The following recommendations can help prepare the technician for performing BERT testing and resolving problems:

- Attend Nortel Networks course 0481, *DMS-100F Low Bit Error Rate Maintenance*

- Attend Nortel Networks course 0442, *DMS-100F Network Advanced Hardware Maintenance*

- For ENET, attend Nortel Networks course 0449, *DMS SuperNode ENET Maintenance*

- Utilize the subsection that describes network maintenance tools and describes integrity and parity.

- Review the "Digital Switch Bit Error Rate Criteria" within this subsection, which reviews the criteria for establishing BER performance (BERP) requirements and confidence levels that determine successful testing.

- Review the previously listed references.

- For offices with ENET, review the "ENET Overview and Maintenance" subsection within the *System Products* section of this manual—and review the supporting ENET maintenance NTPs.

BERT preparation

The following are suggestions for preparing for BERT testing:

1. Monitor office logs and determine how the office is performing (see IM925, Section 483, for ideas to determine performance).

2. Determine what level the office network is performing at. Do this by looking at the XPM_PARITY_THRESHOLD parameter value in table OFCSTD and the number of NET102 logs (ENCP102 for ENET) that are being generated. The XPM_PARITY_THRESHOLD value should be representative of what the whole office is set for. Remember, the FILTER command is used between cold restarts or reloads to lower the parity for individual XPMs, and the default value of the XPM_PARITY_THRESHOLD parameter is loaded in the XPMs after a cold restart or reload—for NA004 NoRestartSWACT/Maintenance SWACT can be used.

3. Set up OMs for assessment results during testing (see IM925, Section 483 for guidance). Route to them to a local printer or disk.

4. Whether the office is under warranty or not, contact your customer support group to determine the latest procedures for handling packs returned from *High Speed Data Grooming* testing. There are set procedures for billing of offices out of warranty and identification of the returned packs from high speed data testing.

5. Ensure extra network packs are available before testing.

6. Verify the existence of software packages NTX881 and NTX885 for local switches and NTX882 for toll switches.

7. Ensure that all reference material has been reviewed and is available for use. The latest NTPs for the current PCL load should be available.

8. Review circuit pack handling and electrostatic discharge procedures.

9. Take an office image prior to changing any of the office translations.

10. For DMS-100 and DMS-100/200 offices, ensure that the office is equipped with the recommended number of IBERT testers. NTI recommends one NT6X99 IBERT Line Card (ILC) per LCM for testing or an office minimum of 24 ILCs. The minimum of 24 ILCs is recommended for testing 24 DS1 channels at a time. Digital Test Unit (DTU) NT4X23 Cards can be used with or in place of the NT6X99 cards where equipped. If the office is equipped with IBERT testers, a list can be obtained by inputting:
   >MAPCI NODISP;MTC;LNS;LTP;POST CARD 6X99AA PRINT

NOTE: use 4X23AA for listing the DTUs

11. If the NT6X99 IBERT Line Card testers have not been assigned, then they should be added to the LNINV table. Select assignments for the IBERT cards from office records or table LNINV availability. The 6X99AA's are double slotted cards, so if you select 0 0 3 0 slot, then 0 0 3 16 slot is also selected. Only slot 0 0 3 0 would datafilled in table LNINV. You should first assign one per LCM if possible, a minimum of 24 per office. If recommended quantity is not available, then assign evenly throughout the office. The following is an example of adding the 6X99AA to table LNINV at the MAPCI level:
   >Table LNINV
   >ADD 0 0 3 0 6X99AA NPDGP HASU N NL Y NIL Y

12. An equal number or greater of software unassigned LENs are needed for use as NO TEST LENs. Assignments are made in table LNINV but an IBERT card is not needed. These assignments allow for looping back at the NT6X54 BIC Card for BERT testing. NO TEST LEN assignments are made opposite from the IBERT assignments, that is, when a 6X99AA is assigned to an even drawer, then the NO TEST LEN is assigned to an odd drawer for the same LCM. An example of assigning a NO TEST LEN is as follows:
   >Table LNINV
   >ADD 0 0 10 0 6X17AC STDLN HASU N NL N NIL Y

   A list of NO TEST LENs can be obtained by using:
   >MAPCI NODISP;MTC;LNS;LTP;POST DF MCARD PRINT

13. For DMS-200 offices, only DTUs can be equipped. DTUs are equipped in MTMs and require datafill for tables CLLI, TRKGRP, TRKSGRP, and TRK-MEM.

14. See the "IBERT resource management" within this subsection, and datafill tables FMRESINV and FMRESUSE, if not already done. An example of adding IBERT to table FMRESINV is as follows:
>ADD IBERT 0 L 0 0 3 0 ALL
(repeat for the same IBERTs added in table LNINV)
For table FMRESUSE, do LIS ALL to check if BERP is in the table.
If not, then add BERP with commands ADD BERP ALL. The other available users are ATT, TTP, and LTP. The available classes are ALL, NONE, and C (C followed by a vector of 0-15).

15. We suggest running all LCMs on active unit 0 for first 800 calls and then SWACT to unit 1 for other 800 calls.

BER testing criteria

The following criteria is for high speed data (HSD) testing in an in-service office:

- LCM call length is set for 10 minutes per unit
- DTC call length is set for 20 minutes per unit
- the minimum number of calls should be 1600 (800 per unit for LCMs)
- Bit Error Rate set for 1×10^{-9}
- no more than 1 call in 70 can be errored
- no call can exceed 3 errored seconds
- no more than 5 NET102 logs per 10,000 network calls
- for trunk testing, no more than 1 errored channel allowed during a 20 minute test covering 24 DS1 channels

BERP testing procedures for lines

1. During BERP testing, all REX tests and NETFAB testing must be disabled. ICTS should not be run unless you are using ICTS for a single network trouble. Disable NETFAB example is as follows:
>TABLE OFCVAR
>POS NETFAB_SCHEDULE_ENABLE
(if not already "N", then change to "N")

To disable REX testing for LCMs within the OFCVAR table:
>POS LCDREX_CONTROL
(if not already "N", then change to "N")

To disable REX testing for the SuperNode and ENET within the OFCVAR table:

>**POS NODREXCONTROL**
(if not already "N", then change to "N")

CC and CMC REX testing for the NT40 cannot be stopped, but their time should be changed outside the time frame for BERP testing. Change the time with the CC_REX_SCHEDULED_HR and CMC_REX_SCHEDULED_HR parameters in the OFCENG table. Changes to any REX related parameters should not be made during REX testing to prevent potential problems.

2. Access the BERP level and input the following information to meet testing criteria. Make sure the start and stop times are outside the REX time for CC and CMC, and that tests are being run during light traffic.

   >**MAPCI;MTC;BERP**
   >**LOOPBK DS30**
   >**SORTKEY ALL**
   >**SELECT ALL** (selects all 6X99AA IBERTs defined in table FMRESINV)
   >**PARMSET BER 9** (criteria for 10-9)
   >**PARMSET SECONDS 3** (3 errored seconds criteria)
   >**DEFINE ADD L X X X X** (define all NO TEST LENS datafilled in LN-INV)
   >**DEFINE ADD LCD 0 0 0** (define all data line cards (DLC) being used)
   >**CALLSET LENGTH 10 MINS** (10 minute call length criteria)
   >**CALLSET DELAY 1 SEC** (delay 1 second between calls)
   >**CALLSET CALLS 800** (calls to be completed for each LCM unit)

   NOTE: The 1600 calls for an LCM—800 per unit—will possibly take several days based upon the number of IBERTs and NO TEST LENS assigned. This is also based upon the limited number of low traffic hours available for testing.

   >**CALLSET ALLCALLS** (all calls to be traced—use ERRORED for tracing only errored calls)
   >**DEFTIME START day hh mm** (define start time for day, hour, and minute)
   >**DEFTIME STOP day hh mm** (define stop time for day, hour, and minute)
   >**REVIEW** (provides review of settings)
   >**CHECK** (performs a consistency and validity check on data entered)

3. Set up the OUTPUT file to direct the output data from the test to a disk or tape. Use DSKUT (Disk Utility) or the OUTPUT command on the BERP level to define a file and disk location. See NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing* for examples of the OUTPUT command.

4. Start the BERP test using the START command off the BERP level. When all LCM unit 0's have been completed, SWACT to LCM unit 1 for the other 800 calls.

5. Use the SUMMARY command to get a display of the last known test results.

6. When testing has been completed for all the LCMs, use the PROCESS command to dump the file that was previously defined using DSKUT or the OUTPUT command on the BERP level. Option to dump the worst card list is possible using the PROCESS command. See NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing* for examples and options that can be used with the PROCESS command.

7. Use the NETPATH, ICTS, NETINTEG, and XBERT tools to clear problems.

8. Ensure that REX testing is restarted, and any previously changed REX start and stop times are reset after BERP testing is completed.

BERP testing procedures for trunks

BERP testing for trunks applies only to trunks with a SIGNALING DATA SELECTOR of STD, STDTL, R1, or R1N5. Groups MTX, RONI, and SS7 trunk groups cannot be tested.

Do not select the DTC 0 0 or DTC 2 2 BITS timing links for BERP testing.

If you have 48 IBERTs, then two spans (links) can be run at the same time.

Ensure trunks selected have more than 24 trunks in a group, or that they route advance. Do not use a final route with only 24 trunks in the group. In general, do not block normal traffic.

1. Halt any automatic trunk testing during the period BERP testing is being performed on trunks.

2. Ensure that the IBERT testers have been assigned using the procedures previously provided in the "BERP testing procedures for lines."

3. Follow the same guidelines for REX and NETFAB testing as was done for BERP for lines.

4. Select the DTC span(s) for testing, access the CARRIER level (MAPCI;MTC;TRKS;CARRIER), post the DTC and busy out the link(s) for testing.

5. BERP tests must be run for each DTC unit; therefore, busy out one of the units (MAPCI;MTC;PM; POST DTC X; BSY UNIT X).

6. After preparing the DTC and links for testing, access the BERP level and perform the following to meet the criteria and setup:
   >MAPCI;MTC;BERP

>**LOOPBK DS1**
>**SELECT ALL** (selects all 6X99AA and 4X23AA IBERTs defined in table
FMRESINV)
>**PARMSET BER 9** (criteria for 1×10^{-9})
>**PARMSET SECONDS 3** (3 errored seconds criteria)
>**CALLSET LENGTH 20 MINS** (20 minute call length criteria)
>**CALLSET DELAY 1 SEC** (delay 1 second between calls)
>**CALLSET CALLS 1** (calls to be completed for each DTC unit)
>**REVIEW** (provides review of settings)

NOTE: This test must be run 34 times if using 24 IBERTs, or 17 times if using 48 IBERTs, to equate to the 800 calls for the DTC unit being tested. Individual 20 minute tests are made to verify the testing criteria of no more than one error for each 20 minute test. The 1600 calls for a DTC—800 per unit—can possibly take several days based upon the number of IBERTs and span assignments in the office. This is also based upon the limited number of low traffic hours available for testing.

7. Set up the OUTPUT file to direct the output data from the test to a disk or tape. Use DSKUT (Disk Utility) or the OUTPUT command on the BERP level to define a file and disk location. See NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing* for examples of the OUTPUT command.

8. Start the BERP test using the START command off the BERP level.

9. Use the SUMMARY command to get a display of the last known test results.

10. When the BERP test has completed the 20 minute test, use the PROCESS command to dump the file that was previously defined using DSKUT or the OUTPUT command on the BERP level. Verify that no more than one error has occurred during the 20 minute test.

11. Troubleshoot the DTC NT6X50 DS1 Interface Card first and use the NET-PATH, ICTS, NETINTEG, and XBERT tools to clear other problems.

12. Ensure that REX testing is restarted and any previously changed REX start and stop times are reset after BERP testing is completed.

NETFAB testing procedures

NETFAB testing is used to groom an office for high speed data and to keep the office groomed on an ongoing basis. It is recommended that NETFAB and ENETFAB testing be run nightly.

1. The objective of NETFAB testing is to lower the *parity* threshold settings for each XPM using the FILTER command. If the office is running at a threshold setting of 20, then the parity value should be lowered 5 points at a time for each XPM — until a value of 1 is reached. At that point, the

XPM_PARITY_THRESHOLD parameter value in table OFCSTD can be set to a value of 1 for the whole office.

2. During NETFAB testing all REX tests should be disabled (see previous procedure "BERP testing procedures for lines"). ICTS should not be run unless you are using ICTS for a single network trouble. To enable and schedule NETFAB, access table OFCVAR:

   >TABLE OFCVAR
   >POS NETFAB_SCHEDULE_TIME (schedule for low traffic and outside other tests)
   >POS NETFAB_SCHEDULE_ENABLE (if not already "Y", then change to "Y")

3. Use the NETPATH, ICTS, NETINTEG, and XBERT tools to clear problems. If a test on a reported NET102 problem passes, then we suggest reversing the path and retesting.

4. After NETFAB has finished, ensure that REX testing is restarted and any previously changed REX start and stop times are reset.

Carrier Maintenance

Carrier facilities

A carrier, by definition, maintains communication on links connecting DMS peripherals to channel banks, DMS peripherals to remote DMS peripherals, or remote-to-remote DMS peripherals.

Three carrier standards are served by the DMS family of switches; the 24-channel (DS1) carriers are used for North American switches and the 30-channel (PCM30) carriers are generally used for international switches. A third type of carrier DS0 (digital signal level 0) card type NT6X55AB (DS0 interface card) is used in North America with Digital Trunk Controllers (DTC).

The DS0 carrier allows a Service Switching Point (SSP) office the capability of Common Channel Signaling 7 (CCS7) link access to a Signaling Transfer Point (STP) node. The DS0 interface also is capable of responding to network-initiated maintenance actions, such as loopbacks.

For maintenance purposes, a DS0 link acts as a DS1 trunk except that it

- only contains a single trunk

- supports 64- and 56-Kbit/s data rates

- responds to remote loopback requests from the network

- does not transmit or detect remote carrier group alarm (RCGA) and alarm indication signal (AIS)

Performance

The transmission performance of the digital line facilities serving the DMS-100F switch directly affects the service experienced by the operating company subscriber. In today's environment with the rapid deployment of high-speed data services, it is essential for customer service that the entire telephone network be as bit error free as possible.

Error free digital transmission facilities are essential since the switch is dependent upon digital facilities for message and data transmission and signaling to other switches. Errors in the digital transmission facilities affect the subscribers as follows:

- lost calls
- wrong numbers
- cutoffs
- noise ("popcorn" clicking, "sawmill buzzing")
- crosstalk
- data errors
- total DS1 loss (potential network blockage)

NOTE: Data transmission is more susceptible to corruption than voice, especially at higher data baud rates.

Digital line facilities are derived from the following:

- trunk cables conditioned for T1 type carrier
- optic fiber cables and related multiplex equipment
- digital radio systems and related multiplex equipment
- microwave systems

Remote digital line facilities

Some types of terminating equipment interconnected by the digital line facilities between the DMS-100 host and the far-end termination, are shown in the following figure.

The remotes supported by the DMS-100F host switch are generally connected via DS1 facilities up to 200 miles—100 miles for the OPM/RLCM—from the central office (CO). Except for the pair-gain remotes that are connected directly to the CO, most remotes support intraswitching and the emergency stand-alone (ESA) mode.

The remote configuration shown in the figure on the next page is not an all inclusive block diagram of all the remote connecting options. Following is a description of the acronyms:

- Subscriber Carrier Module SLC-96 (SMS_SLC-96)
- Remote Concentrating SLC-96 (RCS)
- Subscriber Carrier Module Urban/DMS-1U (SMU_DMS-1U)
- Subscriber Carrier Module Rural/DMS-1R (SMR_DMS-1R)
- Subscriber Carrier Module Access (SMA)
- Fiber Central Office Terminal (FCOT)

- Remote Digital Terminal (RDT)
- Subscriber Module SLC-96 Remote (SMS-R)
- Remote Line Concentrating Module (RLCM)
- Outside Plant Module (OPM)
- Remote Line Module (RLM)
- Small Remote Unit (SRU)
- Remote Switching Center (RSC) (RCC + SMSR = RSC)
- Remote Switching Center - SONET (RSC-S) (RCC2 for RSC-S)
- Remote Switching Center - SONET Extended Distance Capability (RSC-S EDC)
- Remote Switching Center - SONET NI-1 (RSC-S NI-1)

Figure 2-14 — Diagram of DMS-100F facilities and nodes
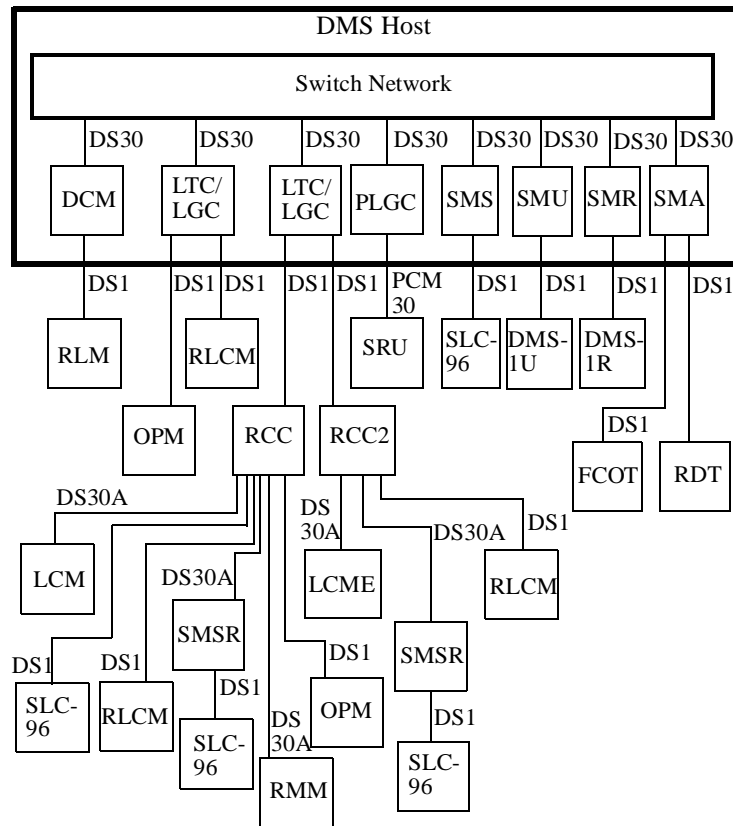
NOTE: The RCC and SMSR or RCC2 and SMSR are Remote Switching Centers (RSCs).

Carrier maintenance

Carrier maintenance can be performed through any manual or mechanized method that can access the facility to be tested. Carrier maintenance features are usually designed within carrier products, and may or may not, require external test equipment to perform testing. This subsection focuses mainly on carrier maintenance performed from the DMS-100F switch.

CARRIER level

The CARRIER level of the MAP is used to access carriers, check alarm status of active span lines, and perform maintenance on carriers. To access individual trunks of a carrier, the TTP level must be used. The CARRIER level is accessed by typing in MAPCI;MTC;TRKS;CARRIER. When the CARRIER level is accessed, an automatic check is made to ensure that the state of every carrier is known to the system. There are three sublevels off the CARRIER level that have to be accessed before anything is posted: POST, DISPLAY, or CARPAC. When the CARRIER level or its three sublevels appear on the MAP, a carrier status display appears.

CARPAC level

The carrier pretest and cutover (CARPAC) level off the CARRIER level of the MAP is used to test a digital carrier and then cut it into service. CARPAC is used for international 30-channel carriers and 24-channel domestic carriers.

CARRIER status display

There are four classes of carrier displayed with the status display (see Figure 2-15 on page 2-264 for an example of a CARRIER level MAP display). They are displayed under the CLASS header as follows:

- TIMING (those functioning as timing links)
- TRUNKS (those serving trunks)
- REMOTE (those linking remote PMs)
- PROTL (those serving protection lines)

Also displayed with the carriers are various status indicators that have the following meaning:

- ML (maintenance-limit count for slips and loss-of-framing has been exceeded)
- OS (out-of-service limit has been exceeded for slips and loss-of-frame count)
- ALARM (the quantity of carriers that are causing alarms)
- SYSB (the quantity of carriers that are system busy)
- MANB (the quantity of carriers that are manually busy)
- UNEQ (the quantity of unequipped carriers)
- OFFL (the quantity of off-line carriers)
- CBSY (the quantity of C-side busy carriers)

- PSBY (the quantity of P-side busy carriers)
- INSV (the quantity of carriers in service)

Figure 2-15 — CARRIER Level MAP display showing CARD alarm

```
     CM     MS      IOD     Net      PM     CCS      Lns     Trks     Ext    APPL

      .      .      .       .       .      .       .       .       .      .

     POST      CLASS     ML OS     Alarm  SysB  ManB  Uneq  Offl CBsy PBsy InSv
 0   Quit_     TRUNKS     9  0       50    42     2     0     0    4     0   31
 2   Post_     REMOTE     4  0       10     6     0     0     0    0    27    4
 3             TIMING     0  0        0     0     0     0     0    0     0    2
 4               DS1
 5   Loop_     N CLASS SITE SMU CK D ALRM SLIP FRME BER   ES SES STATE PROT
 6   Tst_      0 REMOTE HOST 0  0  C          0    0 <-7. 110 0  INSV
 7   Bsy_      1 REMOTE HOST 0  2  C          0    0 <-7.   2 0  SYSB-T
 8   RTS_      2 REMOTE HOST 0  3  C          0    0 <-7.   0 0  PBSY
 9   Offl_     3 REMOTE HOST 0  4  C CARD    0    0 -6.3   0 0  SYSB-T
10  DispOpt_
11  Disp_     SIZE OF POSTED SET  :   4
12  Next      POST:
13
14  Detail_
15
16
17
18

      userid
   TIME hh:mm>
```

CARRIER level commands

Other than the commonly used commands—QUIT, POST, TST, BSY, RTS, OFFL, and NEXT—a brief description of some CARRIER commands are as follows:

LOOP — The LOOP command and its parameters establish or cancel a loop between a carrier of the posted set and the DS1 interface card. Parameters with the LOOP command allow for the loop to be toward the near-end or far-end of the carrier.

Looping the carrier allows for bit error rate tests (BERT) to be run on the carrier. The carrier must be manually busied before the loop can be made. Alarms are also displayed at the CARRIER and PM levels of the MAP; therefore, the use of the LOOP command should be planned and properly coordinated with both carrier ends.

DETAIL — The DETAIL command off the CARRIER POST level displays more detailed information about a specified carrier and its trunks, including the remote-end of the carrier if specified.

DISP — The DISP (Display) command and its variables—ALARM, CBSY, INSV, MANB, ML, OFFL, OS, PBSY, SYSB, and UNEQ—allow for carriers to be displayed upon specified states.

PROTSW — The PROTSW command—displayed with SMS-100s—controls the protection switching for a Subscriber Module SCM-100 (SMS-100).

FELP — The FELP disables, enables, queries, and provides a PCM test for a DS1 link at the Remote Concentrator SLC-96 (RCS).

CARRIER level references

Various CARRIER level and sublevel commands can be found in NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide* and NTP 297-1001-822, *DMS-100F Commands Reference Manual*. Other supporting information on carriers and bit error rate performance (BERP) testing can be found in NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing.*

CARRMTC table

The Carrier Maintenance Control (CARRMTC) table contains information describing the DS1 links between the DMS-100 and the switching node at the far-end. It defines the line coding and frame format used in the DS1 link and provides maintenance control information for the link. out-of-service limits for alarms, and system return-to-service information.

Maintenance performance settings

The DS1 carrier maintenance and out-of-service limits for *slips* and *frame* loss are set using CARRMTC table. Default values are specified as follows:

PARAMETER	MTCE LIMITS	OUT-OF-SERVICE LIMITS	TIME FRAME
SLIPS	4	255	24 hr.
FRAME LOSS	17	511	24 hr.
BPV	10-6	10-3	

NOTES:

1. DS1 systems with bipolar violations greater than $1{\times}10^{-6}$ (MTCE limit) should be investigated and corrected. The out-of-service (OOS) limit is $1{\times}10^{-3}$.

2. The SETACTION command on the CARRIER MAP level is used for establishing action to remove selected DS1 carriers from service should the OOS limit specified for slips or loss-of-framing (LOF) in table CARRMTC be reached. Another method to remove faulty carriers from service is to set the ACTION field to "Y" in table LTCPSINV for any selected carrier system. Removing faulty carrier systems from service helps to maintain top quality voice and data standards on the DS1 links. Its greatest benefit is found on sys-

tems supporting data calls by removing substandard DS1 performing facilities from service. Removing faulty carrier systems also forces action to be taken.

Carrier maintenance recommendations

1. Ensure that the carrier interface pack settings are correct to help minimize slips. See NTP 297-8991-805, *DMS-100F Hardware Description Manual* or if not available, then use the *General Specifications* (GSs) or IM sections.

2. All equipped, but unassigned, DTCs should be looped back at the DSX bay to simulate a working span. The switch will monitor the looped signal for faults.

3. All provisioned, but unassigned, T1 lines must be properly terminated and energized with a 1.544 Mb/s digital signal. This prevents the T1 line from oscillating and spilling interference into other T1 lines working in the same cable sheaths or equipment bay.

4. For a source of information on DS1 maintenance and troubleshooting, see NTP 297-2401-502, *DMS-100F ISDN Primary Rate Interface Maintenance Guide.*

Carrier faults

The DMS-100 switch monitors T1 carriers for two fault detection parameters—*loss-of-signal* (LOS) and *loss-of-frame* (LOF). LOS occurs when the hardware detects 175 +/- zeroes in the incoming signal. This condition terminates as soon as a valid signal framing is detected. LOF is declared when an *out-of-frame* (OOF) situation lasts 2.5 seconds.

The DMS-100 switch monitors T1 carriers for two performance parameters—bit error ratio (BER) and *out-of-frame* (OOF) data. BER determines the fraction of bits not received correctly during a certain time. Only bipolar violation (BPV) is used to approximate BER. OOF represents the number of frame bit errors that have occurred on the T1 carrier.

The DMS-100 switch monitors T1 carriers for three service quality parameters— errored seconds (ES), severe errored seconds (SES), and unavailable seconds (UAS). ES is the number of seconds during which a BPV or OOF condition occurred. SES is the number of seconds during which a standard BER was experienced. UAS is the number of unavailable seconds. After 10 consecutive SESs, the service is considered to be unavailable.

To support maintenance function on the DS1 facility, Extended Superframe Format (ESF) incorporates a block error detection scheme (CRC-6), and a data link. Errors on the DS1 can be detected by:

*   cyclic redundancy check (CRC)

*   bad framing pattern or loss of framing

*   non-B8ZS bipolar violations (BPV)

*   controlled slips (if customer interface is in a synchronized network)

*   replication or deletion of a frame

Carrier transmission criteria

Digital transmission performance at the DS1 rate (1.544 Mbps) is measured for errors by the host DMS-100F, using the following three parameters:

Bit error ratio criteria

Bit Error Ratio (BER) is the ratio of the number of digital errors received in a specified time period to the total number of bits received in the same time period. BER may be measured directly by generating a known signal and detecting errors in that signal, or it may be approximated, based on a count of code violations or framing bit errors. For supporting information on BER for the switch, see the "Network Maintenance" subsection within the *Preventive Maintenance* tab.

Normal, error free, bipolar transmission pulses always alternate ones and zeroes. Any irregularities in the T1 transmission are counted as bipolar violations (BPV). Acceptable BER for DS1 transmission is 1×10^{-7} (one BPV in 10 million bits). A BPV occurs when two consecutive nonzero signal elements of the same polarity occur in a bipolar signal. DS1 systems with bipolar violations greater than 1×10^{-6} should be investigated and corrected (MTCE limit). The out-of-service (OOS) limit is 1×10^{-3}.

The two types of signaling that BPVs can occur in are:

- alternate mark inversion (AMI)—a signal conveying binary digits, in which successive *marks* are normally of alternative polarity buy equal in amplitude, and in which *space* is of zero amplitude (bipolar signal)

- bipolar eight zeros (8-bits) substitution (B8ZS)—a transmission coding technique that substitutes a specific bipolar violation pattern in place of eight consecutive zeroes so that a link will not go down

AMI is the most commonly deployed T1 signal format, although B8ZS is being used for clear-channel applications.

Slip criteria

Slip occurs when there is a change in the relative bit rates between two connected digital facilities (i.e., DS30 and DS1). Buffers are used to handle short term variations. However, if the changes are great enough, the buffer either overflows, or is empty when the next frame is to be transmitted. If overflow occurs, a buffered frame must be thrown away to make room for the next frame. If the buffer is empty, the last frame transmitted must be repeated to allow time for a new frame to arrive in the buffer. In either case, the result is impulse noise on voice connections, or errors in data transmission.

Slips are measured in events at the host DMS-100F switch. Slips indicate transmission delay variations and clock rate differences (jitter) between the host switch and the far-end termination. An acceptable slippage rate for DS1 transmission is <4 in 24 hours.

NOTE: DMS-100F technology uses a "Controlled SLIP" process that minimizes the detrimental effects. To control slip, elastic buffering is used to take care of bit-rate variations between the external DS1 and internal DS30. In this context "slippage" is simply defined as the exhaustion of the elastic buffer located on the NT6X50 DS1 Interface Card.

Loss-of-framing criteria

Loss-of-frame (LOF) is measured and reported as CARRIER LOF in events at the host DMS-100F switch. The frame pulses are monitored by the DMS-100F and must fall within certain timing parameters (so that the individual time slots within the frame can be precisely identified). An *out-of-frame* (OOF) parameter counts the frame bit errors. A *loss-of-frame* condition occurs when an *out-of-frame* situation persists for a predetermined length of time. Any *loss-of-framing* for more than 2.5 seconds causes an alarm and log message to be generated. Framing pulses must be detected for at least 10 seconds—the recommended datafill in table CARRMTC—before a carrier system can be restored.

Acceptable *loss-of-framing* is <17 in 24 hours—the recommended datafill in table CARRMTC. *Loss-of-frame* can be caused by such problems as massive slips, power, facility, lightning, and work activity on carriers.

> **CAUTION**
> Some types of digital multiplex equipment place a healing signal to maintain continuity and stability on the DS1 line while in trouble. When measuring bit error seconds, ensure the true signal is being evaluated.

Carrier alarms

Carrier alarms are characterized by steady-state and hit-state properties:

- an alarm reaches its steady state if the switch records a continuous occurrence of signals that do not meet the appropriate specification (for example, local carrier group alarm (LCGA) or remote carrier group alarm (RCGA))

- an alarm reaches its hit state if the switch records isolated or intermittent occurrence of signals that do not meet the appropriate specification (for example, *loss-of-frame* and slip alarms)

Local carrier group alarm (LCGA), remote carrier group alarm (RCGA), and alarm indication signal (AIS), are DS1 carrier alarms. When frame loss reaches its steady-state, a local carrier group alarm (LCGA) is activated. The DMS-100 switch places a carrier OOS when an LCGA is raised and returns the carrier to service when the alarm is cleared and the frame is regained. Operating company personnel can place a limit on the number of times a carrier is RTS. This limitation prevents a carrier from bouncing between system busy (SysB) and in-service (InSv) states indefinitely. The

default for the consecutive number of times the system may return the carrier to service is 255.

A carrier remains temporarily SysB until the carrier is successfully returned to service by either of the following:

- manual action—the tests of the RTS sequence pass—indicating that no faults persist in the carrier.

- system action—when the carrier audit finds no alarms persist in the carrier.

A carrier that is permanently SysB must be manually returned to service. DS1 maintenance signaling is done in-band in the superframe (SF) format, or in the data link of the extended superframe (ESF) format. Both support the following signals:

- Remote alarm indicator (RAI)—is the yellow alarm sent to the remote-end, indicating a loss of incoming data from the remote-end. The signal has a minimum duration of 1 s, and lasts for the duration of the outage. For SF, the RAI signal sets bit two to zero (0). For ESF the RAI signal consists of alternating hexadecimal digits FF and 00

- Alarm indication signal (AIS)—is the blue alarm indicating the loss of an originating signal or other service disruption. The signal is a continuous unframed binary one (1) digit. AIS can also indicate a loss of network synchronization

Carrier trouble conditions and possible causes

Identifying DS1 carrier problems

Methods of identifying DS1 carrier problems using the DMS-100F surveillance features are as follows:

- monitoring carrier level generated alarms and associated PM109 logs

- log message PM110 is generated when the maintenance limit or out-of-service limit is reached for slips or LOF as specified in table CARRMTC

- posting the MAP CARRIER level will display the status of carriers and provide information on BER, slips, and LOF counts. The counts are cumulative from the last reset, except when maintenance limits have been exceeded, then the counts are unavailable

- review OMs derived from the DS1CARR OM group and related registers collected in a dedicated accumulating class—such as is described within the "Operational Measurements (OMs)" subsection located in the *Preventive Maintenance* tab. Review this printout daily to identify problem carrier systems and initiate corrective action

- the OM thresholding feature can be used for alerting the maintenance personnel of carrier system problems. Add the DS1CARR OM group registers associated with the suspected carrier system to table OMTHRESH. A threshold of one, a scan time of one, and setting the alarm ON can generate a real-time alarm and

log with the first trouble event. When the trouble is cleared, remove that system from the OMTHRESH table and replace with another carrier system that has a problem

Possible causes of BER logs and alarms

DS1 bipolar violations that cause the bit error ratio (BER) to be exceeded usually result from span line cable faults, line repeaters, or multiplex faults such as:

- T1 type repeater in the span line or office repeater
- NT6X50 DS1 Interface Card in the DTC
- far-end D-type channel bank common board equipment
- noise or crosstalk within the cable sheath causing spurious pulses to be generated or pulses to be deleted by the regenerative line repeater
- poor connection in the outside plant cable when splicing two different gauge conductors using crimp connectors
- unterminated spare T1 type span lines generate high-level signals that spill over into adjacent working span lines

Possible causes for slips

Slips are commonly caused by incorrect compensation for distance between the office repeaters and the digital switch terminations or carrier terminals. Following are examples:

- DMS-100F NT6X50, NT2X35 & NT3X48 cards S1 and S2 build-out settings
- Granger transmux build-out settings
- D-type channel bank build-out settings (far-end)
- D-type channel banks must be set for the synchronous (loop clock) mode. Verify loop clock mode is functioning. Loop clock function is an absolute necessity
- Oscillating line repeater (T1 type)—due to tuned circuit drift—allowing the repeater to jump off frequency
- D4-type bank—missing or defective Office Interface Unit (OIU)

NOTE: Compensating settings for the various DS1 cards can be found in
NTP 297-8991-805, *Hardware Reference Manual.*

Possible causes of framing errors

Framing errors can be caused by *massive slippage* triggered by the same faults for slips described above, as well as:

- transmit and receive cable pair open on one side at any point
- AC current superimposed on the DC power feeding the line T1 type repeater

---

- maintenance activity on an in-service carrier

The AC current adds and subtracts from the available repeater power. If the line current drops below the repeater cutoff point, the repeater power is lost causing framing errors or loss of signal.

- high AC ripple current
    — poor cable sheath bonding

    — cable path routed near high-tension power lines

    — unbalanced cable pairs

    — unbalanced power feed (130 volt supply within 1%)

NOTE: AC current ripple has been found to be the primary cause of intermittent and no trouble found (NTF) T1 type span faults.

DS1 interference from T1 fault locate facilities

Faulty T1 trouble locate circuitry, associated with T1 type span lines, can cause DS1 transmission impairment that affects service. For example, an open in the fault locate pair, a missing or improperly wired filter can cause severe ripple in the digital signal resulting in bipolar violations or slips.

Since the trouble locate circuitry is in the T1 transmission stream, the importance of a correctly installed and maintained fault locate circuitry cannot be over emphasized.

Poorly performing T1 span lines should be checked for faulty trouble locate circuitry by the carrier maintenance personnel.

The switching and carrier managers should review the status of DS1 interference caused by span line fault locate facilities.

NT6X50 DS1 Interface Card loopback

For fault isolation purposes, DS1 loopbacks can be operated from the CARRIER level of the MAP for NT6X50 DS1 Interface Cards. For the NT6X50AB cards it is possible to operate a DS1 loopback towards the far-end (remote loopback). The following are suggestions before applying a loopback:

- remove the service from the DS1 carrier before proceeding with the DS1 loopbacks

- coordinate the carrier testing with the distant office since looping causes alarms

- see NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide* for use of the LOOP command on the CARRIER level of the MAP. Also see NTP 297-1001-533, *DMS-100F Bit Error Rate Performance Testing*, and "Carrier Level Tests" for other loopback testing information.

> **CAUTION**
>
> The RTS command will not return-to-service a DS1 line looped back on itself. This is due to a change in diagnostics for the loopback relay in the 6X50 card. The RTS FORCE command must be used to condition the looped span so that it appears to be a normal situation.

NT6X50AB DS1 card

The NT6X50AB DS1 Carrier Interface Card is a general replacement for the NT6X50AA card on both the C-side and P-side of an XPM. Initial implementation was for ISDN Primary Rate Interface (PRI) applications.The NT6X50AB card provides:

- extended super frame format (ESF)
- bipolar eight-bit zero substitution (B8ZS)
- alarm indication signal (AIS)

The following functions are supported by both AA and AB versions of the card:

- frame format, super frame (SF)
- zero code suppression (ZCS)
- bit error ratio (BER) based on bipolar violation (BPV)
- data links
- local loops
- alarm detection: local (red), remote (yellow)

The following functions are supported by the AB version:

- extended super frame format (ESF)
- bipolar eight-bit zero substitution (B8ZS)
- bit error ratio (BER), cyclic redundancy check (CRC)
- data links for SLC-96 and facility data link (FDL) to enable the carrier facility
- remote loops
- alarm indication signal (AIS) detection

The following combinations are invalid for the NT6X50AB card:

- SF with BER based on CRC
- SF with FDL
- ESF with SLC-96

Carrier troubleshooting strategies

Audits of DS1 links are executed automatically by the DMS switch. When a fault condition is detected on DS1 links, a maintenance action is required. Operating company maintenance personnel use fault isolation tests to determine which component is causing the fault, and remove the fault condition or report it to the appropriate maintenance support organization. When troubleshooting DS1 links, operating company personnel post the link at the CARRIER level of the MAP terminal and enter the DETAIL command to obtain information on the link in question. Methods for handling specific scenarios are provided in the following paragraphs.

Operating company personnel can execute the following operations on DS1 carrier links at the CARRIER level of the MAP terminal:

- detail information about a specified carrier
- display carriers in a specified state
- post a carrier or group of carriers
- protection switch a carrier

NOTE: Protection switching does not apply to host office PMs.

When frame losses, slips, bi-polar violations (BpV), or other faults occur on a carrier, the PM signals transmitted do not meet specifications. The DMS-100 switch monitors these signals. When they do not meet specifications, OMs are pegged and the maintenance limit (ML) and OOS limit are incremented. Steady frame loss or excessive frame losses, slips, or bi-polar violations normally cause a carrier to be put OOS.

NOTE: Operating company personnel use the SETACTION command at the MAP terminal to allow a carrier to be put OOS when it exceeds its OOS limit. Excessive bi-polar violations cause a carrier to be put OOS, regardless of how the SETACTION command is used.

Isolated or intermittent faults, such as frame losses, slips, or bi-polar violations, are accumulated. When they reach the ML, a field marked ML is updated on the MAP display. This indication serves as a warning to maintenance personnel that faults have occurred or are occurring on the carrier. A carrier is placed temporarily SysB or permanently SysB, depending on how many times the system has returned the carrier to service. The carrier is set temporarily SysB if both of the following criteria are satisfied:

- a steady state alarm has been raised for a carrier, excess bi-polar violations have occurred, or the carrier has exceeded the OOS limit for frame losses or slips
- the SETACTION command is in use with the carrier, but the carrier has not exceeded the OOS limit for RTS

If the same carrier exceeds its OOS limit for RTS, it is set permanently SysB and must be manually returned-to-service (RTS).

For a source of information on DS1 maintenance and troubleshooting, see NTP 297-2401-502, *DMS-100F ISDN Primary Rate Interface Maintenance Guide.*

Carrier troubleshooting techniques

Following are some general carrier troubleshooting techniques that can be used:

- Remove the related trunks from service before proceeding with the trouble clearing process when it involves disrupting the DS1 line by diagnostics, frogging, looping, or replacement.

- From the MAP, perform diagnostic tests on the DMS 100F peripheral module and carrier card to verify proper operation. If necessary, loop at DSX patch jacks to verify operation. Bit error rate tests (BERT) can be used to test for line errors. BERTs are invoked from MAPCI;MTC: TRKS;TTP;LEVEL DATA.

- Normally, hard faults are referred to the carrier maintenance force, who restore the DS1 system by patching to spare span lines.

- Constant and intermittent faults are more difficult to sectionalize and require close coordination during the troubleshooting process, which, may involve spare span line replacement, frogging and looping techniques on the DS1 line.

- Slippage caused by a T1 type line repeater losing sync and jumping to its natural resonant frequency may be identified by substituting a DS1 line test signal containing repetitive strings of sixteen consecutive zeroes. This test would be performed by the carrier maintenance personnel.

- Cabling and jumpers on the DSX cross connection panel should have two twists per inch for noise and crosstalk purposes.

Disturbance parameters

Timing jitter

Timing jitter is the short term variation of the digital signal's significant instances from their ideal position in time. Short term implies phase oscillation of 10 Hz or higher.

Basically, jitter is an unwanted phase modulation of the pulse code modulation (PCM) signal that can occur in digital facilities. The rate of the phase modulation is the actual jitter frequency and the amplitude is the peak to peak amount of the angular or phase displacement of the PCM signal.

The effects of jitter on the digital switching network are varied. Intermittent problems with data transmission, DMS messaging, or synchronization may be traced to excessive jitter in the DS1 facilities.

Some causes of jitter are:

- external interference noise that is induced on the cable pairs
- incorrect tuning of repeater clock or decision circuitry

- incorrect equalization
- defective regenerative repeaters
- bad near-end or far-end crosstalk
- intrinsic phase noise in the basic oscillators of some digital radio equipment

Another source of jitter is T1 to T1C multiplexers. Some multiplexers cause what is called *waiting time jitter*. It is the result of the bit or pulse stuffing operation within the multiplexer. Since the output rate is slightly higher than the sum of the two incoming T1 lines, additional pulses are added by removing data from the receive elastic buffer at the T1C rate.

Typically the higher the jitter frequency, the more susceptible the connected equipment is to malfunction because of the jitter impairment.

Wander

Wander is the long term variation of the significant instants of a digital signal from their ideal positions in time. Variations are of low frequency less than 10 Hz.

Delay

Delay is the time elapsed between the transmission of a signal and the reception of that signal.

DMS-100F switch synchronization

Digital switching is highly dependent on accurate timing (via synchronization) so that each bit of the signal interleaves into its appropriate time slot. Network synchronization is achieved by locking the frequency of all DMS-100F switches to a primary frequency source. Maintaining network synchronization depends upon:

- clock accuracy while in synchronization
- variations in the synchronization signal
- clock accuracy when synchronization link fails

The digital network should be synchronized at all times to minimize slips, related data errors and cutoffs.

Table SYNCLK

Table SYNCLK specifies the synchronous clock arrangements for the office. Some key items are:

- Switching units (SU) with synchronous clocks are classed as one of the following:

    — Master External, SU SYNC from external reference clock.

    — Master Internal, SU SYNC from free running oscillator as network master clock.

— Slave SU SYNC to MASTER on another SLAVE via clock signals on one of two assigned DS1 timing links.

— MASTER OF SLAVES (MOFS) enter "Y" when other digital switching units, including digital PBXs SYNC from this host SU.

NOTE: Table SYNCLK enables the user to specify, within certain limitations, the location of the clock source and the DS1 timing links with regard to the peripheral module (DTC, LTC, or DCM).

Synchronization clock MAP levels

There is a MAP clock level for the SuperNode to provide timing link and status displays for synchronous clocks, and to provide manual adjustments. The clock levels control the system clocks and synchronize them to a clock source extracted from incoming digital trunks.

The SuperNode CLOCK MAP level is accessed by MAPCI;MTC;MS;Clock and is described in NTP 297-5001-549 *DMS-100F SuperNode and SuperNode SE Message Switch (MS) Maintenance Guide*

Digital testing parameter

For anyone that needs more details on test parameters that have been defined for measuring digital links and facility sections, see the Institute of Electronics and Electrical Engineers (IEEE) document—*Methods and Equipment Standard for Measuring the Transmission Characteristics of PCM Telecommunications Circuits and Systems.*

Exhibit A

Carrier maintenance quick reference

Purpose:
Checks alarm status of all active span lines.

Recommended Operation:
Should be performed daily.
At CI level enter:
MAPCI;MTC;TRKS;CARRIER
Display alarms will provide/display all alarms on all span lines.
Review DS1CARR OM Group for slips, LOF, and bit error problems
Identify alarms in terms of:

- Local carrier group (LCGA)alarms
- Remote carrier group (RCGA) alarms

Available: 126 individual alarms for appropriate action.
Use commands DISPLAY and DETAIL for more information.

Carrier maintenance quick reference (continued)

Activation:

See CARRMTC table for maintenance and out-of-service settings

See "Carrier maintenance" on page 2-263.

References:

- NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide*
- NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide.*
- NTP 297-2401-502, *DMS-100F ISDN PRI Maintenance Guide*

NOTES:

1. Ensure correct switch settings on circuit packs NT2X35, NT3X48 & NT6X50 to minimize slips between the office T1 repeater and DMS-100. See IM 925-190 or NTP 297-8991-805, *DMS-100F Hardware Description Manual* for pack settings.

2. The bogey for T1 carrier transmission faults is zero.

3. All equipped, but unassigned, DTCs should be looped back at the DSX bay to simulate a working span. The switch will monitor the looped signal for faults.

4. All provisioned, but unassigned, T1 lines must be properly terminated and energized with a 1.544 Mb/s digital signal. This prevents the T1 line from oscillating and spilling interference into other T1 lines working in the same cable sheaths or equipment bay.

THIS PAGE INTENTIONALLY LEFT BLANK

Corrective Maintenance — General

Corrective maintenance—sometimes referred to as reactive maintenance—consists of reacting to trouble indicators, analyzing troubles down to a repairable unit, and repairing the trouble. This is usually after a service affecting event has occurred. Unfortunately for customer service, many companies operate in the "reactive maintenance" mode instead of in a "proactive maintenance" mode. Once in this mode of operation it is very difficult to change since work habits are formed and resistance to change is very strong.

For those that are interested in a proactive approach to maintenance, see the "Maintenance Strategy" and "Maintenance By Exception" subsections within the *Introduction* tab of this manual. These subsections provide an overview of the DMS-100F tools that can be used to set up a proactive maintenance mode of operation. Other subsections within the MOM provide more detail on the various tools and references to NTPs for further support.

The subsections within this tab provide an overview of corrective maintenance in the following areas:

- Maintenance, Troubleshooting, and Recovery References
- Trouble Indicators
- Trouble Repair
- Trouble Analysis Tools
- Display Call (DISPCALL) & Show Audit (SHOWAUD) Commands

Maintenance, Troubleshooting, and Recovery References

Maintenance, troubleshooting, and recovery NTP references are provided in the following tables arranged by equipment category or function.

The best way to determine if a document has been cancelled or reassigned is to reference the NTP 297-8991-001, *Index* or NTP 297-8991-002, *DMS-100F North American (NA) Publications Cancellation Index.*

Table 3-1 — Maintenance and Troubleshooting NTP References	
Equipment Category or Function	**Maintenance & Troubleshooting NTP References YYYY=PCL Layer**
1-Meg Modem	297-8063-200 1-Meg Modem Service Implementation Guide
Automatic Call Distributor (ACD)	297-2041-500 DMS-100 ACD Maintenance Guide
	297-2041-900 M5212 ACD Set Gen. Description, Installation & Maint.
Advanced Intelligent Network (AIN)	297-5161-021 AIN Essentials, Services Implementation Guide
	297-5161-022 AIN Service Enablers, Services Implementation Guide
	297-5161-510 AIN/LRN-LNP Maintenance Guide
	297-8981-021 LRN/LNP Service Implementation Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
BMC II BISYNC	297-6201-501 BMC II BISYNC Quick Reference Guide
	297-6201-502 BMC II BISYNC OA&M Guide
CCS7 Signaling	297-1001-531 DMS-100 CCS7 Maintenance Reference Manual
Conference Circuits	297-1001-530 DMS-100 Conference Circuit Guide
Data Packet Controller	297-1001-525 DMS-100 Data Packet Controller Reference Manual
DataSPAN Frame Relay	297-5111-501 DMS-100 SN DataSPAN Frame Relay Maint. Guide
Digital Recorded Announcement (DRAM)	297-1001-527 Digital Rec'd Annc. Machine DRAM & EDRAM Guide
Continued on next page	

Table 3-1 — Maintenance and Troubleshooting NTP References	
Equipment Category or Function	**Maintenance & Troubleshooting NTP References YYYY=PCL Layer**
Device Independent Recording Package (DIRP)	297-1001-345 DMS-100 DIRP Administration Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Disk Maintenance Subsystem	297-1001-526 DMS-100 Disk Maintenance Subsystem
Distributed Processing Peripheral (DPP)	297-1001-539 DMS-100 DPP Hardware Replacement Guide
	297-1001-547 DMS-100 DPP Maintenance Procedures Guide
	297-1001-544 DMS-100 DPP Quick Reference Guide
	297-YYYY-543 DMS-100 DPP Alarm & Performance Monitoring Proc.
DMS Voicemail	297-7001-503 DMS VoiceMail Trouble Loc. & Clearing Procedures
E911	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Equal Access	297-2101-500 DMS-100 Equal Access Maintenance Guide
Ethernet	297-8991-910 Ethernet Interface Unit User Guide
EXT External Alarms	297-1001-593 DMS-100 External Devices Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
Input/Output Device (IOD)	297-1001-590 DMS-100 Input/Output Devices Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
ISDN Lines	297-2401-501 DMS-100 BRI Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
ISDN Trunks	297-2401-502 DMS-100 PRI Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Junctor Network (JNET)—NT40	297-1001-591 DMS-100 Networks Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Continued on next page	

Table 3-1 — Maintenance and Troubleshooting NTP References	
Equipment Category or Function	**Maintenance & Troubleshooting NTP References YYYY=PCL Layer**
Lines (LNS)	297-1001-594 DMS-100 Lines Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
LPP Peripheral	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
MDC CLASS	297-1421-503 DMS-100 Subscriber Services Maintenance Guide
OM Troubleshooting	297-1001-318 DMS-100 Service Problem Analysis Admin. Guide
Outside Plant Access Cabinet (CPAC)	297-8211-550 DMS-100 Outside Plant Access Cabinet Maint. Guide
Peripheral Modules (PMs)	297-1001-592 DMS-100 Peripheral Modules Maintenance Guide
Extended Peripheral Modules (XPMs)	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Ringing System	297-1001-131 DMS-100 Ringing System General Description
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
RLCM/OPM	297-8201-550 DMS-100 RLCM/OPM Maintenance Manual
RSC	297-8221-550 DMS-100 RSC Maintenance Manual
RSC SONET Model A (DS1)	297-8261-550 DMS-100 RSC SONET Model A (DS1) Maint. Manual
RSC SONET Model B (DS1)	297-8281-550 DMS-100 RSC SONET Model B (DS1) Maint. Manual
RSC SONET Model A (PCM30)	297-8271-550 DMS-100 RSC SONET Model A (PCM30) Maint. Man.
RSC SONET Model B (PCM30)	297-8291-550 DMS-100 RSC SONET Model B (PCM30) Maint. Man.
Small Remote Unit	297-2781-500 DMS-100 Small Remote Unit Maintenance Guide
Subscriber Carrier Module-100S	297-8231-550 DMS-100 Subscriber Carrier Module-100S Maint. Man.
Subscriber Carrier Module-100U	297-8241-550 DMS-100 Subscriber Carrier Module-100U Maint. Man
Subscriber Carrier Module-100R	297-8301-550 DMS-100 Subscriber Carrier Module-100R Maint. Man
Subscriber Carrier Module-100 Access	297-8263-550 DMS-100 Subscriber Carrier Module-100A Maint. Man
Subscriber Carrier Module-100A (MVI-20)	297-8253-550 DMS-100 SCM-100A (MVi-20) Maintenance Manual
Subscriber Services	297-1421-503 DMS-100 Subscriber Services Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
Continued on next page	

Table 3-1 — Maintenance and Troubleshooting NTP References

Equipment Category or Function	Maintenance & Troubleshooting NTP References YYYY=PCL Layer
SuperNode Data Manager	297-5051-900 SDM Simplex User Guide
	297-5051-904 SDM Enhanced Terminal Access user Guide
	297-5051-906 SDM Fault-tolerant User Guide
	297-5051-912 SDM Exception Reporting User Guide
	297-5051-913 SDM Secure File Transfer user Guide
	297-5061-912 SDM Exception Reporting User Guide
	297-5061-913 SDM Secure File Transfer user Guide
SuperNode and SuperNode SE Computing Module	297-5001-548 DMS-100 SN & DMS SN SE CM Maintenance Manual
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
SuperNode and SuperNode SE Message Switch	297-5001-549 DMS-100 SN & DMS SN SE MS Maintenance Manual
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
SuperNode System Load Module	297-1001-590 DMS-100 Input/output Devices Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
SuperNode ENET	297-1001-591 DMS-100 Networks Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
SuperNode SSP/SP	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
TOPS 04	297-2271-300 DMS-200 TOPS 04 Operator Guide
	297-2271-310 DMS-200 TOPS 04 Force Management Guide
TOPS MP and MPX	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures
TOPS Message Switch (TMS)	297-8341-550 DMS-200 TOPS TMS Maintenance Guide
Continued on next page	

Table 3-1 — Maintenance and Troubleshooting NTP References	
Equipment Category or Function	**Maintenance & Troubleshooting NTP References YYYY=PCL Layer**
Trunks (TRKS)	297-1001-595 DMS-100 Trunks Maintenance Guide
	297-YYYY-543 DMS-100 Alarm and Performance Monitoring Proc.
	297-YYYY-544 DMS-100 Trouble Locating and Clearing Procedures
	297-YYYY-547 DMS-100 Card Replacement Procedures

Table 3-2 — Recovery Documentation References	
Equipment or Product	**Recovery NTP References** **YYYY=PCL Layer**
DMS NT40 Recovery Procedures	297-YYYY-545 DMS-100 Recovery Procedures
DMS SuperNode Recovery Procedures	
DMS SuperNode STP Recovery Procedures	
DMS SuperNode SP/SSP Recovery Procedures	
DMS SuperNode SCP II Recovery Procedures	
DMS SuperNode STP/SSP Recovery Procedures	
DMS SuperNode SE Recovery Procedures	
DMS SuperNode SE SP/SSP Recovery Procedures	
Lines, Trunks, and Peripheral Recovery Procedures	
DTC Emergency Recovery Procedures	
RLCM/OPM Recovery Procedures	297-8201-550
RSC Recovery Procedures	297-8221-550
SMR (Rural) Recovery Procedures	297-8301-550
SMS Recovery Procedures	297-8231-550
SMU (Urban) Recovery Procedures	297-8241-550
SMA (Access) Recovery Procedures	297-8251-550
RSC-SONET Model A (DS1) Recovery Procedures	297-8261-550
RSC-SONET Model B (DS1) Recovery Procedures	297-8281-550
RSC-SONET Model A (PCM30) Recovery Procedures	297-8271-550
RSC-SONET Model B (PCM30) Recovery Procedures	297-8291-550
TOPS MP Recovery Procedures	297-YYYY-545 DMS-100 Recovery Procedures
TOPS MPX Recovery Procedures	297-YYYY-545 DMS-100 Recovery Procedures
DIRP Recovery Procedures	297-YYYY-545 DMS-100 Recovery Procedures
CompuCALL Recovery Procedures	297-YYYY-545 DMS-100 Recovery Procedures
DPP Recovery and Routine Maintenance Guide	297-YYYY-545 DMS-100 Recovery Procedures

Trouble Indicators

There are several trouble indicators that play an important role in identifying trouble conditions in the DMS-100F switch. Some of the more common indicators of trouble are described in this subsection. The topics described within this subsection is as follows:

- alarms
- operational measurements (OM)
- customer reports
- performance indicators
- log messages

Other indicators, such as real time tools and the "Maintenance Managers Morning Report," are described within subsections located in the *Performance* tab of this manual.

Alarms

Audible and visual alarms alert maintenance forces that the system has detected a problem that may require corrective action.

The urgency of the corrective action is generally indicated by the level of the alarm: minor (MIN), major (MAJ), or critical (CRIT).

Minor alarms usually indicate a non-service affecting condition.

Major alarms usually indicate a service degrading condition to several customers or that another similar failure can cause a service outage to several customers.

Critical alarms usually indicate a service outage condition to a large number of customers, or that another similar failure can result in a service outage to a larger number of customers. Critical alarms can also result from fire alarms.

Alarms in the DMS-100F office can be locally detected, system detected, and externally detected as follows:

- locally detected alarms
    — hardwired non-DMS power, fuse, fan

- system detected alarms
  - software detected system faults: central control, central message controller, network, peripheral, input/output devices, lines, trunks, external, and dead system alarm
- externally detected alarms
  - alarms generated by assigned scan points
  - fire alarm from a scan point
  - see Table ALMSC in NTP 297-YYYY-350 for PCL loads and higher

See NTP 297-1001-122, *DMS-100F Alarm System Description*, for information describing the DMS-100 Alarm System. Also, see NTP 297-1001-593, *DMS-100F External Devices Maintenance Guide* and NTP 297-YYYY-543, *DMS-100F Alarm and Performance Monitoring* NTPs.

Operational measurements

Operational measurements (OMs) consist of monitoring and counting the occurrences of events within the DMS system. These events include items such as: call counts, usage, errors, dial tone speed recording (DTSR), receiver attachment delay recorder (RADR), and hardware and software faults (that are excellent for identifying trouble conditions).

It is recommended that selected OMs be printed daily, weekly, and monthly for use as the primary method of trouble analysis.

The OM thresholding feature provides the mechanics for automating the surveillance, detection, and alerting of key OMs for maintenance. This feature and OMs are described in the *"Operational Measurements"* subsection within the *Preventive Maintenance* tab of this manual.

Troubleshooting with OMs

NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*, provides a section to assist in identifying many of the most common service related problems associated with the DMS switch. A table within the NTP provides helpful descriptions and procedures for resolving DMS switch problems. Also included in the table are recommendations for threshold limits and monitoring frequency of OM groups and key fields.

Customer reports

Customer reports are another source of trouble indicators. Experience has shown that when proactive maintenance is properly performed, it can result in minimal customer reports.

The following is a list of typical customer reports and some possible sources of trouble conditions. This list is only a guide and may not include all types of customer reports, nor all sources of trouble:

Can't call category

No dial tone (NDT)

- open cable pair, heat coil or MDF jumper
- defective telephone set or wiring
- defective line card or wrong loop option
- line in wrong state (CUT or MB)
- incorrect translations
- sleepy lines (idle state, NDT)
- babbling line condition (ICMOLINE)
- defective LCM/RLCM/LM/LGC
- office or PM overload

Slow dial tone (SDT)

- office or PM overload
- insufficient DGT or UTR receivers
- shortage of speech links
- shortage of call processing (CP) resources
- deny originations (CP ORIGDENY OM)

Dial tone returns

- wait deny (CP WAITDENY OM)
- defective line card
- rough movement of line drawer
- network module crosspoint trouble
- translation or software trouble
- switching processors in LCM/LGC/DTC

No ringing signal to set

- ringing generator trouble or option error
- defective line drawer or bay wiring
- ring pre-trip condition due to a defective cable pair
- defective carbon or gas protector causing pre-trip

- defective Bus Interface Card (BIC)

Reaching reorder tone or announcement

- defective dial (i.e., mutilated digits)
- defective cable pairs of MDF jumper
- translation troubles
- no circuits available
- defective line card
- defective receiver
- high digitone level from PBX
- overloaded circuits
- SS7 messaging problem

Can't be called category

Bells don't ring

- defective set, ringer turned off, too many sets or exceeds loop requirements
- grounding problem at customers station (party lines)
- defective cable pair or MDF jumper
- defective ring generator or option
- defective line drawer or bay wiring
- translation error (possibly assigned to wrong line)
- ring trip condition on line
- software trouble

Reach busy (line not being used)

- line in wrong state (MB or CUT)
- babbling line condition (cordless phone?)
- translation error
- software trouble
- line on call forwarding (CFW)
- reorder tone being mistaken for busy indicating another problem caused report

Transmission/noise categories

Noisy

- defective set or set cord

- defective line card
- defective carbon or gas protection
- defective cable pair or MDF (repeater, loading problem)
- repairman working on cable or technician working on MDF
- line card balance network not set (see "Balance network testing" in the "Line Maintenance" subsection of the *Preventive Maintenance* tab)
- defective peripheral module (LGC, LCM, RLCM, LM)
- defective office ground, battery, or battery filter
- defective speech links
- defective network modules
- defective trunk(s), or carrier(s)
- defective ring generator

Cut-off category

Cuts off (returns to dial tone)

- defective line card or line card removed while inservice
- rough movement of line drawer
- switching processors in LCM/LGC/DTC
- reinitializing peripheral modules
- network module troubles
- parity or integrity problems within switch
- defective trunks or carriers
- defective line facilities
- warm or cold CPU restarts

Performance indicators

A performance results indicator—such as Nortel Networks Switch Performance Monitoring System (SPMS) feature—can identify weak areas of equipment performance when measured components exceed acceptable levels. These measured components should be examined and analyzed for trouble conditions or trouble trends. See the *Performance* tab of this manual for information on SPMS.

Various types of hourly, daily, weekly and monthly operational measurement reports can be used as an indicator of switch performance. This type of data can be used for corrective analysis as well as a proactive maintenance indicator of office performance. See the "Operational Measurements (OMs)" subsection within the *Preventive Maintenance* tab for details on the use of OMs.

Log messages

Log messages are primarily an analysis tool, they can be a good indicator of trouble conditions when there are:

- sudden increases in volume of logs
- large numbers of similar logs
- alarmed logs

WARNING: nn REPORTS NOT PRINTED, or messages containing the text "Lost logs". When you see these messages, you should suspect a problem with the way logs are being administered within that office. This is an indication that logs are being lost due to the log buffers being overloaded. This could be caused by an excessive number of logs due to a serious problem, or an overload due to poor management of logs. Log administration is affected by the DMS-100 SuperNode Data Manager (SDM) feature, if it is present.

To understand more about how to manage log messages within your switch, see subsection "Log System Administration" within the *Office Administration* tab for management of logs.

Logs are used by DMS-100 switch software to record all significant events that occur, and to make them visible to the operating company personnel at the MAP terminal. Examples of significant events are: an equipment fault, a change in state of equipment, and the failure or success of a test.

The log system in the DMS-100 switch creates a report containing this information, stores the report in data store (DS) for online retrieval, and distributes the report to one or more output devices where it is displayed. Log reports are usually displayed in the order they occur. The log prioritizing feature—described in the "Log System Administration" subsection within the *Office Administration* tab—allows the log reports with the highest alarm level to be displayed first.

PM log reports are generated when a PM has a fault condition, when there is a change in the PM state, or when a PM passes or fails a test. PM logs 179 and 180, the most important PM maintenance logs, are always generated by a change in the PM state. Other causes for these significant logs, and the appropriate actions that operating company personnel should follow are described in NTP 297-1001-592, *Peripheral Modules Maintenance Guide*.

PM180 log reports

The peripheral module (PM) subsystem generates the PM180 log report when a software exception is encountered. A software exception is an occurrence of improper execution of the software. PM180 is used by software experts to identify and correct software defects. PM180 may also be generated due to a hardware related software exception.

The PM subsystem generates this report when a software condition that affects normal operation of the DMS or its peripherals occurs.

Exhibit A, on the following page, lists PM180 messages (identified by their text fields) that are known to be associated with hardware problems. Following each PM180 is a brief description and trouble locating aid. For more detailed information on the PM180 log, see NTP 297-YYYY-840, *Log Reference Manual*.

PM180 log cleanup

The number of PM180 logs has grown to a volume that makes it difficult to track and analyze. To make it more difficult, the data contained within the PM180 logs is often not meaningful to the operating company maintenance personnel, and is not well documented.

To aid the customer with PM180 logs associated with hardware problems, a feature called "PM180 cleanup" provides a software analysis of PM180s. If a hardware fault is found, a   PM777 log is generated to indicate the suspected hardware. The conversion of hardware related PM180s reduces the number of logs and enable the customer to perform corrective hardware maintenance by using plain English information documented in the log reference manual.

Exhibit A   —   PM180 Messages Corrective Maintenance and Partial List of Hardware Type Problems

TEXT	DESCRIPTION
bad addon key_id	bad addon key _id in trtkarb. POSSIBLE CAUSES: P-phone add on set; P__ phone line card; w87 chip.
bad key__id	bad key id for group in tptkarb. POSSIBLE CAUSES: no add on set; w87 chip.
fmis drop	Too many false 'may i send' seen on a plane from the network, the other plane was already closed. POSSIBLE CAUSES: 6X40; network fault.
fmis1	Too many false mis seen from the network on a given plane. POSSIBLE CAUSES: 6X40; network fault.
fmis2	Lots of false mis coming in from the network. We can't determine which plane they are coming from as the h/w doesn't tell us the plane it occurred on. POSSIBLE CAUSES: 6X40; network fault.
link_downl	inbound message: CSC detected that the link between HDLC and network is not working. POSSIBLE CAUSES: Bad link to Cell Site Controller (physical link or circuit pack).
checksum	POSSIBLE CAUSES: Bad RAM in 6X51
Continued on next page	

Exhibit A — PM180 Messages Corrective Maintenance and Partial List of Hardware Type Problems (continued)

TEXT	DESCRIPTION
ptsi	pots screen error, LCM message invalid for current terminal state (bad digitone digit). POSSIBLE CAUSES: phone set; line card; bad tones from traffic test set.
bic ch rcl	Due to an audit detecting that a BIC channel marked busy in hardware is not being used by call processing. POSSIBLE CAUSES: Faulty BIC card if H/W. It is H/W if a lot of these messages occur. **NOTE: For bic ch rcl, use the first two HEX digits of the 4th word of the data to determine the drawer number; i.e., 8789 000 4C1B 06D1 8001 .... 06 : is a hex number - multiply it by 2 to get the drawer number (2x6 = 12/12)
dcc ch rcl	chan_ not. ..in _use POSSIBLE CAUSES: faulty Digroup Controller Card (DCC) 6X52
dmsx msg 1	This means the LCM has run out of resources and is starting to lose messages from the LTC. POSSIBLE CAUSES: Overload condition. Babbling line card.
iuc msg 1	Indicates overload in transferring calls to mate. POSSIBLE CAUSES: Overload condition.
rv locked	Stack overflow. POSSIBLE CAUSES: Overload condition. Babbling condition.
xmt dsmx 0	POSSIBLE CAUSES: Overload condition.
mxt iuc 0	POSSIBLE CAUSES: Overload condition.
DMSX MATE	shorted pins in LGC cables going to LCM
`BWD Q FULL'	RCT is not responding or SMR not correctly receiving response to request to send Bwords. Most likely cards are: • QPP419 Digroup card at RCT • QPP417 Address controller at RCT • 6X81AA on active unit of SMR — if this card is suspect, warmswact • SMR and monitor for further occurences.
`RSP MISMTCH'	Response Mismatch. Data sent to the RCT is not the same as data received from the RCT. Most likely cards are: • QPP436 repeater at RCT • QPP417 Address controller at RCT

Exhibit A — PM180 Messages Corrective Maintenance and Partial List of Hardware Type Problems (continued)

TEXT	DESCRIPTION
STUCKBWD OR STUCKBWD2'	SMR has not received a response from a sent Bword for .5 seconds. Most likely cards are: • QPP419 Digroup card at RCT • QPP417 Address controller at RCT • 6X81AA on active unit of SMR.
`BAD CHNLY OR BAD CHNLX'	This is a discrepancy between SMR/RCT as to the status of a particular channel. BAD CHNLY says that the RCT thinks the channel is CPB and the SMR thinks it's idle. BAD CHNLX says that the RCT thinks the channel is idle and the SMR thinks it's CPB. Most likely cards are: • QPP417 Address controller at RCT • 6X81AA on active unit of SMR

Trouble Repair

In most cases involving a switch, trouble repair consists of circuit pack replacement, line options, or translation table changes. However, in some cases trouble repair involves such activity as: correcting inter-bay cabling problems, straightening bent pins in connectors, clearing up noise in power circuits, changing circuit pack options, changing out bay fans, and inserting/removing software patches or images to correct software bugs.

Electrostatic discharge precautions

Touching, handling, and storage of maintenance spare circuit packs—as well as the actual removal and replacement of circuit packs in the system—must be done according to the applicable NTP card replacement procedures and associated warning bulletins. Established electrostatic discharge (ESD) protection procedures are described in NTP 297-1001-010, *DMS-100F Electrostatic Discharge Protection*.

Line service caution

In any situation involving the temporary removal or replacement of a line card, perform the BALNET test in NTP 297-1001-594, *DMS-100F Lines Maintenance Guide* that adjusts the line circuit network to ensure optimum transmission (echo and loading). BALNET should be run immediately after any initial office cutover or any new line that is placed in service. Scheduled automatic BALNET testing can also be set up through automatic line testing (ATT). See the "Line Maintenance" subsection within the *Preventive Maintenance* tab for more information on BALNET testing.

Maintenance spares

The office maintenance spare set of circuit packs is, in many ways, similar to a test set. Any serious technician would not like to try and clear a trouble with a defective or uncalibrated test set. The same is true for clearing a trouble with the maintenance spare circuit pack that has not been tested in a working switch. Therefore, it is essential that the maintenance spare circuit packs be reserved as a proven, marked set of cards (previously tested in your office).

This can be accomplished only after a maintenance spare that has been used to clear a trouble is replaced with a pack that has been returned from repair. The maintenance

spare pack is then returned to the maintenance spare kit. This procedure uses the repaired card before the repair warranty elapses and could save in maintenance costs. The following procedural steps will provide some guidance to maintain a good set of maintenance spare circuit packs:

1. Upon arrival of a replacement or repaired circuit pack from Nortel Networks, check the release of the card to insure it is the same or a higher release, check switch settings if applicable, remove the on-site spare—do not forget to use a wrist strap—that was used in its place, and insert the replacement. It's a good idea to keep track of spares placed in service by marking or tagging them—see the note with next step.

> **CAUTION:** This should be performed at a time that minimizes any potential service affect or service impact, especially with some of the critical front-end circuit packs.

2. Run a complete set of MAP diagnostics on the replacement circuit pack according to the NTP circuit pack replacement procedures. If the card passes the test, place it in service. If it fails the test, immediately return the defective pack to your own pack storage center or Nortel Networks. Return the working spare pack to service.

NOTE: It is recommended that the *known good* spares inventory be identified in some manner (such as a colored stick-on tag) so they can be readily recognized, if stored in the switch. This identified spare inventory should be used for troubleshooting and for defective card replacement until another card arrives.

3. Record the failed circuit pack results on some type of log or use the "Repair and Return Circuit Pack Log". See the exhibits in the *Office Administration* section of this manual for an example of the log.

4. Any circuit pack returned as a no fault found (NFF) should be retested in the original slot, shelf, and frame in which it initially failed. Run several tests in case it was an intermittent problem.

Retest circuit pack cards

It is desirable to retest defective circuit pack cards during the trouble clearing activity. Testing the circuit pack in another equipment slot validates that the fault was not a seating problem and the trouble has been cleared by replacing the defective unit. Service precautions associated with retesting are contained under "Cautions and suggestions" below.

While the retesting procedure is not appropriate under all circumstances, this practice sharpens and enhances the trouble clearing process. Retesting verifies the true source

of the trouble for no fault found circuit packs, and identifies intermittent problems with associated equipment such as: connectors, bay cabling, and line connections.

Minimize service degradation

Precautions to minimize service degradation during retesting, or replacement should be observed. It is suggested that retest activity be performed during light traffic hours, with the exception of line cards. Normally, light traffic load is between 2:00 a.m. and 6:00 a.m. Any retest activity during light load should have virtually no effect upon service to the customer.

Line card retesting

Retesting line cards may be done during the normal work day, providing proper measures have been taken to prevent cutoffs. When the retest is completed, verify the line has been rebalanced and is returned to service.

It is recommended that stickers with references to a warning bulletin(s) be applied to all circuit packs in the office that are covered by active warning bulletins.

Circuit pack acceptance testing

Test new and repaired circuit packs on receipt from Nortel Networks to ensure proper operation. Establish local policy for testing critical processor related packs. Follow the NTP card replacement procedures and warnings when replacing cards in an inservice or non-working office. Manual tests should be run new or repaired cards to ensure proper operation. Normally, this card remains in service. The card removed becomes a spare or is returned to the maintenance spare set of cards.

Cleaning optical connectors

When an optical connector needs to be cleaned, use the process described on the following page.

NOTE: Optical connectors should be cleaned at installation time, or when required in a NTP trouble clearing procedure. Optical connectors should <u>not</u> be cleaned on a routine basis.

As part of the Data Grooming program Nortel Networks recommends that Series II peripherals fiber connectors be cleaned on a corrective maintenance basis, if replacement of cards (cross point, etc.) does not resolve the XPM PCM parity failures. Clean the connectors after all other repairs fail, and clean only the connectors involved in the failures. Also, perform this work during safe periods.

Materials

- can of compressed air (for example, Accuduster II OS-TX705)

- solvent dispenser (for example, Menda SD-6)
- lint-free cloth (for example, Absorond - TX404)
- ethenol, denatured grade 2-A 95 percent
- swabs (for example, Tiny head Texswab - TX709)

Cleaning Procedure

> **CAUTION:**
> Avoid direct exposure to laser beam or fiber. Invisible light than can blind is present. Keep all optical connectors capped.
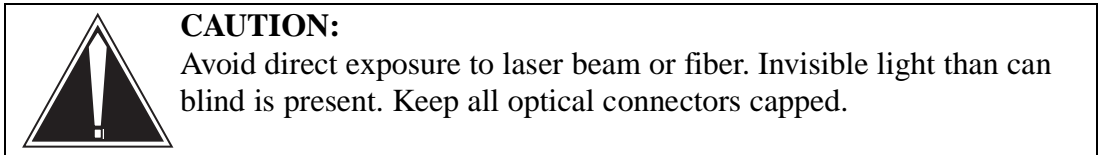
Figure 3-1   —   Optical connector cleaning
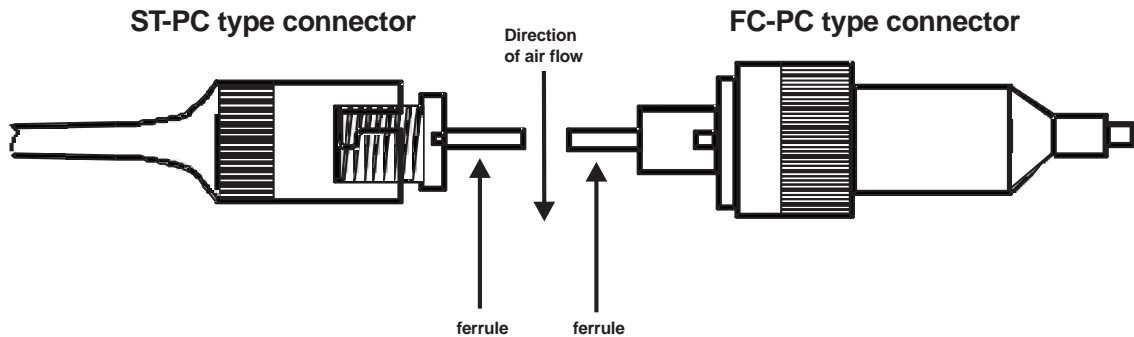
1. Using a can of compressed air, apply a short burst of air perpendicular to the ferrule of the connector—see next figure.

2. Moisten a cotton swab with ethanol, wipe completely around the ferrule twice, and then wipe across the end of the ferrule in a single stroking motion. Avoid moistening the entire connector with ethanol.

NOTE: Do not use the same swab to clean several connectors.

3. Use a lint-free cloth to gently wipe the surface of the ferrule, paying special attention to the tip of the ferrule.

4. Immediately apply a short burst of air—perpendicular to the ferrule of the connector—to remove any foreign particles.

5. Apply a short burst of air inside the coupler before reinserting the connectors for final mating.

Cautions and suggestions

On occasion it may be necessary to rotate or replace more than one circuit pack while attempting to repair a trouble. On these occasions, it is recommended that the cards be temporarily marked as to their original locations and a control record be established to keep track of card movements. This facilitates returning cards to their original positions at the conclusion of the maintenance actions.

Log all circuit packs that have been replaced using the circuit pack repair log forms described in the *Office Administration* section of this document.

Recording card replacement activities. When a card is replaced, the following information should be recorded in office records:

- the serial number of the card replaced
- the date the card was replaced
- the reason the card was replaced

The practice of referring to the log form before changing a circuit pack has saved site technicians from replacing the same card several times when the fault lies elsewhere. The log forms help to identify repeated circuit pack type failures and track the repair and return process.

Suggest using two log forms, one for line cards, the second log form for all other circuit packs to facilitate analysis and tracking. Information logged should include the LEN or DN on line cards, the fault indication, date, and the initials or name of the technician. All other card types should show frame, card, and slot as well.

Missing or incorrect translation data for lines, trunks, customer group, and trunk groups can cause trouble conditions. Also, missing data can cause:

- call processing deaths (see the "Display Call" subsection within this tab);
- unsuccessful translation verification (see TRAVER within the "Trouble Analysis Tools" subsection of this tab);
- and audit log messages (AUD395 and AUD398).

Incorrect data can route or process calls to the wrong destination or treatment. Since the DMS has processed the call, it will not generate any trouble log reports. Performing translation verification shows successful translation verification results. It requires a critical and knowledgeable interpretation of the translation data to identify the translation trouble.

Not all troubles are caused by defective circuit packs or translation errors.

Some troubles are caused by open, short-circuit or interchanged cable pairs or bent connector pins. Refer to intraconnectivity schematic (IS) drawings and perform investigative troubleshooting during very low traffic periods.

Some troubles can be caused by electro-magnetic interference (EMI). This can be caused by cables that are incorrectly placed, poor grounding, noisy power circuits, or

cable pair or cross-connect jumpers in close proximity—this is especially true in the speech link connector (SLC) frame. Noise in power supplies can be found using oscilloscopes.

CAUTION: Remember, always observe NTP procedures when replacing circuit packs, wear wrist straps when handling cards, observe release levels, check switch settings if applicable, and review warning bulletins for circuit pack information.

Trouble Analysis Tools

When trouble indicators—alarms, OMs, customer reports, log messages, and performance results indicators—show that a trouble condition may exist, the following are some examples of tools that can be used by a technician to analyze the fault down to a repairable unit:

- Log messages
- MAP level menus
- Diagnostic tests
- Network Integrity (NETINTEG)
- DISPCALL command
- TRAVER command
- TRNSLVF command
- DTSR and RADR
- SPMS
- Node Assessment Graph (NAG)
- Switch Status Report (SSR)

Log messages

Log messages provide detailed information on hardware and software failures, call errors, diagnostic results, and subsystem status that may require maintenance action. Log messages can be requested from the log subsystems using LOGUTIL subcommands, printouts, and databases that store log messages. Detailed information about logs can be found in NTP 297-YYYY-840, *DMS-100F Logs Reference Manual.* Also, see subsection "Log System Administration" within the *Office Administration* tab for more information on how to manage logs.

MAP level menus

The MAP levels and sublevel commands provide the human-machine-interface (HMI) and is the most used tool within the DMS-100F switch. For a description of the MAP and its use, see NTP 297-1001-520, *DMS-100F Maintenance System User Interface Description.*

Diagnostic tests

Diagnostic tests are intended to find hardware faults down to a replaceable card level and can be system initiated, scheduled for automatic testing, or manually initiated.

Examples of when manually initiated diagnostics should be used are as follows:

- resolving customer reported problems
- when log messages indicate a common equipment problem
- when OMs show high error counts
- when system detected alarms indicate a problem
- assessment testing
- testing new equipment or routine testing

Having observed a status change on the system VDU display, maintenance personnel can request sublevel information, showing overall subsystem status. Further information is retrievable from the logging mechanism on diagnostic, error and status messages stored therein. Based on this information the fault is repaired and the maintenance personnel then request that the component be returned to service. This request results in a diagnostic being run, which if successful, then performs the action of returning the repaired component to service. The associated action and status messages are also generated at this time. If the diagnostic fails, a diagnostic message is sent, resulting in a repetition of the repair attempt and a rerun of the diagnostic. The fault will continue to be displayed as an alarm on the VDU, even if the audible alarm is off, until the diagnostic is successful.

System initiated diagnostics are generated when internal counters exceed fixed levels. System initiated diagnostics may not be as comprehensive as manually initiated diagnostics, and out-of-service diagnostics are more extensive than in-service diagnostics. In some instances, repeating a diagnostic test can help locate marginal or intermittent faults.

System or manually initiated diagnostics may not always detect or find existing real faults. Where high error counts, log messages, and customer reports indicate a trouble condition, it may be necessary to rotate or replace circuit packs on speculation even though diagnostic tests reveal no faults.

CAUTION: Replacing line cards on speculation could be very costly. Where there is a high return on line packs, suspect that poor maintenance processes are being performed and that packs are being changed out unnecessarily.

Network integrity (NETINTEG)

The network integrity (NETINTEG) MAP level can used to analyze network module troubles from peripheral to peripheral.

Network trouble conditions may cause the following customer reports:

- cutoffs (see note below)
- transmission/noise
- data errors for high-speed data services
- dial tone returns (DTRs)

NOTE: Cutoffs in the DMS caused by network module troubles are counted by the CPSUIC counter in the CP table of the OM. The CPSUIC counter also counts other types of failures such as call process deaths. Experience has shown that this counter should not exceed a count of ten per one million calls.

See the *Preventive Maintenance* tab and the "Network Maintenance" subsection. For the Enhanced Network (ENET), see the "ENET Overview and Maintenance" subsection within the *System Products* tab.

DISPCALL command

The display call (DISPCALL) command level is used to capture all available information on the death of a call or a call that is being held for trouble analysis.

The death of a call can occur due to:

- call processing errors
- translation omissions
- network module speech errors or faults

DISPCALL is further described in the "Display Call (DISPCALL)" subsection next.

TRAVER command

Translations verification (TRAVER) is a tool that allows the user to examine the translation and routing of a particular call. A TRAVER report can display the possible results of a call, the translation of a call, or both. TRAVER was designed to help the user quickly identify translations errors, oversights, or misdirection while debugging and testing software. This allows the user to correct datafill problems more efficiently.

TRAVER is best used at the CI level of the MAP. TRAVER can verify up to 24 digits from lines or trunks. With TRAVER, the user can specify the type of call originator, the number being processed or the trunk taken, and the kind of report desired.

Composing a TRAVER command involves several different pieces of information. These are the code for the call originator, the identification of the originator, the directory number being processed or the outgoing trunk, and the type of report desired. The originator ID and the directory numbers being processed are dependent

on the particular configuration of the switch involved. The originator type and report code are part of the TRAVER program.

Both verifications can verify and display routing tables used, trunk routes available, digit control, and alternate conditional route. They also identify missing customer data, but cannot identify incorrect coding that requires knowledgeable interpretation.

Do not substitute a TRAVER for a call-through test. Many call-through tests fail even after TRAVER operated satisfactorily. TRAVER can help discover why a call-through test failed.

The TRAVER command has been modified for Advanced Intelligent Network (AIN) traces. If the office is an AIN office, TRAVER displays all AIN-specific translation, routing, and trigger subscription information regardless of whether or not AIN is active for that office. For an active office, the information displayed allows the trigger detection point (TDP) flow to be analyzed after AIN tables have been datafilled—but before the office is made an active AIN office. If the office is not an AIN office, TRAVER does not display any AIN-specific information.

AIN TRAVER has been modified so that the trigger activation state will be checked and displayed for the AIN trigger types Off-Hook Immediate, Off-Hook Delay, and Termination Attempt.

NOTE: TRAVER treats the activation state as another criterion to be checked during criteria checking, and so the displayed output contains a message stating that the trigger criteria was or was not met.

For more detailed information on TRAVER, and how to set up TRAVER with examples, refer to NTP 297-1001-360, *DMS-100F Basic Translations Tools*.

TRNSLVF command

The TRNSLVF command—located on the TTP level of the MAP—is used to display routing data for a call originated on a posted incoming or outgoing trunk. TRNSLVF can verify up to 18 digits (max 18 for called and max 15 for calling) from trunks only.

With the trace option set, an AIN subscribed trunk TRNSLVF checks the trigger activation state and displays the AIN trigger types: Off-Hook Immediate; Off-Hook Delay; and Termination Attempt. The output of TRNSLVF in this case is identical to that of AIN TRAVER.

DTSR and RADR

The DMS-100 offers two features for monitoring and measuring the frequency of significant delays in originating calls: dial tone speed recording (DTSR) and receiver attachment delay recorder (RADR). Although both measure the delay encountered by originating calls, their application is different. DTSR tests only the delay for originat-

ing lines. RADR measures the delay for originating lines and for trunks if they need receivers to originate.

DTSR

A delay in receiving dial tone of less than three seconds is generally considered acceptable by most operating companies. More than three seconds is considered unacceptable. Grade of service indicates the maximum permissible percentage of calls with dial tone delay of more than three seconds. During the average busy season busy hour (ABSBH) the limit is 1.5 percent, but during the high day busy hour (HDBH) the limit rises to 20 percent of calls.

The DTSR feature obtains data by simulating calls on line modules (LMs), and by observing actual calls on line concentrating modules (LCMs). DTSR activity is reflected in OM groups DTSR and SITE, which record the following information:

- line types available
- number of calls recorded during the accumulation period
- number of calls delayed more than three seconds

From this it is a simple matter to calculate the percentage of delayed calls and compare the results with the acceptable grade of service.

OM group DTSRPM records dial tone speed for each peripheral module.

A dial tone delay of more than three seconds is registered within the Dial Tone Speed Recording (DTSR) and DTSRPM OM groups, for local DMS-100 applications. Remotes use OM groups SITE, SITE2, and DTSRPM. The DTSR OM group provides measurements for the whole DMS switch while the DTSRPM group provides measurements for individual PMs.

In the DTSR OM group, the KEY column identifies the line types for testing. They are as follows:

- LMDP for dial pulse phones in LMs
- LMDT for digitone phones in LMs
- LCMDP for dial pulse phones in LCMs
- LCMDT for digitone phones in LCMs
- LCMKS for key-driven sets in LCMs
- DLMKS for data line module key sets
- RCTDP for dial pulse phones in RCTs
- RCTDT for digitone phones in RCTs
- RCSDP for dial pulse phones in RCSs
- RCSDT for digitone phones in RCSs

Analysis of dial tone speed problems can be found in NTP 297-1001-318, *DMS-100 Service Problem Analysis Administration Guide*, under the "Troubleshooting with OMs" section. Descriptions of the registers within the DTSR OM groups can be found in NTP 297-YYYY-814, *DMS-100F Operational Measurements Reference Guide*. More information on DTSR is provided in the *Performance* tab within the "Real-Time Performance Indicators" subsection.

RADR

RADR provides information about receiver attachment delay recorder (RADR) tests. The RADR generates test call originations to determine the interval between a request for attachment to a receiver and the time of connection to a receiver.

Every receiver type available at the switch is tested. Switch congestion can be determined by comparing the test results to threshold values set by the operating company.

Unlike DTSR, which is preset to record all delays of more than three seconds, the delay threshold for RADR is definable. The delay threshold is defined in table RADR, where you can also define the receiver type to be monitored. Calls delayed by more than the specified time are recorded in OM group RADR.

NOTE: Activating RADR for line receivers may affect OM groups DTSR and SITE, and cause dial tone delay for customers. Because both DTSR and RADR require receivers for testing, they may compete for the same receivers if they are both active at the same time.

SPMS

A performance results indicator—such as Nortel Networks Switch Performance Monitoring System (SPMS)—can identify weak areas of equipment performance when measured components exceed acceptable levels. SPMS should be used as a proactive maintenance tool but can be used after the fact as a corrective maintenance tool.

See the *Performance* section of this manual for information on SPMS.

DMSMON

DMS Monitoring (DMSMON) enables you to monitor performance, gather equipment data and various counts, and to compare the performance of a new software release in your office with the earlier version. Printouts provide a wide range of information about the system configuration and operation over a specified period. DMS-MON is available on all DMS-100 Family systems. For more detailed information on this feature and its commands, see the "DMSMON" subsection within the *Performance* tab of this manual

Node assessment graph (NAG)

The node assessment graph (NAG), an hourly log (NAG400) showing nodes that are out of service or are experiencing routine exercise (REX) problems. To qualify for inclusion in the report, a node must have a REX problem or be in one of the following states: system busy (SYSB), C-side busy (CBsy), in-service trouble (ISTB), or manual busy (MANB). REX problems that trigger a log are a failed, aborted, or incomplete REX test or a condition where the REX test is turned off. A total count of all off-line (OFFL) nodes appears at the end of the report. In addition to the logs, the feature can also provide the same information through a command interface (CI) NAG command.

Technicians can use the snapshot of problem areas—provided by this feature—to quickly identify trouble spots and take corrective measures.

Following is an example of a NAG400 log report:

```
NAG400  JUN20  11:09:08 5800   INFO Node Assessment Graph
Front End Load: BCS36CJ
CM:     .   /        MS:     .   /         IOD:   .   /         Net:    .   /
PM:     .   /        CCS:    .   /         Lns:   .   /         Trks:   1 GC/*C*
Ext:    .   /        APPL:   .   /
CI:
        Front End Load:  BCS36CJ
        Level    Node        Status REX INFO          Unit 0 Unit 1
        --------------------------------------------------------------
           CPU     1         ACT
        CM                   NORMAL
        MS                   NORMAL
        IOD                  NORMAL
        NET                  NORMAL
        PM  DTC     0        .      FAILED                .       .
            DTC     1        .      FAILED                .       .
            DTC     4        .      OFF                   .       .
            LGC     0        .      FAILED                .       .
            LGC     3        .      OFF                   .       .
            LTC     0        .      FAILED                .       .
            LTC     1        .      FAILED                .       .
            SMS     0        .      FAILED                .       .
        Offline Node count: 4
```

Switch status report (SSR)

The switch status report (SSR), provides a concise readout showing call originations, call traps, and other indications of switch status. The default SSR600 log, which can be generated every 15 minutes, is a useful tool for spotting potential problems in the switch. Along with a report on current switch conditions, SSR logs also produce readouts on conditions during a previous 15-minute reporting interval and on average conditions for that time of day. Besides providing the default logs, this feature also allows network provider personnel to define additional SSR log reports based on OM calculations. For more information, start with a HELP SSR command at the CI level.

Following is an example of an SSR600 switch status report:

```
SSR600 JAN20 08:47:08 5800 Switch Status Report

Current data reported from Jan-01 8:32 to Jan-01 8:45

                                               00:14    00:15    00:15

Name         Description                        CURR     PREV     AVG

-------------------------------------------------------------------------

TOTAL_TERM: Combined line and trunk terminations  5831     3507     4243

BLKD_CPRES: Blocked calls due to no CP resources     0        0        0

TOTAL_ORIG: Combined line and trunk originations  7102     5966     5426

BLKD_MISC:  Miscellaneous blocked calls             33        3       27

TRK_INC:    Incoming calls (trunk originations)   3442     3010     2265

DROPPED:    Established calls dropped by system      2        0        0

LINE_ORIG:  Line originations                     3660     2956     3154

CP_TRAPS:   Call processing software traps          0        0        0

TANDEM:     Trunk to trunk calls                   167      122      123

CP_SUICIDE: Call processing detected software errors  0       0        0

INTER_OFC:  Line to trunk calls                   1720     1312     1551

1TRIALFAIL: First trial failures (no network path)   0        0        0

INTRA_OFC:  Line to line calls                     678      402      551

CPU_OVERLD: Minutes of CM (CC) overload             0        0        0

PSIG_PDIL:  Permanent signal/partial dials          43       35       41

PM_OVERLD:  Calls denied due to peripheral overload  0        0        0

CALL_CAP:   BRISC average call processing capacity   0       17        0

SYSB_PM:    PM transitions to SYSB w/o CBSY first     0        0        0

NONCP_TRAP: CPU traps excluding CP traps             0        0        0

MANB_PM:    PM transitions to MANB from IS or ISTB    0        0        0

SWER_LOGS:  SWER log count                           0        0        0

C7MSU_TX:   CCS7 MSUs transmitted and terminated  26422    14777    17259

C7LNK1_ERR: CCS7 link sync and link error counts     0        0        0

C7MSU_RX:   CCS7 MSUs received and originated     26422    14777    17258

C7RS_ERR:   CCS7 routeset congestions and failures   0        0        0

AMA_RECS:   Count of AMA records generated        2312     1452     1835

ORIG_CHG:   Percent Chg of TOTAL_ORIG from last Rprt  27       45       31

-------------------------------------------------------------------------

TRK_LOW_1:  Trunk with most failures          ACME0205T321            1

TRK_LOW_2:  Trunk with 2nd most failures      ABCD0205T321            1
```

DISPCALL & SHOWAUD Commands

Analysis Application

The Display Call (DISPCALL) feature, when turned on, captures all available data associated with the death of a call. This includes: software and hardware resources used on the call, originating and terminating terminals of the call, and digits listed. The output provides network paths used and shows all translation data and tables used for the call.

The following are general guidelines for using DISPCALL:

1. The analysis approach is to look for missing or corrupted data on a repeating equipment unit; therefore, retention of hard copy DISPCALL outputs is recommended for this analysis.

2. A quick translation verification (TRAVER) should be made on the called number (see CALLED-DR on DISPCALL output) to verify that translation information is complete.

3. The NetInteg MAP level should be used to analyze any repeating Network Module (See PATHEND on DISPCALL output) for defective cards.

4. When all efforts have been exhausted to find a problem locally, and the problem has been determined to be service affecting, the problem should be escalated through the control center, and as needed, the NT-Regional Support group or TAS support.

Technical Assistance Manual TAM-1001-003, *DISPCALL User Guide*, provides instructions for the use of DISPCALL (approximately 70 pages).

Recommendation: After becoming familiar with what DISPCALL can provide, it is recommended that the advantages of the CI level SHOWAUD command be evaluated.

Formatted output

DISPCALL is a tool that displays popular call processing data areas in a formatted form. This speeds up the task of debugging since the chore of conversion from hex to symbolic is done for you.

DISPCALL is a CI increment found in all loads. It can be used to take *pictures* of calls and print them in a formatted form. There are several ways to take these pictures. One is to save the call data when the call *dies* (see the death command).

Another is a command entered manually that saves the call data at that instant (see the SAVETID and SAVELEN commands). The last is to call one of the procedures in CDUMPUI at the point the picture is to be taken.

DISPCALL is entered by typing the command DISPCALL at the CI level. While in DISPCALL, the prompt will be "DISPCALL >." DISPCALL can be exited by the command QUIT.

DISPLAY CALL (DISPCALL)
(Suggested Utilization Guidelines)

Purpose:
To analyze trouble conditions causing call deaths and audit log messages AUD395, AUD398, AUD414, and AUD416

Recommended Operation:
Set CCB, CDB, EXT, PRDT, UMPROT, and MBUFF to 10
Set DEATH ON (to run feature continuously).
As required, QUERY DISPCALL to determine how many buffers are in use.
Show (to obtain hard copy of) all in use buffers.
Retain hard copies for trouble analysis.
CLEAR buffers for storing more failures.

Activation:
This feature should be left in continuous operation and periodically copied, analyzed, and buffers cleared. This will provide a continuous record of call deaths in the office.

DISPCALL commands

While in DISPCALL, the following commands are available:

HELP	Displays brief information and syntax of the command
QUIT	Quits from the DISPCALL environment
SET-	Set various parameters
SHOW-	Display saved calls
SAVETID-	Save a call based on TID (The terminal ID of the agent) (see note)

SAVELEN	Saves an active lines CCB and protected and unprotected data
CLEAR-	Clear all buffers
QUERY-	Query the status of various things
DEATH-	Set call death parameters
FREE-	Free allocated buffers
DISPTID-	Convert TID to CPID (call processing ID, the two-word identifier used to identify a member of an agency. It consists of a CP (call processing) selector and an agent identifier).

NOTE: Using the command SAVELEN with the SITE NAME and LEN number performs the same function as the command SAVETID, on the line side.

A brief description of some of these commands follows:

SAVETID

This is the command used to take a snapshot of the call. The call is specified by supplying the TID of an agent in the call.

The various parameters are:

    Parms: <NODENO>   (0 to 4095)
    Parms: <TERMNO>   (0 to 4095)

CLEAR

Clears the buffers of their contents.

QUERY

Displays the number of buffers allocated and the number in use and the current setting of the *death* parameters.

DEATH

Enables/disables collecting of data when a call dies. The various parameters are:

    Parms: <Optn>   ON   — Save the call death.
                    OFF   — Does not save the call.
                    PUP ON   — Save the protected and unprotected data
                    PUP OFF   — Do not save the protected and unprotected data

NOTE: Saved data includes CCB, Extension blocks, protected and unprotected data for agents, and CDB.

SEARCH ON — Search for agents linked to the call
but do not appear in any port in the call
SEARCH OFF — Do not search for agents linked to the call

SET

This command is used to allocate the buffer needed to save the call data.
The various parameters are:

<TYPE>   EXT <NUM> (0 to 34) — Extension Blocks
CCB <NUM> (0 to 30) — Call Condense Block
CDB <NUM> (0 to 31) — Call Data Block
MBUFF <NUM> (0 to 600) — Message Buffers
PROT <NUM> (0 to 20) — Protected terminal table
UNPROT <NUM> (0 to 17) — Unprotected terminal table

SHOW

This command is used to display the collected data.
The various parameters are:

Parms: <What> Call   Display all buffers containing data belonging
to the given call
CCB   Display the given CCB
CDB   Display the given CDB
Ext   Display the given ext block
Prot   Display the protected data
Unprot Display the given unprotected data
P1P   Display port1 permanent data for the CCB
P2P   Display port2 permanent data for the CCB
<Which> 0 to 255
Which indicates the buffer number to be diplayed. Buffers are filled from 0 upward. The query command indicates the number of buffers used.
<Format> H (H = hex)
F (F = formatted)

FREE

Frees all allocated buffers

DISPTID

Converts a TID to text.

Parms: <NODENO>   (0 to 4095)
<TERMNO>   (0 to 4095)

SHOWAUD Command

This tool is used to display audit log dumps of CCBs, CDBs, and EXTs in text format. Simply specify the file name containing the audit logs and the data is then formatted and displayed. The SHOWAUD command should be run on the same node (CM or SVR7) that generated the AUD log. If the AUD log is generated on the SVR7 and the SHOWAUD command is run on the CM, then a TRAP will be generated.

Note: You might have to erase RECORDFILE (>ERASESF RECORDFILE) in store file before using.

SHOWAUD <filename> <ALL> displays audit log dumps of CCBs, CDBs, and EXTs in symbolic format

Following is a sample procedure for using SHOWAUD:

>LOGUTIL

>RECORD START ONTO SFDEV

>OPEN AUD
find AUD logs (i.e. AUD395, AUD398) using BACK and FORWARD commands

>RECORD STOP ONTO SFDEV

>LISTSF
list storefile to verify that RECORDFILE exists.

>SHOWAUD RECORDFILE ALL
displays audit log dumps of CCBs, CDBs, and EXTs in symbolic format

LEAVE or QUIT
leaves or quits LOGUTIL.

Data Grooming DMS-100F Networks

Description

The DMS-100 switch default for XPM_PARITY_THRESHOLD is 20. This is an acceptable value for voice service. This default value allows the switch to report consecutive PCM parity faults that endure for 800 milliseconds, on a per channel basis.

A XPM_PARITY_THRESHOLD value = 20 is acceptable for voice grade service, however, it is not satisfactory for data grade service.

Data grooming involves lowering the XPM_PARITY_THRESHOLD, and clearing faults until a value of 1 is achieved. In effect, this causes the switch to react to any parity faults in a 40 millisecond period, within an XPM channel. This is an ongoing program and must be maintained by performing BER/BERP tests and monitoring parity faults on replaced circuit packs. Nortel Networks recommends that all operating companies perform data grooming in switches that support ISDN, DataPath, or wideband data. If the DMS switch has not been groomed for high-speed data transmission, or is not maintained at the required integrity/parity error level after grooming, customers may experience data troubles that could be very difficult to isolate and resolve.

The parameter XPM_PARITY_THRESHOLD is found in table OFCSTD and sets the default parity threshold for XMS-based Peripheral Modules (XPMs) after reloads and cold starts. Parameter XPM_PARITY_THRESHOLD determines the threshold of parity errors that are required (40 milliseconds x XPM_PARITY_THRESHOLD) in a consecutive time period, to invoke corrective activity by the PM (e.g., transfer to the other network plane and initiate diagnostics). This assumes that no FILTER is in effect.

The FILTER command allows operating company personnel to query or set the threshold on a specified PM basis. Use the FILTER command to set the parity threshold for failing XPMs only. FILTER, is a non-menu command that is part of the NETINTEG level. Filter alters the integrity or parity error threshold level (or both) in the specified XPM. When this command reduces the threshold value, the problem identification sensitivity increases.

For further information on data grooming a DMS-100F switch and the use of various tools to maintain the DMS-100F switch at the proper level for data, see the Preventive

Maintenance tab and the "Network Maintenance" subsection. Also, Data grooming for ISDN.

ENET

The Enhanced Network is a single-stage, non-blocking, constant delay, junctorless time switch that supports narrow band services as well as services requiring bandwidth greater than 64 kilobits per second (kb/s). With the constant delay and independence of the traffic load, ENET can support wideband services (n by 64 kb/s switching), such as videoconference, image transfer, high speed FAX, and private-line backup.

ENET is compatible with all DMS-100F PMs, including the fiber Series II PMs. You can convert series II PMs to connect to the ENET through DS512 fiber links. An example of a series II PM is a digital trunk controller (DTC).

XPM PCM parity and integrity

Frequently Nortel Networks documentation refers to XPM parity without making a distinction. There are two kinds of XPM parity failures, and they are quite unrelated. To avoid confusion we will differentiate by including "memory" or "PCM" in the name.

Memory parity

The primary way that the CC informs the operating company personnel that there is a XPM memory parity fault is the PM181 log. These faults are distinct from XPM PCM parity, and are not associated with data grooming.

PCM parity

The primary way that the CC informs of a parity fault detected in the PCM channels is the NET100 or ENCP100 log. Data grooming is all about elimination of PCM channel parity failures.

PCM channels

ENET is a channel-matrixed time switch that provides PCM voice and data connections between XPMs. All PCM channels through the network are 10-bit speech. Eight bits are voice, the ninth bit is CSM, and the tenth bit is a parity bit representing an EVEN parity calculation of the other nine bits.

The CSM comprises a repeating 40 bit CSM frame made up of a 24 bit framing pattern (the CSM bit is equal to 1 for 24 frames), 8 bit integrity value, and 8 bit CDB value (Call Data Byte is used to pass specific call information). On a single PCM channel 40 frames contains:

- 40 bytes containing PCM samples
- 40 parity bits

•40 bits where 24 framing bits=1, 8 bits integrity byte, and 8 bits CDB

The CSM and parity bits are generated on the 6X42 card and are transmitted toward the C-side, through the network (ENET), and received on the 6X42 card of the other XPM (or same XPM) involved with the call path.

XPM PCM parity

The intent of parity bits is to detect any bit errors over the network path between the two XPMs involved in the call path. Software scans and clears the parity bits every 40 milliseconds, which is the equivalent of every 320 frames (40 milliseconds/125 microseconds per frame) on a per channel basis to see if any network PCM parity errors have occurred. Parity is checked every frame time. A parity error is latched in the 6X42 hardware, indicating that at least one frame in 320 frames has had a parity error.

In table OFCSTD, parameter XPM_PARITY_THRESHOLD is the filter value for parity errors, indicating the number of software cycles that a parity error must be present for a network PCM parity error to be reported. The initial default value is 20, meaning that the XPM must see a parity error indicated for 20 consecutive software scan cycles (20 * 40 milliseconds = 800 milliseconds). This threshold can be set as low as "1". If the threshold is met, the ENCP100 PARITY error indication log is output and the XPM will switch planes to receive PCM from the other plane of the network. If the other plane is unavailable (SysB, ManB, etc.) or the XPM cannot establish integrity due to network link faults, the call is taken down.

XPM PCM parity failures are hardware failures in the PCM or CSM channel. Marginal cross point cards in ENET or dirty optical connectors in Series II peripherals have been identified as some possible causes of these parity failures.

Recommended procedures for cleaning optical connections can be found in the "Trouble Repair" section of the "Corrective Maintenance" tab of this document.

WARNING Nortel Networks does <u>not</u> recommend indiscrimately cleaning optical connectors, as this may cause serious service impairment. Clean optical connectors only after all other corrective maintenance procedures fail to clear the problem. Cleaning optical connectors should be performed by following all recommended cleaning procedures, safety policies, and safe time policies.

XPM integrity

The intent of the integrity value is to allow the XPM to ensure that the network is providing and maintaining a proper connection between the XPM path-ends.

Upon call setup, the XPM receives a transmit CSM and expected CSM value from the CC. The transmit CSM value equals the expected CSM value that the other XPM path-end is given. Software then scans the integrity match bits every 40 milliseconds (it alternates parity and integrity checking every 20 milliseconds) to check that integ-

rity still matches. As only one integrity value is sent/received every 40 frames, there are effectively eight integrity checks (40 milliseconds/125 microseconds per frame/40 frames per integrity value). However, integrity is not latched, meaning that if integrity does not match for seven CSM frames but does match on the eighth CSM frame and software scans at that time, integrity is good. This is likely done to prevent parity bit errors from making integrity look bad if an integrity bit is errored.

Parity detects bit errors and integrity indicates if the network path between the call's XPM path-ends is good or bad (i.e. no physical connection).

As with parity, integrity checking also has a filter value normally set to a default of 12 (12 * 40 milliseconds = 480 milliseconds). It does not appear that the XPM_INTEGRITY_FILTER value can be datafilled, as it seems to be soft coded to a value of 12 in XPM CM software. However, it can be manually read and set for a given XPM unit with the FILTER command at the NETINTEG level of the MAP. Nortel Networks does not recommend setting XPM_INTEGRITY_FILTER to any value other than 12.

Integrity failures are most likely software problems. However, they can be caused by hardware or software, and are influenced by office load.

Network integrity

This explanation is somewhat redundant, but is included to help clarify your understanding of integrity.

Prior to sending a Switching Network connection control message, the central control processor informs each PM of the integrity value to be received from the other PM. These values can be different. The control component selects integrity values on a per-connection basis. Therefore, each connection gets a different integrity value (by cycling through the existing 256 values, some of which are not allowed). Since there are delays in the completion of the various functions on call connection, the integrity byte allows each PM to verify that a connection has been established before proceeding with its call processing function.

The integrity digit is checked to ensure that a connection continues to exist for the duration of the call. Since a large amount of PM hardware and software is involved in the transmission of the integrity byte, the functioning of the PM is verified with integrity value continuity. In addition, since each call connection is assigned a different integrity value, software error occurring in the Switching Network path selection, which overwrites an existing connection, will be detected through a change in integrity value.

Since the Switching Network connection provides a duplicate path (plane 0 and plane 1), the Central Controller processor also tells the PMs which plane is the "preferred plane." PMs transmit over both planes. However, they accept only PCM signals from the preferred plane, but this is different for each call (that is for each connection).

Since the Switching Network operates in "duplex" mode, that PMs have access to a duplicated link and a duplicated Switching Network plane. Upon loss of integrity or parity, a PM switches activity to the mate link and attempts to reestablish integrity with the other PM. A link or Switching Network hardware fault is recoverable since a duplicated path is available; therefore, there is no loss of connection. Loss of connection can be caused by logic errors or by PM hardware failures.

For more information refer to *DMS SuperNode Technical Specification BCS36 and up,* PLN-5001-001.

PCL upgrade impact through LEC0014

PM firmware impact on parity

There are no 88k firmware changes that affect parity of the PCM byte. The MX77 pack has firmware, the rest don't (6x41, etc are C-side entirely driven from software).

CC software impact on parity

Parity is primarily affected by hardware. However, it is possible that software may affect timing and the interaction of hardware and software. New PCL software may affect parity testing sensitivity, thus allowing existing marginal packs to be detected.

In LEC0011 software, XPM assembler was translated to C-programming. This was done to facilitate processor upgrades in the XPMs. This has been thoroughly tested and in release for a few years. Problems associated with the recoding would affect all Series I & II peripherals. A recoding software problem would show on all peripherals evenly (i.e. SMU, LGC, LTC, DTC, ISDN versions (LGCI, LTCI, DTCI), DTC7, and SMS) and would appear globally in all DMS-100F products with XPMs. There is no evidence of a LEC0011 software problem globally.

One operating company has reported DMS-100F switches on LEC0011 have an increased sensitivity to marginal cross point cards or dirty fiber connectors. The problem was corrected by data grooming the offices.

CC software induced integrity failures

CC software problems can create integrity failures if correct protocols are not followed. The system does not always report integrity failures on the call that first set up the network path. For example, a call is set up between call A and call B. At the termination of the call, call B can continue the search for integrity. According to CC software, the network connections are free, but the network hardware connection is not released. When a new network connection is established, the connection can use that same network path again or part of that network path again. This connection disrupts the CSM from the previous call. If the original endpoints are not part of the new call, the result is a NET101 log. The result is a NET101 log because the PM port and channel do not have a connection. The channel reports the integrity failure. If one of the original endpoints is part of the new call, the result is a NET102 log. When the

integrity failure report generates, the new connection is in the CC software MAPs area.

There are no known issues with CC software that affect data grooming.

PM software induced integrity failures

Maintenance actions on a PM, or messages to a PM lost during call assembly or disassembly, can result in integrity failures. Commands to transmit an integrity value or commands to look for integrity are part of other call set up functions. Because commands are part of other call set up functions, lost messages cause failures in other aspects of call set up. Slow mapping of the CSM to one end of a call causes a failure mode that results in NET101 logs. When CC receives an on-hook message, CC releases the network connection. With the connection free, the connection is available for use again by another call. The CC receives and processes the on-hook message, and the original network connection is available for use again. An integrity failure generates if two conditions occur at the same time. One condition is if the call at the other end did not receive a request to stop looking for integrity. The second condition is if another call uses part of the original network connection again.

During a call set up that can be on a separate PM, the PM receives instructions to transmit a specified integrity value. According to traffic and message loads, delays in the CC, network, PM, or processing of these messages can occur. If long delays occur, one PM can start to look for integrity before the second PM transmits the new integrity value. The system generates a NET101 or NET102 log report.

There are no known issues with PM software that affect data grooming.

Mishandled calls

The call completion rate for a DMS-100 Family System is equal to or greater than 99.99% (no more than one call in 10,000 mishandled). A mishandled call is a call attempt that arrives at an incoming port of the switching system, but was mishandled due to a hardware and/or software error. Three results are expected:

- Misrouting
- Premature release by the switching system
- Switching system transmission failure as detected by a continuous parity check.

Calls that cannot be completed due to the unavailability of engineered equipment are not included in this definition unless the congestion is caused by a system or subsystem fault or error.

For more information refer to *DMS SuperNode Technical Specification BCS36 and up,* PLN-5001-001.

Tips

If you experience parity failures after an upgrade, did you have integity failures the day before upgrade? Marginal crosspoint cards would also explain integrity problems. If you are experiencing both parity and integrity failures this would indicate marginal cross point cards exist.

Integrity failures are worse than parity failures.

Parity failures detected during callsetup are not service affecting.

Integrity can be affected by busy hour, is the problem affected by office load?

Every 6.5 minutes CSMDIAG diagnostics are run in XPMs on 6X42 cards.

6X40 and paddle boards are not tested from XPM (cannot loop back to itself), they must be tested from ENET.

Look for problems in the network first, then investigate software.

The NET test is the only path test option that allows you to test a fiber end. The NET test is also the only test option that allows you to test all 512 channels of a DS512 fiber link.

Attachment A contains an example ENCP100 log message. Use the "to" and "from" data to develop a pattern, and identify the source of the failure.

Keep good records of the packs that you change while data grooming. The failing packs should be labeled as "Data Grooming" and returned for repair.

Keep good records of all network repair activities. Office data grooming is an ongoing process. As packs are changed in the network, pay particular attention to parity and integrity logs. An increase in failures may be due to a recent pack replacement.

Exhibit A   Typical ENCP100 log

```
ENCP100 JUN04 07:19:43 2140 INFO ENET Integrity Fault
Call State: CALLSETUP     Fault: PARITY
ICTS Connection: NO
From:  Plane: 1 Shelf: 00 Slot: 14 Link: 02 Channel: 006
To  :  Plane: 1 Shelf: 00 Slot: 13 Link: 17 Channel: 459
From:  PM: MTM 43  Active Unit: 0 Number of Units: 1 Terminal: CKT     CF3P 1130
To  :  PM: LGC 4   Active Unit: 0 Number of Units: 2 Terminal: LEN HOST 18 0 13 22  DN 8776147  KEY  1
Conn Verified:   Pass
Remade:          No attempt
Conn Reverified: No attempt
Fault Found:  None         Slot at Fault: None
Mtce Enabled: No           Slot at Mtce:  None
Diagnostics Submitted: No, channel reserved.
```

The significance of each field is:

- ENCP100 indicates that the connection does not go out-of-service because of the fault

- Integrity fault detection detected parity fault during the CALLSETUP state (the call was up prior to the failure)

- Fault indicates that the XPM_PARITY_THRESHOLD was reached

- ICTS Connection indicates that the log was not caused by the integrity check traffic simulator

- Analyze from and to equipment to identify a suspect XPM or ENET component

- The system verified the connection

- No attempt to remake the connection was necessary

- No attempt to reverify the connection was necessary

- No fault was found, therefore no slot at fault

- Maintenance is disabled, therefore no slot

THIS PAGE INTENTIONALLY LEFT BLANK

TOPS Overview and Maintenance

This subsection provides a Traffic Operator Position Systems (TOPS) summary overview, and maintenance related topics for MP, MPX, MPX-IWS, TOPS ISUP, and TOPS IP. Documentation references are provided for those that need more detailed information on the topics presented. Information on TOPS maintenance follows the overview.

TOPS overview

What is TOPS?

TOPS provides the interface—when required—between telephone users and the services supplied by the telephone operator. TOPS is a highly mechanized system, performing many of these tasks automatically, some without any operator intervention. The TOPS call processing system is integrated into a DMS-200 or DMS-100/200 switching system (a stored program control toll switch).

The growth of automation has made operator assistance services more effective than ever, in many cases completely eliminating the need for operator involvement in a routine call. However, there will always be a need for skilled, thoughtful operators to deliver the customer care that only a person can provide.

To get a better understanding of all the TOPS services that are available, see TOPS optional services starting on page 4-3. Also, it is suggested that Nortel Networks *Directory and Operator Services Planning Guide* be referenced.

Operator assistance services

Operators commonly provide the following types of assistance and services to business and residential customers:

- Completing local, interLATA, intraLATA, national, and international calls
- Billing (third-number, collect, person-to-person, calling card) for calls
- Processing calls for which the customer requests quoting of time and charges
- Processing calls for which the customer requests additional information
- Processing calls that require trouble reports and charge adjustments
- Processing calls that originate from public coin telephones

- Completing emergency calls
- Processing calls for which the customer requests specialized assistance (i.e., verification and/or interrupt of a busy line, emergency assistance, etc.)

Directory assistance (DA) services

Directory Assistance (DA) service allows a caller to request assistance from an operator in looking up a directory number. Rather than dialing "0," the caller dials, in North America, one of the following: 411, 1-555-1212, or 1-NPA-555-1212. Internationally, callers dial access codes as determined by service providers.

The DA call is presented to the operator on a screen that immediately identifies the call as a DA call. In a basic call scenario, the operator gets the necessary information from the subscriber and initiates a DA database search. The DA database returns all listings that match the search criteria. In basic DA, the operator selects the appropriate listing and quotes it to the caller. If DA is optionally configured to include back-end automation, the operator releases the call to an audio response unit that quotes the requested number to the subscriber. Front-end automation is also available. This capability expedites the collection of information from the caller and minimizes the time required for the operator to obtain the correct listing. In some cases, DA calls may be completely automated. Automated call completion is also available in conjunction with all types of DA calls, and provides a new source of potential revenue for service providers.

Enhanced directory assistance services

Enhancements to Nortel Networks Directory One DA offering include: Directory Assistance Call Completion (DACC), which gives subscribers the option of having their call completed to a requested number, for an additional charge; Quest411, Nortel Networks national DA service, which provides ready access to more than 120 million listings; and the forthcoming Global Database Access, which provides a gateway for service providers to search a variety of databases without encountering problems of language, database type, or search strategy differences.

Automated directory assistance services (ADAS)

Automated Directory Assistance Services includes Automated Directory Assistance Call Completion (ADACC), ADAS Base, and ADAS Plus.

ADACC offers callers automatic connection to the requested number after the listing is located. After the requested listing is provided, callers can choose to let the switch complete the call without having to dial the number.

ADAS automates the greeting and inquiry portion of the directory assistance call— "What city?" "What listing?" — to reduce operator work time and costs.

ADAS Plus carries that automation a step further with bilingual speech-recognition technology, using Nortel's industry-leading Flexible Vocabulary Recognition technology.

Intercept services

Nortel Networks call intercept services portfolio includes Basic Intercept, Enhanced Intercept Services, and Automated Intercept Call Completion (AINTCC).

Basic Intercept is a database-driven service that provides status information on out-of-service telephone numbers. In the most common application, when a subscriber's phone number changes, the old and new numbers are entered as records in an intercept database. Calls placed to the old number are routed to the switch, which automatically queries a database, which returns the new number. An announcement of the new number is delivered to the subscriber by an operator or an audio system.

Line Information for Open Networks (LION), resides on a separate platform, and provides enhanced intercept services. LION Intercept enables customized announcements to be created that include information about the called number or party.

Automated Intercept Call Completion (AINTCC) is based on the TOPS switch and the LION platform. Feature NC0146 provides Automated Intercept Call Completion (AINTCC) and routes invalid calls to a specified directory number (DN), as datafilled in the database.

TOPS switch

A key element of the public telephone network is the DMS TOPS switch, which can support over 1,000 operator positions that can be divided into numerous operator teams. The DMS TOPS switch is equipped with TOPS software, capable of processing 120,000 operator/agent calls per hour.

The switch—housed in six-foot metal cabinets with double doors front and rear—provides central processing, messaging among processing components, switching, maintenance, and billing. It is also a multicomputing platform for CCS7 (Common Channel Signaling No. 7) and advanced data processing applications, and provides interfaces to peripheral processors, subscribers, and other switching systems.

Peripheral modules (also housed in six-foot cabinets) perform signaling supervision, certain message-handling control operations, maintenance, and billing functions. Line cards and trunk circuit packs reside in peripheral modules, and interface voice and data lines and trunks to the switch. Connections between subscribers and operator/agent service centers are made through peripheral modules. A closely linked multiservice processor, the Link Peripheral Processor (LPP), cost-effectively supports advanced applications. All of this is managed through the Maintenance and Administration Position (MAP) which provides a "window" to the switch and its peripheral modules.

TOPS optional services

Primarily, TOPS optional services are enhancements that can reduce work time associated with TOPS operator tasks. Selected optional services are listed below, and highlighted in the following paragraphs:

- Automated Directory Assistance (ADAS)

- Automatic Coin Toll Service (ACTS)
- Automatic Alternate Billing Service (AABS)
- Mechanized Calling Card Service (MCCS)
- Exchange Alternate Billing Service (EABS)
- Automatic Calling Card Service (ACCS)
- Operator Reference Database (ORDB)
- TOPS closedown.
- TOPS InterLATA Carrier Service (TICS
- Automatic DA Call Completion (ADACC)

TOPS has additional capabilities that cannot be classified as services, but do offer cost savings associated with call processing and administration. In addition, some of these capabilities provide the necessary platform to provide one or more of the services listed above. Some of those capabilities are as follows:

- Operator Centralization (OC)
- TOPS Equal Access (EA)
- Exchange Access Operator Services Signaling (EAOSS)
- Equal Access Feature Group D (EAFGD)
- Extended Bellcore Automatic Messaging Accounting (AMA) format (EBAF)
- Position sanity timer
- Queue Management System (QMS)

Following is a brief description of some of the services listed above—including the Operator Centralization (OC) capability. For further information on services and capabilities for TOPS systems, see volume 4 of PLN-8991-104, *Provisioning Guides*.

Automated Directory Assistance Service (ADAS)

Automated Directory Assistance Service (ADAS) automates the initial greeting and inquiry portion of directory assistance call processing. By involving the operator only after this information has been received, ADAS trims approximately two to four seconds from the length of each call. ADAS is built on Nortel Networks experience with AABS—as a voice processing service—and fits into a family of similar services, such as voice mail, message delivery, and interactive automatic call distribution.

ADAS is the first application developed for the voice process platform (VPP), VPP is a software platform which supports enhanced voice and data service applications and is integrated with a DMS SuperNode switch.

ADAS is the first automated service which does not require automatic number identification (ANI), this feature is accomplished by datafill.

Automatic Coin Toll Service (ACTS)

The ability to handle calls from coin telephones is part of the TOPS system base functionality. Automatic Coin Toll Service (ACTS) allows the operating company to automate the handling of 1+ dialed calls from coin telephones.

With ACTS, the subscribers can place 1+ seven-digit or ten-digit calls from coin telephone stations without operator assistance. After dialing the digits, the subscriber is prompted by a digital recorded announcement machine (DRAM) to make the necessary coin deposit. ACTS keeps count of the coins deposited. When the necessary deposit has been made, ACTS DRAM plays a "Thank You" announcement and the called number is outpulsed.

The Coin Detection Circuit (CDC) is a necessary part of Automatic Coin Toll Service (ACTS). The CDC is an NT3X08AB digital tone receiver pack that counts the coins deposited from coin operated telephones and reports the amount collected to the DMS-100 call processing programs.

The NT3X08AB card physically occupies one card slot in an MTM. However, the next three slots must be left vacant. An MTM can support a maximum of three NT3X08AB cards. Altogether, they can support 24 simultaneous coin station calls.

The NT3X08AB card determines coin types by analyzing on and off patterns of the tones generated as the coins are deposited. It counts coin collection data and reports the amount collected to the call processing programs.

The NT3X08AA uses a dual-frequency tone in a predetermined on/off pattern to distinguish one coin type from another. The two dual-frequency tones are shown in Table 4-1 below. Table 4-2 lists the on/off patterns per coin type.

Table 4-1 — Dual frequency tones

Frequency	Minimum dBm Level
1537 Hz + 2200Hz 2.5%	28 dBm
1700 Hz + 2200Hz 2.5%	28 dBm

Table 4-2 — Coin-type on/off patterns

Coin	Tone duration	Silent interval
Nickel	35–160 ms	> 160 ms
Dime	35–160 ms	25–160 ms
	35–160 ms	> 60 ms
Quarter	20–100 ms	20–110 ms
	20–60 ms	20–60 ms
	20–60 ms	20–60 ms
	20–60 ms	20–60 ms
	20–100 ms	> 60 ms
Dollar	600–700 ms	> 60 ms

Automated billing service

Automated billing service allows the operating company to verify billing for a call with minimal or no operator involvement. On the TOPS MP system, there are two types of automated billing services:

- Exchange Alternate Billing Service (EABS)
- Automated Alternate Billing Service (AABS)

EABS automates the billing verification process for collect and third-number billed calls by querying a Line Information Database (LIDB) to determine if billing is allowed, conditionally allowed, or not allowed.

AABS is very similar to EABS; however, besides obtaining billing verification, it also obtains billing acceptance without involving an operator in cases where the billing verification results in a conditional acceptance of billing. For example, on a third-number billed call, the database query indicates that acceptance of charges must be obtained for any calls charged to that number. AABS will connect to the third (billed) number and obtain billing acceptance from the third party without involving the operator.

Calling card service

Calling card service is a service that allows a subscriber to dial a local or toll call and charge it to a 14-digit calling card number usually provided by the operating company. For example, a subscriber dials 0+ 10 digits from a coin telephone. A "bong" type tone prompts the subscriber to input their calling card number, or they can dial 0 for an operator. If the subscriber chooses to input their calling card number, and if all numbers are valid, the call is completed and billed to the calling card number.

On the TOPS MP system, there are two types of calling card services:

- Mechanized Calling Card Service (MCCS)
- Automatic Calling Card Service (ACCS)

The only differences between these two services are the type of database they use to perform the queries and the signaling format and protocol used for these queries.

NOTE: The MCCS service uses CCS6 common channel to access the BVN database. Both database and signaling were discontinued in December 91.

NOTE: MCCS and ACCS are stand-alone features. Calling card service is embedded in the EABS and AABS automated billing services. ACCS can be engineered as a backup for AABS.

Calling card service in features MCCS, ACCS and EABS are transparent to the subscribers, since they present no change in their operation. Throughout the process, the subscriber has the option to access the TOPS operator.

Operator Reference Database (ORDB) interface

The Operator Reference Database (ORDB) interface is an optional TOPS feature (NTXA20AA for the TPC and NTXN84AA for the host switch).

It is a database that stores information such as dialing instructions, rating information, emergency numbers, city to NPA conversion information, and so on. Currently, this information is available to the operator, but only through paper directories or a separate system. The operator has to flip through these directories, like flipping through a telephone book, to obtain required information. With an ORDB, this type of information is available to the operator through on-line database access.

TOPS closedown

TOPS closedown allows the operating company to consolidate all operator services at one central location (host office) during periods of light traffic. Essentially, what the operating company is doing with TOPS closedown is temporarily shutting down operator services at a switch, and rerouting the operator assistance traffic originating at that switch to a host switch that will provide the operator assistance.

When TOPS closedown is in effect, the subscriber and the operator are unaware that the other party may be in a different geographical area. For the operating company, TOPS closedown represents a more efficient way of handling operator service. TOPS closedown allows workforce requirements to be commensurate with traffic demands, thus reducing the cost associated with operators and maintaining separate host offices.

Operator Centralization (OC)

Operator Centralization (OC) allows the operating company to provide operator services for several offices from one central location. Refer to Figure 4-1 for an illustration of a sample office configuration.

From the point of view of the subscriber at the remote office, there is no noticeable difference in the way a call is handled. In addition, there is no difference in the way the call is handled by the operator. For the operating company, OC represents cost saving by being able to centralize all operator functions at one location, thus reducing the quantity of equipment required, the number of operators required, and the administrative cost associated with both.

Operator centralization establishes communication links between the remote offices and the host offices. These links are data links and voice links.

Figure 4-1 — Sample of OC system architecture
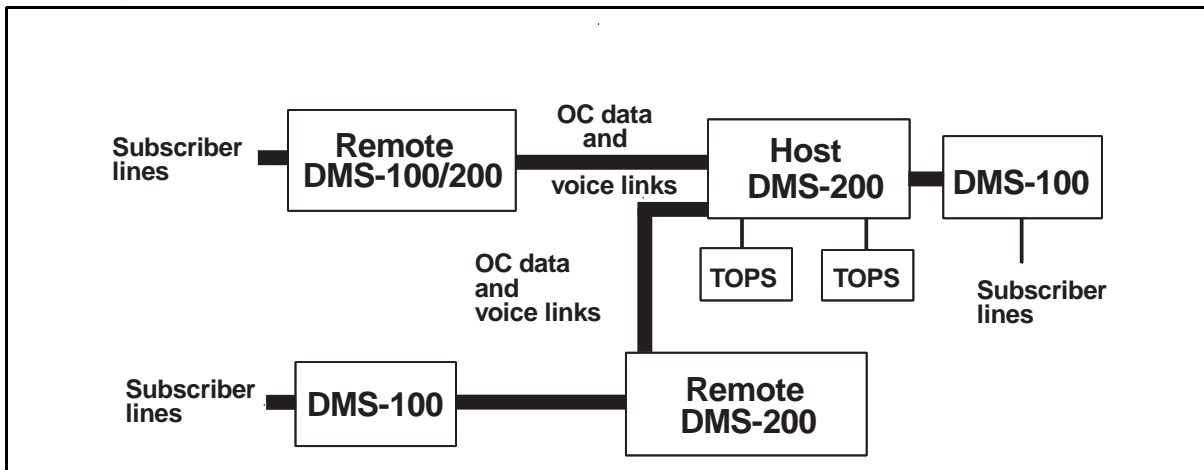
Queue Management System (QMS)

The TOPS system uses queues to manage calls requiring operator assistance. Calls can be assigned to queues based on information contained in trunk signaling, trunk-group identification, dialed digits, or data matched to QMS screening tables in the DMS switch.

The Queue Management System (QMS) is a software package that provides enhanced capabilities for the management of call and agent queues. With QMS, the switch can support up to 255 unique call queues, and up to 255 unique operator profiles that define the service capabilities of individual operators and teams.

Personal Audio Response System (PARS)

Personal Audio Response System (PARS) is an optional feature that offers the ability to supply customized challenge and prompts. These announcements use the voice of the operator occupying the position. The PARS equipment at the OSC is vendor-specific. It involves a PARS node cabinet that is cabled to each TOPS position and bridged to the headset jacks. The PARS node is connected to the host DMS via a MPC data link.

PARS provides custom announcements to a subscriber on call presentation to a TOPS position. The announcements, determined from the call attributes sent by the DMS to PARS, are given in the voice of the operator occupying the TOPS position. The playing of the prerecorded announcement allows the operator time to rest between calls, thus reducing the operator fatigue. The announcements also provide a consistency in the tone of voice on call presentation.

An example of a scenario with PARS would be as follows:

* A hotel call arrives at the TOPS position.

- From the call attributes sent to PARS from the DMS, PARS plays the following announcement: "Operator, can I help you?" Both the subscriber and the operator hear the announcement. This frees the operator from having to repeat the same phrase for all hotel call arrivals; thus, providing the operator a brief rest between calls.

- The operator then proceeds as normal for hotel call handling.

TOPS OSC administrative activities

TOPS administrative features provide traffic management, in the Operator Service Center (OSC), with the tools to determine staffing requirements, quality of service, and traffic volumes on a per-operator or per-group basis.

The TOPS position equipment is assigned in datafill to meet the following work functions:

- TOPS operator position
- TOPS service assistance position
- TOPS in-charge position
- FORCE Management position

TOPS equipment for administrative functions have been organized to meet single and multi-office configurations as follows:

Single traffic office operation

In a single traffic office operation, the operators and the force administration personnel are all administratively located in the same group or office. The minimal equipment normally found in a single traffic TOPS office includes the following:

- in-charge position
- service assistance position(s)
- operator positions
- System Administration Data System (SADS) TTY

Multi-traffic office operation

In a multi-traffic office operation, the operator work force is located administratively in different groups or offices and these offices are generally in different geographical areas. Each office is referred to as a traffic office (TO). The minimal equipment normally found in a multi-traffic TOPS office includes the following:

- force management position
- in-charge position
- service assistance position(s)
- operator position
- Force Administration Data System (FADS) TTY

- Traffic Administration Data System (TADS) TTY

TOPS OSC administrative tools and application

TOPS service assistant position

The TOPS Service Assistant (SA) position consists of the same screen, keyboard, and monitor controller as the operator position. An SA using a TOPS position can do the following tasks, among others:

- answer assistance requests
- page an operator or operator position
- initiate outgoing calls
- monitor operator positions

The areas on the service assistant position screen are the same as those for the toll and assist screen, except that there is a miscellaneous assistance status information menu in the right portion of the screen, overlaying the menu and list area.

TOPS in-charge position

Following are examples of the capabilities provided the in-charge supervisor using a TOPS position:

- all capabilities provided at the SA position
- special office monitoring capabilities
- special operator monitoring capabilities
- capability to accept or deny general assistance requests from operators

The in-charge position screen displays the following data:

- position number of the operator requesting assistance
- position number of the operator receiving assistance (steady)
- number of positions in the traffic office in the following states:
  - occupied
  - operator made busy
  - unoccupied position, call in progress
  - unoccupied position, call disconnect
  - controlled traffic
  - out-of-service positions
  - accessed loop
- upon request, position numbers for operators in the preceding states
- status of positions providing operator assistance

- calls waiting (CW) and calls deflected (CD) by CW and CD display

TOPS Force Administration Data System (FADS)

A Force Administration Data System (FADS) is applicable to multi-traffic TOPS office configurations. FADS system collects the following basic data:

- Initial Position Sequence (IPS)
- Calls Waiting (CW)
- Occupied Positions (POS OCC)
- Work Volume (WV)
    - Call-Busy Work Volume (CBWV)
    - Non-Call Work Volume (NCWV)
    - Idle Time (IDCT)

The above force management data becomes the input to the FADS system to determine:

- offered load
- number of operators
- speed of answer
- average work time

The calculated data from the above indicators is printed at the FADS teleprinter.

Mechanized Force Administration Data System (MFADS)

The Mechanized Force Administration Data System (MFADS) allows TOPS force management measurements to be polled at 15- or 30-minute intervals.

MFADS is a minicomputer system that extracts force management (FM) measurements from a port in TOPS. The minicomputer uses the data sent by the DMS to calculate service and force statistics. These statistics are used to determine the number of operators required. The minicomputer format summaries are similar to FM periodic reports (those output at the SADS or FADS TTY).

System Administration Data System (SADS)

A System Administration Data System (SADS) can only be used by a single-traffic office. The SADS enables the in-charge position, which provides force management for this office configuration, to track administrative data for that office and assist a maximum of six assistance positions using a SADS TTY. In this capacity, the SADS TTY has the combined capabilities of the FADS and TADS TTYs. The SADS TTY is generally located near the in-charge position.

Traffic Office Administration Data System (TADS)

Traffic Office Administration Data System (TADS) is provided in multi-traffic office configurations. TADS provides the in-charge managers located at the remote TOPS locations with traffic data information, and the ability to activate and deactivate management features. TADS enables the in-charge manager to access the following information:

- allow operators to receive transferred calls
- request hard copy data on specific operator
- place operator in or out of controlled traffic mode
- place in-charge or assistance positions in-service or out-of-service
- generate 15 or 30-minute, 6-hour, and 24-hour traffic data summaries for the individual traffic office
- operator feedback system and TTY registers
- broadcast messages
- password administration

Hotel Billing Information Center (HOBIC)

The Hotel Billing Information Center (HOBIC) is an operator-attended location in the operating company or in a centralized, off-site location. If on the operating company premises, the HOBIC is either in a separate area or in the TOPS operator area. A HOBIC can be part of a single-traffic or multi-traffic office configuration.

The HOBIC allows the operating company to offer the following services:

- quotation of call details to hotels for guest-dialed long distance calls
- quotation of time and charges information to guests requesting such information
- a centralized location for handling billing inquiries and charge adjustments

The TOPS system provides two types of quote services for hotels:

- AutoQuote (AQ) guest billing information is automatically transmitted to a receive-only TTY in the hotel that outputs the call details.
- VoiceQuote (VQ) Guest billing information is transmitted to a receive-only TTY at the operating company site. A voice quote clerk relays the call details to the hotel staff or calling party.

Following are four types of TTYs associated with a HOBIC:

- AQ TTY — This TTY is a receive-only TTY at the hotel that provides the AQ service; it must have a 1200 baud automatic answer modem.
- VQ TTY — This TTY is a receive-only TTY located at the HOBIC that provides VQ service; it also serves as a backup if the AQ TTY fails.
- Record (REC) TTY — This is a receive-only TTY located at the HOBIC. This TTY receives a duplicate copy of messages sent to the AQ and VQ TTYs. It serves as a backup if any AQ or VQ TTY malfunctions.

- Hotel Administration Data System (HADS) TTY — This TTY is a send-receive TTY located at the HOBIC. The HADS provides HOBIC personnel administrative control over the HOBIC system. The HADS gives HOBIC personnel three capabilities:

    — query the status of the AQ, VQ, or REC TTYs, or place TTYs out-of-service

    — collect call details from a VQ TTY and transmit them to an AQ TTY if the AQ TTY is out-of-service

    — transmit call details to an AQ printer for calls processed by a nonTOPS MP system operator, such as mobile or conference operators

NOTE: The HADS TTY is always in the HOBIC. However, the VQ and the REC TTY can be in either the HOBIC or the TOPS MP office.

TOPS system configurations

The equipment required to establish a TOPS system can be divided into four main parts: the position equipment, the DMS switch hardware, DMS switch software, and the facility to interconnect the DMS switch with the TOPS Operating Center (OC) (this is generally remotely located with third-party vendor equipment).

The key hardware that makes up the three basic TOPS systems are summarized in the following paragraphs by TOPS system type (MP, MPX, and MPX-IWS—described later, within this subsection). See "TOPS optional services" starting on page 4-3 for a description of the enhanced TOPS services and special applications.

TOPS MP System

The TOPS MP system was introduced in 1987 (see Figure 4-2). This universal operator position includes a new keyboard design that reduces the keystrokes an operator enters. It has an enhanced screen that displays call handling data for toll, directory assistance, intercept, and revenue-generating databases. The traffic administrative positions use identical keyboards and terminal equipment. Administration positions must be within 1000 cable feet of the serving TOPS Position Controller (TPC). Since the TPC for all TOPS positions is consolidated in a central Position Controller Equipment (PCE) cabinet, the actual TOPS position (keyboard, Visual Display Unit (VDU) and headset interface) can be physically configured in various layouts, such as integrated console design, or into a new modular free-standing unit that can be placed on customer-supplied furniture.

Sometimes an operator position is referred to as a *workstation* and includes the position equipment as well as the furniture. For this subsection, *position* will be used in place of *workstation* since both basically mean the same thing.

The TOPS MP position interconnects to its assigned TPC located in the Position Controller Equipment (PCE) cabinet through four-pair conductors. The DMS equipment architecture for a TOPS MP application is configured in two ways, standard base and

integrated system (Figure 4-2) base that uses the TOPS Message Switch (TMS) peripheral. The TMS acts as a link concentrator and message switch for DMS-to-TPC and TPC-to-database communications such as DA (Directory Assistance).

Figure 4-2 — TOPS MP (integrated configuration)
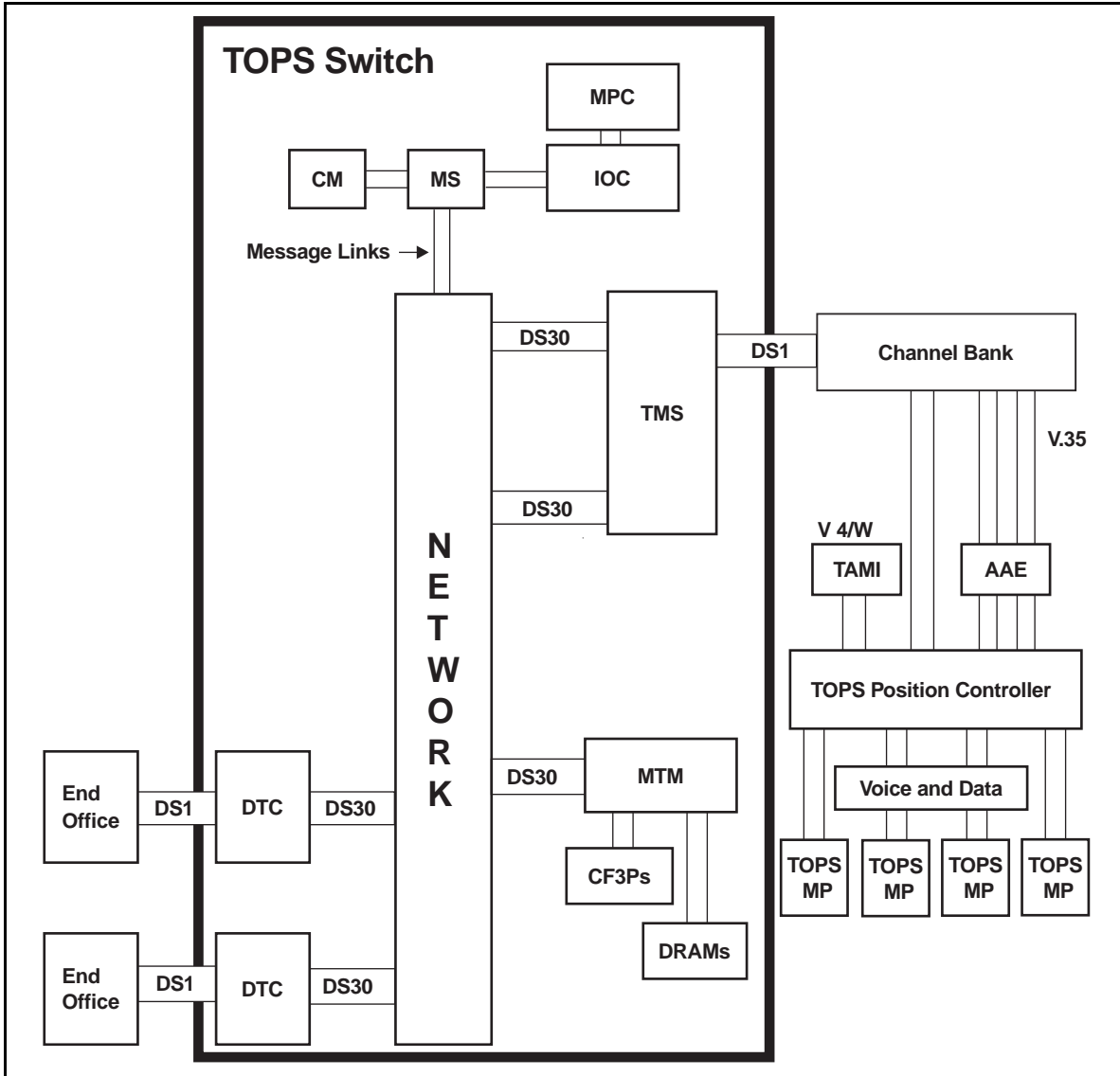
TOPS MP system hardware

For a detailed list of TOPS MP hardware and PEC codes, see volume 4 of PLN 8991-104, *DMS-100F Provisioning Guides.*

In addition to the standard DMS switch configuration, the following hardware is required for TOPS MP service:

- DTC (NT6X50) when using digital trunking

- TM8 (NT2X72AA) when using analog trunking (DTC and TM8 peripherals used in the TOPS MP standard base configuration

- TM/MTM (NT3X67) 6-port conference circuits

- TM/MTM (NT3X02, NT3X03) digital modems

- TMS (NT6X021 LTC) when using an integrated system base

- MPC (NTIX89AA) or the EMPC (Enhanced Multi-Protocol Controller) (NTIX89BA) high-speed data channel termination and digital line facilities (see optional features for additional information).

The TOPS MP stand-alone system uses similar DMS switch equipment. Similarly, the TOPS MP integrated and TOPS MPX systems are equipped with the same DMS switch equipment.

TOPS MPX system

TOPS MPX was introduced in 1991. It provides directory assistance (DA) and intercept (INT) service (see Figure 4-3). It is an extension of the TOPS MP integrated system base that uses the TOPS Message Switch (TMS) peripheral at the host DMS switch and an intelligent type terminal at the OSC position.

TOPS MPX allows operator positions to access the IBM DAS Directory Assistance System database to provide directory assistance and intercept service. Data links between the TMS and IBM DAS are not required. Toll and assist (TA) and access to the operator reference database (ORDB) are planned as a future offering.

The keyboard, monitor screen, and base unit associated with the TOPS MPX positions are based on IBM's PS/2, model 55SX, except for the physical keyboard that is a look-alike of the TOPS MP keyboard.

The MPX position equipment does not use TOPS Position controllers (TPC) per se, but uses virtual position controllers (VPC). The VPC function serves a cluster of four MPX positions using a LAN token ring bus connection. Physically, the VPC requires one data link, DSU, and termination in a type 2 MPX position. TOPS MPX positions are configured four positions to a cluster, and four clusters to a LAN token ring bus. The recommended number of positions per token ring is 16, but 20 can be used as the maximum at the operating company's discretion.

The traffic administration positions in-charge (IC) and service assistance (SA) use the same monitor screen and keyboard as a regular MPX operator position. However, some of the keyboard functions are modified by PS/2 software. The IC display screen serves a dual purpose, one for IC functions, the other force management information. The TOPS MPX system does not support the force management cathode-ray tube (FM CRT) screen. This function should be provided through a TOPS MP position. TOPS MPX terminal and position can be physically configured in various layouts using furniture determined by the customer.

.

Figure 4-3 — TOPS MPX system configuration
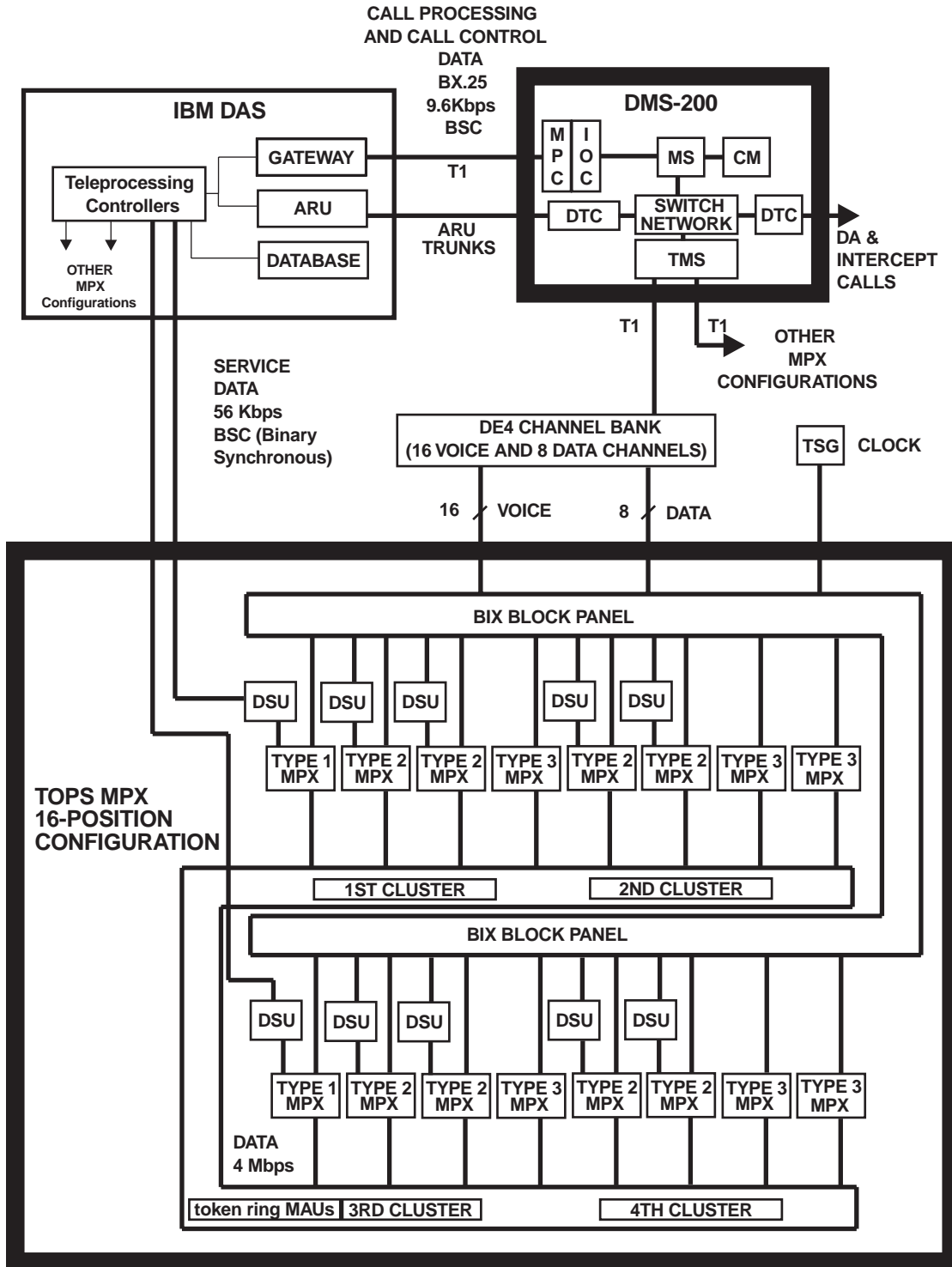
TOPS MPX system hardware

For a detailed list of TOPS MPX hardware and PEC codes, see volume 4 of PLN 8991-104, *Provisioning Manual.*

The interface between the TMS and the MPX positions is through a customer-supplied D4 channel bank. The recommended channel bank units are:

- Voice channels, per position QPP-554B
- Data channels, per type 2 position QPP-553A

A customer supplied timing signal generator (TSG) is required to provide a digital clock timing source for the digital telephony card (audio board) in the MPX terminal. The TSG is usually collocated with the D4 channel bank. The recommended time source generator is:

Telecom Solutions model DCD-400 Digital Clock Distributor

The pack fill for the DCD-400 is as follows:

- DCD-400 shelf assembly 990-40000-01
- Fuse and Alarm card (FA) 090-40014-01
- Clock Input card (CI) 090-40010-01
- Stratum 3 clock 090-40013-01
- Timing Output card (TOCS) 090-40011-01
- Hot spare TOCS 090-40011-01
- Matrix Control card (MCA) 090-40015-01

DS1 line facilities

The T1 line facility or equivalent is the umbilical cord between the host DMS and the OSC location. These line facilities provide the DS1 rate (1.544 Mbps) digital connectivity between the DE4 channel banks, located at the TOPS MPX OSC, and the TMS peripheral at the host DMS. The quantity of DS1 facilities provisioned is governed by the number of TOPS MPX positions.

A digital facility equipped with protection switching is essential for maintaining uninterrupted service to the remote OSC. Where available, digital line diversity should be assigned and maintained. Channel service units (CSUs) are used to terminate T1 type facilities in a noncentral office environment. CSUs are active devices that require power that should be from an uninterrupted source. Surveillance of the T1 carrier facilities is performed from the CARRIER level of the MAP and is further described in the "Carrier Maintenance" subsection within the *Preventive Maintenance* tab.

Record for future reference and trouble investigating activity, the transmission results of the data facilities, including T1 line, at the time of installation and commissioning.

TOPS Message Switch

The TOPS Message Switch (TMS) is a DMS XPM peripheral module, based on the ISDN Line Trunk Controller (LTC). The TMS provides the data communications link concentration and switching subsystem between the DMS CC, the Virtual Position Controller (VPC) and service nodes (external databases). The TMS is a store and forward process that interconnects the CC, VPC, and reference databases using high-speed data links.

TMS provides the following basic improvements to TOPS MPX:

- link switching concentration
- CC messaging/X.25 protocol conversion
- high-speed CC-VPC communications
- X.25 implementation between TMS and all subtending nodes
- X.25 protocol parameters
- network coordination
- elimination of digital modems for CC-VPC messaging
- Virtual TPC and MPX maintenance from the MAP

The TMS performs the following functions:

- provides a MAP user interface for the TMS and MPX terminals
- provides maintenance messaging for the TMS and virtual TPC
- performs building and downloading of static data tables
- receives static data download from the CC
- provides message rooting and network coordination

For detailed information on the TOPS TMS, see NTP 297-8341-550, *DMS-100F TOPS Message Switch (TMS) Maintenance Manual*. For information on TMS maintenance, see "TOPS (TMS) maintenance resources" later in this subsection.

MPC (Multi-Protocol Controller)

The MPC is a programmable controller card, located in the DMS switch IOC, and is used by the DMS to transfer data from the switch to a downstream computer, in this case the IBM DAS (Directory Assistance System). The data transferred between the IBM DAS (gateway) and the DMS switch MPC is for call setup. This connects a specific audio announcement response from the ARU over the T1 link, and is routed through the DMS switch to the subscriber making the inquiry. The application of the audio response is controlled by the MPX operator. When invoked, the MPX operator is released from the call and becomes available for the next call.

The direct data link between the TOPS MPX LAN token ring and the IBM teleprocessing controller, provides the connections for searching the DA database and displaying the response on the VDU screen.

The data transmission between the IBM and operating company interfaces is bisynchronous (BSC) transmission. BSC is an IBM protocol. It uses a defined set of control characters for synchronized transmission of binary-coded data.

MPC IBM DAS application

Redundant data links are the minimum provisioned for IBM DAS. Each link should terminate on its own MPC card. Using the two ports of an MPC card for different applications should be avoided. For service protection, the links should be assigned on physically separate data facilities and physically separate MPC equipment.

MPC application notes

When commissioning an MPX system, consider the following information when evaluating the BSC data links between the MPC and the IBM DAS center.

Modems for MPX are set to 9.6 Kbps for MPC applications. Modems used with the Enhanced Multi-Protocol Controller (EMPC) are set to 9.6 or 19.2 Kbps, depending on the required traffic density.

The settings of packet (Level 3) and frame windows (Level 2) affect MPC or EMPC performance. The default for both packet window and frame window is two. For MPX these should be set to 2 and 7, respectively. The window size settings at the IBM DAS must correspond with the settings of the corresponding MPCs or EMPCs at the TOPS switch.

For the DA application, the recommended setting for the MPC Tl retransmit timer is two seconds. The recommended setting for the N2 transmit attempts counter is two seconds.

To minimize the effect of IOC failure, MPC or EMPC to IOC links should be engineered to spread DA call control link loads evenly over the available IOC units.

Avoid using the two ports of one MPC or EMPC for different applications (i.e., IBM DA and VSN, especially if the applications use different baud rates, and more especially if the traffic density in each application is widely different).

Avoid using both MPC and EMPC cards in the IBM DA application. This does not preclude mixed use of the two types of protocol controllers in the DMS; only the mixing of the two types for use in a single application should be avoided.

The provisioning of one call control link per MPC or EMPC is recommended.

The speed of modems used on the call control links is assumed to be 9.6 Kbps for both transmit and receive.

Synchronous modems are used on call control links. The speed setting of the MPC or EMPC card is automatically derived from the link's synchronizing clock.

Additional MPC information can be found later under "MPC maintenance activities." within this subsection.

IBM DAS system

The IBM Directory Assistance System (DAS) is a stand-alone computer complex maintained as a separate entity, usually by the vendor. For an overall TOPS MPX system appreciation, a brief description of the IBM DAS computer complex follows.

The purpose of the IBM DAS is to find telephone numbers. The DAS consists of computers and programs that help a telephone company retrieve telephone numbers from a computer database, thereby reducing the work time of an operator by automating selected parts of the directory assistance service. DAS combines the judgment and decision-making abilities of the telephone operator with the computer's ability to search through large volumes of data. This provides faster responses to subscribers' requests for directory assistance.

DAS is divided into two major subsystems, the Inquiry Subsystem and the Database Subsystem. The Inquiry Subsystem performs the actual search function and the Database Subsystem maintains and updates the database files used by the inquiry function. Each subsystem comprises basic and optional programs running on separate processors that support the DAS operation.

For details on the operation of the IBM DAS for the TOPS MPX, see NTP 297-2291-300, *DMS-100F TOPS MPX IBM DA Operator Guide.* For the TOPS MPX-IWS—described next—and the IBM DAS, see NTP 297-2251-300, *DMS-100F TOPS MPX-IWS IBM DA Operator Guide.*

TOPS MPX-IWS system

The TOPS MPX Intelligent Workstation System (TOPS MPX-IWS)—introduced in 1993—provides turnkey traditional operator services such as operator services (OA), directory assistance (DA), and intercept—in addition to new services (such as open information access (OIA)) that can be custom-developed and defined by the operating company.

The operator positions for TOPS MPX-IWS are based on IBM's Personal System/2 (PS/2). The IWS positions follow Bellcore's specifications for an Intelligent Workstation System (IWSS). With its open architecture and programmable interface for new applications, the TOPS MPX-IWS is designed to suit evolving multiple-service and multiple-vendor operator centers. See Figure 4-4 for the TOPS MPX-IWS configuration with the DMS-200 switch as the host.

TOPS MPX IWS architecture

For details on the TOPS MPX-IWS architecture and other supporting hardware and software, reference the NTP 297-2251-ZZZ layer of documents dedicated to this product.

Figure 4-4 — TOPS MPX-IWS system (shown with DAS)
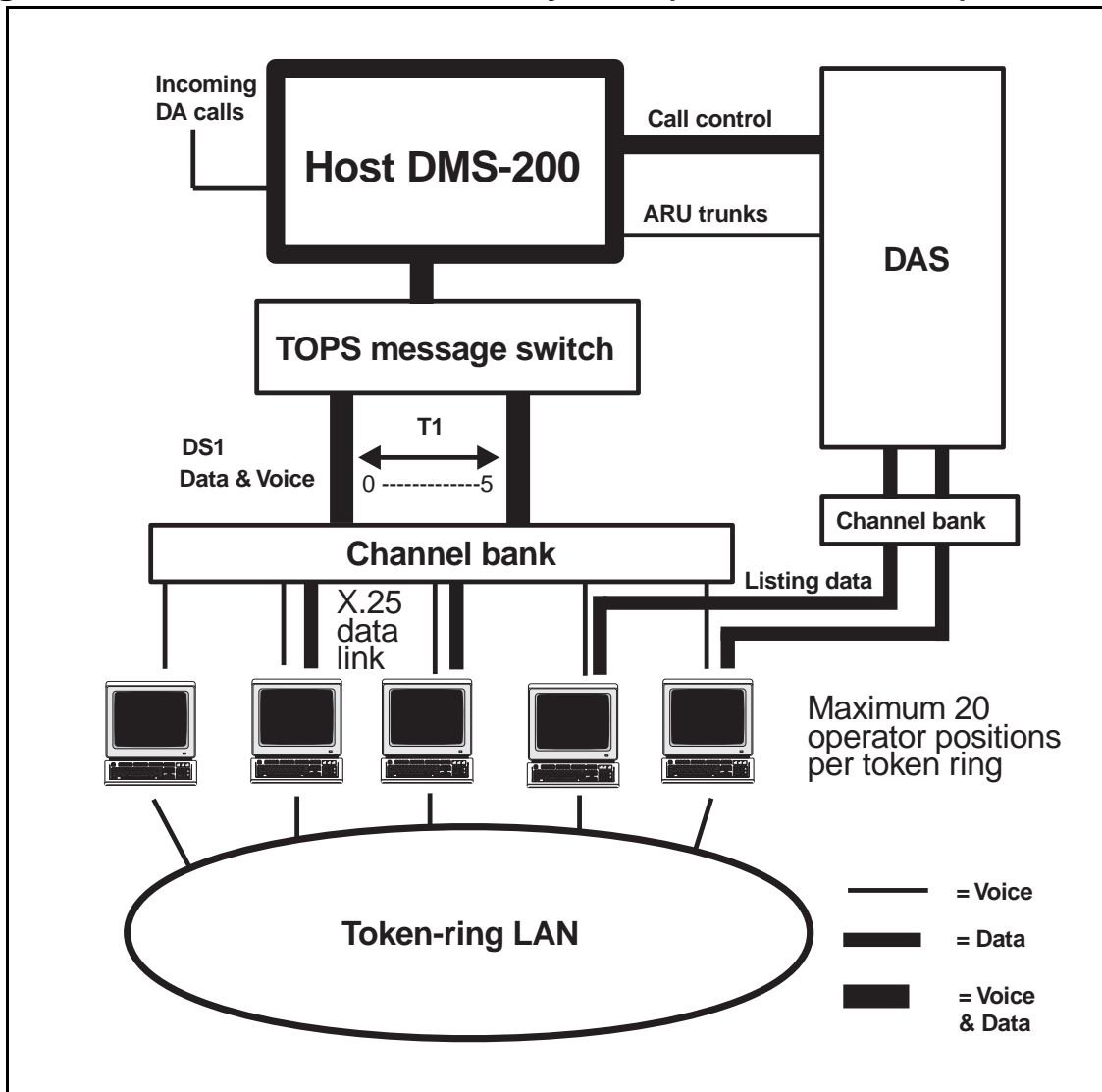
Power and grounding

TOPS MP grounding integrity

All AC-powered equipment normally provided at the TOPS MP operator position is grounded to the DMS single point ground (SPG) and is plastic encased.

The Nortel Networks provided furniture has all metallic members and panels internally grounded and brought to a ground stud that is grounded intentionally to the furniture ground bus. The furniture top working surface is ESD dissipative and grounded internally.

The furniture top should not be used as an isolated or insulating surface. This furniture is also designed to use isolation pads and mounting bushings to maintain isolation from incidental grounds when used in the Isolated Ground Plane.

Any partition dividers or furniture that is provided by the customer with metallic structure or components should have provisions to connect grounding conductor(s) to the serving DMS SPG or CO GRD Bus (or equivalent bus when the CO GRD Bus is not available).

For a complete description of power and grounding for TOPS MP, see NTP 297-2281-156, *DMS-200 TOPS MP Power Distribution and Grounding System*.

TOPS MPX grounding integrity

The TOPS MPX position equipment is designed and recommended for installation in the integrated ground plan, as described in NTP 297-2291-156, *TOPS MPX Power and Grounding Guide*.

TOPS MPX position equipment is compliant with Bellcore's Isolated Ground Planes: *Definition and Applications to Telephone Central Offices*, TR-EOP-000295;, and as an option, can be installed in an isolated ground plane.

TOPS MPX-IWS grounding integrity

Nortel Networks recommends that TOPS MPX-IWS operator position equipment be powered from a "protected" 120 VAC, 60-Hz power source supplied by the operating company. Also, the recommended method of installation is in the common bonding network. Power and grounding arrangements for the TOPS MPX-IWS must conform to the requirements specified in NTP 297-2291-156, *TOPS MPX Power and Grounding Guide.*

Personnel safety and ESD considerations

TOPS MP

The TOPS MP operator positions are susceptible to personal hazards arising from Electrostatic Discharge (ESD) and different ground references.

Every reasonable precaution should be taken to minimize these hazards for maintenance personnel, the operator, and the equipment.

For TOPS MP located in an Isolated Ground Plane, a seven-foot separation should be maintained between the TOPS MP and other equipment that is not connected to the DMS SPG. If the seven foot separation is not possible, then either or both of the following guidelines must be observed:

- Insulating screens or barriers shall be installed between the TOPS MP and the integrated equipment.

- Any metallic objects that are located within seven feet of the TOPS MP shall be bonded to the DMS SPG through an Integrated Collector Bus (ICB). This

bonding is not required if these metallic objects are insulated from contact by an insulating screen or are already bonded to the DMS SPG.

NOTE: AC equipment powered from an AC source that is not part of the TOPS MP dedicated AC distribution should be at least seven feet from the TOPS MP operator positions located in the Isolated Ground Plane.

- Technicians working on the TOPS MP should stand on ESD floor mats and wear ESD wrist straps. If servicing is performed at a work bench, the bench top should be covered with a grounded ESD dissipative mat. AC circuits serving the workbench should be equipped with a Ground Fault Circuit Interrupter (GFCI).

TOPS MPX-IWS

The TOPS MPX-IWS display monitor and terminal base unit shall be UL listed under the requirements of UL1950,"Standards for Safety for Information Technology Equipment Including Electrical Business Equipment," and CSA Certified under the requirements of CSA 22.2 #950 "Information Technology Equipment Including Electrical Business Equipment."

All TOPS MPX-IWS equipment will be tested at level one (2 kV), level two (4 kV), level three (8kV), and level four (15 kV). Tests will be performed with both polarity (positive and negative) discharges. The required level of ESD tolerance is level 4 (15 kV). Tests will be performed per Bellcore TR-N-WT-001089 "*Electromagnetic Compatibility and Electrical Safety Generic Criteria for Network Communications Equipment"* Issue 1, October 1991.

For further information on requirements related to safety for the TOPS MPX-IWS, see NTP 297-2251-001, *DMS-100F TOPS MPX-IWS Product Description/Technical Specification (Base with OA and OIA Applications)*

Electrostatic discharge considerations

ESD floor coverings

Properly installed ESD vinyl or carpet floor coverings are recommended for use in the operator position area for any TOPS configuration. An ESD ground mat at each operator position can be used instead of an ESD floor. Ordinary floor wax should not be used on ESD vinyl flooring. Refer to manufacturer recommendations for care of the flooring.

Only carpeting intended for ESD control and that meets American Association of Textiles, Chemists, and Colorists (AATCC) Test Method 134, without the use of antistatic sprays, should be used in the operator area. Normal carpeting can cause excessive buildup of electrostatic charge. Antistatic carpet sprays are not dependable, need frequent replenishing, and can damage plastic surfaces and finishes of equipment in the operator area.

See NTP 297-1001-156, *DMS-100F Power Distribution & Grounding Systems*, and NTP 297-1001-010, *DMS-100F Electrostatic Discharge Protection*, for supporting information on ESD and grounding.

TOPS maintenance

TOPS maintenance activity can be split into four distinct parts:

- TOPS position and related equipment located at the TOPS OSC
- DMS switch equipment and administration
- third-party vendor equipment and maintenance for such systems as DAS and VSN
- line facilities (T1 carrier and data links) interconnecting the various sites and databases that make up the TOPS configuration

TOPS maintenance management

Various work forces may be required to perform this maintenance activity because of logistics and technical complexity—such as: third party vendors for their computer centers, transmission and data maintenance groups, remote operating company and vendor for TOPS OSC site maintenance, and other DMS switch locations. In this environment, one location must be prime for all facets of TOPS maintenance activity— generally this is the control and surveillance center for the host DMS switch serving the TOPS OSCs.

The control center for TOPS maintenance and service should meet with the various work forces involved, and determine their respective areas of responsibility for sectionalizing trouble reports and their maintenance territory. Also necessary are reporting and escalation names and telephone numbers for seven days a week 24 hours contacts. Established methods and communications between the various work forces who provide TOPS maintenance helps reduce procedural delays and confusion— resulting in faster correction of specific faults and minimal system degradation.

User access for TOPS maintenance

MAP access is required for MP integrated and MPX TOPS OSC sites. It is used primarily to gain access to the TOPS Message Switch (TMS) peripheral and its testing and administrative functionality. MAP access from the TOPS OSC site may be a dial-up port into the DMS switch (with appropriate security and screening restrictive measures).

User access to the TOPS MP TAMI interface is required by the control center responsible for TOPS maintenance. Also required is MAP access at MP integrated and MPX TOPS OSC sites, for maintenance activity by the on-site technician.

TAMI access is required at both MP stand-alone and MP integrated sites. Access may be derived over the POTS network by assigning a telephone number and 212-type modem to the TAMI port on each TPC cage. Using a VT220 terminal at the control

center responsible for TOPS maintenance, connected to a POTS line through a 212-type modem, the remote surveillance force can access any MP position. The remote surveillance center can now access the TAMI maintenance and administration menus (log information, equipment diagnostic testing, and administration). Appropriate security measures are required to restrict unauthorized access to the TAMI TPC interface.

TOPS TTP testing

TOPS position maintenance involves the following components and is tested from the TTP level of the MAP:

- data and voice circuits associated with the TOPS position
- conference circuits associated with the TOPS position
- DMODEM circuits associated with the TOPS position
- receivers for ACTS (RCVRCOIN)

TOPS position status

The status of the TOPS positions that are displayed at the TTP level is affected by the components previously listed. If a trunk circuit becomes system busy—or communication between the TPC and the DMS is dropped while an operator is processing a call—the carrier is dropped and the entire TOPS position is marked system busy (SysB). The state of each component within the DMS is defined by its separate data field (TRUNK_STATE).

The DMS TOPS components can be manually busied, tested, and returned to service using the TTP MAP commands that are described in the following paragraphs.

When testing conference circuits, a circuit is posted and manually busied. A series of tests can then be run. Since a conference circuit is not dedicated to a specific MP terminal, testing a circuit does not disable a position.

When testing digital modems and four-wire trunks, an MP terminal must be posted, manually busied, and installation busied. These actions disable the position. A series of tests can then be run on the digital modem and on the set of four-wire trunks associated with each position. They are described in the following paragraphs.

If a posted voice trunk is not connected to a TOPS position, the technician can change the state and test the trunk. If the posted trunk is marked Call Processing Busy (CPB), it is possible to Force Release (FRLS) the voice trunk of the position by using the FRLS command.

> **CAUTION:**
> If a voice trunk in the CPB state is force released while a call is attached to its associated TOPS MP position, *the call will be lost*.

TOPS position MAP access and status

Enter MAPCI;MTC;TRKS;TTP at the CI level to gain access to the TOPS position maintenance functions such as POST, BUSY, TEST, and RTS. To perform a function use the POST command to select the TOPS position number to be worked on. Once the TOPS position has been posted, use the remaining menu command for the described maintenance function. To perform a diagnostic test, the TOPS position must be placed in the manual busy state using the BSY command.

Testing position voice and data circuits

TOPS position voice and data trunk circuits can be tested from the TTP level. All TOPS positions are listed in table TOPSPOS. At the TTP level, use the following steps to post and diagnose the position circuits:

ACTION   **RESULT**

>POST T TOPSPOS #   Requested TOPS position will be posted
or:
>POST G TOPSPOS   All TOPS positions can be posted by typing NEXT

>TST_   Diagnose the posted circuit

The result of the diagnostic test will be displayed as:

DIAG OK, or **DIAG CRDFL**

If a card fails, replace the faulty card using NTP procedures and repeat the diagnostic tests on the card.

3-port conference circuit diagnostics

The TTP diagnostic command performs a two-part test on the posted 3-port confer-ence circuit (CF3P).

- The first part of the diagnostic is to exercise the scan points of the trunk logic circuits (TLCs) associated with the three ports of the circuit. The TLCs are sequentially written to and read. If all sequences are correctly written and read, the TLC scan points are initialized to the idle state.

- The second part of the diagnostic is a transmission test through the CF3P. The sequence for the transmission test is to establish a two-way connection between the TTT and a port of the CF3P. A signal is then sent from the TTT and a power level measurement is made on the returned signal. If the two-way con-nection is successfully tested, a one-way connection is sequentially added between the TTT and both free ports of the conference circuit. A signal is then sent from the TTT, and a power level measurement is made on the returned sig-nal. If all transmission tests are successful, the circuit is initialized to the state that the diagnostic began with (i.e., two-way connection to port 0). All CF3Ps are listed in table CONF3PR.

At the TTP level, use the following steps to post the CF3P to be tested:

ACTION	RESULT
>POST T CF3P #	The requested CF3P will be posted*:*
or	
>POST G CF3P	All CF3Ps will be posted by typing NEXT

NOTE: # (number) must be the EXTRKNM listed in table CONF3PR or Port 0 of the CF3P under test.

>TST_   Diagnose the posted circuit

The result of the diagnostic test will be displayed as:

DIAG OK, or **DIAG CRDFL**

If a card fails, replace the faulty card using NTP procedures and repeat the diagnostic tests on the card.

Digital modem diagnostics

The digital modem (DM) is a four-port I/O controller, and consists of two circuit packs—a NT3X02AA Control Processor and a NT3X03AA Digital Signal Processor. Each of the four DMs for every card pair must be diagnosed individually by first posting the DM and then running a diagnostic test on it.

All DMs are listed in table DMODEM.

At the TTP level, use the following steps to post and test the DM.

ACTION	RESULT
>POST T DMODEM #	The requested DM will be posted
or, (# = EXTRKNM)	
>POST G DMODEM	ALL DMs will be posted by typing NEXT
>TST_	Diagnose the posted circuit

The result of the diagnostic test will be displayed as:

DIAG OK, or **DIAG CRDFL**

If a card fails, replace the faulty card using NTP procedures and repeat the diagnostic tests on the card.

CDC maintenance (NT3X08AB card)

The Coin Detection Circuit (CDC) receivers are maintained from the TTP level of the MAP—similar to other receiver-type service circuits. Look up table RECEIVER to get the RECRCOIN CLLI name for the CDC.

Once you have the correct CLLI name for the receivers, you can check the status of these receivers by typing:

>MAPCI;MTC;TRKS;STAT
>ITEM 0

>**SELGRP RCVR COIN**
>**HCPYTRK**

The CDC receivers will now be displayed.

If some of the receivers are BUSY or OFFL, you may want to bring them into service. If the receivers have not been tested, then test them. You can test the receivers by posting them up by their CLLI using the TTP level.

Example:

>**MAPCI;MTC;TRKS;TTP**
>**POST G RCVR COIN**

You can now perform the desired action on the posted set. For instance, if all receivers are IDLE, you can busy, test, and RTS every one of the posted receivers by typing the following:

>**REPEAT nn (BSY;TST;RTS;NEXT)**

NOTE: **nn** is the number of receivers in your posted set.

Coin station test

The ACTS coin tone generation test is performed by outside plant station repair persons. It is documented here to inform the central office maintenance personnel of the test and its potential in resolving ACTS station problems.

The ACTS coin tone generation test tests the ability of coin phones to correctly generate coin tones to indicate the deposit of a coin. The coin may be a nickel, dime, or quarter.

The coin test is invoked by dialing the ACTS test telephone number from a coin phone. The call is routed to the TOPS ACTS switch. ACTS calls are usually dialed as 1+CLD. Listen for prompts and deposit the appropriate coins in a nickel, dime, quarter sequence.

If the coin test passes, the following will be heard:

- an acknowledgment, such as, "Thank you, nickel test has ended"
- a prompt to deposit the next denomination of coin
- an end-of-cycle alert tone after the quarter is deposited and acknowledged

If the test fails, the following will be heard:

- a failure alert tone
- a prompt to deposit the next denomination of coin

The person performing the test may hang up at any time to end the test even before depositing all the coins. All coins will be returned. A hang up will not cause a failure unless the hang up occurs before the failure alert tone is heard and the next coin denomination prompt starts.

The time-out is datafillable. If an incorrect coin is deposited, the time-out period is reset, and the correct coin may be deposited.

The datafillable time-out value is found in table ACTSOPTS as ACTS-COIN-TEST-TIME-OUT. Units are measured in seconds.

At the end of a test call that fails, a TOPS 117 COIN TEST FAIL log is generated to indicate: the denomination of the coin or coins that failed, the calling number, called number, incoming trunk number, CDC number, and calling time. If a test on a particular coin denomination fails, then a failure is reported in the log, even if a test on that particular coin denomination subsequently passes during the same test call. In addition, the CDC associated with any failed test call will have standard DMS receiver maintenance performed on it, in case the CDC was faulty and caused the coin tones to fail. If a test was not performed for a particular coin denomination, that fact will also be reflected in the output of the log.

There is no restriction on the number of ACTS coin tone generation tests that may be performed simultaneously, as long as an ACTS DRAM and a CDC are available for testing purposes. If an ACTS DRAM or CDC is not available, then the test is aborted, and the call is routed to treatment NOSC (No Service Circuit, datafilled in table TMTCNTL). Existing TRKl38 (TRMT) logs are generated. These logs can be turned on or off by datafilling table TMTCNTL.

If an ACTS DRAM or CDC is force-released during a coin test call, the test will end as if an on-hook occurred, and a TOPS102 INFO ACTS TROUBLE log and a TOPS1O4 POS UNEXPECTED MSG log are generated.

Calls from noncoin phones or any other phone—that are not normally able to make ACTS calls—are blocked and routed to treatment "Reorder" (RODR, datafilled in table TMTCNTL).

A switchhook flash is ignored, and test calls never go to a TOPS position.

Alarms associated with TOPS

NTP 297-YYYY-543, *Alarm and Performance Monitoring Procedures* provide the alarm clearing procedures.

Trouble reports from the TOPS operators (all configurations) alert the maintenance personnel of faults. Subscriber-identified problems, difficulties identified by the TOPS operator while processing a call, and position faults, would be the stimulus for initiating TOPS trouble reports. Alarms are associated with the following SNAC logs:

- SNAC102 —maintenance trouble server enough to generate a minor alarm
- SNAC103 —maintenance trouble server enough to generate a major alarm
- SNAC105 —excessive PIN entries potential fraud minor alarm

The following types of TOPS OSC faults are reported directly to the TOPS maintenance force:

- screen display dim, out, or permanently on

- incomplete screen
- logon procedure fails
- broken, loose, sticking, or missing keys
- crossed TOPS positions
- failure to collect or return coins
- headset—can't hear or be heard
- position idle, but hear conversations

Key functions associated with TOPS optional features are monitored using the EXT MAP level display and commands. These are software alarms that have been extended from the vendor's system for operating company surveillance purposes.

External alarms are generated for the following features:

- Voice Service Node (VSN) associated with AABS
- Directory Assistance System (DAS) associated with DA service
- Personal Audio Response System (PARS) associated with TOPS position

The following table records the alarms that are triggered by the vendor system and the related EXT alarm and log assignment.

Table 4-3 — TOPS Vendor Alarms

SYSTEM	LOG NAME	EXT alarm assignment			
		LOG105 NA	LOG106 MN	LOG107 MJ	LOG108 CR
PARS	TOPS_PAR_LINK		Đ		
	TOPS_PAR_NODE		Đ		
	TOPS_PAR_APPL			Đ	
VSN	VSN_NO_ALM	Đ			
	VSN_MIN_ALM		Đ		
	VSN_MAJ_ALM			Đ	
	VSN_CRIT_ALM				Đ
	VSN_NO_LINKS			Đ	
	VSN_ONE_LINK	Đ			
DAS	VR1 MINOR		Đ		
	VR1 MAJOR			Đ	
	VR1 CRITICAL				Đ
	VR2 MINOR	Đ			
	VR2 MAJOR			Đ	
	VR2 CRITICAL				Đ

The following paragraphs record the conditions from the vendor equipment that triggered the alarm indication.

- TOPS_PAR_LINK — when any MPC data link for the TOPS PARS application is taken out-of-service

- TOPS_PAR_NODE — when all MPC data links to any PARS node are taken out-of-service

- TOPS_PAR_APPL — when all MPC data links for the TOPS PARS application are out-of-service

- VSN alarms — are datafilled in the following VSN ALARMS table. The VSN software alarms are triggered by the error code in the maintenance notice message sent by the VSN. Contact the vendor for this data. Typical assignment:

    — VSN_NO_LINKS when all of the logical links to a particular VSN are out-of-service

    — VSN_ONE_LINK when only one data link to a particular VSN remains in a set of two or more data links

    — VR1 MINOR when the number of data links available reach or fall below the minimum threshold

    — VR1 MAJOR when the number of data links available reach or fall below the major threshold

    — VR1 CRITICAL — when the number of data links available reach or fall below the critical threshold

Table 4-4   —   VSN ALARMS

EXT LOG #	EXT ALARM	VSN ALMCODE	ALMTEXT
108	CRIT	1	FAULTY_PRU
108	CRIT	2	FAULTY_SRU_DEVICE
107	MAJ	3	DISK_FULL
107	MAJ	4	EXT_ALARM
106	MIN	5	INSERV_T1_FAILED
106	MIN	6	BUSIED_T1_FAILED
108	CRIT	7	ACPE_CAPACITY_LOST

NOTES:

1. VR1 designates the first vendor's DA system. If a second DAS system is installed, it would be identified as VR2, and triggered by the same causes. The threshold values are set in table SERVICES.

2. EXT105 thru EXT108 log reports are generated only if the REPORT field in table SFALARM is set to "Y" (Yes).

Maintenance surveillance indicators are required for stand-alone power plants and carrier transmission equipment provisioned for remote TOPS OSC locations.

Use the EXT level alarm functions to provide the necessary indicators and alarm severity at the host DMS switch. NTP 297-1001-593, *DMS-100F External Devices Maintenance Guide* describe the EXT alarm maintenance subsystem.

Extension alarms from vendor equipment locations or remote TOPS OSC sites should be tested periodically to verify their description and operation.

TMS alarms

TOPS MP (integrated) and TOPS MPX configurations use TOPS Message Switch (TMS) peripheral equipment at the DMS switch. The TMS peripheral generates the following alarm conditions:

- PM DCH minor alarm

- PM TMS critical alarm

- PM TMS major alarm

- PM TMS minor alarm

- PM TPC critical alarm

For TMS alarm clearing procedures, see NTP 297-8341-550, *DMS-100F TOPS Message Switch (TMS) Maintenance Manual.*

Logs associated with TOPS

For detailed information on individual TOPS logs, see the NTP 297-YYYY-840 log reference manuals. Specific TOPS logs are also described within supporting TOPS NTPs.

Log reports for the TOPS systems are generated from two sources and some system dependencies as follows:

- TAMI logs (TPC administrative maintenance interface) are associated with MP TOPS position equipment located at the remote TOPS OSC site. These logs are generated by the TPCs and the output is printed on a TAMI teleprinter.

- The Logutil system generates the TOPS-related logs using various categories within the DMS switch. The application is TOPS system type dependent.

The TAMI log system only produces one log category (TPCXXX). TPC logs are complex. Associated with log reports are general diagnostic error codes that expand the meaning of the log message. Refer to NTP 297-2281-530, *DMS-100F TOPS MP TAMI User Guide* for the diagnostic error code meanings. The three TAMI logs are:

- TPC100 are logs associated with the terminal and controller position equipment, sonalert, ORDB applications. These are complex logs identifying over 40 individual trouble conditions.

- TPC101 are logs associated with the computer based training (CBT) system.

- TPC103 are logs generated by the high-speed data access (HSDA) circuit packs and associated data links for TOPS MP TMS, CCI/DAS, and ORDB.

Log categories for TOPS

TOPS related trouble information, when identified, is reported using the following log categories in the LOGUTIL subsystem:

ACCS100—generated by the ACCS when the system detects pin hunting (potential fraud condition). It is a trial and error method to find the PIN # associated with a CCN.

ADAS—related logs are HSDF, UADA, UAPM, UCDM, UOAM, USLG, VMTS, OMX, etc.

AUDT—checks integrity of peripheral module software and attempts to correct errors when detected.

CCI—Computer Consoles Inc. reports on messaging errors between the DMS switch and a CCI (DAS/C) system. Reports error information, and indicates when the call should be handled by an operator.

DAS—Directory Assistance Service (DA and INT) identifies specific deficiencies during call processing.

DCH—DCH subsystem generated report (part of the TMS) identifies system busy channels and improperly datafilled PVC information.

DFIL—Datafill reports on call cutoffs during call processing or testing.

EXT—External Alarm OAU—also vendor systems for DMS surveillance indicators.

IBM—International Business Machines (IBM) reports on messaging errors between the DMS switch and the IBM (DAS/C).

IOD—Input and output device (IOD) controls the hardware entities associated with devices used to achieve a duplex data exchange.

MPC—Multi-Protocol Controller (MPC) subsystem generated when MPC level shows link state changes. Datalinks CC to DAS or DAS gateway Audio Response Unit (ARU) may be malfunctioning.

PM—Peripheral Modules (PMs), the TOPS TMS is the PM used for TOPS integrated MP and MPX applications. Controls all the hardware, software interfaces with the external facilities.

PARS—generated when an MPC data link for TOPS PARS application is removed from service or entire link set.

RONI—Remote Operator Number Identification (RONI) checks for ANI failures troubles encountered during remote CAMA call attempts.

SNAC—Switching Network Analysis Center (SNAC), method the OPS operators report troubles by entering a two-digit trouble code that causes the SNAC system to generate a log report detailing the trouble (performs same function for NOTIS).

TCCI—detects errors in messaging between the DMS and CCI DAS/C database.

TIMB—detects errors in messaging between the DMS and IBM DAS/C database.

TOPS—detects various faults, errors and troubles, predominantly associated with TOPS MP stand-alone systems.

TRK—controls the hardware and software entities associated with trunk equipment, including peripheral circuit cards and facilities.

TVSN100—detects errors in the AABS protocol (invalid data sent by VSN).

VSN—detects various errors in the AABS protocol, such as audits, maintenance notices, action request messages.

VSND200—identifies datafill discrepancies between tables VSNMEMBER and TRKMEM.

Ensure that the log message groups associated with your TOPS system configuration, including the various optional feature packages, are added to table LOGCLASS and routed to the MAP position responsible for the activity using table TERMDEV. Consider establishing a message routing category for TOPS maintenance by using table LOGCLASS.

The following table lists the DMS related log messages for TOPS events—including related alarm information. A log report is a message output by the DMS whenever a significant event has occurred. Log reports include status and activity information, hardware or software faults, and other events likely to affect switch performance.

Table 4-5 — TOPS LOG Events

LOG	ALARM CLASS	INDICATES	NOTES
ACCS100	NIL	PIN hunting detected for a CCN	Potential fraud situation
AUDT131	NIL	diagnostic tests failed for system initiated tests for a system busy TOPS position in a TMS configuration	
AUDT205	NIL	DRAM fails to return the same message as sent by the CC.	
AUDT207	Major	CC unable to communicate with DRAM or there is a power loss on a DRAM.	
CCI100	NIL	messaging error between DMS and the CCI DAS/C system (message was invalid at this point in the call)	complex log - see the current NTP "Log Reference Manual"
DAS100	NIL	No DAS call IDs for new calls.	resources required to message DMS to DAS.
DAS102	NIL	DAS fails to respond to an operator LOGIN or LOGOUT procedure	
DAS103	NIL	ARU signaling or ARU datafill problem.	
DAS104	NIL	Billing type is not valid for auto DA call completion.	
DCH100	NIL	generated when a TDC channel becomes system busy	
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
DCH104	NIL	generated when a TDC channel is made Cbsy	
DCH105	NIL	generated when an attempt is made to RTS a TDC channel and the RTS fails because of improperly datafilled PVC information	
DFIL130	NIL	generated when an operator attempts to logon to a position that provides DA service through the IBM-DAS and table OPRCMPLX contains nil data for the given operator, a valid operator complex number/unit number must be datafilled in table OPRCMPLX for an operator to successfully logon to the IBM-DAS	
EXT105	NIL	external system generated alarm which is translated into a DMS alarm for action or surveillance. VSN indicates a maintenance notice message sent from the VSN and has been received by the DMS, informing the DMS or an abnormal or maintenance condition at the **VSN**	
EXT106	Minor	external system generated alarm which is translated into a DMS alarm for action or surveillance. PARS - MPC data link(s) out of service PARS - all MPC data links to any PARS node are taken out-of-service. VSN - indicates a maintenance message notice sent from the VSN and received by the DMS, informing the DMS of an abnormal condition at the **VSN** (minor alarm category)	PARS application PARS application VSN application
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
		VSN ONE LINK - only one link in a set of two or more in-service	VSN application
		VR-1 Minor - Vendor one system available data links fell below minimum threshold (minor alarm setting)	DAS application
		VR-2 Minor - Vendor two system available data links fell below minimum threshold (minor alarm setting),	DAS application
EXT107	Major	external system generated alarm which is translated into a DMS alarm for action or surveillance	
		PARS - all data links for the TOPSPARS application are taken out-of-service	PARS application
		VSN - indicates a maintenance message notice sent from the VSN, and received by the DMS, of an abnormal condition at the **VSN** (major alarm category)	VSN application
		VSN NO LINKS - all logical links to a particular VSN are out-of-service.	VSN application
		VR1 - Major - vendor one's system available data links fell below the major threshold alarm setting.	DAS application
		VR2 - Major - vendor two's system available data links fell below the major threshold alarm setting.	DAS application
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
EXT108	Critical	VSN - indicates a maintenance message notice sent from the VSN, and received by the DMS, of an abnormal condition at the **VSN** (critical alarm category)	VSN application
		VR1 Critical - Vendor One's system available data links fell below the critical threshold setting.	DAS application
		VR2 Critical - Vendor two's system available data links fell below the critical threshold setting	DAS application
IBM100		invalid message received from the IBM DAS/C system. (IBM protocol error)	DAS application - complex message
IODxxx		supports input/output devices, including MPC hardware	see MPC logs
MPC101	NIL	software condition in the MPCSUB that could prevent normal operation of MPC functions	complex (various reasons given: approx. 200)
MPC102	NIL	software condition in the MPCSUB or X25SUB that could prevent normal operation of X.25 protocol support functions	complex (various reasons given: approx. 100)
MPC103	NIL	record of traps occurring in the MPC software	
MPC104	NIL	audit trouble report that could prevent normal operation of MPC functions	
MPC106	NIL	configuration change using SETPRAM command and nonresident software.	
MPC201	NIL	MLCs in the MPC fast application were used. MLCs represent the MPC number, link number, and conversation number.	may highlight repeated lost resources.
MPC299	NIL	an I/O or resource problem occurred with an MPC Fast application	
MPC901	NIL	an MPC was manually made UNEQ.	
MPC902	NIL	an MPC was manually made OFFL.	
MPC903	NIL	an MPC was successfully man-busied.	
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
MPC904	NIL	a serious MPC fault occurred that caused the MPC to go system-busy	
MPC905	NIL	an MPC was successfully returned to service.	
MPC906	NIL	minor incoming message overload (ICOM)	
MPC907	NIL	ICOM cleared	
MPC908	NIL	a link status change has occurred	
PARS100	NIL	MPC link for PARS application removed from service	also triggers MPC299 log
PARS101	NIL	linkset for PARS application removed from service	
PARS102	NIL	messages from the PARS processor other than audits	
PARS103	NIL	difference in PARS protocol and DMS load for PARS.	
PARS104	NIL	DMS unable to receive messages from the PARS processor	
PM107	NIL	generated when TMS peripheral module changes state to CBsy due to a system busy request or manual busy request of its C-side node	
PM128	Minor	generated when TMS peripheral module encounters trouble during normal operation. The peripheral module state changes as a result of a system or manual request.	
PM190	Major	D-Channel Handler (DCH) changes state to SYSB due to detected fault in the DCH itself.	
PM235	Major	D-Channel Handler (DCH) takeover has occurred.	see PM190
PM270		DCH to DCH congestion fault	
RONI100	NIL	trouble was encountered during an RCAMA call.	
SNAC100	NIL	customer or operator initiated, trouble detected during the course of the call. TOPS operator reported for a nonmaintenance item.	
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
SNAC101		customer or operator initiated, trouble detected during the course of the call. TOPS operator reported. Not serious enough to generate an alarm.	
SNAC102	Minor	customer or operator initiated, trouble detected during the course of the call. TOPS operator reported. Serious enough to generate a minor alarm.	
SNAC103	Major	customer or operator initiated, trouble detected during the course of the call. TOPS operator reported. Serious enough to generate a major alarm.	
TCCI100		CCI protocol error messages between DMS and CCI DAS/C	DAS application - complex message
TIMB100		IBM protocol error messages between DMS and IBM DAS/C	DAS application
TOPS100		TOPS trunk (position) is system busy. Trouble was encountered during a TOPS call attempt.	
TOPS101		data transmission error during messaging between the TOPS position and DMODEM, causing DMODEM to go system busy	
TOPS102	NIL	unexpected message arrives at a TOPS position. Also ACTS coin station testing	
TOPS103	NIL	unexpected message forcing TOPS device (modem) SYSB.	
TOPS104	NIL	unexpected messages from ACTS or DRAMS or operator keys in a SUSPCDC trouble condition.	
TOPS105	NIL	SYSB TOPS operator centralization (OC) trouble	
TOPS106	NIL	SYSB TOPS data link trouble	
TOPS107	NIL	TOPS resource trouble equipment unavailable	
TOPS111	NIL	LATAXLA mismatch indicates datafill problem associated with EA EO signaling	
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
TOPS112	NIL	virtual circuit is busy, but not linked to a real call. Sys idles virtual ckt.	
TOPS113	NIL	DRAM play trouble - cannot find announcement in table DRMUSERS	ACTS system, MCCS system
TOPS114	NIL	datafill absent for branding annc's	
TOPS115	NIL	MP state change (TMS configurations) system busy, in-service state	
TOPS117	NIL	coin test fail detected during ACTS coin tone generation testing from the coin station.	ACTS
TOPS118	NIL	position sanity timer expired, generally resulting from procedural actions by TOPS operators.	log printed at host and remote TOPS.
TRKxxx		supports TOPS position status, since they are tested from the TTP and identified as trunks. Also related service circuits.	
TVSN100		invalid data from VSN detected from an error in the AABS protocol	AABS system
VSN100	NIL	an error occurred in the AABS protocol between the VSN and the DMS for audit messages.	
VSN101	NIL	an error occurred in the AABS protocol between the VSN and the DMS for maintenance notice msg's.	
VSN107	NIL	an error occurred in the AABS protocol between the VSN and the DMS for maintenance notice messages.	
VSN108	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request messages with a connect party action ActID.	
VSN109	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request messages with an alter port connection ActID.	
VSN110	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request messages with a request operator ActID.	
Continued on next page			

Table 4-5 — TOPS LOG Events (continued)

LOG	ALARM CLASS	INDICATES	NOTES
VSN111	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request message with an abort call ActID.	
VSN112	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request messages with a float call ActID.	
VSN113	NIL	an error occurred in the AABS protocol between the VSN and the DMS for action request messages with resources unavailable ActID.	
VSN115	NIL	an invalid operation is present (or is requested) in a message sent by the VSN.	
VSND200	NIL	a voice link to the VSN that is not datafilled in table VSNMEMBER	
End			

OMs associated with TOPS

This TOPS related operational measurement (OM) information augments the OM information in the *Preventive Maintenance* tab of this manual. The "Operational Measurements" subsection describes the DMS-100 maintenance, administrative, and surveillance applications using OMs.

TOPS OM data covers all facets of the system and provides information for key work functions and groups such as provisioning, traffic management, surveillance, and trouble isolation. For in-depth trouble investigation, review the total OM package and select specific OM data for analyzing the current problem.

OMs for TOPS functions span over 50 groups and most are summarized below. Reference NTP 297-YYYY-814, *DMS-100F Operational Measurements Reference Manual* for detailed information on the individual registers within the TOPS OM groups listed below, and those not listed in this manual.

The TDCSHOW command, accessed at the ISG level of the MAP, displays the TOPS Message Switch operational measurements in OM groups TDCPROT and TDCROUT. When using the TDCSHOW command, the information is collected on a per-link basis, rather than summed for all links on each channel type when accumulated in the OM reporting system.

OM groups for TOPS maintenance and surveillance

ANN OM group

This OM group provides information for DRAMs. It records attempts, overflow, usage, system busy, and manual busy.

AABS OM group

This OM group measures the automated alternate billing service call attempts and dispositions. OM group VSNCOM and registers supersede AABS OM group.

AAMSFILT OM group

This OM group measures the overall usage of AABS filtering based on billed number as well as the individual reasons for the filtering (fraud or bad voice). A call is considered filtered, if the normal call flow is interrupted and the call is sent to an operator. This may be useful in deciding what billed numbers should be filtered and for what reasons.

ACCSBNS OM group

This OM group provides counts for valid and invalid Billed Number Screening (BNS) queries.

ACCSCCV OM group

This OM group provides counts for valid and invalid Calling Card Validation (CCV) queries.

ADASAPU OM group

This OM group records the various call processing statistics for the Automated Directory Assistance System (ADAS) application running on the LPP based Application Processor (APU).

AMA OM group

This OM group records the total number of initial AMA record entries that have been output for downstream processing, the number of occurrences of emergency transfer between the AMA tape units, and the number of times that an AMA call is routed to TOPS MP.

AOSSVR

The AOSSVR group provides information on Auxiliary Operator Services System (AOSS) call actions that occur in offices that use audio response.

CDACTS OM group

This OM group provides measurements for calls that can receive Automatic Coin Toll Service (ACTS). Data records include calls that attempt to route to ACTS for the following:

- initial coin charges
- coin charges due collection
- initial coin period notification
- nonstandard notification
- time and charge information

Registers are also incremented each time a customer walks away from a coin phone without paying and each time a customer could receive ACTS, but does not, because the customer allowed two successive time-outs to occur, or because the customer flashes the switchhook.

CDMCCS OM group

This OM group provides counts for the number of attempted Mechanized Calling Card Service (MCCS) calls and the number of failures caused by hardware problems with either MCCS receivers (RCVRMCCS) or the Digital Recorded Announcement Machine (DRAM). Registers in this group also count the number of attempts to make MCCS sequence calls and the number of sequence call failures caused by hardware problems with either MCCS receivers or DRAM.

CF3P OM group

This OM group records TOPS application for three-port conference circuits (CF3Ps), the number of times that a circuit is seized, and the number of times that a circuit is unavailable. This OM group also records queue overflows, abandons, and use.

CF6P OM group

This OM group records the use of a six-port conference circuit (CF6P), the number of times that a circuit is seized, and the number of times that a circuit is unavailable. This OM group also records queue overflows, abandons, and use.

CP2 OM group

This OM group provides information on the use of Extended Call Control Blocks (ECCB) and contains the high water mark OMs for call processing software resources. This group is an extension of the CP OM group.

CPUSTAT OM group

This OM group provides information on CPU occupancies. CPU occupancy is the ratio of real time spent on a function to the time allowed for a function. CPU occupancy is expressed as a percentage value.

DALINK OM group

This OM group pegs events that relate to messaging between the DMS central control and the Directory Assistance System (DAS).

DAMISC OM group

This OM group pegs miscellaneous events that relate to TOPS and the DAS.

DUAQ OM group

This OM group counts activities of the dial-up autoquote feature associated with HOBIC.

DUAQMOD OM group

This OM group counts dial-up autoquote modem activities associated with HOBIC.

ISDD OM group

This OM group provides information on grade of service given to incoming trunk calls to a DMS through three types of XMS based Peripheral Modules (XPM). When the length of time required to complete a call exceeds a defined threshold, the register for each XPM is scored.

MPCBASE OM group

This OM group collects data within Multi-Protocol Controller (MPC) and Central Control (CC) software. This data includes measurements relating to the use and availability of MPC boards and nodes, and data transfer through an MPC.

MPCFASTA OM group

This OM group measures maintenance and usage activities on logical links datafilled in table MPCFASTA (one set of four registers per application).

MPCLINK2 OM group

This OM group provides information on traffic and faults occurring in the physical, link, and network level peripheral hardware and software for link two on a MPC. The data is collected at the MPC card level in the MPC software. See MPCLINK3 OM group below for LINK2 and LINK3 clarification.

MPCLINK3 OM group

MPCLINK2 and MPCLINK3 OM group register allocations are identical and collect similar information for two different data links assigned to the MPC card NTIX89. The NT1X89 has two assignable ports numbered 2 and 3.

OFZ OM group

This OM group provides information for traffic analysis.

OGTMP OM group

This OM group records when an outgoing trunk is accessed at a TOPS MP operator position. OGTMP provides one tuple for each OGT key datafilled in table OGTMP-KEY.

RCVR

This OM group counts successful and failed attempts to obtain receiver circuits in the DMS. These include the following receiver for TOPS application: RCVRCDC coin detection circuit; RCVRCOIN for ACTS receiver; RCVRMCCS for MCCS.

TCAPERRS

TCAPERRS counts protocol errors detected by the Transaction Capabilities Application Part (TCAP) for each subsystem (ACCS for the TOPS application). This information is part of the CCS7 signaling system and is described in the "SS7 Overview and Maintenance" subsection within this tab.

TDCPROT OM group

This OM group provides information on errors in protocol, noisy links, or downed links. D-Channel Handler (DCH) protocol OMs include the X.25 layers one, two, and three OMs. Note that the peg counts are kept in the TOPS Message Switch (TMS) and transferred to the CC prior to the transfer of the active registers to holding status. See page 4-59 and the TDCSHOW command for accessing this OM data on a per-channel basis.

TDCROUT OM group

This OM group provides router information on the TOPS TMS data channels in the DCH and the ISDN Signal Processor (ISP). Note that the peg counts are kept in the TMS and transferred to the CC prior to the transfer of the active register to holding status. See the "TDCSHOW command for displaying TMS OMs" heading on page 4-59 and the TDCSHOW command for information on accessing this OM data on a per-channel basis.

TOPSAICC OM group

This OM group provides measurements for Automated Intercept Call Completion (AINTCC) utilization.

TOPSALT OM group

This OM group measures the number of calls that are routed to an alternate host.

TOPSARU OM group

This OM group pegs DA and intercept calls in the TOPS MP offices that are routed to an internal or external Audio Response Unit (ARU).

TOPSBRND OM group

This OM group records the number of successfully or unsuccessfully played branding announcements or call abandonments during branding.

TOPSCCAB OM group

This OM group provides information about the method of billing used for Automated Directory Assistance Call Completion (ADACC).

TOPSDA OM group

This OM group pegs the types of Directory Assistance (DA) service call originations as either DA or intercept, and pegs recalls that are handled by the TOPS Voice Recording (VR) system.

TOPSDACC OM group

This OM group counts call completions that are handled by an operator and by Directory Assistance Call Completion (DACC). DACC allows a subscriber making a DA call to be connected to the requested number without originating a new call. The subscriber can be connected to the requested number manually by an operator or automatically by an ARU.

TOPSDEV OM group

This OM group counts messages that are printed on TOPS output devices. A tuple is provided for each output device.

TOPSEA OM group

This OM group counts the number of calls handled for a carrier, transferred to a carrier, and forwarded to a carrier. It also counts inward service calls received from a carrier.

TOPSINCC OM group

This OM group pegs information about the use of CCITT calling cards as special number for TOPS calls that are alternately billed. Registers are defined to record the number of special numbers that are considered potential CCITT calling cards, to record the results of format checks on CCITT calling cards, and to record the type of validation performed on CCITT calling cards.

TOPSKFAM OM group

This OM group provides information on AMA billing records that are produced by TOPS operators using the SVCS key on TOPS MP positions.

TOPSMISC OM group

This OM group provides information on trouble reports entered by the operator and messages lost in TOPS MP operator centralization offices.

TOPSMTCE OM group

This OM group provides maintenance information on TOPS MP equipment.

TOPSOC OM group

This OM group provides information on calls that are routed from a remote toll switch to a TOPS operator at an Operator Centralization (OC) host office. The OC feature enables a TOPS switch to handle the operator traffic for several remote toll switches. The data provided by this OM group is used to monitor OC traffic and to assess the demand for TOPS MP OC positions.

This OM group is indexed on a remote switch basis, and it resides in the host offices. TOPSOC provides one tuple for each OC host office.

TOPSOCPS OM group

This OM group provides information on calls received at a TOPS MP operator centralization host office or at a TOPS stand-alone office. The OC feature enables a TOPS switch to handle the operator traffic for several remote toll switches. The data provided by this OM group is used to monitor the traffic that is handled by a TOPS OC host or TOPS stand-alone office.

TOPSOCPS provides one tuple for each class of calls for the TOPS OC host and remote toll offices, or for the TOPS MP stand-alone office.

TOPSPARS OM group

This OM group monitors the use of the TOPS personal audio response system.

TOPSPSZ OM group

This OM group provides information about calls made to operators at TOPS MP positions. TOPSPSZ provides a tuple for each call queue.

TOPSQMS

This OM group records queuing events for TOPS calls that request an operator position from the queue management system (QMS) call and agent manager (CAM). It also records the action taken by the QMS CAM in response to these requests.

TOPSQS OM group

This OM group provides information on TOPS MP queues. TOPSQS provides a tuple for each call queue.

TOPSRON OM group

This OM group provides information on RONI calls that are received at a TOPS switch. RONI is a feature that enables a TOPS operator at a distant TOPS toll switch to perform calling number identification for calls originating at another toll switch. RONI service performed by a TOPS operator is required for ONI calls and ANI fail calls.

The data provided by this OM group is used to monitor RONI traffic at a TOPS switch. See TOPSMISC OM group, register RONITBL for maintenance information.

TOPSTRAF OM group

This OM group provides information on TOPS MP traffic for TOPS MP stand-alone offices and operator centralization host and remote offices. The data provided by this OM group is used to monitor TOPS MP traffic and to assess the service provided by TOPS MP.

TOPSUSE OM group

This OM group provides information on occupied TOPS MP positions, maintenance busy TOPS MP positions, and the volume of work handled by TOPS MP positions.

TOPSVC OM group

This OM group counts events that occur when TOPS MP attempts to connect to a virtual circuit. This OM group is indexed on a switch basis, and resides in both the host and remote offices.

TRMSCRND OM group

This OM group counts domestic calls from coin stations that are billed to a domestic credit card, which, when screened, is shown to be compromised for domestic calls.

TRMSCRNO OM group

This OM group counts overseas calls from coin stations that are billed to a domestic credit card, which, when screened, is shown to be compromised for a call to that country.

VSNCOM OM group

This OM group measures, on an application basis, call attempts and dispositions for Voice Service Node (VSN) related calls.

VSNLINK OM group

This OM group measures the application level activities on the data links connecting the DMS with the VSN. The VSN and DMS use an application protocol to exchange messages relating to:

- billing
- network connections
- call disposition
- maintenance notification
- audits

TOPS MP maintenance

The DMS equipment architecture for a TOPS MP application has two configurations:

- Standard base (stand-alone) (DTCs or trunk modules)
- Integrated base (TOPS Message Switch (TMS))

Site tests (TOPS MP terminal and TPC equipment standard base)

This most basic test is activated when the TOPS MP terminal is initialized. A satisfactory test is indicated with checks in the small boxes on the VDU. If a failure is encountered, the check marks are missing. A log is recorded in the TAMI (TPC Administrative Maintenance Interface) system. TAMI is menu-driven, and performs the following traffic administration and maintenance functions:

- TPC logs
- TPC datafill
- position status and control
- HSDA status and control
- diagnostics
- date and time
- reset TPC
- Sonalert

NOTE: The above features apply to the MP standard base system. For the TOPS MP integrated system, some functions have migrated to the DMS MAP function (those functions are listed starting on page 4-53).

Selecting the diagnostics menu from the TAMI terminal accesses the following sub-menu maintenance tests:

- HDISK (hard disk)

- FDISK (floppy disk)
- POSDIAG (MP terminal and the TPC equipment)
- HSDA (high speed data for optional features)

Telescope into the POSDIAG level to perform the following MP terminal and TPC tests:

- CARD (9 functions tested in TPC)
- HSLI (loopback diagnostics)
- VOICE (loopback)
- PATTERN (VDU screen check)
- SCREEN (VDU diagnostic)
- MANKEY (keyboard test)
- TCD (Terminal Component Diagnostics 9 tests)

Site tests (TOPS MP terminal and TPC equipment integrated base)

Self check test is the most basic test and is activated when the TOPS MP terminal is initialized. A satisfactory test is indicated by check marks within the small boxes on the VDU. If a failure is encountered, the check marks will be missing. A log is recorded in the TAMI system.

TOPS MP terminals and TPC testing are initiated from the MAP TPC;MP level. The MAP workstation may be remotely located at the TOPS OSC and should have appropriate security safeguard measures. The following test functions are performed from the MAP MP sublevel:

- Test MP terminal and HSLI card diagnostics (TSTMP)
- Test MP terminal diagnostics (TST TERM)
- Test HSL1 card diagnostics (TST HSL1)
- Busy status (BSY, BSY MB, BSY INB)
- Return to Service (RTS)
- Force Release (FRLS)

POSDIAG tests

Refer to NTP 297-2281-530, *DMS-100 Family TOPS MP TAMI User Guide*, for further information about POSDIAG.

The POSDIAG command performs the following diagnostic tests on an MP position:

The POSDIAG command: performs diagnostics on TOPS MP position. The position number range is 0 to 3.

The CARD subcommand: performs the TOPS HSLI card diagnostics. Card diagnostic tests 1-6 are performed unless the individual option (#) is specified. If the individual option (#) is specified, only that test is performed. A message for each diagnostic is displayed to indicate which diagnostic is being performed. The diagnostics and option numbers are as follows:

1. Training port register test

2. CC port register test

3. Training port internal loopback test

4. CC port internal loopback test

5. HSLI port register test

6. HSLI port RAM test

7. Training port external loopback test

8. CC port short internal loopback test (through USART)

9. CC port external loopback test

The HSLI subcommand: performs a loopback diagnostic that tests the communication with the MP terminal. This diagnostic requires the MP to be connected to pass.

The VOICE subcommand: is used to enable and disable the voice circuitry of the MP. The MP is downloaded with its application software and the voice circuitry is enabled. A prompt to exit is displayed. If the user enters EXIT, the DIAG command is exited. When the voice circuitry is enabled, the voice line to the TPC is connected to the headset output of the MP.

The LOOPBACK option: sets loopbacks in the voice path of the TOPS HSLI card, such that the input from the DMS is looped back as output to the DMS and the input from the MP is looped back to the MP. The LOOPBACK option is used to test the TPC and MP voice circuitry.

The PATTERN subcommand: performs the MP pattern diagnostic. The MP is downloaded with its application software. A prompt to continue to the next pattern (NEXT) or exit the diagnostic (EXIT) is displayed on the TAMI before each pattern is displayed on the MP. The patterns are grid, character set, grey scale, and spiraling maze.

The SCREEN subcommand: performs the MP screen diagnostic. The MP is downloaded with its application software, and lines of h's are continuously displayed on the MP screen. The user is prompted at the TAMI to exit the diagnostic (EXIT).

The MANKEY subcommand: performs the MP manual keyboard diagnostic. The MP is downloaded with its application software, and a picture of the MP keyboard is displayed on the MP screen. When the user presses a key on the MP keyboard, the corresponding key in the picture is highlighted. The user is prompted at the TAMI to exit this diagnostic (EXIT). The CODES option displays the keycodes of each key pressed at the TAMI.

The TCD subcommand: performs the Terminal Component Diagnostics (TCD) of an MP. All the TCD diagnostics are performed, unless the individual option (#) is specified. If the individual option (#) is specified, only that test is performed.

A message for each diagnostic is displayed to indicate which diagnostic is being performed. The TCD option (#) and related diagnostics are as follows:

1. ROM test
2. CPU test
3. Exceptions test
4. RAM test
5. HSLI port test
6. UART test
7. Display controller test
8. Keyboard test
9. Telephony test

NOTE: The RAM test takes approximately 3 minutes. The keyboard test will fail if no keyboard is connected.

HSDA diagnostic tests

The HSDADIAG command performs the following diagnostic tests on the High-Speed Data Access HSDA card. Following are subcommands and descriptions:

The BASIC subcommand: performs the basic SDA diagnostic that resets the HSDA card. This initializes the HSDA card, including power-up and reset diagnostics. Also, diagnostics are run to test the communication path between the SBC and HSDA card. Before each step of the basic HSDA diagnostic is performed, a message is displayed indicating which step is being performed.

The EXTENSIVE subcommand: performs the extensive HSDA diagnostic. This includes the basic HSDA diagnostic, plus some extensive diagnostics. Before each step of the basic and extensive HSDA diagnostic is performed, a message is displayed indicating which step is being performed. If the individual option (#) is specified, only that diagnostic is performed. The HSDADIAG option (#) abd related diagnostics are as follows:

1. System RAM test
2. Timers and interrupt test
3. Data communications test

The data communications parameters (<dcomm>) specify the link or links (0, 1, or both), the loop back path (internal or external), and the clock source (internal or external). A baud rate can be specified for the internal clock source. The values for the baud rate are 1200, 2400, 4800, 9600, 19.2 Kbps, 38.4 Kbps, 56 Kbps, and 64 Kbps.

The default data communications parameters are both for the link or links, internal for the loopback path, and internal (64 Kbps) for the clock source.

The data communication test (test 3 described above in the EXTENSIVE subcommand) is a procedure for identifying and sectionalizing V.35 data link faults. Use the internal and external loopback path parameter and known loopback points on the data link to sectionalize the fault into the far end, near end or data link facility. When an error is detected, an error message is displayed on the screen.

TOPS MP integrated maintenance (OSC site)

TOPS MP integrated maintenance involves the following OSC site equipment:

- TOPS MP position
    - VDU (screen)
    - keyboard
    - base
- Teleprinters
- TPC
- Link maintenance
    - T1 carrier
    - data links (see note)
    - DSUs

NOTE: The TOPS integrated configuration utilizes HSDA cards, DSUs, and V.35 data links between the TMS and TPC. The two V.35 data links carry all the data for the four MP positions and associated TPC.

The TOPS position and TPC are maintained from the MAP TPC level and the TAMI. The entrance of the TMS peripheral, related HSDA links, and resulting high-speed data links through the TOPS message switch, provide the means to extend some TPC and MP maintenance and administrative functions to the MAP TPC level. TTP maintenance activities for the 3-port conference circuits, position status are described starting on page 4-25.

The TOPS MP integrated system has affected a migration of some maintenance and administrative tasks from TAMI to the MAP. These are:

- TOPS MP positions can be datafilled at any time from the TAMI. However, the datafill will only take effect after the position is busied and returned to service from the MAP
- TOPS MP position states cannot be controlled from the TAMI in the integrated TOPS MP system.

- TPC diagnostic routines cannot be executed from the TAMI in the integrated TOPS MP system. The remaining disk based diagnostics performed from the TAMI are:
    — TPC logs
    — TPC datafill
    — HSDA status and control
    — diagnostics (less TPC tests)
    — date and time
    — SONALERT

TOPS MPX maintenance

TOPS MPX maintenance involves the following OSC site equipment:

- TOPS MPX position
    — IBM PS/2 VDU and base
    — keyboard
- Link maintenance
    — T1 carrier
    — Datalinks
    — DSUs

NOTE: The TOPS MPX site configuration is interconnected using connectorized cabling. A wiring closet with BIX (Building Interoffice Crossconnect)and MAU (Multi-station Access Unit) connectors facilitate cable terminations. This is a passive device. However, when troubleshooting, these connectors and related cabling must be included in the fault process.

TOPS MPX position is maintained from the MPX position and MAP TPC level. TTP maintenance activities for the 3-port conference circuits and position status are described starting on page 4-25.

MPX terminal maintenance involves power on self tests and a series of diagnostics tests run from the floppy disk drive associated with each position. MPX power on self test of the PS/2 terminal is a series of diagnostic tests performed each time the MPX terminal is powered up. These tests are:

- memory tests
- checksum verification of the read-only memory
- keyboard tests
- verifies all configured plug-in cards are seated

If a trouble is detected, the MPX screen shows no message or an auto booting message. RESET does not work: only "*" appears on the VDU screen.

Failures occurring during the power on self test are detected by a system audit via the token ring and VPC position 2. The fault is alarmed and logged at the host DMS as a TOPS position fault.

MPX terminal tests use the following diskette test programs. These MPX terminal hardware tests are to be run by qualified MPX/PS/2 technicians, or in some cases, contracted to a third party.

- The system disk is used to troubleshoot TOPS MPX hardware and to boot the TOPS MPX terminal to a DOS prompt, regardless of what may be installed (correctly or incorrectly) on the hard drive. The system disk also provides diagnostics for the digital telephony (audio) card.

- The hardware reference disk is used to configure and to test the TOPS MPX base hardware. It contains diagnostics for the Real-Time Interface Coprocessor (RTIC) card, token-ring network adapter card, and TOPS MPX keyboards. This hardware is similar to the IBM PS/2 Model 55 SX hardware. Documentation is provided by IBM Personal System 2 Model 55 SX Quick Reference.

LAN surveillance

The token ring Local Area Network (LAN) provides the connectivity for the individual MPX positions to the VPC in their cluster, and IBM DAS for the configuration.

During operation, each of the TOPS MPX positions in a cluster continually sends audit messages to the active VPC (type 2 position) indicating that all is well. If a position fails, it will not send an audit message. The VPC detects that no audit message was received from the failed position and sends an unsolicited maintenance message to the DMS. On receiving the maintenance message, the DMS CC changes the position state for the failed position and generates appropriate logs and MAP indications.

The hardware that provides the VPC function is located in position Type 2 and the IBM DAS link termination position Type 1.

When a fault is indicated, gather all pertinent information and analyze it to sectionalize the fault and restore service. Information would include:

- Reported fault(s)
    - database access
    - DA calls and distribution
    - audio announcements
- Scope of fault
    - all positions
    - 4 positions (cluster)
    - one position affected

- DMS switch indications
    - alarms
    - logs

An assessment of the initial fault information should provide the direction for specific testing and trouble sectionalization for the following:

- DMS switch fault
- IBM DAS fault
- MPX position fault
- DATALINK faults
    - MPX to IBM DAS
    - MPX to DMS switch
    - DMS switch to IBM DAS

MPX MAP maintenance activities

The maintenance of the TOPS MPX from the MAP is essentially the same as maintenance of the TOPS MP on TMS. It includes the ability to return to service, manual busy, and test the TOPS MPX. Also, all audits that attempt to recover positions are applicable.

Knowledge at the DMS MAP of the TOPS MPX components is limited to the TOPS MP and TPC, where TOPS MP is equivalent to the TOPS MPX operator position and TPC represents the Virtual Position Controller (VPC) residing in the TOPS MPX type 2 position.

TPC MP level is required even though a physical TPC does not exist. The TOPS MPX provides a VPC—associated with a cluster of one to four TOPS MPX positions—that is functionally equivalent to the TPC. The VPC is resident in the type 2 TOPS MPX positions.

When receiving a TPC RTS or busy message, the TOPS MPX, acting as the VPC, always replies with a positive message if it is able to respond. If the VPC cannot respond to an RTS message, the RTS will fail with no reason reported. If the VPC does not respond to a busy message, the TPC will still go busy at the MAP level.

The MPX handling of RTS, BSY, and TST commands is as follows:

- Return-To-Service (RTS) — command is sent by the DMS to the TOPS MPX being returned to service. The TOPS MPX takes the appropriate action to return the position to service and sends a positive response back to the DMS. If the TOPS MPX cannot respond within a time-out period or sends a negative reply, the position will fail to return to service. No reason for the failure is indicated at the MAP, only that the return to service failed.

- Busy (BSY) — command is sent by the DMS to the TOPS MPX being busied. The TOPS MPX takes the appropriate action to make position busy, and sends a

positive response back to the DMS. If the TOPS MPX cannot respond within a time-out period, or send back a negative reply, the position will still be made busy at the DMS.

- Test (TST) — command is sent by the DMS to the TOPS MPX being tested. The TOPS MPX will normally return a positive reply. If the TOPS MPX fails to reply or returns a negative response, the test will fail. No reason for the failure is indicated, only that the test failed.

TOPS MPX-IWS maintenance

For TOPS MPX Intelligent Work Station (MPX-IWS) and supporting maintenance tools and procedures, see NTP 297-2251-524, *DMS-100F TOPS* MPX-IWS *Maintenance Guide*. The following trouble locating procedures are provided in this NTP:

- Activating TOPS MPX-IWS maintenance tools
- Using the TOPS MPX-IWS log display tool
- Using the profiler tool
- Using the position message trace tool
- Using the keyboard scan coder tool
- Using the generate test log tool
- Using the Nortel Networks digital audio adapter card test tool
- Using TOPS MPX-IWS maintenance tools through remote access
- Using the OIA (Open Information Access) trace tool
- Using the OIA post analyzer tool

Winchester disk drive tests

HDISK command runs the following diagnostic tests on the Winchester disk drive:

- System initialization test
- Controller internal diagnostics
- Controller internal RAM test
- Track format check
- Seek test
- Sector read test

Floppy disk drive tests

FDISK command runs the same set of tests on the floppy disk as recorded above for the HDISK.

TOPS Message Switch (TMS) maintenance

For details on the TOPS Message Switch (TMS) maintenance, reference NTP 297-8341-550, *DMS-100F TOPS Message Switch (TMS) Maintenance Manual.*

TMS datafill

The datafill for a TMS system is supplied with the TMS software load. However, the capability to datafill TPCs and MPs in a TOPS with TMS configuration is provided from the MAP—MPXs are loaded at the PS/2 base. The TMS is datafilled in table LTCINV. TMS P-side link information is datafilled in table LTCPSINV. These are existing tables and have not been changed to support the TMS, except that the range of the key field (PM_TYPE) has been extended to include TMS. DCHs are datafilled in table DCHINV. The ranges of three fields in this table have been extended (PMTYPE, SERVICE, and DCH_CHNL_TYPE).

Datafill for TMS subtending nodes involves the following tables:

- Table TPCINV
- Table TMSPSDEV
- Table TOPSPOS
- Table TOPSDEV
- Table TMSPVE
- Table SPECCON

The system is placed in-service in the following order:

- TMS
- Links
- TPC
- Operator positions

The TMS system maintenance hierarchy is as follows:

MAPCI (MAP command interpreter)

MAPCI;
    MTC; (Maintenance)
        PM; (Peripheral Module
            TMS; (TOPS message switch)
            DCH; (D-Channel Handler)
            ISG; (ISDN Services Group)
        TPC; (TOPS Position Controller)-(VPC)
            MP; (Multipurpose Position)-(MPX)

NOTE: The TMS, DCH, and ISG MAP levels are derived from the ISDN LTC.

The TMS MAP level is used to support TMS peripheral equipment:

- The DCH MAP level is used to support the D-channel handler.

- The ISG MAP level is used to support the TMS data channel maintenance.

- The TPC MAP level is used to support the TOPS position controller and associated hardware, including VPC associated with MP positions.

- The MP position MAP level is used to support the multipurpose position, MP and MPX.

Maintenance at the TMS level

The TMS MAP level is used to perform maintenance on the TMS peripheral module that is similar to ISDN LTC for maintenance activity. These include REX tests, ROM tests, SWACT activity, P-side link, in-service and out-of-service tests, and other tests and administrative functions. Access the TMS MAP level by entering the following commands from the CI level:

MAPCI;MTC;PM;POST TMS.

Maintenance at the DCH level

The DCH MAP level is used to monitor and maintain DCH channels. The DCH maintenance subsystem allows you to load, test, busy, offline, return to service, and query the operation of the DCH. Access the DCH MAP level by entering the following command from the CI level:

MAPCI;MTC;PM;POST TMS #;DCH.

Maintenance at the ISG level

The ISG MAP level is used to perform maintenance on the TDC channels (TMS data channel) used by the TPC, DA, and ORDB for data access. The ISG directory may be accessed from the ISG level of the MAP. The ISG directory (ISGLTCDIR) and the ISG level are accessed by entering the following (from the CI environment):

MAPCI;MTC;PM;POST TMS #;ISG

TDCSHOW command for displaying TMS OMs

Registers in OM groups TDCPROT and TDCROUT peg data link faults that can be interrogated at will using the ISG MAP level and command TDCSHOW. This near real-time access to data link performance provides information on a per-link basis. Analysis of these registers should help in locating constant and marginal problems.

The data being displayed is for the pegs tallied in the active OM registers. The OM system transfers the information periodically (typically 15 or 30 minutes). After each transfer from active to holding, the registers are set to zero.

The TDCSHOW command displays for the selected OM group, registers, and link the peg count for that interval of time. To use the TDCSHOW command, the channel must be a connected in-service TMS data channel. The TMS, DCH, and associated

DS1 must be in-service and the status of the special connection in table SPECCONN must be set to ACTIVE.

TDCPROT OM group

This OM group provides information on errors in protocol, noisy links, or links that are down. DCH protocol OMs include the X.25 network layers 1, 2, and 3 OMs. Note that the peg counts are kept in the TMS and transferred to the CC prior to the transfer of the active registers to holding status.

TDCROUT OM group

This OM group provides router information on the TMS data channels in the DCH and the ISP. Note that the peg counts are kept in the TMS and transferred to the CC prior to the transfer of the active registers to holding status.

Maintenance at the TPC level

The TPC MAP level is used to perform maintenance on the TOPS position controller and virtual position controllers (VPC) associated with MP and MPX positions. The TPC directory may be accessed from the PM level of the MAP. The TPC level allows TPC/VPC and MP/MPX to be posted, busied and returned to services. Busying a TPC/VPC from the MAP also busies in-service MP or MPX positions subtending the TPC/VPC. The TPC level is accessed by entering the following from the CI level:

MAPCI;MTC;PM;TPC

Maintenance at MP MAP level

The MP MAP level is provided to perform maintenance on MP integrated and MPX terminal positions on TPCs that subtend a TMS. The MP MAP directory is accessed from the TPC level of the MAP by entering the following from the CI level:

MAPCI;MTC;PM;POST TPC;MP

Optional features — maintenance considerations

Maintenance for TOPS optional feature functions such as DAS, ORDB, AABS, and ADAS involve the following activities:

- surveillance and trouble detection
- sectionalize trouble to the maintenance force responsible:
  — vendors stand-alone computer system
  — data link facilities and DSUs
  — DMS switch data link terminations (MPC/DTC)
  — OSC TOPS site (TPC)
  — DMS software feature
- HSDA maintenance testing from the TAMI
- fault connection by the responsible maintenance force

- follow-up, including escalation, if required
- return-to-service (RTS)

Assumptions

1. The maintenance center responsible for the host DMS switch is prime—in control—for all activities required for surveillance, trouble detection, sectionalization, escalation, and return to service.

2. Accepted Nortel Networks surveillance and maintenance procedures are in effect for the host DMS switch hardware and software.

Maintenance considerations for AABS

Maintenance considerations are required for the following elements that make up an AABS system:

- VSN
- T1 carrier facilities
- Datalink facilities
- MPC
- DTC
- software
- embedded DMS switch maintenance activities

The Voice Service Node (VSN) is external to the DMS switch and TOPS OSC, and can be provided by Nortel Networks or other vendors.

The stand-alone VSN equipment is maintained by a third party.

VSN log (VSN100/VSN115, TVS, and VSN200) types are generated at the DMS switch when errors in protocol—between the VSN and DMS—are detected. Also, unexpected messages or messages that cannot be interpreted generate logs at the OMS.

The VSN sends maintenance notice messages to the DMS switch to inform the operating company personnel of any abnormal or maintenance conditions occurring at the VSN. Generally, these log reports are information only. These are software alarms and generate logs EXT105 to EXT108 levels of severity, accompanied by a brief explanation that is set in tables VSNALARM and SFWALARM. In addition, two other software alarms are generated when only one data link is available, and when all logical data links are out-of-service.

The T1 carrier facilities serving the VSN are maintained using the existing DMS switch T1 carrier surveillance alarms and logs. Carrier testing is accessed from the CARRIER level of the MAP.

The T1 line interface between the VSN and the DMS switch includes one backup T1 line facility for sustaining service levels when a failure occurs.

The Automated T1 Line Switchover feature, in software package NTG230AA, is applied to Nortel Network's VSN. Prior to BCS32, N+1 redundancy of T1 links between the DMS-100 and the VSN required manual intervention to utilize backup T1 capacity in the instance of a link failure. Manual intervention was also required to return the backup link to its original state once the failed link recovered. The automated T1 link switchover feature eliminates the need for manual intervention at both link failure time and recovery time.

The T1 switchover feature is transparent to the DMS (i.e., the DMS does not know if it is selecting a channel on a standby or a nonstandby link). When a standby link becomes available for traffic, it looks to the DMS like a nonstandby link.

Telco surveillance indicators for the data links are derived from the logs and alarms generated by the MPC and reported through the Logutil subsystem and MAP alarm banner.

Maintenance for the MPC, DTC, other switch hardware, and software is embedded into the existing overall DMS switch surveillance and maintenance procedures.

Calling card validation maintenance considerations

The maintenance considerations for calling card validation (CCV) comprise the following elements:

- CCS7 connectivity to the LIDB
- DRAM hardware
- software
- embedded DMS switch maintenance activities

The ACCS uses the CCS7 (Common Channel Signaling System 7) network to access the LIDB database. CCS7 is an integral part of the DMS switch with its own dedicated maintenance activities that are embedded in the overall DMS switch surveillance and corrective activities. See the "SS7 Overview and Maintenance" subsection within this tab for a description of CCS7 and maintenance related information.

DRAM card NTIX67CA is associated with the ACCS. The card is installed in a modified MTM shelf for DRAM service (NT2X58AK). The recorded output messages should be checked periodically. DRAM maintenance is described in the "DRAM Maintenance" subsection within this tab.

Various software feature packages are required to establish CCV services. It becomes part of the PCL load for the switch, including software audits for feature monitoring.

Accepted Nortel Networks surveillance and maintenance procedures are in effect for the host DMS switch hardware and software.

ACTS maintenance considerations

Maintenance considerations are required for the following elements that make up an ACTS system:

- DRAM (NTIX76AE card)
- CDC (Coin Detection Circuit) NT3X08AB card
- CF3P (3-port conference circuits for recall activity)
- software
- embedded DMS switch maintenance activities
- coin phone station maintenance.

DRAM cards NTIX67AE are associated with the ACTS. The card is installed in a modified MTM shelf for DRAM service (NT2X58AK). The recorded output messages should be checked periodically. DRAM maintenance is described in the "DRAM Maintenance" subsection within this tab.

The CDC (Coin Detection Circuit NT3X08AB) occupies one card slot in an MTM, but uses eight time slots. Therefore, four consecutive card slots are required (3 slots are unusable). A maximum of three CDC cards can be mounted in any MTM shelf (NT2X58AC). Each card houses eight coin detection circuits for ACTS application. CDC maintenance is described on page 4-27 in this subsection.

The CF3P (three-port conference circuit) occupies one slot in the MTM. Maintenance access is from the MAP TTP level. Periodic routine testing is scheduled using the ATT feature.

Various software feature packages are required to establish ACTS service. It becomes part of the PCL load for the switch, including software audits for feature monitoring.

Accepted Nortel Networks surveillance and maintenance procedures are in effect for the host DMS switch hardware and software.

Feature NTX208AB (AL001) tests the ability of ACTS coin phones to correctly generate tones—indicating the deposit of coins such as nickels, dimes, quarters, and dollars. This test is performed by station repair personnel. Before initiating this ACTS station test for pay phones, establish the test line access telephone number in tables HNPACONT, and HNPACODE. ACTS coin station testing is described on page 4-28, within this subsection.

TOPS ISUP

TOPS ISUP provides the ability for calls utilizing ISUP signaling to connect to a TOPS environment and receive Operator Services. This gives TOPS the ability to provide Operator Services for IECs and/or LECs which use ISUP signaling on their trunking.

Supported trunk groups

There are two-types of trunk groups that support ISUP to TOPS:

- IT trunk group type.
- ATC trunk group type.

These two trunk groups can route incoming ISUP calls to TOPS using existing translations including the T, S, and N selectors with the following restrictions:

- IT trunk calls can only use the T selector.

- ATC trunks support the T, N, and S selectors.

NOTE: Refer to feature AN1515: ISUP to TOPS Enhancements for a description of TOPS ISUP signaling.

ISUP protocols

GR317 Protocol

All non-equal access calls using a trunk group with ISUP signaling use the GR317 protocol. All calls using ISUP must use the T selector to route to TOPS since the GR317 protocol can only send prefix information (OA/DD) in the called number. It is important that the end office not strip off the prefix digit when sending the called number to TOPS. The only exception is when the OA and DD call types have dedicated trunk groups handling 1+ and 0+ traffic on separate trunks.

GR394 Protocol

All equal access calls on either IT or ATC trunk group types with ISUP signaling use the GR394 protocol. The protocol signals the prefix information using Nature of Address (NOA) Indicator. Even though the NOA is provided in both the 317 and 394 protocols, only the 394 protocol supports the additional parameters that indicate the prefix information. Thus, the End Office can strip off the prefix digits from the called number.

If the end office sends the 0ZZ+CIC as part of the called number requiring operator assistance, the 0ZZ+CIC is stripped from the called number prior to translations.

Tables used in TOPS ISUP

- AABSOST
- DNBKSUR
- DNBKSURI
- ISUPTRK
- MCCSOST
- TMTMAP
- TOPEATRK
- TOPSBC
- TOPSPARM
- TOPSTOPT
- TRKGRP

- TRKMEM
- TRKSGRP
- XFROPSEL

Optional Tables used in TOPS ISUP

- CLSVSCRC
- DNSCRN
- LCASCRCN
- TDBCLASS
- TOPSDB

Table ISUPTRK is a table created for ISUP trunks that interact with the TOPS environment. It provides for the definition of screening parameters, equal access information, call source type, ANI forwarding parms, a Release Link Trunking parm, a CLI restriction parm, a DNLOOKUP indicator, and a DISPLAY indicator.Local Calling Area Screening -- determines if the called number is local for the calling number.

LCA Screens can be entered in either Table ISUPTRK or Table TOPSBC but SHOULD NOT BE ENTERED IN BOTH. Call processing checks both tables and a called number can be set local by the system if it appears in either table.Class of Service Screening -- determines a route for the called number.

Class of Service Screening can be entered in either Table TRKGRP or Table TOPSBC but SHOULD NOT BE CONTAINED IN BOTH.Table TRKGRP supplies pretranslator name and an operator assisted call may be datafilled for both trunk IT and ATC group types.

Table STDPRTCT.STDPRT(ISIT)

FROMDIGS	TODIGS	PRERTE
00	0	T OA 1 TOPS OH 1 2 NONE
01	0410	T OA 1 TOPS OA 8 11 NONE
0411	0411	T OA 1 TOPS 411 4 4 NONE
0412	09	T OA 1 TOPS OA 8 11 NONE
10	10	T DD 5 TOPS DD 12 16 NONE
11	1410	T DD 1 TOPS DD 8 11 NONE
1411	1411	T DD 1 TOPS 411 4 4 NONE
1412	19	T DD 1 TOPS DD 8 11 NONE
2	9	N DD 0 NA

NOTE: The end office MUST NOT strip off prefix digits when using GR317 signaling protocol.

> **NOTE:** For GR394 Protocol, even though the above contains an example of the end office stripping off the prefix digits, TOPS will append it back for translations using the NOA parameter.

Carrier Identification

An incoming ISUP call is marked a carrier call if one of the following is true:

- A Carrier Identification Code is received in the IAM message or
- The incoming trunk has a CARTYPE datafilled in Table ISUPTRK with IEC (makes all calls carrier).

The call then utilizes the characteristics set forth in Tables TOPEATRK and TOPEACAR for the carrier.

Carrier Identification Parameter -- CIP

The CIP indicates the Carrier selection the originator chooses. The CIP is an optional parameter that is sent in the forward direction to the transit network as part of the IAM message. The CIP is loaded with the CIC for the inter exchange carrier and is activated in datafill of option fields in the ATC trunk group information and datafill of Table CICSETS.

TABLE TRKGRP

ISUP2 ATC 0 ELO NCRT 2W NIL MIDL NSCR 414 ITT Y EAPLAN Y 0 COMB N (CICSET CARRIER_A)$

TABLE CICSETS

CARRIER_A   7219

Billing Restrictions

Sent paid billing can be restricted for ISUP calls arriving at TOPS based upon how the call arrives. This can be done several ways from table datafill or information contained in the IAM message if the call is unacceptable to be SENT PAID.

- The Originating Line Identifier indexes Table OSSCAT and, if the index is assigned as a restriction, the system will follow the same process as if the call has originated on an MF trunk group type. If an OLI is not received, the call is marked as STATION PAID.

- Table ISUPTRK datafilled with field DNLKUP to Y forces the DMS to search Table DNSCRN for a match to either the Charge Number (if present in the IAM message) or the Calling Line Identifier contained in the IAM. If a match is found in Table DNSCRN, the call then proceeds through Tables TOPSDB, TDBCLASS, and RESTBILL (the appropriate RESTBILL table is determined by whether the call is DA or TA).

Table TOPSOPT

Datafilling Table TOPSTOPT for ISUP trunks is required for the same reasons Table TOPSTOPT is required for MF trunks. Several choices are made which determine what services the trunk group is allowed to access.

NOTE: If The ANITOCLI field is set to Y it has subfield BLKCLI that also needs datafill.

Limitations

There are several limitations using GR317/GR394 ISUP signaling

1. Open Number signaling is not supported

2. Operator hold is not supported and calls requiring Operator hold should not be routed over ISUP trunks

3. Coin control signaling and coin signaling ACTS functions are not supported. Other ACTS functions such as Notify and Time and Charges are supported.

4. Any function that manipulates the keypad for a coin station such as AABS or MCCS is not supported unless the keypad is enabled for the entire call.

5. GR317 does not support sending the prefix information in the NOA, and the End Office must not strip off the prefix digits for non-EA calls over IT trunks.

6. TOPS does not support terminating an Equal Access call to an ISUP IT trunk group.

7. Intercept call completion is not supported.

8. TOPS cannot pass along Calling Party Name information.

Release link trunking (RLT)

Release Link Trunking is used when the call completes back through the originating office because the originating and terminating subscribers belong to the same tandem office. That office must be a Universal Carrier (UCS) DMS250 Switch. The originating office connects the two parties and releases the trunk to the TOPS switch.

Release Link Trunking was introduced in LET007 with SOC code ENSV0019. It requires GR317/GR394 ISUP to/from TOPS, OSEA0005.

RLT-2, an enhancement to RLT, was introduced in LET0009 with SOC code OSEA0009

RLT-2 Enhancements

1. Calling Card (CC) and CC sequence calls.

2. CC automated handling by the MCCS and AABS systems as well as manual validation for TOPS IV, MP and IWS positions.

3. Supports proprietary CCs by the Operator System Services Advanced Intelligent Network (OSSAIN). In addition, OSSAIN calls using AABS for alternate billing are supported -- they use the trigger profiles for operation.

4. Intercept calls should not use RLT.

5. Call types supported by RLT are Sent Paid ADACC, Collect, Person, and Third party.Hotel, coin, and unspecified Class charge calls are EXCLUDED from RLT.

ISUPTRK Notes

1. Ensure the incoming trunk supports the correct VARIANT (specified in Table ISUPTRK) of RLT. Even if the SOC for RLT is on, RLT is not attempted if the trunk does not have the correct datafill in field RLT in Table ISUPTRK.

2. If the outgoing party has a connection, ensure the outgoing trunk supports the correct VARIANT and VERSION of RLT in Table ISUPTRK. This release requires the DMS250 have a software load of UCS08 or higher.

3. The Bridging Connection configuration requires that the Originating Point Code (OPC) of the originating trunk and the Terminating Point Code (TPC) of the terminating trunk be the same. The point code check ensures the originating office is holding a connection for both legs of the call.The Bridging condition must ensure that both the incoming and outgoing trunks have the correct VERSION in field RLT_VERSION.

4. If a call fails RLT, the system handles the call the same as without RLT. Two trunks are used to complete the call without the release of the originating and terminating trunks.

TOPS IWS

This describes the hardware and software enhancements for each combined IWS and TOPS release. The information begins with the most recent release.

IWSS013 with TOPS013

The IWSS013 release provides these enhancements:

- Conversion of IWS from 16-bit to 32-bit applications
    — keeps pace with operating system improvements
    — increases potential for integrating many other applications onto the position
    — allows better handling of multiple applications through pre-emptive multi-tasking
- Inclusion of additional customized IWS character sets for international customers
- Ability to adjust the default volume for operator headsets
- Addition of a Locality-to-Name key to NTDA, which allows the user to copy the location field entry to the Name1 field with a single keystroke. This key action is especially useful for government and business searches.

The TOPS013 release provides these enhancements:

- Introduction of TOPS over Internet protocol (IP)
    — enables MIS reporting using either existing X.25 interface or new QMS-MIS IP interface

— enhances operator centralization to allow IP transport of voice and data

- Development of Operator Services Network Capabilities (OSNC), providing a greater variety of services using ISUP signaling

- Enhancement of OSSAIN to support database-independent directory assistance automation

- The TOPS IWS Operator Guide, 297-2251-304, describes the use of ANI.

- The ability to recall to an operator for time and charges and to make external database queries at the end of calls on TOPS ISUP and R2 trunks.

IWSS0041/TOPS005

The IWSS0041 and TOPS005 releases provide the following enhancements:

- service allowing an end user in a foreign country to use an access code to reach an operator in a country in which the call is to billed

- ability for calls using pre-OSS7 Integrated Services Digital Network User Part (ISUP) signaling to connect to TOPS environment and receive operator services

- authorization code screening service for intra-LATA 1+calls

- enhanced audiogram delivery services, formerly called Message Delivery Services

Pre-OSS7 signaling

Calls using pre-OSS7 signaling can connect to a TOPS environment and receive operator services. The feature, called ISUP to TOPS Enhancements, also provides the following services:

- support for the conversion of ANI from an incoming multifrequency trunk to Calling Line Identification for an outgoing ISUP trunk with the added ability to block the calling party's number from being presented to the terminating party

- support for release of connection to a party if that party hangs up while the call is at an operator position or automated system

- expansion of support for operator assistance for ISUP

- searches in DN tables to determine calling station type and billing restrictions

- support of TOPS Release Line Trunking, which allows a TOPS office to request an originating office to complete a call

- support for the receipt and transmission of charge number and CLI if both are received

Carrier release link trunking

With release link trunking, you can maximize your use of the Signaling System 7 ISUP inter-machine trunks by releasing connections between a previous Universal Carrier Switch DMS250 and a TOPS switch. The TOPS switch uses the Universal Carrier Protocol ISUP protocol to signal call completion information to the previous office. This feature provides release link trunking to calling card services. With

release link trunking, the TOPS switch provides card validation and requests the previous DMS 250 to complete the call and maintain the connection. This feature also allows sequence calls to use release link trunking.

ISDN user part (ISUP)

A Common Channel Signaling 7 (CCS7) message-based signaling protocol that acts as a transport carrier for ISDN services. The ISUP provides the functionality in a CCS7 network for voice and data services.

IWSS010 with TOPS010

- The ability to recall to an operator for time and charges and to make external database queries at the end of calls on TOPS ISUP and R2 trunks.

The *TOPS IWS Operator Guide*, 297-2251-304, describes time and charges recalls.

Operator Services Agreements

In order to allow the operator services provider to wholesale their billing agreements in cases where CLECs do not want to secure their own agreements, two new parameters are added to table TOPSPARM:

- ALL_CALLS_USE_OPR_SVC_AGRMTS

This parameter is set to Y (Yes) when all calls incoming on TOPS/ISUP trunks are to use the operator services billing agreements to do the checks. The agreement groups are obtained from parameter OPR_SVC_AGRMTS. If the ALL_CALLS_USE_OPR_SVC_AGRMTS parameter is set to N (No), then whether or not to use the operator services agreements will be determined on an individual basis via field BILAGRMT in tables TOPEACAR or SPIDDB.

- OPR_SVC_AGRMTS

This parameter identifies the billing agreement groups with which the Operator Services wholesaler has billing agreements. Fields CCVAGRMT and BNSAGRMT provide an index into Tables CCVAGRMT and BNSAGRMT respectively. This parameter allows CLECs to use their own billing agreements or use the billing agreements already established by the Operator Services wholesaler. Field NOSPDERR, which shows up as a refinement field when parameter OPR_SVC_AGRMTS is data-filled as 'Y', allows the Operator Services wholesaler to define a default handling when the LIDB does not return an AO or BSP SPID in the query response. This field has three possible values:

- ACCPT - Accept the call
- BLOCK - Block the call
- OPER - Send the call to an operator if not at one (i.e., at an automated system), or if at an operator, block that billing method and allow operator to prompt for another method of payment.

Operator Services Network Capability (OSNC)

Operator Services Network Capability (OSNC) provides Integrated Services Digital Network User Part (ISUP) signaling capabilities based on Generic Requirements GR-1144-Core for a Traffic Operator Position System (TOPS) office.

In an earlier release, PRSDOC BK04281 provided very basic support of ISUP connections to TOPS. In TOP05, feature AN1515, ISUP to TOPS Enhancements, provided additional support for allowing calls using ISUP signaling to connect to a TOPS environment and receive operator services processing. The signaling provided by AN1515 is referred to as TOPS/ISUP. At the time, the signaling described in GR-1144-Core had been proposed, but was not finalized or ready to deploy to any market. The functionality provided by TOPS/ISUP was created as an interim solution to connect TOPS switches to the ISUP network prior to the wide scale deployment of Operator Services Signaling System 7 (OSS7).

For more information refer to PLN-8021-004, *DMS-100 Family North American DMS-100 Release Document*, "Operator Services Network Capability."

Feature Overview

This activity is the TOPS implementation of GR-1144, Section 8: Common Channel SS7. Note that this implementation is partially compliant with GR-1144.

The messages, parameters and values that are supported by TOPS are documented in the OSNC Protocol Specification.

The functionality provided by this activity is an enhancement to the functionality provided by TOPS/ISUP. Therefore, this document assumes that the reader has prior understanding of the functionality and signaling provided by AN1515.

This activity implements connection hold, coin signaling, network recall, forwarding of parameters received, the ability to combine direct dialed (DD) and operator calls on the same trunk group, and end-to-end signaling, allowing a larger variety of operator services to be deployed over ISUP.

Unless otherwise specified, all functionality available under TOPS/ISUP is also available to calls requiring OSNC functionality. Calls requiring OSNC functionality can be received on the same trunks as TOPS/ISUP calls. The new functionality implemented by this activity is divided into the areas below:

- Datafill
- Incoming Connections
- Outgoing Connections
- Mid-Call Functionality
- Releasing Connections
- MA
- Connectivity to Other Signaling Types
- Upgrade Strategy

DMS-100 Family OSNC Protocol Spec TOPS14 and up, 297-8403-907 describes the new functionality implemented for GR-1144. Call flows and detailed signaling information can be found in the OSNC Protocol Specification.

Throughout this document, unless specifically stated otherwise, the term "operator" refers to a TOPS operator; TOPS automated system, or a service node. This activity is specific to the North American TOPS product, and is not supported in the global environment.

Table 4-6 — New or modified logs

Log name	Log number	NEW/MOD/DELETED	System (SOS/UNIX)
TOPS	613	New	SOS

Table 4-7 — New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
TOPSCOIN	Changed	Unchanged
HNPACONT:RTEREF	Changed	Unchanged
FNPACONT:RTEREF	Changed	Unchanged
OFRT	Changed	Unchanged
OFR2	Changed	Unchanged
OFR3	Changed	Unchanged
OFR4	Changed	Unchanged

OSNC interworking call flows

The following provides an alphabetical list of the OSNC interworking call flows.

- OSNC-to-ATC trunk with TOPS ISUP signaling, delayed cut-through

- OSNC-to-ATC trunk with TOPS ISUP signaling, immediate cut-through

- OSNC-to-ATC trunk with TOPS ISUP signaling, transfer to carrier

- OSNC-to-IT trunk with TOPS ISUP signaling, delayed cut-through

- OSNC-to-IT trunk with TOPS ISUP signaling, immediate cut-through

- OSNC-to-IT trunk with TOPS ISUP signaling, intercept call completion

For detailed information on OSNC interworking call flows, refer to *DMS-100 Family OSNC Protocol Spec TOPS14 and up*, 297-8403-907.

Originating TOPS OSNC trunks

In order for a OSNC call originating on an IT or ATC trunk to be processed by TOPS, the trunk group must be datafilled in table ISUPTRK. The datafill provides a means for the TOPS software to determine if the call should be processed in this switch or tandemed on the to next switch. The reason behind this check is the fact that TOPS software is packaged in the LET PCL for the North American Incumbent Local Exchange Company (ILEC) market and the LLT PCL for the North American Competitive Local Exchange Company (CLEC) market. The TOPS software exists in the switch, but there may not be any operator services provided on that switch. The lack of datafill in table ISUPTRK is the stimulus for the TOPS software to bypass handling on the call.

ISUPTRK

Datafill in table ISUPTRK is specific. For detailed information on Datafilling table ISUPTRK for SS7 trunks, refer to OSNC Data Schema, *DMS-100 Family OSNC Protocol Spec TOPS14 and up*, 297-8403-907.

TOPS IP

Description

Position/Device Evolution IP was introduced in TOPS11. This feature introduces the following enhancements to TOPS devices.

- Maintenance and Administration Position (MAP) levels TOPSIP and TOPS-DEV are created.

- Communication of TOPS device application information to personal computers (PCs) using the Internet Protocol (IP) based Digital Multiplex Switch (DMS) Local Area Network (LAN). Refer to the *Translations Guide* for information.

- 30 minute, 6 hour, and 24 hour reports for Queue Management System (QMS) force management devices. Refer to the *Translations Guide* for information.

This functionality is provided by the following feature:

AF7827, TOPS Device Evolution

Background: TOPS device IP

Before this feature, TOPS device information was sent to teletypewriters (TTY) using digital modems (DMODEM). This feature provides access to the same information IP based DMS LAN to TOPS devices. In this configuration, device information is made available through Transmission Control Protocol (TCP) / IP telnet connections on the DMS Computing Module (CM). Personal computers (PC) with telnet client software are able to connect to a specific device application on the CM to access this information. The following figure is an example network.

Figure 4-5 — Example IP network
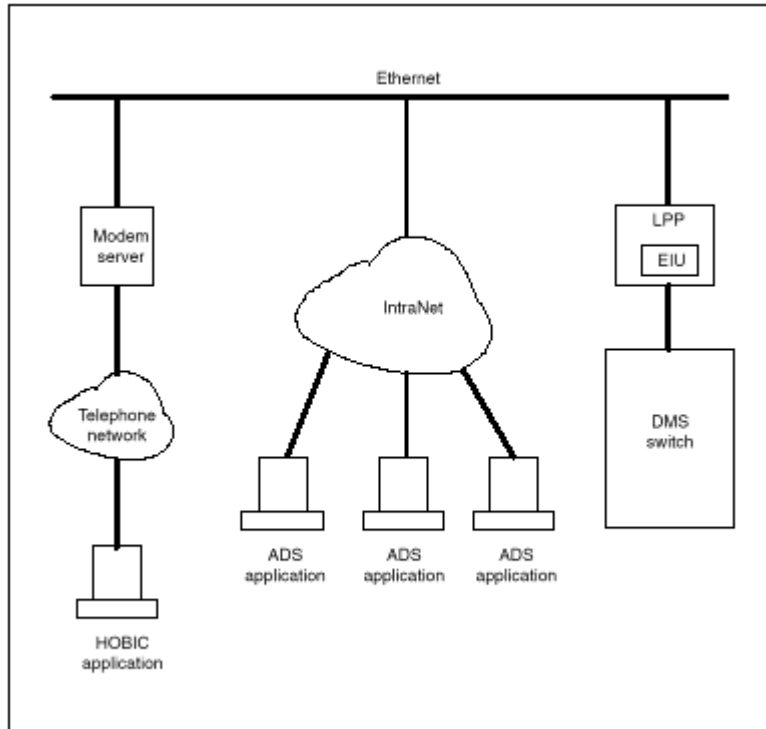
The above DMS switch connects to the Ethernet with an Ethernet Interface Unit (EIU) in the Link Peripheral Processor (LPP). An LPP is also known as a Link Interface Module (LIM). Then, Administrative Data System (ADS) applications can access the DMS switch directly or through Operating Company provided intranet access. Remote access to hotel billing information center (HOBIC) applications can be provided with the telephone network and dial-up modem servers. Network security can be provided using firewalls and secure modem servers.

MAP levels

The new MAP level TOPSIP is available at the MAPCI–>MTC–>APPL level. This level provides access to TOPS device IP specific maintenance. The TOPSIP level supports access to the TOPSDEV (TOPS IP Device) MAP level. This level provides commands and status displays for monitoring and controlling the TCP/IP device application connections. A count of the number of devices in a given state is displayed at the top of the user window. Below this, the status of the currently posted device is displayed. At the bottom of the screen, the TOPS device post set is shown.

The following states are supported by TOPS IP devices.

- UNEQ – Device Is not datafilled.
- OFFL – Device is datafilled.

- MANB – Device has been manually taken out of service and is unavailable for new connections.

- DISC – Device is currently not disconnected but ready to accept client connections.

- CPB – Device has a connection established

- SYSB – System has placed the device in a busy state. This occurs when the TCP transport service becomes unavailable. When the service becomes available, the system attempts to transition to the DISC state.

The left side of the screen shows the available MAP commands for TOPS devices. The following commands are available.

- POST – Either Post a specific device or post all devices in a given state.

- LISTSET – List each device in the post set along with its state.

- BSY – Attempts to transition to the MANB state. When in the MANB state, the device is not available for new connections. CPB to MANB transitions cause the current connection to be dropped. DISC to MANB transitions simply make the device unavailable for connections.

- RTS – Initiates a transition from the MANB to DISC state. Once in the DISC state, the device is ready to accept client connections.

- OFFL – Transitions from the MANB to OFFL state.

- INFO – Displays the device type, such as QFADS, the IP address, and TCP connection state.

- NEXT – Selects the next device in the post set

- QUIT – Exits the TOPSDEV MAP level.

NOTE: Existing XPMs cannot be retrofitted to provide IP functionality; rather, they must be replaced with an IP XPM.

Overview of the managed IP network

The managed IP network is responsible for routing and delivering data and voice traffic between nodes in the private intranet. Figure 4-6 shows a simple managed IP network for TOPS.

Figure 4-6 — Simple managed IP network
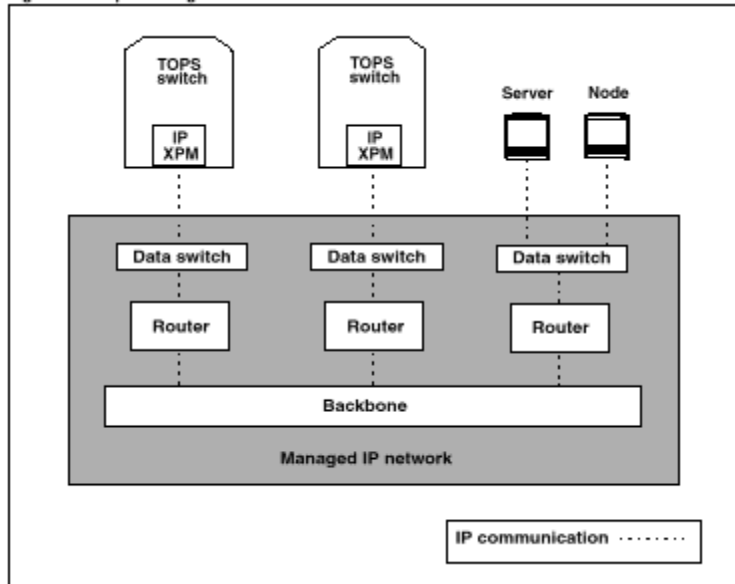
A managed IP network consists of several layers:

- *Data switches* act as hubs for the LANs of Ethernet ports on TOPS nodes (such as DMS switches, servers, and other nodes used by TOPS). Data switches should be used instead of passive hubs to minimize latency and maximize throughput.

- *Routers* connect the LANs served by data switches to wide area backbone networks, and they direct data between TOPS nodes.

- The *backbone* provides wide area transport, which links geographically-distributed host and remote switches, servers, and nodes. Backbone implementation uses technologies such as asynchronous transfer mode (ATM), Frame Relay, or point-to-point facilities.

NOTE: Figure 4-6 does not address practical network considerations such as redundant connections to the data switches and the backbone. For more information, refer to *DMS-100 Family TOPS IP User's Guide*, 297-8403-906: "TOPS IP engineering guidelines."

Engineering the managed IP network for TOPS has the following objectives:

- to handle all IP traffic for a specified operator call volume
- to provide low latency for voice and data traffic
- to provide low message loss for voice control and UDP control messages

Capabilities of TOPS IP

The TOPS IP product implements call processing, provisioning, and maintenance over an integrated IP infrastructure. In LET0013, two TOPS IP applications use the IP infrastructure: Operator Centralization (OC-IP) and Queue Management System Management Information System (QMS MIS).

This section introduces the capabilities of each application.

TOPS OC-IP

In an OC network, a number of TOPS remote switches share the operator positions provided by a TOPS host switch. Calls originate in a remote switch, which is responsible for call control. The host switch provides the operator positions and is responsible for call and agent queue management, force management, and position maintenance.

The OC host and OC remote communicate over voice links and data links to process a call. The OC voice links provide a speech path between the operator in the host and the calling and called parties in the remote. In a traditional configuration, each call must have a dedicated voice link while the operator services the call. The OC data links are used for call control messages, key function messages, and screen update messages. One data link can be shared by many calls in progress.

IP addressing of the SX05DA card

IP addresses are used to route IP packets to the correct node on the network. These addresses must be assigned to hardware before any messaging can occur. The SX05 serves as an IP-addressable network endpoint. The SX05 and the CM appear as a single entity to other nodes on the network. The CM does not use an IP address; rather, a CMIP application uses the IP address of the SX05 as its IP address.

NOTE: Ports are used in routing messages to the correct application software after the correct node on the network has been reached. These ports are unrelated to hardware ports, and are assigned, as applications need them.

A single XPM peripheral consists of two units, unit 0 and unit 1. One SX05DA card corresponds to one unit, for two SX05 cards per IP XPM. Each SX05 card has a single Ethernet interface with a fixed MAC (media access control) address. Only one SX05 is active at a time and the other is in standby mode. Figure 4-7 shows IP addressing of the SX05DA cards.

Figure 4-7 — IP addressing of the SX05DA
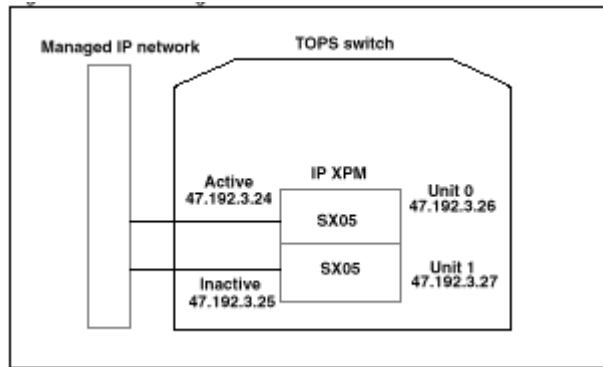
As shown in the figure, one IP address is used by the active SX05 and another IP address is used by the inactive SX05. In addition, the SX05 software internally assigns IP addresses to unit 0 and unit 1. Therefore, IP addressing of the SX05s requires a block of four consecutive IP addresses. The first address must be divisible by four, for example, 47.192.3.24. This address is bound to the current active unit, and is always used to address the XPM, even after it initializes or switches activity (SWACT). The other three addresses are bound as follows:

- second address (N+1) is bound to the inactive unit
- third address (N+2) is bound to Unit 0
- fourth address (N+3) is bound to Unit 1

GARP broadcast message

When the XPM initializes or SWACTs, it dynamically swaps the active/ inactive IP addresses of its two units the ensure that the current active unit is addressed correctly. Then, the XPM sends a GARP broadcast message to notify local hosts that the swap occurred.

Dynamic trunking

Dynamic trunking is the method used by DMS switch trunking applications to send voice traffic over a data packet protocol. With dynamic trunking, there is no fixed connection to the far end. In fact, when the trunk is not in use, there is no far end. Dynamic trunk members resemble TDM trunks, but with a few exceptions as described in the following paragraphs.

Trunk member datafill

The Gateway card does not keep track of its individual C-side trunk member states. So to prevent the possibility of the Gateway presenting a call on an incoming circuit that has not been datafilled in the CM, all possible members of the card must be data-filled in the CM. This task is achieved by automatically datafilling blocks of trunk members when the Gateway card is datafilled. Manual additions and deletions to individual trunk members are not allowed for dynamic trunk groups.

Trunk member maintenance

Because the Gateway does not keep track of the C-side states of the members, the state of the Gateway itself determines the state of each trunk member from the CM. So members cannot be individually maintained at the MAPCI;MTC;TRKS;TTP level. Instead, when the Gateway on the IP XPM is maintained from the MAPCI;MTC;PM level, the CM states and connections of the associated trunk members are automatically updated. It is possible to post trunk members at the TTP level of the MAP and view their states.

NOTE: Many TTP level commands are not supported for dynamic trunks. For a list of supported and unsupported commands, refer to *DMS-100 Family TOPS IP User's Guide*, 297-8403-906, "TOPS IP maintenance activities."

Carrier maintenance

The switch views the IP XPM as a remote node with respect to carrier maintenance. So the commands and functions that may be used at the MTC;TRKS;CARRIER level correspond to those of a standard remote carrier. As with trunk members, it is possible to post and view carriers from the CARRIER level.

NOTE: For a list of supported and unsupported carrier states, refer to *DMS-100 Family TOPS IP User's Guide*, 297-8403-906, "TOPS IP maintenance activities."

ISUP call processing

Dynamic trunking applications use ISUP signaling internally at the switch between the CM and the XPM. Some applications, including TOPS OC-IP, convert both the ISUP call control and the voice (bearer) into IP messages, whereas other applications use the existing SS7 network for call control and either IP or ATM for bearer. TOPS IP applications do not use the SS7 network.

Overview of datafill for IP data and voice

This section introduces the switch datafill needed to provision the IP data and voice infrastructure. It discusses both new and existing tables and gives example datafill.

NOTE: Details on how a particular TOPS IP application uses these tables (and other application-specific tables) are in the individual chapter that discusses the application. Details on table dependencies and the range of valid datafill for every table affected by TOPS IP are in *DMS-100 Family TOPS IP User's Guide*, 297-8403-906, "TOPS IP data schema."

The tables are described in the following order:

1. Hardware provisioning tables:

    — LTCINV (Line Trunk Controller Inventory)

    — CARRMTC (Carrier Maintenance)

    — LTCPSINV (LTC Peripheral-side Inventory)

2. Data provisioning tables:

— XPMIPGWY (XPM IP Gateway)

— XPMIPMAP (XPM IP Mapping)

— IPSVCS (IP Services)

— IPCOMID (IP Communication Identifier)

3. Voice provisioning tables:

— CLLI (Common Language Location Identifier)

— TRKGRP (Trunk Group)

— TRKSGRP (Trunk Subgroup)

— TRKOPTS (Trunk Options)

— SITE (Site)

— IPINV (IP Inventory)

— TRKMEM (Trunk Members)

OC-IP introduction

In an OC-IP configuration, a common IP infrastructure replaces the separate, point-to-point provisioning of data and voice between the OC switches. Through the IP XPM, TOPS IP handles all the data and voice traffic for OC calls across the managed IP network.

General OC functionality remains unchanged in a TOPS IP network. OC host and remote switches have the same fundamental roles in the call as before, and the IP data and voice communication technology is transparent to operators. OC-IP interworks fully with HRNQT and Alternate Host Selection. Figure 4-8 shows an example OC-IP configuration.

Figure 4-8 — **Example OC-IP configuration**
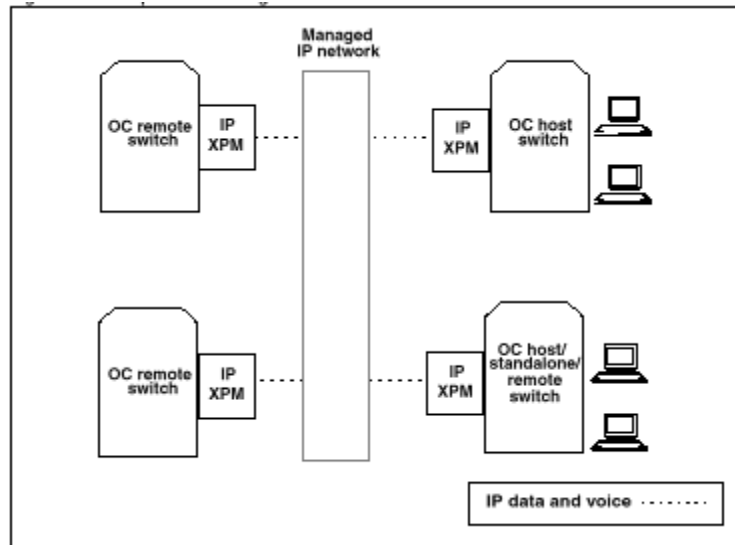
NOTE: The architecture of the operator network is unchanged for LET0013, so details of
position connectivity are not shown or discussed.

OC-IP data communication

This section discusses concepts and terms related to OC-IP data communication.

IP XPM data interface

The SX05DA processor card provides OC-IP data communication, which is used for
call control, key function, and screen update messaging between the OC host switch
and the OC remote switch.

OC-IP data links

The OC-IP application does not have a concept of data link groups. However, it is still
possible to datafill multiple data links to be used for communication with a distant
office. As with traditional OC, the reason for having multiple data links between a
pair of offices is to provide redundancy or to increase throughput capacity (or both).

An OC-IP data link uses the P-side Ethernet LAN connection in the XPM instead of
using a P-side DS1 or PCM30 port. Therefore, a data link no longer represents any
particular physical path to the distant switch. Depending on how the IP network is
configured and managed, it is possible for messages sent on a single data link to take
different routes through the network. But while the path can vary, the two endpoints
are fixed. An OC switch must have datafill for both of the connection endpoints—the
local end and the distant end—of each data link it uses.

Sockets

An IP connection endpoint is represented by a socket, which is a software entity iden-
tified by an IP address and a port.

IP addresses

IP addresses are used to route IP packets to the correct node on the network. For OC-IP data links, this means routing call control, key function, and screen update messages to the correct XPM at the correct distant TOPS switch.

Ports

Ports are used in routing messages to the correct application after the correct node on the network has been reached. For OC-IP data links, this means routing OC data link messages from the XPM to the switch CM software that "knows" about that particular data link. These are software ports, and they are unrelated to any hardware port.

Communication identifiers (COMID)

The local connectivity information is represented by a COMID, which is datafilled against the data link. COMIDs, introduced by TOPS IP data communication software, are not transmitted over the IP network. While it is not an industry-standard entity, the COMID is recognized by the XPM and by the CM, where it is visible in datafill, logs, and OMs. Each OC-IP data link is associated through datafill with a unique COMID.

Related switch datafill

The switch datafill for the local connection endpoint of an OC-IP data link identifies the XPM whose SX05 provides the data link LAN connectivity. Datafill also identifies a local port number that distinguishes this data link on the XPM from any other data links or applications that might be using the XPM for IP connectivity. Datafilling the XPM specifies its active IP address indirectly.

The switch datafill for the far endpoint of an OC-IP data link specifies the distant socket directly, as follows:

- It specifies the IP address of the SX05 XPM that provides LAN connectivity for the data link in the distant switch.

- It specifies the port number that is datafilled in the distant switch against its end of the data link. The CM cannot learn the far-end IP address from the network.

Parallel datafill requirements

Datafill for XPM IP addresses and ports must be coordinated between switches in the OC network. In addition, if the Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) is used to configure XPM IP addresses, the CM datafill at one end of a link must be consistent with the information provided by the DHCP or BOOTP server at the other end of the link. If the datafill between switches is inconsistent for a data link, it will not be possible to bring the data link into service.

NOTE: For more discussion, refer to "Parallel datafill for OC-IP data links" in *DMS-100 Family TOPS IP User's Guide*, 297-8403-906.

OC-IP voice communication

This section discusses concepts and terms related to OC-IP voice communication.

IP XPM voice interface

The 7X07AA Gateway card provides OC-IP voice communication, which is used to convert between circuit-switched voice and packet-switched voice in an OC call.

Dynamic voice trunks

OC-IP voice links use dynamic trunks to send voice traffic over a data packet protocol. With dynamic trunking, there is no fixed connection to the far end.

ISUP call processing

From the CM perspective, dynamic voice trunks appear as ISUP trunks that use the Q.764 protocol. This capability takes advantage of the existing ISUP signaling interface between the CM and the XPM. The XPM handles OC-IP calls differently from SS7 ISUP calls. With OC-IP, the CM includes proprietary information such as terminal identifiers (TID) in the IAM message used to establish the voice connection. Traditional ISUP call processing routes and receives messages from the SS7 network through the LIU7, whereas OC-IP ISUP call processing routes and receives messages through the IP XPM. The XPM then converts both the ISUP call control and the voice into data packets for the managed IP network.

NOTE: The SS7 network and associated datafill are not used in OC-IP.

Voice signaling

From the suite of H.323 multimedia communication protocols, OC-IP uses H.225-based messaging to set up voice connections between Gateways across the managed IP network. The proprietary OC protocol, rather than a gatekeeper, provides call signaling and control over OC-IP data links. H.225- based messaging uses the TCP data transport.

Voice packetization

The G.711 and G.729A codecs, also from the H.323 protocols, are used for voice packetization. G.711 provides uncompressed voice packetization and G.729A provides compressed voice packetization. An uncompressed voice stream provides carrier-grade voice quality at the expense of increased bandwidth; whereas compressed voice consumes less bandwidth but may provide lower voice quality. Both codecs use the UDP data transport.

NOTE: DTMF tones are not supported on the G.729A codec.

OC-IP unified topology

Figure 4-9 illustrates the paths for voice and data in the OC-IP unified topology. A description follows the figure.

Figure 4-9 — **OC-IP unified topology**
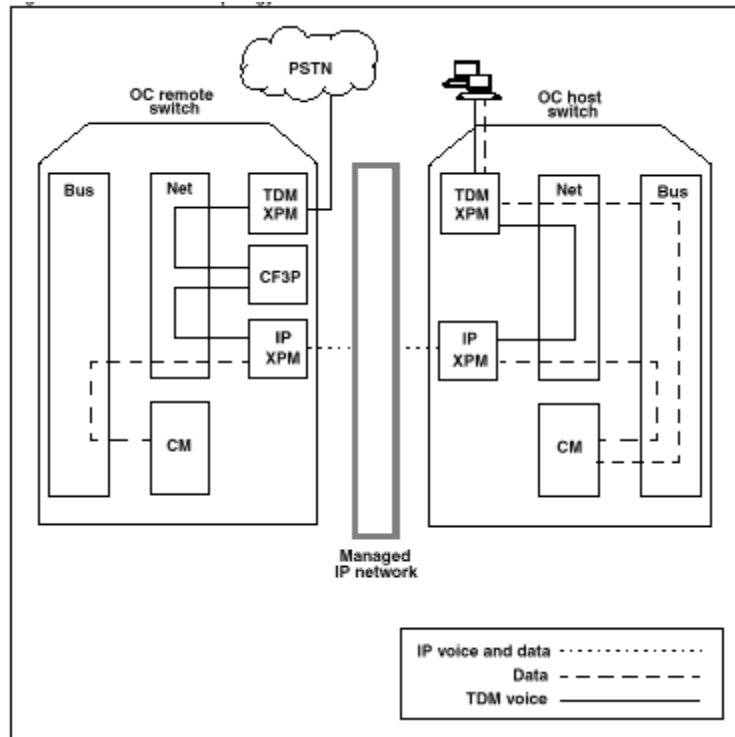
In the figure, the subscriber voice path originates at the OC remote switch from a TDM trunk in the Public Switched Telephone Network (PSTN), and is connected to a conference circuit (CF3P) through the switch. The OC voice link connects to the same CF3P and terminates to the C-side of the IP XPM 7X07 Gateway card. The XPM converts TDM voice to either G.711 or G.729A packetized voice, and presents the voice stream to the managed IP network. The switch CM communicates with the IP XPM Gateway using ISUP signaling. The XPM converts ISUP to H.225 and delivers it to the managed IP network.

TOPS IP maintenance activities

Refer to *DMS-100 Family TOPS IP User's Guide*, 297-8403-906 for a discussion of switch maintenance activities for the following TOPS IP areas:

- IP Gateway node maintenance

- OC-IP maintenance

- TOPS QMS MIS IP maintenance

TOPS IP CI tools

The XIPVER (XPM IP Verification) command interface (CI) tool is used at the DMS switch.

NOTE: For information on using switch CI tools, refer to: "TOPS IP CI tools" *DMS-100 Family TOPS IP User's Guide*, 297-8403-906

XIPVER

XIPVER is a multi-user tool that allows users to test IP data communication through the SX05 card on the IP XPM. With XIPVER, users initiate User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) transactions through the IP XPM. Up to ten sessions of the tool can be used simultaneously. XIPVER is not controlled by any SOC state. It uses non-menu commands.

NOTE: Users should have a basic knowledge of TCP/IP internetworking before using the XIPVER tool.

TOPS IP logs

This section provides information on logs for TOPS IP. For each log Table 4-8, "TOPS IP Logs," lists associated OM group(s), and associated OM register(s).

Table 4-8 — TOPS IP Logs

XPM IP data communication (XIP) logs	OM group(s)	Associated OM register(s)
XIP600	XIPCOMID	UMSSNF UMSRCF TMSSNF TMSRCF
	XIPDCOM	UMSGSNF UMSGRCF TMSGSNF TMSGRCF ICREQSF ICREPF
	XIPSVCS	UMSGSNDF UMSGRCVF TMSGSNDF TMSGRCVF
	XIPMISC	PKTSNER PKTRCER
XIP890		
XIP891		

XPM IP data communication (XIP) logs	OM group(s)	Associated OM register(s)
XIP892		
XIP893		
External alarm (EXT) logs		
EXT106		
EXT107		
EXT108		
QMS MIS (QMIS) logs		
QMIS102		
QMIS103		
TOPS logs		
TOPS105	TOPSVC	VCFL MSGLOST OPRLOST
TOPS106	TOPSVC	VCFL
TOPS112		
TOPS304		
TOPS504		

NOTE: For complete information on all log reports for the DMS switch, refer to *North American DMS-100 Log Report Reference Manual*, 297-8021-840.

TOPS IP OMs

This provides information on operational measurements (OM) for TOPS IP. For each OM group there is a brief description, a list of registers, an OMSHOW example, and a list of any associated OM groups and logs.

Table 4-9, "TOPS IP OMs," lists each OM group associated with TOPS IP and the associated register, a brief description, associated OM group(s), and associatef log(s).

NOTE: For complete information on all OMs for the DMS switch, refer to *North American DMS-100 Operational Measurements Reference Manual*, 297-8021-814.

Table 4-9   —   TOPS IP OMs

OM group	Register	Description	Associated OM groups	Associated logs
QMSMIS	BUFIP1SX	Buffer IP 1 success. This register is pegged each time a buffer is successfully sent across the first IP connection.	TOPQOCPS	
	BUFIP1S2	Buffer IP 1 success extension register		
	BUFIP2SX	Buffer IP 2 success. This register is pegged each time a buffer is successfully sent across the second IP connection.		
	BUFIP2S2	Buffer IP 2 success extension register		
	BUFIP3SX	Buffer IP 3 success. This register is pegged each time a buffer is successfully sent across the third IP connection.		
	BUFIP3S2	Buffer IP 3 success extension register		
	BUFIP4SX	Buffer IP 4 success. This register is pegged each time a buffer is successfully sent across the fourth IP connection.		
	BUFIP4S2	Buffer IP 4 success extension register		
	BUFIP1TL	Buffer IP 1 total. This register is pegged each time a buffer is attempted to be sent across the first IP connection.		
	BUFIP1T2	Buffer IP 1 total extension register		
	BUFIP2TL	Buffer IP 2 total. This register is pegged each time a buffer is attempted to be sent across the second IP connection.		
	BUFIP2T2	Buffer IP 2 total extension register		

OM group	Register	Description	Associated OM groups	Associated logs
	BUFIP3TL	Buffer IP 3 total. This register is pegged each time a buffer is attempted to be sent across the third IP connection.		
	BUFIP3T2	Buffer IP 3 total extension register		
	BUFIP4TL	Buffer IP 4 total. This register is pegged each time a buffer is attempted to be sent across the fourth IP connection.		
	BUFIP4T2	Buffer IP 4 total extension register		
TOPSOC	OCINI	OC initiation. This register is pegged each time a call that requires a TOPS operator is routed to an OC host switch from an OC remote switch.	TOPQOCPS	
	OCMCCS	OC mechanized calling card service. This register is never pegged, as its related functionality (inwards MCCS) is no longer supported.		
	OCQABN	OC queue abandons. This register is pegged each time a call that originates at an OC remote switch and queues at an OC host switch is abandoned before being served by a TOPS operator.		
TOPSVC	VCATT	Virtual circuit attempts. This register is pegged each time the switch attempts to obtain a virtual circuit.	TOPS102 TOPS105 TOPS106 TOPS107	
	VCFL	Virtual circuit failure. This register is pegged each time a virtual circuit fails to send a message.		
	VCNMSG	Virtual circuit number message. This register is pegged each time a virtual circuit sends a message.		
	VCNMSG2	Virtual circuit message extension register		
	VCDEF	Virtual circuit deflection. This register is pegged each time an attempt to obtain a virtual circuit is deflected due to none available.		

OM group	Register	Description	Associated OM groups	Associated logs
	MSGLOST	Message lost. This register is pegged each time an expected OC message is not received by the remote or host during an OC call.		
	OPRLOST	Operator lost. This register is pegged each time a call is terminated in the remote or the host because of an expected OC data link message not being received.		
XIPCOMID	UMSSN	UDP message send. This register is pegged when the CM sends a UDP message for a particular COMID to the XPM for transmission to the IP network.	XIPDCOM XIPMISC XIPSVCS	XIP600
	UMSSN2	UDP message send extension register		
	UMSSNF	UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message for a particular COMID from the CM to the XPM for transmission to the IP network.		
	UMSRC	UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network for a particular COMID from the XPM.		
	UMSRC2	UDP message receive extension register		
	UMSRCF	UDP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular COMID from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		

OM group	Register	Description	Associated OM groups	Associated logs
	TMSSND	TCP message send. This register is pegged when the CM sends a TCP message for a particular COMID to the XPM for transmission to the IP network.		
	TMSSND2	TCP message send extension register		
	TMSSNF	TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message for a particular COMID from the CM to the XPM for transmission to the IP network.		
	TMSRC	TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network for a particular COMID from the XPM.		
	TMSRC2	TCP message receive extension register		
	TMSRCF	TCP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular COMID from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		
XIPDCOM	UMSGSN	UDP message send. This register is pegged when the CM sends a UDP message to the XPM for transmission to the IP network.	XIPCOMID XIPMISC XIPSVCS	XIP600
	UMSGSN2	UDP message send extension register		
	UMSGSNF	UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message from the CM to the XPM for transmission to the IP network.		

OM group	Register	Description	Associated OM groups	Associated logs
	UMSGRC	UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network from the XPM.		
	UMSGRC2	UDP message receive extension register		
	UMSGRCF	UDP message receive failure. This register is pegged when a failure occurs during the receiving of a UDP message from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		
	TMSGSN	TCP message send. This register is pegged when the CM sends a TCP message to the XPM for transmission to the IP network.		
	TMSGSN2	TCP message send extension register		
	TMSGSNF	TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message from the CM to the XPM for transmission to the IP network.		
	TMSGRC	TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network from the XPM.		
	TMSGRC2	TCP message receive extension register		
	TMSGRCF	TCP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		
	ICREQS	ICMP request send. This register is pegged when the CM sends an ICMP request to the XPM.		

OM group	Register	Description	Associated OM groups	Associated logs
	ICREQSF	ICMP request send failure. This register is pegged when a failure occurs during the sending of an ICMP request from the CM to the XPM.		
	ICREPRC	ICMP reply receive. This register is pegged when the CM receives an ICMP reply from the XPM.		
	ICREPF	ICMP reply failure. This register is pegged when a failure occurs during the receiving of an ICMP reply from the XPM to the CM.		
XIPMISC	PKTSN	Packet send. This register is pegged when the CM sends a packet to the XPM.	XIPCOMID XIPDCOM XIPSVCS	XIP600
	PKTSN2	Packet send extension register		
	PKTSNER	Packet send error. This register is pegged when an error occurs during the sending of a packet from the CM to the XPM.		
	PKTRC	Packet receive. This register is pegged when the CM receives a packet from the XPM.		
	PKTRC2	Packet receive extension register		
	PKTRCER	Packet receive error. This register is pegged when an error occurs during the receiving of a packet from the XPM to the CM.		
	BUFERR	Buffer error. This register is pegged when the CM cannot obtain a buffer to store messages received from the XPM.		
XIPSVCS	UMSGND	UDP message send. This register is pegged when the CM sends a UDP message for a particular service to the XPM for transmission to the IP network.	XIPCOMID XIPDCOM XIPMISC	XIP600
	UMSGSND2	UDP message send extension register		

OM group	Register	Description	Associated OM groups	Associated logs
	UMSGSNDF	UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message for a particular service from the CM to the XPM for transmission to the IP network.		
	UMSGRCV	UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network for a particular service from the XPM.		
	UMSGRCV2	UDP message receive extension register		
	UMSGRCVF	UDP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular service from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		
	TMSGSND	TCP message send. This register is pegged when the CM sends a TCP message for a particular service to the XPM for transmission to the IP network.		
	TMSGSND2	TCP message send extension register		
	TMSGSNDF	TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message for a particular service from the CM to the XPM for transmission to the IP network.		
	TMSGRCV	TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network for a particular service from the XPM.		
	TMSGRCV2	TCP message receive extension register		

OM group	Register	Description	Associated OM groups	Associated logs
	TMSGRCVF	TCP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular service from the XPM to the CM. **Note:** If the message is severely corrupted, this register may not be pegged.		

ISDN Overview and Maintenance

This subsection provides an overview and maintenance for Integrated Services Digital Network (ISDN). See the "List of terms" at the rear of this subsection if you need help with ISDN terms and acronyms. Also, see NTP 297-1001-825, *DMS-100F Glossary of Terms and Abbreviations* for any terms or acronyms that cannot be found in the MOM.

ISDN overview

What is ISDN?

ISDN (Integrated Services Digital Network) is an all digital communications network that provides the customer with end-to-end connectivity through a single access point to support multiple services for voice, data, and images.

ISDN allows a customer to:

- connect a variety of computers, data terminals, or telephone sets to a data loop using a single type of connector
- send and receive voice and data information simultaneously on this loop

ISDN is based on a set of standard interfaces and protocols defined by the ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union). ISDN services use Common Channel Signaling (CCS) between the customer and Exchange Termination (ET), and Common Channel Signaling No. 7 (CCS7) between ISDN nodes.

The 2B1Q (2 binary, 1 quaternary) interface standard protocol provided the foundation for standardized ISDN-1. The 2B1Q protocol also complies with American National Standards Institute (ANSI) and Telcordia requirements for circuit-switched voice and data services, and for packet switched data services.

National ISDN

The National ISDN Council (NIC) (http://www.bellcore.com/orgs/nic/index.html) was formed to support the development of ISDN services that require network connectivity, compatibility, and integrity on a nationwide basis, and for which uniformity of operation is necessary from the customer's viewpoint to render the service usable on an efficient basis ("National ISDN").

> **NOTE:** Telcordia Technologies was formerly known as Bellcore.

NIC is a forum of telecommunications service providers and switch suppliers that participate in Telcordia's National ISDN Platform Evolution projects. Its purpose is to exchange ISDN-related technical information and concerns among the forum participants and Telcordia; to discuss and resolve technical and policy problems related to National ISDN; to identify and investigate the needs of potential ISDN end users and interconnectors for capabilities to be included in National ISDN; and to provide input to Telcordia on development and product directions, on industry expectations and on the course of National ISDN.

National ISDN 1999, SR-3875, Issue 3, May 1998 is a special report that summarizes the features and capabilities supported by National ISDN through the first quarter of 1999. It provides a cumulative view of the service capabilities that are available as of March 1995, March 1996, March 1997, March 1998, and the additional capabilities that will be introduced by March 1999. This report can be ordered from Telcordia at 1-800-521-2673 (or 1-732-699-5800 from outside the U.S.).

National ISDN has been implemented on the DMS-100 system in a way that delivers maximum flexibility while reducing equipment and maintenance costs. Basic Rate Interface (BRI) ISDN replaces conventional modem technology with transmission speeds up to 128 kbps--and beyond 500 kbps with compression. Primary Rate Interface (PRI) ISDN offers speeds of 1.54 mbps—selectable in increments of 64 kbps—with the Dialable Wideband Service (DWS) feature.

Key components of ISDN

The key components (see Figure 4-10) of the ISDN network are:

- The ISDN switch, which is a combination of a circuit-switched network and a packet handler network consisting of:
    - a Data Packet Network (DPN) series packet handler
    - or an ISDN switch with a Link Peripheral Processor (LPP) based Packet Handler (DMS-PH)
- The Operations, Administration, and Maintenance Processor (OAMP)
    - optional with the DPN series of packet handlers
    - ISDN Operations, Administration, Maintenance, and Provisioning (OAM&P) functions will be an integrated part of the DMS-PH
- Customer premises equipment (CPE)

The individual components of an ISDN network vary according to the services required and the vintage of ISDN hardware purchased.

Figure 4-10 — Key components of the ISDN network (Example with DPN series of packet handler)
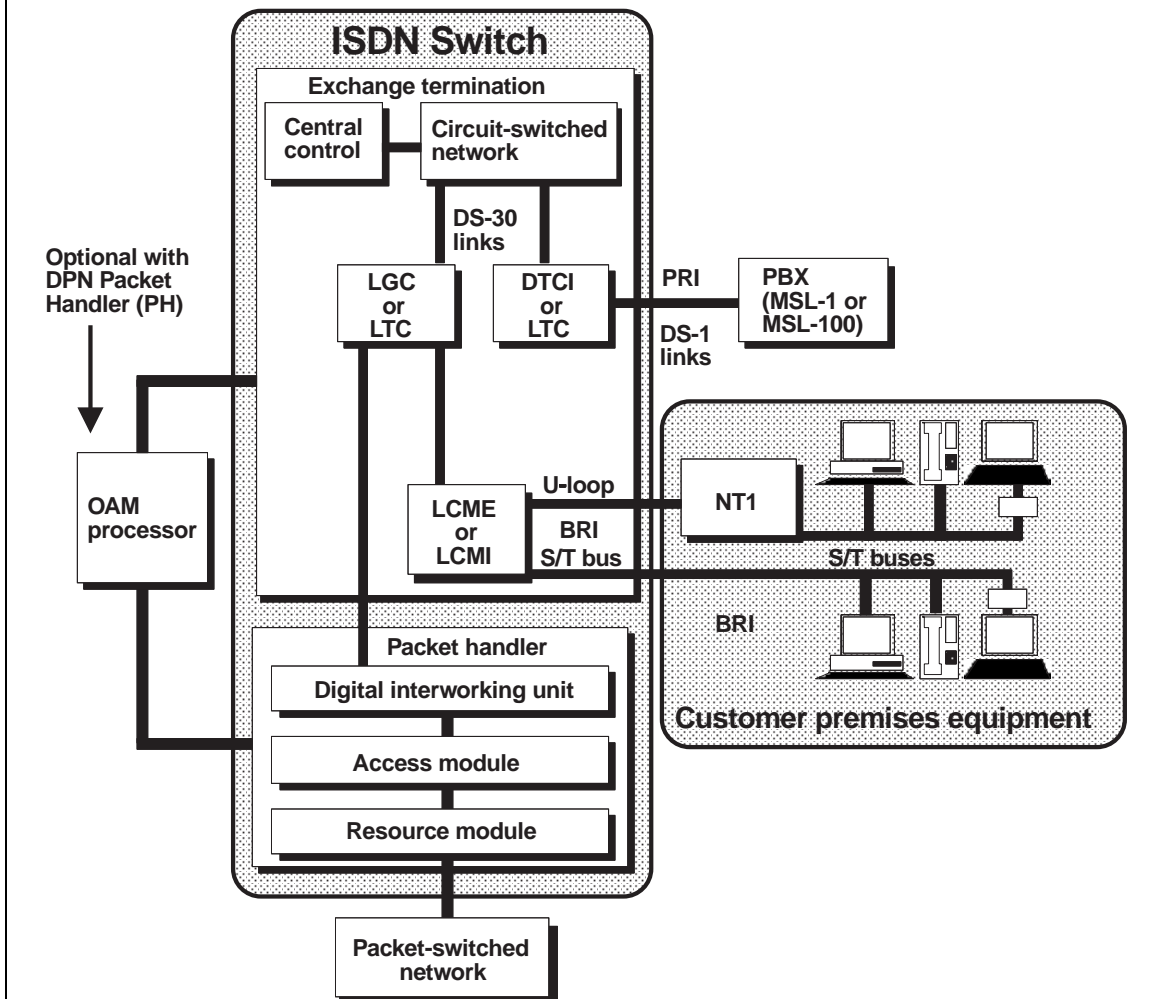
Legend:

DPN	Data Packet Network
LGC	ISDN Line Group Controller (formerly LGCI)
LTC	ISDN Line Trunk Controller (formerly LTCI)
DTCI	ISDN Digital Trunk Controller
LCME	Enhanced ISDN Line Concentrating Module
LCMI	ISDN Line Concentrating Module (replaced with LCME)
NT1	Network Termination 1
PBX	Private Branch Exchange
BRI	Basic Rate Interface (formerly Basic Rate Access (BRA))
PRI	Primary Rate Interface (formerly Primary Rate Access (PRA))
OAM	Operations, Administration, and Maintenance
OAMP	Operations, Administration, and Maintenance Processor

ISDN switch

As shown in Figure 4-10, an ISDN switch consists of a DMS-100 circuit switch and a data networking system switch such as the DPN series of packet switches, or a Link Peripheral Processor (LPP) based ISDN packet handler (DMS-PH). The circuit switch is called the Exchange Termination (ET) and is based on the standard DMS-100F SuperNode switch peripherals and software. It is a gateway to the circuit-switched network. The packet handler performs packet switching (data) operations. It is a gateway to the packet-switched network. The ISDN switch supports both ISDN and non-ISDN lines and trunks.

The ET routes the voice and data channels for outgoing and incoming calls through the appropriate peripheral. Because the switch consists of a number of modular hardware and software units, the ET can be configured for a variety of applications. Depending upon the applications, the ET may consist of a combination of the following modules:

- ISDN Line Group Controller (LGC)
- ISDN Line Trunk Controller (LTC)
- ISDN Remote Cluster Controller (RCCI)
- ISDN Digital Trunk Controller (DTCI)
- Enhanced ISDN Line Concentrating Module (LMCE)
- ISDN Line Concentrating Module (LCMI) (old standard)
- ISDN Link Peripheral Processor (LPP) (DMS-PH based)

ISDN Line Group Controller (LGC) and ISDN Line Trunk Controller (LTC), previously termed LGCI and LTCI, perform similar functions to their non-ISDN counterparts. The following two cards have been added to the LGC and LTC when these PMs are used to provide ISDN BRI services:

- the ISDN Signaling Preprocessor (ISP)
- the D-channel Handler (DCH)

NOTE: Even though LGCI and LTCI are terms being phased out in some documentation, the LGCI and LTCI designation for hardware is still supported.

The ISP provides a call control messaging interface between the DCH and the other processors in the LGC and LTC. It also provides D-channel maintenance functions for ISDN.

The LGC or LTC peripheral, when equipped for ISDN, switches calls within the ISDN switch and routes them to the circuit-switched network or a packet handler. For further detailed information on the ISDN LGC and LTC and their configurations, see NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide.*

ISDN Remote Cluster Controller (RCCI) is a dual-unit node that provides the same functions as the non-ISDN RCC interfacing remote networks to the circuit-

switched and packet switched networks. To enable the RCC to support ISDN ser-
vices, it must be modified in the following ways:

- using P-side DS1 slots so that DCH cards can be provisioned
- changing the Frame Supervisory Panel (FSP) to support DCH cards
- adding appropriate software loads

ISDN Digital trunk Controller (DTCI) is used as an interface for Primary Rate
Interface (PRI). The DTCI supports PRI trunks, as well as A/B bit signaling trunks.
The two types of trunks can be provisioned on the same DS1 link.

The DTCI provides call control for PRI functional signaling (PRI does not support
stimulus signaling). See the next subsection for a description of both PRI, and stimu-
lus and functional signaling. See NTP 297-1001-592, *DMS-100F Peripheral Modules
Maintenance Guide* for more detailed information on the DTCI.

**Enhanced ISDN Line Concentrating Module (LCME) and ISDN Line Con-
centrating Module (LCMI)** are dual-unit peripheral modules (PMs) that terminate
Basic Rate Interface (BRI) loops on line cards. The LCMI, that used Alternate Mark
Inversion (AMI) line cards (the old standard), has been replaced with the LMCE and
the standard 2B1Q line cards as part of the ISDN-1 compliance requirements.

Enhanced ISDN Line Concentrating module (LCME) terminates:

- ISDN 2B1Q U-type lines
- ISDN S/T-type lines
- POTS lines
- Electronic Business Sets (EBS)
- Datapath lines
- provides access to ISDN B-, D-, and M-channels

See Table 4-11 below for LCME specifications with link characteristics and Figure 4-
11 for the LCME shelf layout. Further, more detailed information on ISDN LCMs
can be found in NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance
Guide.*

DPN series of packet handler (PH)

The packet handler (PH) prior to BCS34 is based on Nortel Networks DPN series of
packet switches. It routes data packets between terminals in accordance with the orig-
inating and destination terminal addresses associated with the call.

Table 4-10 — LCME specifications

Enhanced ISDN Line Concentrating Module (LCME)				
C-side links				
Minimum	Maximum	Link type	Channels	Remarks
2	18	DS30A	32	Access to LGC/LTC links time-switched by DCCs to 12 P-side digroups of 32 channels each.
P-side links				
Minimum	Maximum	Link type	Channels	Remarks
0	480	U-loop	2B, D, M	Single cable pair connecting LCME to 2B1Q NT1 links exists when U-line card used.
0	240	S/T-bus	2B, D, Q/S	An 8- wire interface between (up to) 8 ISDN terminals and LCME link exists when the S/T-line card used.

Figure 4-11 — Line Concentrating Array ISDN (LCAI) LCME Unit 0 shelf (NTBX31BA)

BX32 LINE DRAWER 0 01 LSG 00	BX32 LINE DRAWER 1 03 LSG 02	BX32 LINE DRAWER 2 05 LSG 04	BX32 LINE DRAWER 3 07 LSG 06	FUSE PANEL 18	BX35 DCC1 19	BX35 DCC0 20	BX34 PROC 21	6X53 POWER 22	BX72 BAT R&NG 25

NOTES:

1. Unit 0 serves line subgroups 0-7 and unit 1 serves subgroups 8-15.

2. The BX35 Digroup Controller Card 1 (DCC-1) is used by the LCME in a "takeover" state to address the mate unit subgroups.

3. The NTBX31BA shelf is enhanced with respect to the NTBX31AC so that each Line Drawer can contain up to 12 additional line cards.

4. Shelves NTBX31AA and NTBX31AC have a NT6X53BA equipped in slot 25 and a NT6X53EA in slot 22.

5. For further description of the following LCM and LCME Line Concentrating Array (LCA) packs, see NTP 297-8991-805, *Hardware Description Manual*.

6X05 —Line Drawer   **BX32** — LCME Line Drawer
6X51 —LCM Processor   **BX34** — ISDN LCME Processor
6X52 —Digroup Controller   **BX35** — ISDN LCM Digroug Contr
6X53 —Power Converter   **BX36** — ISDN LCME BIC
*6X54 —Bus Interface Card (BIC) **BX72** — ISDN BAT & Ring Router
**EX54 — Data BIC (1-Meg Modem)

As shown in Figure 4-10 on page 4-97, the three key components of the DPN series of packet handlers are:

- the Digital Interworking Unit (DIU).
- the Access Module (AM).
- the Resource Module (RM).

The **Digital Interworking Unit (DIU)** ensures an efficient connection between the DMS-100 controller peripheral and DPN access module through the use of 1.544 Mbps DS1 digital trunks. The DIU demultiplexes the DS1 signals received from the DMS-100 controller into V.35 format 64 Kbps serial data streams, that are sent to the ports on the access module. For data sent in the opposite direction, the DIU changes data in the V.35 format to DS1 format.

The **Access Module (AM)** is the access protocol processor of the packet handler. The AM provides access to the resource modules of the DPN from local subscriber packet lines and from the DIU. The AM supports the Link Access Procedure on the D-channel (LAPD) link layer protocol for user packet mode data, as well as B-channel services such as X.25 LAPB. In addition, the AM supports X.75/X.75 prime gateways to public and private packet-switched networks.

The **Resource Module (RM)** provides X.75/X.75 prime gateways for interworking with public packet-switched networks, and DPN trunking for interpacket handler communications.

The OA&M functions for the DPN series packet handler are provided by the data networking system that consists of the following two main systems:

- the Network Administration System (NAS)
- the Network Control System (NCS)

These systems may be accessed at one or more terminals: NAS terminals for the administration system, or NCS for the network control system. These two types of terminals are the main tools for:

- creating and modifying service
- monitoring system performance

- trouble recognition and troubleshooting

For more detailed information on the DPN series PH, see the NTP 241-YYYY-ZZZ series of documents.

LPP based packet handler (DMS-PH)

During the BCS35 timeframe, the fully integrated DMS-PH was made available as an application on the Link Peripheral Processor (LPP) to meet National ISDN-1 and later requirements. The DMS-PH is a particularly cost-effective way to provide ISDN packet services because it can coexist on a single LPP with other applications. Operations, Administrations, Maintenance, and Provisioning (OAM&P) functions have been fully integrated with the DMS-PH.

The LPP-based PH is equipped with interface units to support the DMS Packet Handler feature. These are the Network Interface Unit (NIU) and the X.25 or X.75 Link Interface Units (XLIUs). The XLIUs, also known as Packet Handler Interface Units (PHIU), handle physical, data link, and network level protocol services.

Customer premises equipment (CPE)

Customer premises equipment (CPE), sometimes called "customer provided equipment," is located at the customer's site and includes:

- the 2-wire U-loop that is the subscriber loop between the switch and customer's Network Termination 1 (NT1)
- the 4-wire S/T-bus loop that connects the customer's terminals to the NT1
- the NT1 interfaces the terminals on the 4-wire S/T-bus to the 2-wire U-loop
- ISDN terminals, including digital telephone sets
- terminal adapters (TAs) that allow non-ISDN terminals to be connected to the network

Data grooming for ISDN

High-speed data grooming for the DMS switch is required for ISDN. If the DMS switch has not been groomed for high-speed data transmission, or is not maintained at the required integrity/parity error level after grooming, ISDN customers may experience data troubles that could be very difficult to isolate and resolve.

For further information on data grooming a DMS-100F switch and the use of various tools to maintain the DMS-100F switch at the proper level for ISDN, see the *Preventive Maintenance* tab and the "Network Maintenance" subsection.

ISDN BRI overview

ISDN subscriber side interfaces connect switching systems to privately owned equipment such as computers, telephones, voice-mail devices, and private branch exchanges (PBXs). There are currently two major subscriber interfaces:

- Basic Rate Interface (BRI) line service
- Primary Rate Interface (PRI) trunk service

Basic Rate Interface

Basic Rate Interface (BRI) allows a variety of computers, data terminals, and digital telephone sets to be connected to an S/T-bus—see Figure 4-17. The 4-wire S/T-bus is connected over the 2-wire U-loop through an NT1, or directly to an S/T line card at the ISDN switch, and provides the circuit-switched and packet-switched services needed to:

- set up outgoing, and receive incoming voice and data calls
- transmit and receive voice information
- transmit and receive data using high-speed and low-speed connections.

Each BRI line can support a maximum of eight ISDN terminals

The S/T-bus is the portion of the ISDN line that runs between the terminals and the Network Termination 1 (NT1). The S/T-bus can have up to four cable pairs, but usually consists of only two pairs.

When an NT1 is used, the subscriber terminals can be located up to seven Km away from the ISDN switch. When the subscriber's terminals are less than one Km away from the ISDN switch, the S/T line can be tied directly into an S/T line card.

BRI provides two 64 Kbps bidirectional data channels, known as B-channels, and one 16 Kbps signaling channel, known as the D-channel. A BRI line has a transmission speed of 192 Kbps without an NT1. With an NT1, the transmission speed is 160 Kbps on the portion of the line between the NT1 and the line card. This signaling method is referred to as 2B+D signaling and provides access to:

- circuit-switched voice and data services on the 64 Kbps B-channels
- high-speed packet data services on a provisioned B-channel connection
- low-speed packet data services on the 16 Kbps D-channel

In addition to the B & D channels for call placement and control, BRI provides the following maintenance channels:

- M-channel for 2B1Q lines on the LCME
- Q/S-channels

The 8 Kbps bidirectional maintenance M-channel carries messages between the exchange termination LCME, 2B1Q line cards, and the NT1. The 800 bps Q/S maintenance channels run from the ISDN terminals to the NT1. Performance monitoring is done continuously by the line card and the NT1. More about the NT1 can be found on the next page. For further information on NT1 maintenance functions see "Customer premises equipment (CPE) maintenance" on page 4-125.

BRI U-Loop 2B1Q signaling

2B1Q has been chosen by the American National Standards Institute (ANSI) and Telcordia as the North American Standard for ISDN BRI U-Loop Interface. It replaces the old standard Alternate Mark Inversion (AMI). The 2B1Q term stands for two binary one quaternary. 2B1Q has four voltage levels (i.e., +l, +3, -l, and -3) for transmission of binary (0 and l) data. Each two bits of binary data are encoded into one of these four voltage levels.

ISDN signaling methods

Two methods of signaling are used for communication between the subscribers terminal and the ISDN switch: *stimulus* and *functional*.

Stimulus signaling is an older standard that is being replaced by functional signaling. Stimulus signaling is based upon a master/slave relationship between the network and the terminal.

Functional signaling is based on a peer-to-peer exchange of information between an intelligent terminal and the network. Functional signaling moves a portion of the call processing intelligence from the Central Processing Unit (CPU) to the ISDN CPE terminal. The implementation of this method of signaling offers users the ability to access new network features and services, and makes ISDN standardization easier.

Bearer capability and services

For stimulus terminals, bearer capability (BC) indicates the desired transmission characteristics for a call and is associated with each directory number.

For functional signaling, bearer capability is an information element carried in the SETUP message, and indicates the type of call (voice or data) and the rate of transmission required. Authorized bearer services (Authorized Call Type) are used for functional signaling and offers a pool of bearer capabilities.

Network Termination 1 (NT1)

In the US and Canada it is your responsibility to provide the NT1, although in some cases the telephone company may be able to provide one as part of your service package.

The NT1 is located at the customers premises and provides:

- conversion of the B- and D-channel information from the two-wire network side to the protocols for the four-wire S/T-bus on the user side
- a two-wire interface for the subscribers U-loop that connects the NT1 to the exchange termination U-line card and the telephone network
- a four-wire interface for the customers interface bus, known as the S/T-bus, that supports up to eight ISDN terminals
    — a star NT1 is equipped with two S/T-buses
- its own power to remain active

- several loop maintenance functions using the M-channel

NOTES:

1. During the upgrade program to change out AMI to 2B1Q, the NT1s were changed out along with the AMI ISDN line cards.

2. You will need an external NT1 if you intend to share your ISDN line with other devices, for example an ISDN telephone. An external NT1 will also provide additional protection for your equipment in the event of a lightning strike to your ISDN line.

3. Many NT1s will have two sockets marked as S/T interfaces. This does not mean that each carries one B channel; it is simply a convenience to allow you to plug two devices straight into the S/T-bus.

ISDN Terminal adapter (TA)

The ISDN terminal adapter (TA) enables a non-ISDN terminal to access an ISDN line. Personal computers produced by various manufacturers may be connected to the ISDN by using a TA. TAs are interface devices for connecting asynchronous terminals using RS-232 line connections to the S/T-bus. This provides access via the D-channel packet handler. TAs are usually referred to as personal computer terminal adapters (PCTAs) or universal terminal adapters (UTAs).

There are four channels available that can be used for different types of calls. The TA supports circuit-switched voice calls on the B-channel, circuit-switched data calls on the B-channel, and packet-switched data on the D-channel. Up to four different calls can take place simultaneously.

ISDN PRI overview

Primary Rate Interface (PRI) allows private branch exchanges (PBX), inter-exchange carriers (IEC), and large computers to be connected to the ISDN switch over digital trunks—see page 4-97.

PRI provides 23 64 Kbps bidirectional B-channels, and one 64 Kbps D-channel. This signaling method is referred to as 23B+D signaling.

PRI uses a digital primary rate transmission facility. In North America, the DS1 standard 1.544 Mbps 24-channel format is used to carry ISDN signals for PRI between the ISDN exchange termination and a PBX such as the Meridian 1 Communications System, IEC, or large computer.

One DS1 link configured for PRI carries 24 channels. If one channel is used for the ISDN D-channel, the remaining 23 channels can be datafilled as PRI B-channels. One D-channel can support up to 479 B-channels on a maximum of 20 DS1 links (max 16 for MSL-1 PBX), provided all DS1 links reside on the same ISDN peripheral. For increased reliability, the D-channel backup capability is provided as an optional feature.

Line coding for DS1 is bipolar, alternate mark inversion (AMI). Both B8ZS and B7 zero-code substitution (ZCS) techniques are provided as options. The 6X50AB DS1 Interface Card in the DTCI supports either B8ZS or B7 line coding.

NOTE: The B8ZS coding format provides for a 64 Kbps unrestricted channel, while the B7 ZCS coding format requires the B-channels to be used in the 64 Kbps restricted mode.

PRI supports functional signaling only. Supplementary services for customers served by a PRI trunk depend on the provisioning of the local PBX. PRI compatible PBXs generally require software generic upgrades and hardware additions.

As seen in Figure 4-10, both the LTC and DTCI support PRI. The LTC equipped for ISDN supports both BRI and PRI, the PRI capacity being reduced by the amount of BRI service provided.

BRI and PRI datafill

For details on datafill required for ISDN BRI and PRI translations, see Volume 12 of NTP 297-YYYY-350, *DMS100F Translations Guide*. Also, see the service implementation guides (NTP 297-2401-200 for PRI or NTP 297-2401-201 for BRI).

BRI and PRI software

To verify that your system is current with all the software needed for ISDN, including CCS7 and maintenance software, Nortel Networks recommends that you refer to NTP 297-2401-351 *DMS-100F ISDN Feature Provisioning Guide.* For a list of Telcordia's TR's and related Nortel Networks software for ISDN, see the current *Feature Planning Guide* and NTP 297-2401-351, *DMS-100F ISDN Feature Provisioning Guide.*

ISDN maintenance

ISDN maintenance utilizes not only tools specifically designed for ISDN maintenance, but also existing testing and surveillance tools and their supporting procedures. Most of the existing testing and surveillance tools usable for ISDN maintenance are described in the MOM with references to supporting documentation for more detailed information.

Other supporting tools for ISDN include the use of CCS7 tools and logs for analysis of ISDN network problems. A description of the CCS7 related tools, including the CCS and C7UP logs, is described within the "SS7 Overview and Maintenance" subsection within this tab.

This subsection summarizes ISDN maintenance and supporting documentation in the following areas:

- Basic Rate Interface (BRI) maintenance

- Primary Rate Interface (PRI) maintenance
- ISDN Peripheral Module (PM) maintenance
- DPN series Packet Handler (PH) maintenance
- LPP-based Packet Handler (DMS-PH) maintenance
- Customer Premises Equipment (CPE) maintenance
- CCS7 signaling and trunking maintenance
- DMS-100F logs and OMs
- ISDN Parameters (PARMS)

Basic Rate Interface (BRI) maintenance

For BRI maintenance, reference NTP 297-2401-201, *DMS-100F National ISDN BRI Service Implementation Guide* and NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide.*

NTP 297-2401-501 is a document that provides an ISDN maintenance overview, preventive maintenance strategies, and other supporting information on ISDN BRI logs, OMs, protocols, and hardware. Within this NTP is a list of LTPISDN, LTPDATA, DCH, ISG and other MAP level—listed and unlisted—commands used for ISDN line diagnostics. Also, see Figure 4-13 on page 4-113.

In addition to providing information on handling reported no dial tone, noise, ringing, and other problems, the following troubleshooting procedures are included for BRI:

- Line troubleshooting (also, see ISDN line maintenance below)
- DCH and EDCH troubleshooting
- ISG troubleshooting
- Peripheral module troubleshooting
- DMS packet handler troubleshooting
- DPN packet handler troubleshooting
- Advanced troubleshooting DPN PH D-channel packet service
- Advanced troubleshooting B-channel circuit-switched data
- Advanced troubleshooting B-channel data between ISDN lines
- Advanced troubleshooting B-channel packet, ISDN line-to-DPN
- Advanced troubleshooting B-channel circuit-switched voice
- Advanced troubleshooting B-channel circuit-switched voice—phone never rings
- Advanced troubleshooting B-channel circuit-switched voice—no dial tone
- Advanced troubleshooting B-channel circuit-switched voice—call cutoff while talking
- Advanced troubleshooting B-channel circuit-switched voice—noise

- Advanced troubleshooting B-channel circuit-switched voice—delay in getting dial tone
- Advanced troubleshooting B-channel circuit-switched voice—call routed to treatment

ISDN line maintenance

The primary consideration when investigating an ISDN line fault is isolating the fault to one of the line components:

- the LCMI or LCME
- the ISDN line card
- the U-loop facility
- the NT1
- the S/T-bus facility
- the subscriber equipment

NTP 297-2401-501 provides information for personnel who maintain ISDN subscriber lines. It includes descriptions of:

- the Line Test Position (LTP) hardware
- the available types of line and console tests
    - — shower queue
    - — diagnostics for 2B1Q and S/T type line cards
    - — dial-up B-channel loopback testing
    - — Bit Error Rate Testing (BERT)
    - — Integrated Bit Error Rate Testing (IBERT)
    - — test Network Termination 1 (NT1)
- LTP displays that result from line maintenance action
- commands and responses used in line maintenance

Figure 4-13 on page 4-113 lists the maintenance commands used for ISDN. Command descriptions can be found in NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide* and NTP 297-2401-201, *DMS-100F National ISDN BRI Service Implementation Guide*.

Loopback testing

Loopback facilities provide a means for creating a signal at a test generating point along a signal's path, and reflecting it back from another point, called a loopback point. By comparing the signal sent to a loopback point with the signal reflected, the source of a transmission error on a signal's path can be pinpointed. This type of procedure is known as a loopback test. Both the DMS and DPN have facilities for:

- establishing loopback points along pathways used for carrying circuit-switched voice or data, and packet data
- generating either continuity tests or bit error rate tests (BERT) at various points along these pathways

Faulty components that are a source of transmission errors can be pinpointed by operating different loopback points progressively along a pathway, then transmitting signals from the same BERT or continuity test generation point.

The traditional demarcation ends usually at the customer interface. To verify the validity of Layer1 across the demarcation of the line a terminal emulation program (Smartcom, Procomm, etc.) can be launched and connected to loopback test numbers or other terminals. This will test the validity and throughput of the ISDN pipe from the Central Office.

A testing starting point is at the LTP level, run a DIAG to ensure ISDN line card sanity. If the line card has not been tested for a long period of time, it may be necessary to perform the LCO_O and LCO_R command and some preceding diagnostics to ensure dial tone is present at this point. Once this is done and the circuit is being built out to the customer's premise, the line should be observed at the LTPISDN level using the SUSTATE command to check for midspan repeaters and status of the NT1 on the U-loop. Check the ISDN logs at this time to see confirmation of test results, the text within the LINE101—see following example—and other LINE or ISDN logs may give the exact reason for a failure. The technician should use the SUSTATE command to view the components of the ISDN circuit after evaluating the logs.

```
LINE101  FEB15  15:19:12     8800 FAIL   LN_DIAG
 LTID LCME           538    DN  7227078      KEY    1
 DIAGNOSTIC RESULT    No SYNC   at  LU  interface
 ACTION REQUIRED      Sustate
 CARD TYPE      BX27AA
```

To test each component of the ISDN circuit, use the loopbk command to set a B1, B2, or 2B+D loopback at any one of the line units on a MP-EOC equipped line. Use the MPLU parameter with the number of the line unit. Only one loopback is allowed for each loop. Use the LOOPBK command at the LTPDATA level. Loopbacks can be set at four places—see Figure 4-12 for loopback reference points. For Example:

(LOOPBK MPLU <line unit> [1 to 6] <channel> {BBD, B1, B2})

In general, loopbacks should be set at the **T** interface first, because this is the furthest point on the loop. If the loopback test shows a problem, the loopback point can be moved in to the **LU** interface, and lastly the **L** interface to isolate the problem.

Loopback points can be set at the **LTPDATA** level with the **LOOPBK** command. You must then specify which point to set the loopback at, and whether to use **B1** (b-channel 1), **B2** (b-channel 2), or **BBD** (all channels). It is generally best to select **B1**.

Figure 4-12 — Loopback reference points

Loopback testing can be done at one of four places:

T Interface: Network side of NT
LU Interface: Network side of line card
MPLU Interface: Loop extenders between the ISLC and the NT
L Interface: CC side of line card
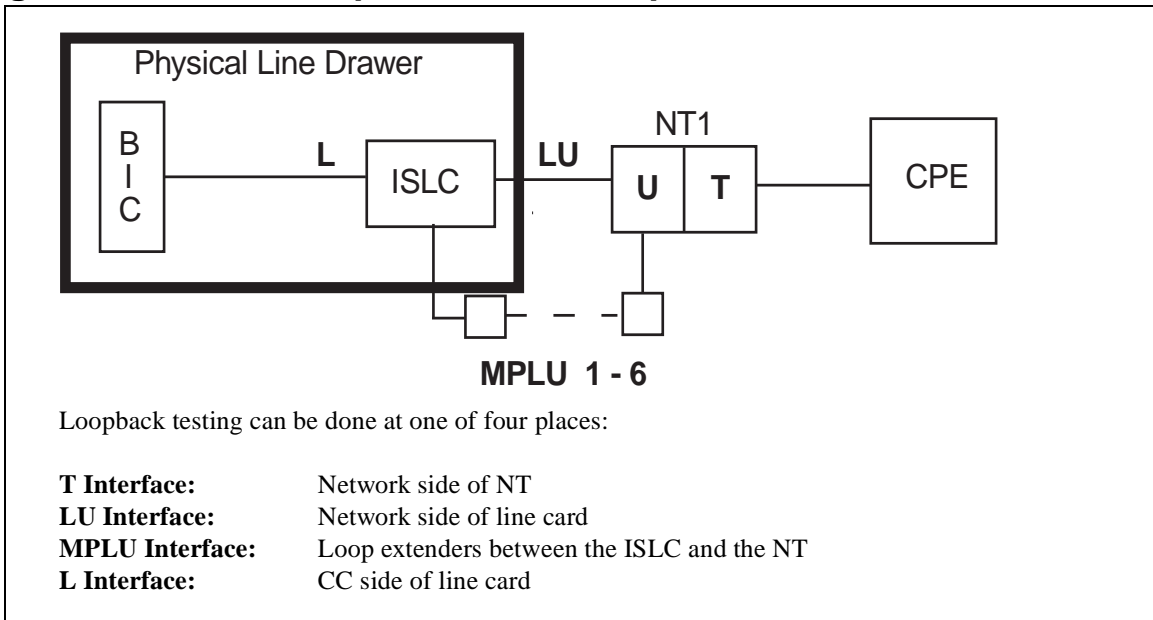
If the **LU** point is selected, it is possible to select **IN** or **OUT** with regards to the direction of the loopback point. **IN** means towards the switch, **OUT** means toward the CPE. The default is **IN**, and this is what usually should be selected. **OUT** should only be selected if you have loopback equipment on site which can be used to test from an ISDN terminal towards the line card.

BERT testing with loopbacks

Loopback points must be preset with the LOOPBK command, which is off the LTP-DATA level, before the BERT test can be performed. The simplified syntax for the LoopBk command is:

LOOPBK {L, LU, MPLU, T} {B1, B2, BBD}

For example, if the **LOOPBK T BBD** command is entered for the **T** interface, the following message will be given.

> **WARNING** - Action may affect Packet Data Service
> Do you wish to continue?
> Please confirm ("YES", "Y", "NO", "N")

After entering the confirmation, the resulting message should say:

"2B+D   Loopback activated at T"

Other possible options for LOOPBK are given if a Q LOOPBK is entered, but it is rare to use any other options than those just given.

```
CM        MS        IOD       Net       PM        CCS       Lns       Trks      Ext       APPL
 .         .         .         .         .         .         .         .         .         .
LTPData
 0 Quit              POST         DELQ              BUSYQ         PREFIX
 2 Post_
 3                 LCC PTY RNG .....LEN.........   DN    STA F S LTA   TE   RESULT
 4 Equip_         ISDN LOOP   HOST 10 1 03 01     484 4030 MB    .  IBERT   4
 5 Connect_
 6 Sustate          BLOCKS RCVD:248
 7 LoopBk_     BIT ERRORS :0
 8 BERT_       BER        :0
 9                  SYNC STATUS:INSYNC
10 BPVO_     BERT  start b1
11 Hold        Obtained IBERT   4
12 Next        Bert test started.
13
14
15
16
17
18
  LAP2050
Time  15:54  Pref> bert start b1
```

NOTE: Note: Unless the 'bert stop' command was used, a LoopBk RLS must be done when testing is finished, to release the loopback point .

BERT testing requires that an IBERT card be present in the LCME (6X99AA). See the "Network Maintenance subsection within the *Preventive Maintenance* tab for further details on IBERT.

BERT is especially useful for ISDN lines which are having problems with circuit-switched data transmission. BERT testing can verify if the line is sending out bad data. BERT testing can also be useful for lines which are experiencing other intermittent problems. If a Bit Error Rate is detected to be something other than 0, move the LoopBk point in closer (from T to MPLU, to LU, to L) to identify the source of the problem.

Above is an example of a BERT START B1 off the LTPDATA level of the MAP. The BERT command will give the Bit Error Rate for the ISDN loop. Issue a BERT STOP when finished. BERT STOP not only stops the testing but also clears the set loopback path.

The syntax for BERT is:

BERT START {B1, B2}   { 56, 64} <--- If no entry for speed, 64 is the default
BERT STOP

After BERT testing is done to the demarcation with positive results, it is possible to extend bert tests through loopbacks from customer CPE equipment, depending on the terminal being used. Also, BERT tests can be run from external test equipment on the U-Loop to verify the circuit. Before the customers software application is launched, it is wise to run a terminal emulation program to verify hardware flow control and other software communication settings. Testing cables that are used must support terminal emulation, and file transfer protocols must match. Zmodem usually works the best for good throughput results on file transfers.

Check the LINE and ISDN Logs and certain Operational Measurements (OMs) to verify that the ISDN line and application are running smoothly. Below are some key ISDN logs and OMs to watch for. Also, see ISDN Logs and OM information later in this subsection.

Log ISDN115 — subscription limits exceeded - too many TEIs. This log is generated when too many devices are plugged into the ST/BUS.

Log ISDN200 — This report is generated daily for up to 10 ISDN lines per generation. It displays the total number of frames received and transmitted, the number of received and re-transmitted frames where errors exceed the threshold value, and the percentage of the total frames represented by these errors.

 Log ISDN203 — This daily report shows the percentage of errored and re-transmitted frames on the ISDN switch.

OMSHOW ISGBRA HOLDING (This OM group can reveal some hardware and or software incompatibilities). See DBRRXDSC OM register next.

Register DBRRXDSC — Frames received from CPE, disregarded due to unregistered TEIs, messages that cannot be decoded, flow control problems, partially received messages, sequencing errors, or unknown SAPIs.

   Associated Logs: PM190, PM194, PM198, PM270

OMSHOW ISGOVLD HOLDING (This OM group can be the result of underprovisioning of D-channel handlers or hardware fault associated with them.)

Register CONGENMTR — Counts the number of times that an ISG enters a congestion state

Register CONGENTR — Counts the number of times that an ISG enters an overload state.

See NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide* and NTP 297-2401-201, *DMS-100F National ISDN BRI Service Implementation Guide* for further information and details on the commands to use for loopback and BERT testing. Also, see the following lines maintenance MAP levels used for ISDN.

Figure 4-13 — Lines maintenance MAP levels used for ISDN

LNS

0	QUIT
3	LTP
4	ALT
5	LNSTRBL

LTP

0	Quit_
2	Post_
4	
5	Bsy_
6	RTS
7	Diag
8	
9	AlmStat
10	CktLoc
11	Hold
12	Next
13	
14	
15	
16	Prefix
17	LCO_
18	Level_
	DATA_SCREEN
	DAV_SCREEN
	FRLS
	LTPRSRC
	RECORD_DTSR
	VOICE_SCREEN
	DCTLTP
	EBSMSG
	ltp_aux_gate_com
	ltp_aux_com
	FULLDN
	EBSMSG

LTPISDN

0	Quit
2	Post_
3	
4	
5	
6	Sustate
7	BCHCON
8	LtloopBk
9	DCHCon
10	TEST_
11	Hold
12	Next
13	
14	TstSgnl
15	TEI_
16	Qloop
17	Qlayer
18	Rlayer

LTPMan

0	Quit
2	Post_
3	
4	Loss
5	Noise_
6	ToneGen
7	Jack
8	TestRing
9	Bal
10	RlsConn
11	Hold
12	Next
13	
14	Ckttst
15	Sustate
16	SetLpBk_
17	
18	
	DCHCON
	GAINSLOPE

LTPData

0	Quit
2	Post_
3	
4	Equip_
5	Connect_
6	Sustate_
7	LoopBk_
8	BERT_
9	
10	BPVO_
11	Hold
12	Next
13	
14	
	BERTTime
	QLLPERF
	QLAYER2
	RLLPERF
	RLAYER2
	QL1PERF
	RL1PERF

LTPLTA

0	Quit
2	Post_
3	MonLTA
4	TalkLTA
5	Orig
6	LnTst
7	VDC
8	VAC
9	Res
10	Cap
11	Hold
12	Next
13	
14	LTA
15	BalNet
16	Coin_
17	Ring
18	DgtTst

CSDDS

0	Quit
2	Post_
3	Seize
4	Cktloc
5	Bsy_
6	RTS_
7	Diagn
8	LoopBk
9	BERT_
10	Rate_
11	Hold
12	Next_
13	
14	Reset
15	Turn_
16	Monitor_
17	Select_
18	NextS

IBNCON

0	Quit
2	
3	Select
4	Next
5	Busy
6	RTS
7	Diagnose
8	
9	
10	Seize
11	Release
12	Clear
13	PrevDM
14	
15	
16	QConline
17	QcustGrp
18	QSeated
	BSY
	FRLS
	SENDMSG
	WAITFMSG

ALT

0	Quit
2	Post_
3	ALTInfo
4	
5	
6	
7	SDiag_
8	Diag_
9	LIT_
10	BAL_
11	Ckttst_
12	BBT
13	BBTSUPDB
14	LCDCUT
15	
16	
17	
18	

NOTES:

1. A description of the use of the menu level commands, and hidden commands, can be found in the commands reference manuals. Also, use the LISTST command to get the directory and then PRINT for a list.

2. See the "Line Maintenance" subsection in the *Preventive Maintenance* tab of this manual for further information on the automatic line testing.

ISDN integrated line testing

Integrated line testing allows ISDN 2B1Q lines to be maintained using transaction language one (TL1) commands from an operations system (OS) over an X.25 data link (see Figure 4-14). The OS is located at an operating company's maintenance operations center and is not part of the DMS-100 switch. The test system controller (TSC) is integrated with the DMS-100 switch. This architecture is more reliable and provides more capabilities than a stand-alone TSC. It also allows the OS and local user interface to use the same metallic test equipment (MTE). TL1 is an optional part of functional group NI0 NI-1 BRI Enhanced Maintenance for ISDN, NI000009.

Some of the line tests require an enhanced services test unit (ESTU)—see the next topic. The tests available with ISDN TL1 line testing are also available through the enhanced ISDN line testing capability at the LTPISDN level of the MAP display. TL1 is the command interface between the OS and the DMS-100 switch. There are four types of commands:

- TL1 protocol commands that perform the following functions:
    - initiate digital and metallic test access to the ISDN BRI line under test
    - disconnect the lines under test
    - indicate the end of a test session
    - indicate when one or more test sessions have failed
    - initialize the data link between the OS and the DMS-100 switch
    - report the status of the data link between the OS and the DMS-100 switch
- information request commands that retrieve information from the DMS-100 switch. This information is sent as a response to the OS and includes:
    - the current state and standing condition of an ISDN line
    - the directory number and call types associated with one ISDN line
    - provisioning information associated with an ISDN line
    - performance monitoring data, such as bit error rate (BER), errored seconds (ES), and severely errored seconds (SES)
- action commands that change the state of a line either by placing a line out of service for maintenance or by returning a line to service
- test commands associated with a test session number that use test resources in the DMS-100 switch and perform the following functions:
    - test the ability of the line card to synchronize to a test NT1
    - perform standard resistance, capacitance, and voltage measurements on an ISDN BRI line
    - perform a bit error rate test on an ISDN BRI line
    - measure the amount of sealing current on the digital subscriber loop (DSL)

— measure impulse noise (bursts or spikes) and background noise on the DSL

— measure 2B1Q signal levels to detect load coils on the loop

— test the ability of a specific line unit to detect and count BER, ES, and SES

— perform an extended set of loop measurements

— test the thresholds of a specific line unit

— perform a diagnostic on the line card and loop

See Figure 4-14 for the physical location of the TL1 interface and the test NT1 with a line emulator. For information on the TL1 commands, see NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide*.

Figure 4-14 — Location of test NT1 and the TL1 in the DMS-100
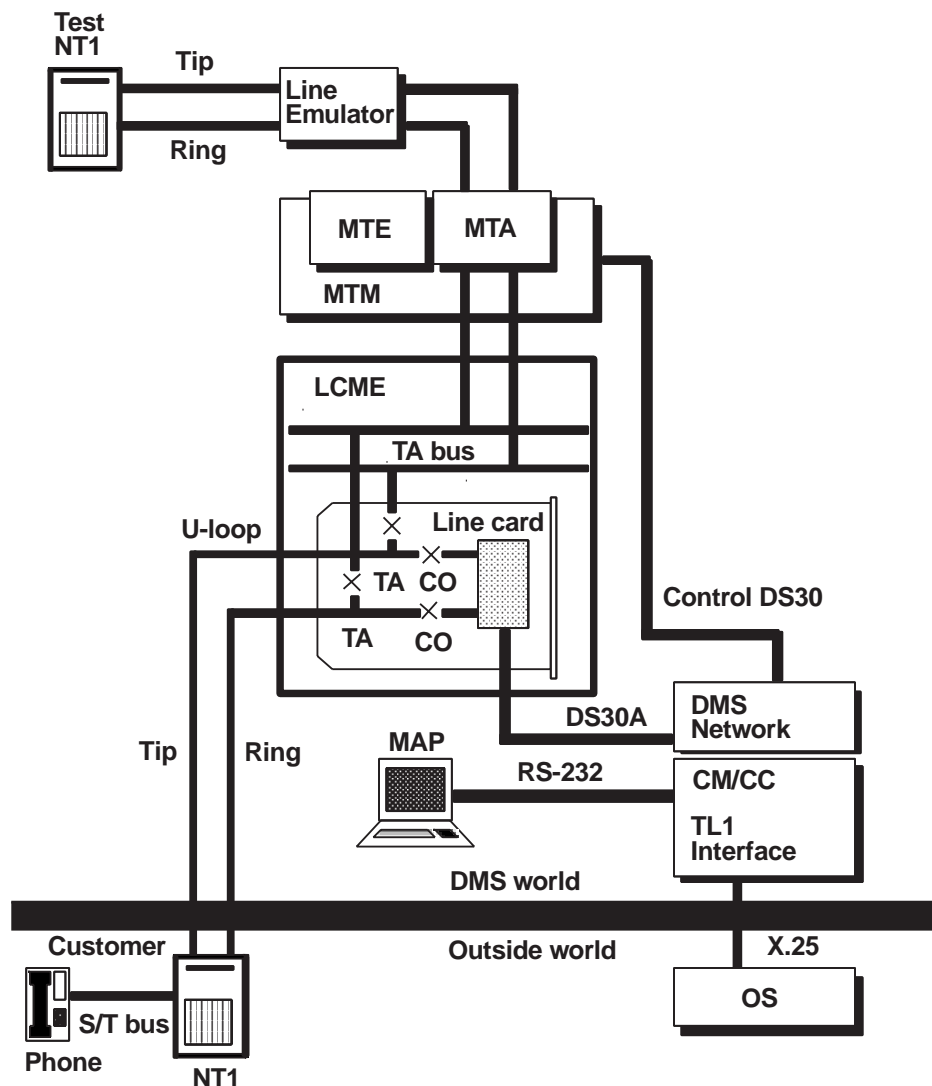
> **NOTE:** The test NT1 is not directly connected to the MTA. Instead, it is connected to a 15-kilofeet 26-gauge wire emulator. This is then connected to the horizontal of the MTA driver card. The wire emulator is required to simulate the maximum loop length, less office wiring, between the central office and a normal NT1.

Enhanced Services Test Unit (ESTU)

The Enhanced Services Test Unit (ESTU) is piece of stand-alone line test equipment located in the miscellaneous equipment frame. The enhanced services test unit (ESTU) can perform metallic and digital line tests for ISDN services. The ESTU unit, which consists of an ESTU Master Module (EMM) and an ESTU ISDN Test Module (ITM), occupies its own miscellaneous shelf space at remote or host sites instead of being integrated into the Maintenance Trunk Module (MTM).

Associated ESTU software allows the interface to the DMS test equipment subsystem for MAP level access as well as the ISDN TL1 interface from the operating companies operations system (OS). This enhanced capability using the ESTU allows for presubscription testing, service verification, and trouble segregation on ISDN lines. The ESTU and future stand-alone test equipment can be accessed from the TSTE-QUIP MAP level off the MTCNA level (MAPCI;MTC;MTCNA;TSTEQUIP). The ESTU supports the TL1 Phase 2 command introduction for National ISDN services. For more detailed information on the ESTU, including diagrams, see NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide*.

Enhanced ISDN line testing

MAP level ISDN line testing capabilities were introduced in BCS35 to meet Telcordia's *Generic Test Access Requirements for Multimeters* in TR-TSY-000476 and the National ISDN service requirements. A new command, TEST, on the LTPISDN level of the MAP, can be used along with hidden commands to execute the following tests:

- NT1 signature detection
- NT1 cold start verification
- sealing current measurement
- basic line monitoring (BLM) tests
- impulse noise measurements
- wideband noise measurements
- insertion loss measurements

An alternating current (AC) resistance measurement is provided through a new option for the existing RES command in the LTPLTA level of the MAP. The ESTU, previously described, is required for the noise, loss, and AC measurements. See Figure 4-13 for the LTPISDN MAP level and NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide*.

Layer 1 ISDN performance monitoring capability for 2B1Q loops was introduced in BCS35 with the NTX750AC software package. This feature allows for the setting and querying of thresholds and error counts for ISDN 2B1Q loops.

New commands, tables, logs, and parameters were added to support this feature. Two new commands—RL1PERF and QL1LAYER—on the LTPDATA level of the MAP, permit the manipulation of Layer 1 ISDN performance data. Tables BLMTHRSH and LNTHRSH support the threshold data. Log LINE147 reports NT1 test mode changes, and new log LINE148 reports mismatches between the 2B1Q line card and CC. The following parameters were added to the OFCVAR table to control the default alarm reporting status of datafilled loops:

- QISDN_LOSS_OF_SYNC_WORD_ALARM
- QISDN_LOSS_OF_SIG_DGASP_ALARM
- QISDN_NT1_TEST_MODE_ALARM
- QISDN_T_SYNC_LOST_ALARM
- QISDN_PERFORMANCE_M0N_ALARM
- ISDN_LOSS_OF_SIG_N0_DGASP_ALARM

In BCS35 a capability was added for the field technician on a BRI ISDN customer's line to dial up a test number that will apply a loopback on the B-channel. This feature, Dial-Up B-Channel Loopbacks (AQ0884) in software package NTX750AC/AD, allows the field technician to verify the T-bus/U-loop without the assistance of the test center or central office personnel.

To establish the loopback for the B-channel, a T108 testline is accessed by dialing 959-1080 or a number chosen for the office. The loopback is applied from the ISDN line card towards the customer premise on the B-channel. It remains set according to the value established for the T108ISDN_TIMEOUT_IN_MINUTES parameter in the OFCENG table.

The following provides a general guideline for activation:

- Datafill the following tables and subtables per NTP 297-YYYY-350, *DMS-100F Translations Guide.*

    — Assign T108ISDN in table CLLI

    — Assign a route in table OFRT

    — Define access code and route in table DN (Telcordia's TR-TSY-000476 recommends 959-1080 however, verify this within your company before assigning)

    — Set the parameter T108ISDN_TIMEOUT_IN_MINUTES in table OFCENG. (We recommend 10 minutes)

Wideband testing

To support the wideband test capability of the ESTU introduced back in BCS35, a wideband test access panel is required. This requirement allows for a major reduction in cable lengths to eliminate errors from excess cable runs.

Wideband noise measurements are required to measure background noise that occurs in the frequency bandwidth relevant to BRI ISDN (wideband noise interference). The background noise is primarily caused by near-end crosstalk (NEXT) that is the electromagnetic coupling of energy between physically separate circuits. It is measured using a mean-squared loss (MSL) meter of the actual decibel readings of the noise on the loop. The TEST command with the hidden NSE command on the LTPISDN level can be used for wideband noise testing.

ISDN Digital Test Access (DTA)

The ISDN Digital Test Access (DTA) feature enables the monitoring of circuit-switched B- and D-channel packet data connections (Bd) of an ISDN BRI loop using a modified external protocol analyzer.

There are two types of DMS ISDN BRI protocol analysis: real time protocol analysis and protocol abnormality count measurement.

Real time protocol analysis is performed using a protocol analyzer or the PMDEBUG utility. A protocol analyzer can be connected to a line card to analyze B-channel or D-channel protocol, but doing this removes the corresponding line from service. However, the combination of a protocol analyzer and the digital test access (DTA) feature provides the ability to analyze protocol without removing a line from service.

DTA allows monitoring of the following streams of data on an ISDN BRI loop:

- provisioned packet data on a B-channel
- call control information on the D-channel
- packet data on the D-channel

Although this feature allows monitoring of the streams in the previous list, it does not allow the monitoring of pulse code modulated (PCM) speech on a circuit-switched B-channel.

With the DTA feature, you can monitor packet data flowing toward the subscriber (upstream data). See Figure 4-15 for optional connections with the protocol analyzer through an ISDN line card or a NT6X50AB DS1 Interface Card. Monitoring is performed with a protocol analyzer connected to one of the following items:

- the S/T interface of a BRI loop that is connected to an ISDN line card in the LCME or LCMI peripheral module.
- two channels on an NT6X50AB DS1 interface card in one of the following PMs:

    — a Digital Trunk Controller (DTC)

— a Line Trunk Controller (LTC)

— a Line Group Controller (LGC)

— an LTC equipped with ISP16 card NT6X02

— an LGC equipped with ISP16 card NT6X02

For protocol requirement features, procedures on the use of the DTA feature, and supporting MAP commands, see NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide*.

Figure 4-15 — ISDN protocol analyzer connection options

Legend:
X = DTA (B)
Y = DTA (D)
Z = DTA (Bd)

NOTE: DTA monitor connections are established through the network using the CONNECT command in the LTPDATA level of the MAP display. Connections terminate at points X, Y or Z, depending on the service being monitored.
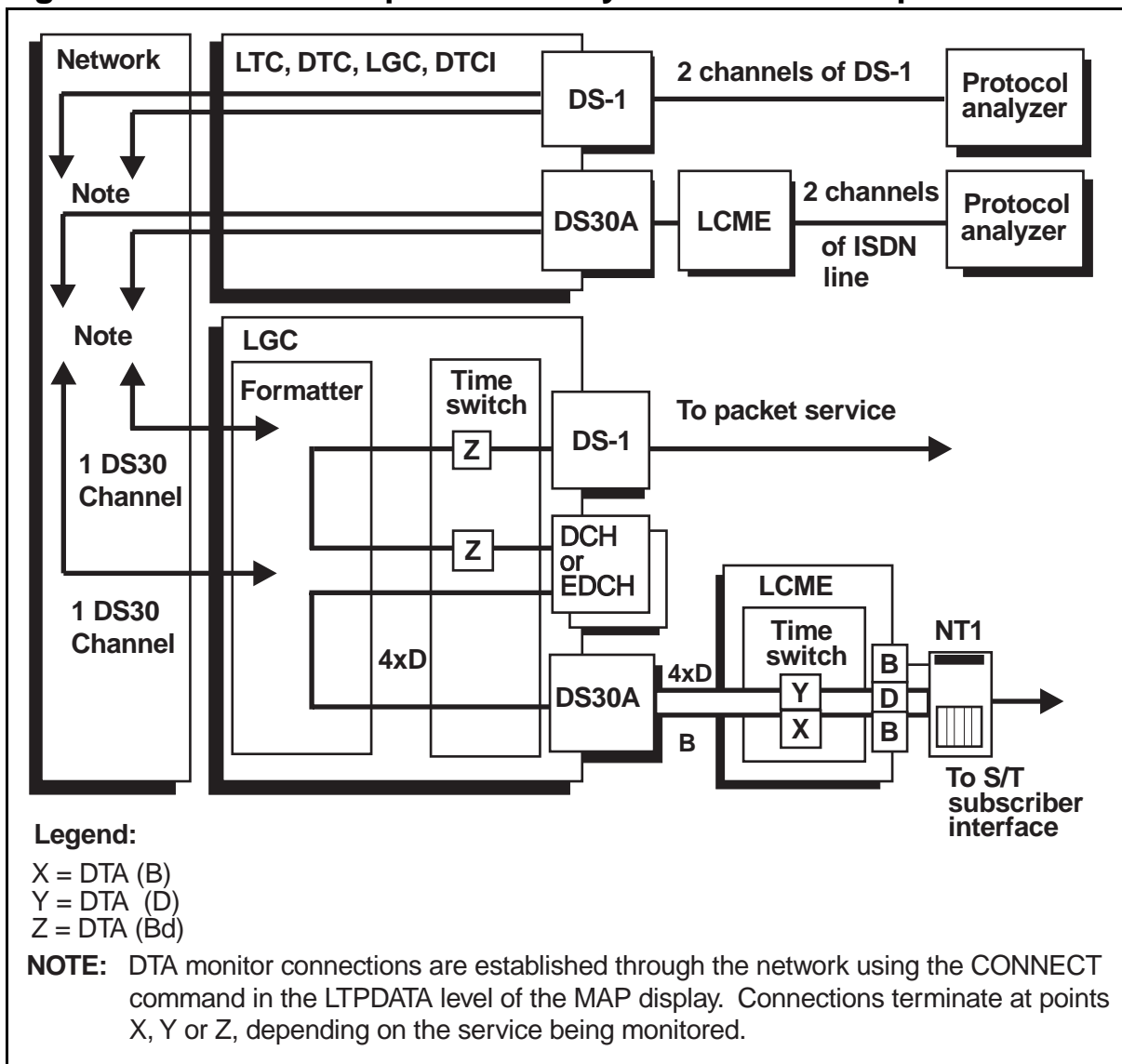
EQUIP and CONNECT commands

The EQUIP and CONNECT commands off the LTPDATA level of the MAP are designed to be used when setting up equipment for monitoring a channel on a BRI loop. The EQUIP command reserves the DS1 interface or ISDN line where the protocol analyzer is to be connected. The CONNECT command connects the channel on the BRI loop—that is to be monitored—to the DS1 interface or ISDN line card associated with the protocol analyzer. The same commands are used to release the connections.

In addition, the CKTLOC command is used to display the index number for the D-channel on an ISDN line.

Due to potential risk of eavesdropping during DTA testing, Nortel Networks recommends that:

- restrict user access to EQUIP and CONNECT commands utilizing the PRIV-CLASS and PERMIT commands
- restrict the use of the EQUIP and CONNECT commands to secure terminals using table TERMDEV.

Error rate verification

Before monitoring data streams on an ISDN loop, ensure that data transmission error rates are low by verifying that the synchronous clocks in the office are free of alarms and are synchronized to the master frequency source. These clocks are used to synchronize operation of the office with external DS1 carriers. A severe frequency difference between the two can cause transmission errors. Attempting to monitor protocols on a BRI loop will be compromised by such errors and can make analysis more difficult.

Primary Rate Interface (PRI) maintenance

It is recommended that one or more of the following documents be referenced when performing maintenance for Primary Rate Interface (PRI).

PRI maintenance-related documents

For PRI maintenance and implementation procedures, reference NTP 297-2401-200, *DMS-100F PRI Implementation Guide* and NTP 297-2401-502, *DMS-100F ISDN PRI Maintenance Guide.*

NTP 297-2401-502, *DMS-100F ISDN PRI Maintenance Guide* is a document that provides an ISDN maintenance overview, preventive maintenance strategies, and other supporting information on ISDN PRI logs, OMs, protocols, and hardware. Within this NTP is a list of MAP levels supporting PRI maintenance—listed and unlisted—commands used for ISDN supporting PM and trunk diagnostics.

In addition to providing information on various test tools—TRAVER, DISPCALL, PMIST, PMDEBUG, CALLTRAK—for troubleshooting PRI problems, the following maintenance related procedures and troubleshooting notes are included for PRI:

- restoring service to DMS-100 PRI trunk, carrier, DTCI & D-channel
- mapping CAUSE values to treatments and treatments to CAUSE values
- MSL-l troubleshooting for errors and alarms
- DS-1 testing and other issues
- D-channel loopback
- Notes for NT6X50AB DS-1 card maintenance
- Auditing data mismatches
- Activity monitoring with PMACT and ISP commands
- Integrated service access (ISA) troubleshooting
- Troubleshooting call processing
- Digital test access
- Advanced troubleshooting B- and D-channels
- Advanced troubleshooting for calls that will not complete

See NTP 297-YYYY-544, *DMS-100F Trouble Locating and Clearing Procedures* that provides the following trouble locating and clearing procedures:

- ISDN PRI trunk
    - — determining the PRI trunk state
    - — restoring a busy PRI trunk

- ISDN PRI single D-channel and PRI primary and backup D-channels
    - — determining the D-channel state
    - — establishing a DS1 loopback for the far-end equipment
    - — restoring a busy D-channel
    - — restoring far-end service for a D-channel
    - — switching manually to a backup D-channel

Also included in this document is a table that provides a list of DMS-100 ISDN PRI trouble symptoms and their corresponding trouble locating and clearing procedure(s). Another table lists ISDN logs ISDN105 through ISDN114 and the reference to the D-channel procedure for resolving or isolating the cause of the log generation.

ISDN peripheral module maintenance

Peripheral modules (PMs) associated with ISDN are controlled from a maintenance and administration position (MAP). Maintenance for ISDN PMs involves monitoring and maintaining the following hardware:

- ISDN Line Group Controller (LGCI)
- ISDN Line Trunk Controller (LTCI)

- DS30A P-side links

- ISDN Remote Cluster Controller (RCCI)

- ISDN Digital Trunk Controller (DTCI)

- PRI D-channels and B-channels on the DTCI and LTCI

- Enhanced ISDN Line Concentrating Module (LMCE)

- ISDN Line Concentrating Module (LCMI) (old standard)

See Figure 4-16 on page 4-123 for MAP level access for most of the ISDN PMs listed above.

See NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide* for information on ISDN PM maintenance.

DPN series packet handler (PH) maintenance

An optional OAM processor (Figure 4-10 on page 4-97) allows maintenance to be performed from the DMS-100 MAP. The maintenance capability provides access to the troubleshooting aids for circuit-switching and packet-switching. The optional OAM processor is treated as if it were a DMS-100 peripheral module for downloading and maintenance. The packet handler faults generate alarms on the DMS-100 MAP. The DMS-100 fault display and correction procedures can be used to correct packet handler faults.

Besides forwarding faults to the host, the NM or RM and the AM also display alarms on the Network Control System (NCS). Commands input by the NCS operator can be used for testing and troubleshooting the DIU, AM, and the NM or RM, as well as for enabling and disabling service.

DPN logs are produced and used differently from DMS logs. The logs produced are of two types:

- Command logs for operator command activity

- Event logs whenever NCS software is used

LPP-based packet handler (DMS-PH) maintenance

Maintenance features for the LPP-based packet handler (DMS-PH) are in software package NTXP47AA or NTXP47AB, DMS Packet Handler Base. The following is a sample of maintenance related DMS-PH features:

- The Packet Processor Maintenance feature provides software to support basic provision and maintenance operations on the XLIU. Register XLIUOM is added to OM group PM1. MAP level XLIU is added with commands: TST, BSY, OFFL, LOADPM, and QUERYPM.

Figure 4-16 — PM command level menus

NOTE: Does not include command level menus for the LPP part of the DMS_PH).

CI Level

PM level

MAPCI

MTC

```
2   Post_
11  Disp_
13  Status
14  IPML
15  PES
16  FMT
```

DTCI level	LCME/LCMI level	ILGC/LTCI levels	DCH level
2 Post_	2 Post_	2 Post_	2 Post_
3 Listset	3 ListSet	3 Listset	3
5 Trnsl_	4 SwRg_	5 Trnsl_	5 Trnsl_
6 Tst_	5 Trnsl_	6 Tst_	6 Tst_
7 Bsy_	6 Tst_	7 Bsy_	7 Bsy_
8 RTS_	7 Bsy_	8 RTS_	8 RTS_
9 OffL	8 RTS_	9 OffL	9 OffL
10 LoadPM_	9 OffL_	10 LoadPM_	10 LoadPM_
11 Disp_	10 LoadPM_	11 Disp_	11
12 Next_	11 Disp_	12 Next_	12 Next_
13 SwAct	12 Next	13 SwAct	13
14 QueryPM	13	14 QueryPM	14 QueryPM
15	14 QueryPM	15 DCH	15 Disp_
16	16	16	16
17 Perform	17	17 Perform	17 Swtch_
18	18	18 ISG	18

WARNING: When using the "Swtch" command on the DCH level, it is recommended that the hidden command "abtk" (abort task) not be used before a "Swtch" command is completed.

NOTES:

1. Menu items may have different parameters.

2. All levels also have command QUIT at item 0.

3. The command PERFORM is not supported for the DTCI or for the LTC used for PRI.

4. The command PERFORM is applicable if feature package NTX750 is present.

5. Use of the ISDN PM commands, including hidden commands, can be found in NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide,* NTP 297-2401-201, *DMS-100F National ISDN Implementation Service Guide,* or NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide.*

- DMS-PH Bd Channel Maintenance feature provides the maintenance capabilities required for Bd channels. This feature addresses the logical connectivity maintenance. The maintenance of physical channels is to be addressed in a future feature. This feature modifies ISG MAP level commands:

    — CONT to test Bd channels connected to the DMS-PH

    — QUERYCH to display ISDN service group channel information

- DMS-PH X.75 Trunk Maintenance I feature provides the initial trunk maintenance for the DMS-PH using a new MAP level X75TTP. Also, this feature modifies TTP MAP level commands:

    — TST to perform internal and external continuity tests

    — BSY to display a message when executed on a trunk with a private virtual circuit

    — CKTLOC to display information on X.75 trunks

- DMS-PH provisioned B-channel maintenance provides line maintenance support by modifying commands BSY, CKTLOC, DIAG, POST, and PTS at the LN_LTP_DIR level of the MAP. This feature adds command BCHCON to the LN_DATA_DIR level of the MAP to perform Bd channel continuity tests on nailed-up B-channels on a posted ISDN line card.

- DMS-PH channel and link maintenance provides integrated processor and frame transport bus-based maintenance of the DMS-PH channels.

- DMS-PH operational measurements provides a set of query commands by modifying commands QDCH, QIT, and QBB at the DMSCI level, and the QLOOP command at the LTPDATA level of the MAP. The following new commands are added:

    — QCOUNTS to display link level counts, packet level counts, link level protocol abnormality counts, and packet level protocol abnormality counts

    — QPHF displays information from the management information tree.

    — QSCOM displays table SPECCONN information for a given XPM P-side port, including the status of the special connection.

- DMS-PH CC Warm Switch Active (SWACT) provides the ability to transfer calls, resource usage, and status from the active to the inactive side of the DMS-PH Computing Module (CM). Packet calls do not survive a Warm SWACT as calls are taken down in the CM and in the peripherals during a Warm SWACT.

- DMS-PH TRAVER provides translation and routing verification for the DMS-PH.

For further detailed maintenance information on these and other features for the DMS packet handler see NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide*.

Customer premises equipment (CPE) maintenance

Customer premises equipment (CPE), also called terminal equipment (TE), is usually supported with documentation for that product, and includes installation, testing, and maintenance. The NT1 is the focal point for maintenance communication with the TEs and the network equipment. See Figure 4-14 on page 4-115 for location of the NT1, and Figure 4-17 on page 4-125 for a more detailed look at the NT1.

For the ease of maintenance and testing, both from the network perspective and the customer perspective, the NT1 supports the following features:

- transmission performance monitoring
- subscriber loop (U-loop) maintenance by the network
- testing by the network to the NT1
- testing by the customer to the NT1

The customer's TEs communicate with the NT1 through the S/T-bus. It is a four-wire loop consisting of transmit and receive pairs. Up to eight (8) TEs can be connected to the S/T-bus in a number of different configurations. The S/T-bus includes two channels used for maintenance messaging:

- the 800 bps S-channel for messages to the TEs
- the 800 bps Q-channel for messages from the TEs

Figure 4-17 — NT1 functional block diagram
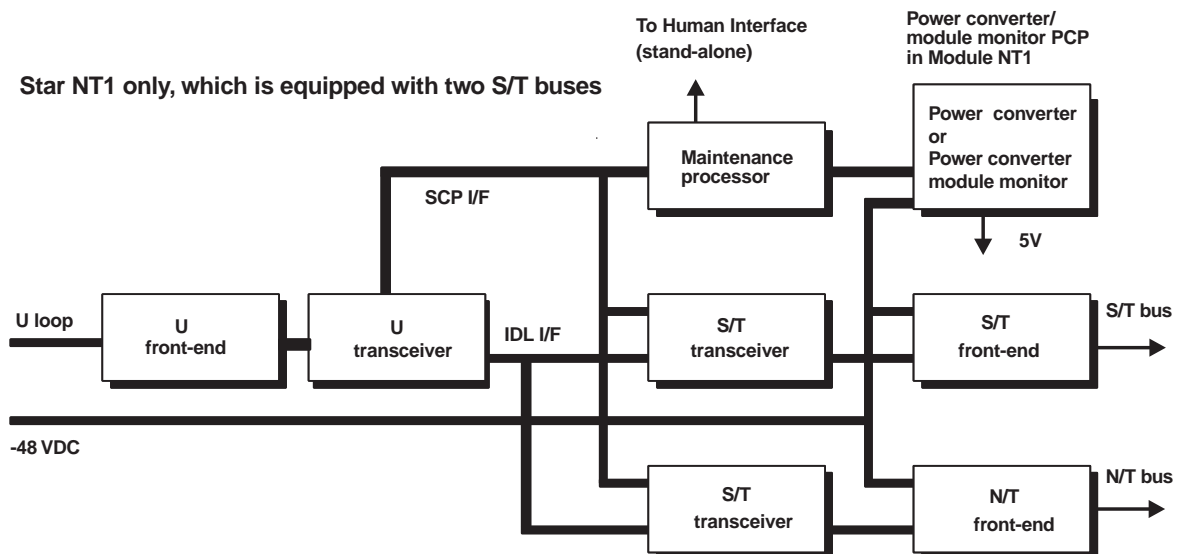
A problem with the S/T-bus installation may be indicated by failure to achieve synchronization between the NT1 and the TEs, or by an error rate performance over the S/T-bus that does not meet specifications. Either of these problems can be indicated by the NT1's LED status display once the NT1 is connected to the bus and TEs.

Within the NT1 is a maintenance processor that supports the maintenance and testing requirements of the network, the subscriber loop, and the customer TEs. The following features are provided to meet these requirements:

- cyclic redundancy check (CRC) handling that supports transmission performance monitoring by the network

- metallic testing, sealing current, and test signal handling, that support U-loop maintenance by the network

- continuous status monitoring and messaging over the embedded operations channel that support the network maintenance functions over the 16 Kbps M-channel for 2B1Q

- 2B+D loopback, loopbacks of individual B-channels (B1 or B2), and testing and status indicators, that support testing by the network

- B-channel loopbacks, messaging over the Q/S maintenance channel, and self-test features, that support testing by the customer.

For a good single source of CPE information on providing ISDN service, installing and testing CPE TEs and related equipment, and trouble reporting and clearing customer complaints, see NTP 297-2401-501, *DMS-100F ISDN BRI Maintenance Guide.*

CCS7 signaling and trunking maintenance

ISDN services use SS7 signaling for interworking with other nodes. Integrated Services Digital Network User Part (ISUP) is a level of the SS7 layered protocol. The main functions of ISUP include the signaling functions required to provide switched services and user facilities for voice and nonvoice applications. For ISDN calls, ISUP provides:

- setting up and taking down ISDN calls
- ISDN access signaling
- monitoring and supervision
- maintenance capabilities

To get a better understanding of what SS7 is and what maintenance capabilities exist to support ISDN, see the following "SS7 Overview and Maintenance" subsection.

DMS-100F ISDN logs and OMs

ISDN logs

The following logs have been created specifically for ISDN service:

ISDN100 is generated when a D-Channel Handler (DCH) associated with an ISDN cannot be put into traffic level because a terminal is unavailable for message traffic. This situation occurs when there is no response to a TEI check or audit.

ISDN101 is generated when a DCH has detected a duplicated TEI on the same loop and removed it from service. If multiple terminals respond to a TEI check, they are all removed from service.

ISDN102 is generated when a DCH has detected duplicated terminal endpoint identifiers on the same ISDN line and has removed the line from service.

ISDN103 is generated when manual action has changed the state of the D-channel used for packet service.

ISDN104 is generated when sync is lost on a D-channel used for D-channel packet service, this loss removes the channel from service.

ISDN105 is generated when synchronization is lost on the PRI B-channel, causing the B-channel to be removed from service.

ISDN106 is generated when layer on of a D-channel fails, causing the loop to go to the DMB state and setting fail flag I.

ISDN107 is generated when the system fails to restore the TEI.

ISDN108 is generated when the TEI is restored by the system.

ISDN109 is generated when a previously failed D-channel is restored to service, causing the loop to return to the IDL state and clearing the fail flag I.

ISDN110 when you have a backup D-channel—indicates that one D-channel is in service (INS) and the other D-channel is on standby (STB).

ISDN111 when you have a backup D-channel—indicates that one D-channel is in service (INS) and the other D-channel is out of service.

ISDN112 when you have a backup D-channel—indicates that both D-channels are out of service.

ISDN113 when you have a backup D-channel—indicates that a manual D-channel switchover of activity has occurred. The log indicates the active and out-of-service D-channels.

ISDN114 when you have a backup D-channel—indicates that an automatic D-channel switchover of activity has occurred. The log indicates the active and out-of-service D-channels.

ISDN115 indicates that an attempted dynamic TEI assignment has exceeded the maximum allowable number of links for a specific set of TEI values. This condition causes the switch to perform a TEI audit.

ISDN116 indicates attempted use of a TEI value that has not been previously assigned to a terminal on the loop. This condition causes the switch to perform a TEI audit.

ISDN118 is generated whenever the subscription counters, which represent the maximum allowable links for a specific set of TEI values would be exceeded by the attempted TEI assignment.

ISDN120 is generated when a periodic TEI audit fails during a routine test. The TEI audit fails when a switch receives more responses from terminals than expected during the audit.

ISDN121 is generated when a terminal initiates an identity verify message that contains a terminal endpoint identifier (TEI) value of 127.

ISDN122 is generated when a terminal sends an unexpected frame to the switching system for the current link access protocol for the D-channel (LAPD) state.

ISDN200 identifies up to 10 faulty ISDN D-channel lines with peg counts and percentages of frames received in error and retransmitted.

ISDN201 indicates the overall switch percentage of frames received in error and retransmitted.

ISDN202 is generated every time the MAP command reset layer (RLAYER) <n> is issued to reset layer 1, 2 or 3 performance counts for a posted LEN. Variable <n> indicates the layer.

ISDN203 provides a daily summary of layer 2 anomalies, up to 10 LENs are displayed along with the total number of anomalies for each line. Only LENS that have exceeded the daily threshold are displayed.

ISDN204 is generated after the layer 2/3 audit that runs once every 24 hours. The report lists a maximum of ten affected line equipment numbers (LEN) that have a high layer 3 abnormality rate. ISDN204 reports layer 3 high abnormality rates for voice services and packet data.

ISDN205 is generated when the layer 2 transmission performance exceeds the value set for office parameter LAYER2_PEGS_THRESHOLD_LEVEL in table OFCVAR.

ISDN301 is generated after the detection of a layer 3 protocol abnormality. Technical Requirement 821 (TR821) specifies the layer 3 protocol abnormality.

ISDN302 is generated to track parameter downloading abnormalities.

ISDN303 is generated when layer 3 packet abnormality counters exceed capacity on a basic rate interface (BRI) line. X.25 Protocol Systems (XPS) generate this log. ISDN303 lists the affected line equipment number (LEN), the type of counter capacity, the type of abnormality, and the counter capacity.

ISDN304 is generated when the D-channel handler (DCH) or enhanced D-channel handler (EDCH) detects a layer-2 protocol abnormality. Technical requirement 821 (TR821) specifies this abnormality. The report includes the type of abnormality.

ISDN305 is generated when an ISDN line exceeds the Service Disruption threshold. This threshold is defined by office parameter LAYER2_SERVICE_DSRPT_THLD, which resides in table OFCVAR.

ISDN306 is generated when layer 2 packet abnormality counters exceed capacity on a basic rate interface (BRI) line. X.25 Protocol Systems (XPS) generate this log. ISDN306 lists the affected line equipment number (LEN), the type of counter capacity, the type of abnormality, and the counter capacity.

ISDN307 is generated when the HDLC frame processor (HFP) encounters a packet abnormality for layer 2. The HFP is part of the DMS packet handler. X.25 Protocol Systems (XPS) generate this log.

ISDN308 is generated if the count of layer 2 service disruptions exceeds the value set for office parameter LAYER2_SERVICE_DSRPT_THLD in table OFCVAR. ISDN308 displays the threshold value for service disruptions, the line equipment number (LEN), and the count of service disruptions.

ISDN309 is generated if the count of layer 3 service disruptions exceeds the value set for office parameter LAYER3_PACKET_SVC_THLD in table OFCVAR. ISDN309 displays the threshold value for service disruptions, the line equipment number (LEN), and the count of service disruptions.

ISP101 is generated when the system cannot establish a communications link between the PH and the operations, administration, and maintenance processor (OAMP). The log also appears if the system detects a link failure when the link establishes.

ISP102 the Packet Handler (PH) subsystem generates this report when the operations, administration, and maintenance processor (OAMP) tries to upload a nonexistent master configuration file (MCF) from the PH.

ISP103 is generated when the operation, administration, and maintenance processor (OAMP) fails to download a master configuration file (MCF) to the PH.

ISP104 is generated when the operation, administration, and maintenance processor (OAMP) fails to activate the data for an access module (AM) on the PH.

ISP105 is generated when a software problem occurs on the SUN.

ISP106 is generated when the system drops the link to the operations, administration, and maintenance processor (OAMP).

ISP107 is generated when an error occurs when the operation, administration, and maintenance processor (OAMP) executes a command from SERVORD. The error can also occur when OAMP executes audit applications.

ISP108 is generated when the merge command is invoked.

ISP109 is generated when a problem occurs on the operation, administration and maintenance processor (OAMP) causing it to halt the processing of commands.

ISP110 is generated when the servord or audit process tried to send data to the operation, administration and maintenance processor (OAMP) and the link was dropped.

ISP113 is generated when the operation, administration, and maintenance processor (OAMP) fails to download processing element/peripheral interface (PE/PI) information to the packet handler (PH). The system generates ISP113 when you use the PH return to service (RTS) command. Failure normally occurs because of differences between data in the PH and in table PHINV.

ISP114 is generated when operating company personnel invoke the merge command.

LINE131 is a loop performance information log that is generated when the error second (ES) or the severe error second (SES) has been exceeded on a 2B1Q line card.

LINE145 is generated when a status change is detected and reported to the central control complex. The state of the loop is changed to lockout (LO) if the loop is in service.

LINE147 reports changes in the NT1 test mode indication (NTM). This log can be triggered by customer initiated maintenance of the NT1.

LINE148 is generated when a mismatch is detected—between the Basic Line Monitoring (BLM) data stored on the 2B1Q line card, and the data stored in the central controller (CC), for the loop identified in the log—causing the Layer 1 BLM audit to occur.

LINE149 reports multipoint embedded operations channel (EOC) configuration changes during LCME audits.

LINE150 generates this report for the Customer Originated Trace (COT) feature. A subscriber dials the COT access code or presses the COT key to initiate a trace of the last call. The LINE150 log provides a dump of the incoming memory slot (IMS) for the COT subscriber.

LINE151 generates this report for the Customer Originated Trace(COT) feature.

AUD510 is generated when there is a data dump for an ISDN extension block.

A number of existing log reports have been modified and can be used for ISDN service analysis. Table 4-11 on page 2-132 provides a list of these logs.

For further information on logs, alarms, detailed meaning, and action to be taken, see NTP 297-YYYY-840, *DMS-100F Log Reference Manual.* Other supporting information on ISDN and related logs can be found in NTP 297-2401-501 *DMS-100F ISDN BRI Maintenance Guide* and NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide*

ISDN OMs

Operational measurements (OMs) are a good source of information for determining ISDN service-affecting conditions that might require maintenance action. The following OM groups have been created for ISDN:

- **ISDN Bd channel (ISDNBD)** provides registers to monitor packet service traffic on D-channels. (With BCS35, this OM group is no longer available)

- **ISDN Logical Link (ISDNLL)** provides registers to monitor traffic on logical links on D-channels. (With BCS35, this OM group is no longer available)

- **Bearer Capability Customer Group (BCAPCG)** provides registers to count the number of unsuccessful call attempts for IBN and ISDN lines due to bearer capability incompatibility for a particular customer group.

- **Bearer Capability Office (BCAPOF)** same as OM group above, except counts for the whole office. It also measures synonym directory number activity.

- **Call Progress Indication Customer Group (CPICG)** provides registers to count ISDN call progress activity events.

- **DCH BD channel performance summary (ISGBD)** provides registers to count the following information on a DCH channel basis:
    - — the number of frames transmitted and received
    - — the number of frames discarded
    - — the number of frames with CRC errors

- **DCH BRA D-channel performance summary (ISGBRA)** provides registers to count the following information on a DCH on a per-channel basis:
    - — the number of frames transmitted & received
    - — the number of frames discarded
    - — the number of frames with CRC errors
    - — the number of link resets by the DCH and the far end
    - — the number of reject frames the DCH transmitted and received
    - — the number of "receiver not ready" frames transmitted and received by the DCH
    - — the number of times a SAP16 frame is shed during a DCH overload

- **ISDN Services Group (ISGCPU) Central Processing Unit Occupancy** provides registers to measure the ISG's CPU occupancy on a per-DCH basis.

- **ISDN Services Group (ISG) Overload summary (ISGOVLD)** provides registers to measure the degree to which an ISG is overloaded on a per-DCH basis.

- **PRA D-Channel Layer 2 performance (PRADCHL2)** provides registers that monitor the layer 2 traffic that travels over the PRA D-channels.

Table 4-11 — Other supporting DMS log reports for ISDN

Equipment	Log	Summary
LGC, LCME, or LCMI	PM100	diagnostic fail
	PM101	checksum fail
	PM102	state change to system busy
	PM103	state change to offline
	PM104	state change to unequipped
	PM105	state change to manual busy
	PM106	state change to in service
	PM107	state change to C-side busy
	PM113	message congestion during high traffic
	PM114	load or test failure on PM
	PM115	misc. trouble during normal operation
	PM116	message error report from PM
	PM117	trouble during normal operation
	PM118	misc. trouble during normal operation
	PM179	PM hardware exception report
	PM180	PM software exception report
	PM190	DCH state change to system busy
	PM191	DCH state change to system busy elation
	PM192	DCH state change to C-side removed from service
	PM193	DCH state change to offline
	PM194	DCH state change from INSV to ISTB (misc. trouble during normal operation)
	PM195	DCH state change to in-service
	PM196	DCH removed from customer table DCHINV
	PM198	DCH fault which is not service-affecting
	PM199	DCH diagnostic results
	PM200	DCH load information
	PM235	DCH takeover occurrence
	PM270	DCH congestion or overload
LINKS	PM181	XLIU maintenance status information
	PM182	state change to manual busy
	PM183	state change to system busy
	PM184	link returned to service
	PM187	carrier state change to system busy
	PM188	return to service or protection switching
ISDN lines	LINE100	diagnostic pass on an ISDN line
	LINE101	diagnostic fail on an ISDN line
	LINE107	insulation test required
	LINE110	foreign potential detected
	LINE118	failure to connect MTA

- **Primary Rate Access Facility (PRAFAC)** provides register to measure traffic that is generated by network ring again (NRAG) on PRA D-channels. PRAFAC data can help identify network problems by measuring facility and facility reject messages from switch to switch.

Besides the OM groups created for ISDN, the following OM groups are likely to be of most use for ISDN:

- Call Forwarding Feature Group (CALLFWD)

- Call Park Group (PRKOM)

- Call Pickup Group (CPICKUP)

- Call Waiting Feature Group (CALLWAIT)

- IBN Customer Group (IBNGRP)

- Local and Remote Line Module Traffic (LMD)

- Message Waiting and Call Request Group (MWYCAR)

- Off-hook Queuing and Call Back Queuing Group (OHQCBQCG)

- Speed Calling Group (SPEEDCALL)

- Subscriber Line Usage (SLU)

- Extension Block (EXT)

- Customer Unauthorized Treatment Extension (TRMTCU2)

For detailed information on the OM groups and their registers, see NTP 297-YYYY-814, *DMS-100F Operational Measurements Reference Guide.* For an overall starting point to understand how OMs support maintenance, see the "Operations Measurements" subsection within the *Preventive Maintenance* tab.

ISDN parameters (PARMS)

Improper values or settings for office engineering parameters can seriously affect ISDN service, maintenance related data, and functional capabilities.

ISDN impacts many existing parameters since provisioning formulas and timing factors have to be considered for ISDN. Some ISDN TR-compliant requirements are dependent on parameter values (i.e., parm ISDN_NET_1A_INTERWORKING).

ISDN office parameter details can be found in NTP 297-YYYY-855, *DMS-100F Office Parameters Reference Guide.* An office parameters administration guide can be found in the back of the NTP document.

The following Table 4-12, "ISDN Parameters," contains a sample list of parameters supporting ISDN. They do not include parameters for ISUP that should be evaluated when suspecting parameters as the cause of ISDN maintenance related problems.

Table 4-12 — ISDN Parameters

Table OFCENG	Table OFCOPT	Table OFCVAR
BC_CHECKING_SCOPE	ISDN_INFO_EXT_REC	DATA_CALL_SMDR
DCH_BD_STATMUS	MAX_BRA_LINES	GEN_CDR300_ISDN_LOGS
DEFAULT_BEARER_CAPABILITY	MAX_PRI_LINKS	
ISDNBRI_CNAMD_CND_ONE_AMA	PI_CALL_TOPO	ISDN_LOSS_OF_SIG_ DGASP_ALARM
ISDNBRI_PRIVACY_CHANGE_ALLOWED	PRI_LINK_PRICING	
ISDN_DPN_PH_GENERIC	TIE_ROUTE_INFO_EXT_REC	ISDN_LOSS_OF_SIG_NO_ DGASP_ALARM
ISDN_NET_1A_INTERWORKING	TRAFFIC_INFO_EXT_REC	
ISGBDOM_BLKSIZE		ISDN_LOSS_OF_SYNC_ ALARM
LAYER2_PEGS_THRESHOLD_LEVEL		
LCDI_SYNC_BURST		ISDN_MPLU_NODE_ FAILURE_ALARM
LCDI_SYNC_DELAY		
MAX_DTA_ON_SWITCH		ISDN_NT1_TEST_MODE_ ALARM
NO_OF_HIS_DATA_BLKS		
NO_OF_MEDIUM_FTR_DATA_BLKS		ISDN_PERFORMANCE_ MON_ALARM
NO_OF_SMALL_EXT_BLKS		
NO_OF_XLARGE_EXT_BLKS		ISDN_T_SYNC_LOST_ ALARM
NUM_SME_CONTROL_BLOCKS		
NUM_SME_DATA_BLOCKS		PERFORMANCE
OAM_HW_PRESENT		
PHINFO_AUDIT_TIME		
T108ISDN_TIMEOUT_IN_MINUTES		

XPM PLUS for National ISDN

To support the continued rollout of ISDN features and enhancements, increased memory, and real time improvement are essential conditions for the ISDN LGC and LTC peripherals. The feature to support these conditions is XPM PLUS. It is in software package NTXR34AA that was available in BCS35. In addition to the new software, a single XPM PLUS circuit pack replaces the master processor and signaling processor configuration and their associated memory packs. XPM PLUS can provide a 60% increase in memory and a 50% improvement for real time.

ISDN line drawer for remotes (ILD-R)

The ISDN Line Drawer for Remotes provides a cost-effective means of provisioning low line-size Basic Rate Interface ISDN into the installed base of DMS-100 remotes.

The ISDN Line Drawer offers a Nortel Networks solution completely integrated into the operations, administration, and maintenance (OA&M) capabilities of the DMS system.

ISDN line drawer for remotes (NT6X05DA)

Each ILD-R supports 28 NTBX27AA U-loop ISDN cards. The ILD-R has internal D-channel handlers that allow the drawer to be independent of external ISDN hardware. For this reason, the host LTC+, LGC+, or RCC2 does not require the installation of the enhanced ISDN signaling preprocessor (EISP) or enhanced D-channel handler (EDCH) cards.

The ILD-R communicates directly with the LTC+, LGC+, or RCC2 over two separate message channels that connect the ISDN drawer controller (IDC) to the LTC+, LGC+, or RCC2. These message channels are independent of Star Hub message channels, which support:

- loading the IDC
- Q.931 signaling messages between the terminal and the LTC+, LGC+, or RCC2
- maintenance and provisioning messages to the IDC
- downloading parameters to ISDN terminals

The IDC provides the LAP-D termination. Circuit-switched messages that originate at the ISDN loop are converted to DMSX protocol by the IDC and transferred to the LTC+ or LGC+. Packet switched messages are converted to frame switching and transferred to the packet handler through the network. The ILD-R has 32 LAPD links, 28 for ISDN loops and four for other purposes.

The ILD-R contains flash memory and can be loaded while in the in-service state.

The ILD-R supports intraswitching in the Star Hub.

NOTE: ISDN lines are not supported during Star Hub emergency stand-alone (ESA). If the Star Hub enters ESA, all ISDN calls are released.

User interface commands are available to support the added functionality required by the ILD-R. These user interface commands are listed in Table 4-14, "Summary of ILD commands."

Line drawer upgrade

To upgrade a POTS line drawer to an ISDN line drawer in the Star Hub:

- delete all lines from that drawer
- remove the POTS line drawer from service
- physically replace the POTS line drawer with an ILD-R
- declare the new ILD-R and return the ILD-R to service

> **NOTE:** This procedure does not cause other drawers to be removed from service.

The ISDN line drawer includes the following key components:

- NT6X54DA – IDC card
- NTBX27AA – ISDN U-interface line card
- NTBX71AA – ISDN point of use power supply (PUPS)

ISDN Drawer Controller card (NT6X54DA)

The IDC is at the front of the ILD-R, behind the front faceplate. The IDC supports up to 28 ISDN loops and

- provides pulse coded modulation (PCM) and data control functionality
- exchanges D-channel messages between the ISDN line cards and the rest of the SuperNode switch
- provides the processing engine that does the D-channel routing, line card maintenance, loop performance monitoring, and local drawer connection management

Communication between the line drawers, or between two LSGs, is completed through the single IDC in each drawer. If one of the RCP cards fails, the activity is moved to the other RCP card. The IDC communicates with the C-side through a single RCP card. The IDC card has three LEDs on the faceplate of the IDC card to indicate faults. The three LEDs are:

- green InSv LED (operates by software and indicates the card is in service)
- red Fault LED (operates by both software and hardware and indicates a fault condition)
- PUPS OK LED (indicates a +5 V supply problem or a blown fuse)

Procedures to replace a ILD-R circuit pack can be found in NTP 297-8001-547, *DMS-100 Family NA100 Card Replacement Procedures.*

> **NOTE:** Effective in NA011 - NA012 all ISDN peripherals (DTCI, LGCI, LTCI) require a NTSX05 and minimum EISP release level of NTBX01AC or BA. If Remote is equipped with ISDN LD, host peripheral must be equipped with NT NTSX05 peripheral processor.

Multi-Point Embedded Operations Channel (MP-EOC) on the ISDN Line Drawer

MP-EOC is a feature that allows craft to test individual legs of an extended ISDN loop. It was available 4Q99 (NA012). It is part of Package ISDN0003

ILD-R OMs and logs

ISDN line drawer for remotes (ILD-R) OMs and logs are associated with the Star Remote System OM Group and ISDN logs. Table 4-13, "ILD-R OMs and logs" provides a description of each group and the name of the associated log.

Table 4-13 — ILD-R OMs and logs

Star Remote System OM Group	Description	Associated logs
ILDBD	This group provides information pertaining to the ISDN line drawer for remotes (ILD-R) Bd-channel. This information enables the operating company personnel to verify normal transit of information (frames) on the links between the ILD-R and the packet handler.	None
ILDBRA	This group provides information pertaining to ILD-R D-channels. This information enables the operating company personnel to verify normal transit of information (frames) on the links between the ILD-R and the NT1.	ISDN200 and ISDN201
ILDSTAT	This group provides information pertaining to the ILD-R processor occupancy. This information enables the operating company personnel to measure ILD-R processor performance.	None
ILDMSGCT	This group provides information pertaining to ILD-R messages to and from the XPM. This information enables the operating company personnel to verify normal transit of messages and DMSX protocol performance on the DMSX data link between the ILD-R and the XPM.	None

ILD STAR menu descriptions

When an integrated services digital network (ISDN) line drawer for remote (ILD-R) data is entered, the ILD command appears on the STAR menu. The ILD command allows operating company personnel to access the ILD level. The ILD level supports maintenance actions on the ISDN line drawers. The ILD level shows the state of the ILD banks (memory areas) and the ILD Bd channels (low speed packet data). From this level, an ILD can be posted and action can be performed on the posted drawer. For example, LOADPM is used to load the ILD firmware.

The ILD drawer numbers are shown in reverse video mode to distinguish them from a standard plain old telephone service (POTS) line drawer. An overview of the ILD commands available at the STAR level follows.

Table 4-14 — Summary of ILD commands

Com-mand	Function	Description
BSY	Busy	Moves the ILD-R or Bd-channel to ManB.
LIST_SET	Lists posted set	Displays the ILD-Rs included in the posted set.
LOADPM	Load PM	Loads the ILD-R. Used to load either a single drawer (LOADPM) or all the drawers on the same Star Hub (LOADPM ALL). The steps of the LOADPM procedure, and the amount of memory already loaded will appear at the MAP display during the LOADPM command.
NEXT	Next	Displays the next ILD-R in the post set.
OFFL	Off line	Moves the ILD-R or Bd-channel to offline (Offl).
POST	Post	Posts one or all ILDs located in the same Star Hub. When POST ALL is invoked, all ILD-Rs located in the Star Hub (up to two) are added to the list.
QUERYCH	Query channel	Displays information about the Bd-channel. It displays the XLIU/XSG number and channel of the Bd special connection, the Bd-channel, and the ILD-R BD operational measurement (OM) index.
QUERYPM	Query PM	Displays information about the ILD-R. Two optional parameters, FLT and CNTRS can be used.
RTS	Return to service	Returns to service the ILD-R or a Bd-channel.
SWBNK	Switch memory bank	Switches activity between the two flash memory banks. Currently, only cold switch bank is supported.
TRNSL	Translate	Displays the ILD-Rs C-side links with their status and message condition.
TST	Test	Tests the ILD-R or its Bd-channels. When BD1 or BD2 is typed, a continuity test between the ILD-R and the packet handler is performed. The test sends a message at the ILD-R, loops it at the integrated packet handler (IPH), and verifies it again at the ILD-R.
QILD	New	This nonmenu command displays all the D-packet switching logical terminal identifiers (LTID) that are mapped into a given ILD-R's Bd-channels. This command can request a certain Bd-channel if one is selected, or request information of both ILD-R's Bd-channels.
QSCONN	Changed	This nonmenu command displays SPECCONN endpoints and segments, depending on the command's parameter. A new option, ILDCHNL, is added to the QSCONN SEG command.

For more details, see NTP 297-8353-550, *DMS-100 Family Star Remote System Maintenance Manual*.

ILD-R alarms

The ISDN line drawer for remotes (ILD-R) does not generate any alarms. As a result of ILD-R failure or problems, the ILD-R either goes into ISTb or SysB states. This, in

turn, causes the STAR level to generate an alarm. The QUERYPM FLT command at the ILD MAP level indicates what problems are causing the alarm.

ISDN list of terms

The list of terms included here supports the ISDN terms used in the MOM—it is not an all-inclusive list for use with other documentation. Most ISDN documentation provide a "List of Terms" section that should be referenced when needed.

2B1Q — Four level pulse amplitude modulation (PAM) code with two binary to one quaternary symbol coding. This is a line protocol.

Abstract terminal — The standard software representation of the physical terminal at the network level. The abstract terminal specifies how the network and the physical terminal interact at the network level.

Access Module (AM) — The unit that provides access to the network modules of a digital packet network switching system from a local subscriber packet line or the digital interworking unit.

Access termination — The functional term to describe the part of the exchange termination that terminates the BRI and PRI access interfaces. It defines the access privileges of the terminals on an interface, and provides the terminals on an interface with access to ISDN circuit and packet switching services.

AMI — Alternate mark inversion (old standard line protocol)

Authorized call type — A characteristic associated with the logical terminal (service profile) in functional signaling. It offers a pool of bearer capabilities to a logical terminal.

Basic Rate Interface (BRI) — A type of access to ISDN service provided by a set of time division multiplexed digital channels of information, including two B-channels, one D-channel and one or more maintenance channels, often described as 2B channels + D-channel. BRI is typically used on lines between customer premises and a central office switch.

Bearer Capability (BC) — Bearer capability is an information element carried in the SETUP message for functional signaling, indicating the type of call (data or voice) and the rate of transmission required.

B-packet — Packet data transmitted over a B-channel

B-voice — Pulse code modulated (PCM) voice carried on a B-channel

Consultative Committee on International Telephone and Telegraphy (CCITT) — The CCITT is now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union). See ITU-T for a description.

Circuit-switched network — Synonym for the telephone network

Common Channel Signaling 7 (CCS7) — Digital, message based, network signaling standard defined by ITU-T. This separates call signaling information from voice channel so that interoffice signaling is exchanged over a separate signaling link.

CS-data — Circuit-switched data carried on the B-channel

Customer Premises Equipment (CPE) — Equipment, such as ISDN terminals, located on the customer's premises. Sometimes referred to as "Customer Provided Equipment".

Datalink layer — Layer 2 in the OSI model. It creates logical links between ISDN terminals and the services they are accessing, and controls the sequence of messages transmitted over a channel.

Data Packet Network (DPN) — A network made up of DPN components that routes data packets within that network of components. See *DMS Packet Handler.*

D-call control — Call control information carried on the D-channel used for establishing, maintaining, or clearing a voice or circuit-switched data call on a B-channel of ISDN.

D-channel — For BRI, the D-channel is a 16 Kbps bidirectional channel. It carries call control messages between a terminal on an ISDN interface and the exchange termination used to set up, maintain, or clear a circuit-switched call on a B-channel. It carries low speed packet data between a terminal on an ISDN interface and a terminal in the packet data network. For PRI, the D-channel is a 64 Kbps bidirectional channel. It carries call control messages between a terminal on an ISDN interface and the exchange termination used to set up, maintain, or clear a circuit-switched call on a B-channel.

D-Channel Handler (DCH) — Card(s) in the LGC/LTC provide the primary interface to all D-channels and perform Q.921 LAPD layer 2 processing.

D-Channel Interface (DCHI) — Interfaces PBXs with the D-channel in ISDN PRI. The DCHI performs link access procedures on the D-channel for PRI.

Digital Interworking Unit (DIU) — The unit in a digital packet network switch that converts B- and D-channel data packets received in DS1 format from the ISDN controller into V.35 format suitable for the access module. For packets sent in the opposite direction, the DIU performs the reverse function.

Digital Multiplex System (DMS) — A central office switching system in which all external signals are converted to digital data and stored in assigned time slots. Switching is performed by reassigning the original time slots.

DMS Packet Handler (DMS-PH) — A DMS-100F packet handler that is part of the Link Peripheral Processor.

D-packet — Packet data carried on the D-channel between the packet handler and the ISDN terminal.

DS-1 or DS1 — A closely specified bipolar pulse stream with a bit rate of 1.544 Mbps. It is a North American standard signal used to interconnect Nortel Networks digital systems. The DS1 signal carries 24 DS0 information channels of 64 Kbps each.

Exchange Termination (ET) — The functional name for the component of the ISDN that serves as the access termination for BRI and PRI interfaces, and provides circuit-switched services to the ISDN switch.

Functional signaling — Functional signaling messages are used for call control and require intelligent processing by the user terminal either in their generation or analysis. Functional signaling terminals track call states related to the setup and take-down of calls at the user network interface.

Integrated Bit Error Rate Test (IBERT) — A test that a MAP operator uses with an IBERT card to test transmission quality of a selected data line. The card resides in the line drawer of a Line Concentrating Module (LCM) and generates the bit stream for an IBERT test. An IBERT test can be used to test most lines connected to the DMS, if the lines support the T-link protocol.

International Organization for Standardization (ISO) — founded in 1946, is a worldwide federation of national standards bodies from some 100 countries, one from each country. Among the standards it fosters is Open Systems Interconnection (OSI), a universal reference model for communication protocols. Many countries have national standards organizations such as the American National Standards Institute (ANSI) that participate in and contribute to ISO standards making. "ISO" is not an abbreviation. It is a word, derived from the Greek isos, meaning "equal", which is the root for the prefix "iso-" that occurs in a host of terms, such as "isometric" (of equal measure or dimensions) and "isonomy" (equality of laws, or of people before the law). The name ISO is used around the world to denote the organization, thus avoiding the plethora of abbreviations that would result from the translation of "International Organization for Standardization" into the different national languages of members, (for example, IOS in English or OIN in French - for Organisation internationale de normalisation). Whatever the country, the short form of the Organization's name is always ISO.

ISDN Service Group (ISG) — An ISG defines the services a DCH provides, as well as their allocation to the channels within the DCH. This allows hardware independent access to service related functions at the MAP. The ISG MAP level provides a view of the services. The DCH MAP level provides a view of the hardware.

ISDN Signaling Processor (ISP) — Provides the call control messaging function and DCH maintenance functions.

ISDN User Part (ISUP) — CCS7 message based signaling protocol that acts as a transport carrier for ISDN services and functionality throughout the public network.

ISP — Acronym for ISDN service provisioning (ISP) with ISP logs, ISDN signaling processor (ISP), or interrupt stack pointer (ISP) used in footprint data logs.

ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union) — Formerly the CCITT, is the primary international body for fostering cooperative standards for telecommunications equipment and systems. Comite Consultatif Internationale de Telegraphique et Telephonique is located in Geneva, Switzerland.

LAPB — Link access procedure - balanced

LAPD — Link access procedure for the D-channel

Logical Terminal (LT) — Datafilled instance of the abstract terminal. This is provided with a subset of the features and services datafilled in the access termination for the abstract terminal. Also called the service profile of a terminal.

Logical Terminal Identifier (LTID) — Unique identifier assigned to the logical terminal when it is datafilled in the access termination.

M5317T and M5317TD ISDN business sets — The Meridian 5317T type of ISDN telephone uses functional signaling to access CS-voice and data. For National ISDN 1, the M5317T and M5317TD are being replaced with new M5317TX and M5317TDX terminals. Support for the M5317T and M5317TD terminals will be provided through firmware upgrade kits.

M-channel — A 16 Kbps, bidirectional, U-loop channel used to transfer maintenance information between the NT1 and the ET.

National ISDN Council (NIC) — NIC is a forum of telecommunications service providers and switch suppliers that participate in Telcordia's National ISDN Platform Evolution projects.

Network Administration System (NAS) — A stand-alone computer that is involved in OEM for ISDN services. The NAS uses data on service and system operation to generate files that contain information on alarms, accounting, billing, and network operation.

Network layer — Layer 3 in the OSI model, used to send call control information.

Network Termination 1 (NT1) — Access point for BRI to ISDN. This component is situated on the customer premises, and is typically located between the terminals and the ET. An NT1 is required when ISDN lines are terminated by U-line cards.

Open Systems Interconnection (OS1) — A seven-layered protocol model for communications networks developed by the International Standards Organization and adopted by ITU-T for ISDN.

Physical layer — Layer 1 of the OSI model provides the raw information channels to layer 2 (datalink layer). Protocols depend on the type of interface (BRI or PRI).

Primary Rate Interface (PRI) — An access protocol connecting an external network device such as a PBX to an ISDN switch. This access is provided by multiple, bidirectional, time-division multiplexed, digital channels of information. Typically, in North America it is arranged as 23 B-channels and one D-channel, referred to as 23B+D.

Q.921 — ITU-T recommendation defining protocols at the datalink layer.

Q.931 — ITU-T recommendation defining protocols for the circuit-switched call control at the network layer.

Q-channel — An 800 bps maintenance channel that runs on the S/T-bus from the network termination to the terminals.

Q/S-channels — Collective name for the Q- and S-channels

S-channel — An 800 bps maintenance channel that runs on the S/T-bus from the terminals to the network termination.

Service Access Point Identifier (SAPI) — Identifier used by the datalink layer (layer 2) protocol to define the type of service allowed for an ISDN terminal.

Service Profile Identifier (SPID) — Layer 3 identifier programmed into the logical terminal by the user during configuration. It uniquely identifies a logical terminal and its service profile to the switch. A SPID may be up to 20 alphanumeric characters long and is typically generated using the primary directory number of the terminal and an optional short suffix. A SPID is unique on a switch and has significance only on the local network.

S/T-bus — An 8-wire bus (only four wires are used to transmit and receive messages) that connects the NT1 to the terminal equipment for access to ISDN. Also known as S/T-interface, or S/T-loop. Formally known as T-bus.

Stimulus signaling — Stimulus mode messages—for call control—are sent by the terminal to the network as a direct result of actions by the terminal user. Terminals that use stimulus signaling have little local intelligence and are driven by the network. Stimulus signaling terminals do not keep records of call states.

S/T-line card — ISDN line card that terminates the S/T-bus in the LCMI/LCME. When S/T-line cards are used, the U-interface and the NT1 are not required. The ET acts as a network termination.

Supplementary services — A set of features such as Ring Again and Dictation Access, provided by the local switching system. Supplementary services are not network-wide, but are provided to an ISDN terminal entirely by the ET it is connected to. These services include circuit-switched services, based on Meridian Digital Cen-

trex (MDC), and packet-switched services, provided by the ISDN PH and packet switching network.

Terminal Endpoint Identifier (TEI) — Identity number used to distinguish between the terminals on an interface

Terminal Equipment (TE) — See *Customer Premises Equipment*

U-line card — ISDN line card that terminates the U-loop in the LCME or LCMI. When U-line cards are used, the NT1, which is located on customer premises, acts as the network termination.

U-loop — Portion of a BRI interface (ISDN line) connecting an NT1 to an LCME or LCMI.

Universal Terminal Adapter (UTA) — A device with associated software that allows a personal computer to connect to a Nortel Networks ISDN.

X.25 — ITU-T defined, network layer protocol used in packet-switching for establishing, maintaining, and clearing virtual circuit connections between an ISDN terminal and a destination in the packet network.

X.75 — ITU-T defined, network layer protocol used in packet-switching for establishing, maintaining, and clearing virtual circuit connections between packet switched networks.

SS7 Overview and Maintenance

Following is an overview of the elements that make up the Signaling System 7 (SS7) system and network, and an overview of the associated DMS-100F SS7 maintenance and surveillance tools. References to supporting documents are also provided.

SS7 overview

Understanding SS7

SS7 provides the foundation for advanced network services using intelligent network capabilities. SS7 is a message-based signaling protocol that segments into layers the interconnection and exchange of information that occurs between signaling points in a network. SS7 is based on the four-layer protocol that was defined by the ITU-T (formerly CCITT). Signaling System 7 is a variation of the seven-layer protocol of the Open Systems Interconnection (OSI) reference model. Protocol layers, and the variations are described later.

Commom Channel Signaling 7 (CCS7) is a digital message-based network signaling standard, defined by the CCITT, that separates call signalling information from voice channels so that interoffice signaling is exchanged over a separate signaling link.

Signaling System 7 (SS7) was developed for North American use.

Signaling System #7 (SS#7) is an international version of Signaling System 7 (SS7) based on the CCITT specification of SS7.

CCITT no. 7 signaling (N7) is a standardized out-of-band (common channel) signaling system that is suitable for terminal working (inside the same world zone) and transit working (between world zones). N7 normally uses a 64-kbit/s transmission rate and occupies one slot in a pulse code modulation (PCM) system. N7 is used by national and international networks, and is designed for digital transmission. The N7 standards that affect national networks are often called CCITT signaling system 7 (CCITT SS7).

NOTE: In this document CCS7 can be substituted for SS7.

Background

A telephone call has two components:

- signaling component
- voice or data component

The signaling component of a telephone call contains the supervisory and address signals that switching offices use to control the setting up, monitoring, and taking down of a call. The voice and data component contain only the traffic between the initiator and the recipient of the call.

In-band signaling (IB)

A signaling method in which signals are sent over the same transmission channel or circuit as the user's communication and in the same frequency band as that provided for the users. The MF (Multi-Frequency) signaling tones are in the voice band of 300 Hz to 3000 Hz. For example, some pay phones use in-band signaling tones to control coin collection and coin return.

Per-trunk signaling (PTS)

A conventional telephony method of signaling that multiplexes the control signal of a call with voice or data over the same trunk, see Figure 4-18. In conventional PTS, the called number (address) and supervisory signals are exchanged between the end-offices (EOs) on the trunk carrying the voice or data part of the call. This method uses in-band signaling.

Figure 4-18 — Per-trunk signaling
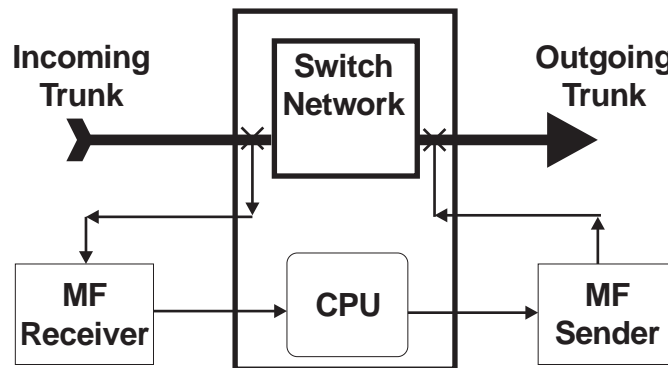
DISADVANTAGES:

- Limited signaling capability
- Slow call setup time

Common channel signaling (CCS)

Common channel signaling separates the signaling component from the voice and data component of a call and puts these two components on different facilities. The facility that is used for signaling is called a signaling link. The facility that is used for voice and data traffic is called a voice trunk.

The amount of signaling information that is placed on the signaling link by a call is small compared to the voice and data component of that call. As a result, a signaling link can be used for a large number of voice trunks without becoming overloaded. To maximize the efficiency of a signaling link, transactions that are not directly associated with a call can also be placed on a signaling link without any loss of call-processing capabilities.

In addition to the usual dialing, call setup, dialing, supervisory signals, and billing, the SS7 network provides transaction capabilities. These capabilities query on-line or external databases that make possible the revenue generating Advanced Intelligent Network (AIN) services and Line Information Databases (LIDBs). SS7 may therefore be regarded as a specialized form of data communication.

SS7 advantages

The advantages of separating the signaling component from the voice path are summarized as follows:

- Voice trunk facilities and interface equipment are less complex since they do not support the signaling function.

- Call setup time is reduced, resulting in shorter trunk holding times and a reduction in trunk provisioning requirements.

- Many error conditions, such as partial dial, are eliminated, thereby reducing the number of ineffective attempts on the network.

- Improved call control is gained through collapsing ineffective attempts and treatment at nearest end.

- Trunk network management is enhanced, since the nodes of a trunk network are able to communicate and exchange status information.

- Services requiring database support can be provided.

- SS7 facilitates the introduction of Advanced Intelligent Network (AIN) services using intelligent network capabilities.

SS7 takes full advantage of the large message capacity offered by high bandwidth digital channels. SS7 voice trunks initially operated at 56 Kbps but eventually were expanded to 64 Kbps for ISDN and other services.

Open System Interconnection (OSI)

The Open System Interconnection (OSI) reference model provides an international standard for modeling the interconnection and exchange of signaling messages between switching offices (SOs). The term *open* implies that by conforming to the

international standards, a system is open to all other systems obeying the same standards throughout the world. The different subsystems of SS7 are modeled on the OSI standard, see Figure 4-19

The OSI reference model is divided into two major functional areas, the Message Transfer part (MTP) (layers 1, 2, and 3) and the User Part (UP) (layers 4, 5, 6, and 7). The MTP provides all the functions that are required to successfully transfer data between two switching offices, and the different types of users, such as ISDN, that are able to use the MTP as a transport medium. These two major functional areas are further divided into layers that provide the boundaries for different users to identify the different functions that are required during the transfer of data between switching offices. The OSI layers are defined as follows:

- **Layer 1** — Physical Layer (1) provides the hardware to transmit a bit stream over the signaling network.
- **Layer 2** — Data Link Layer (2) is where error detection is carried out on signaling messages that have arrived from Physical Layer 1. This layer implements any error recovery procedures that may be necessary as a result of an error detected in a signaling message.

Figure 4-19   —   SS7/OSI architecture
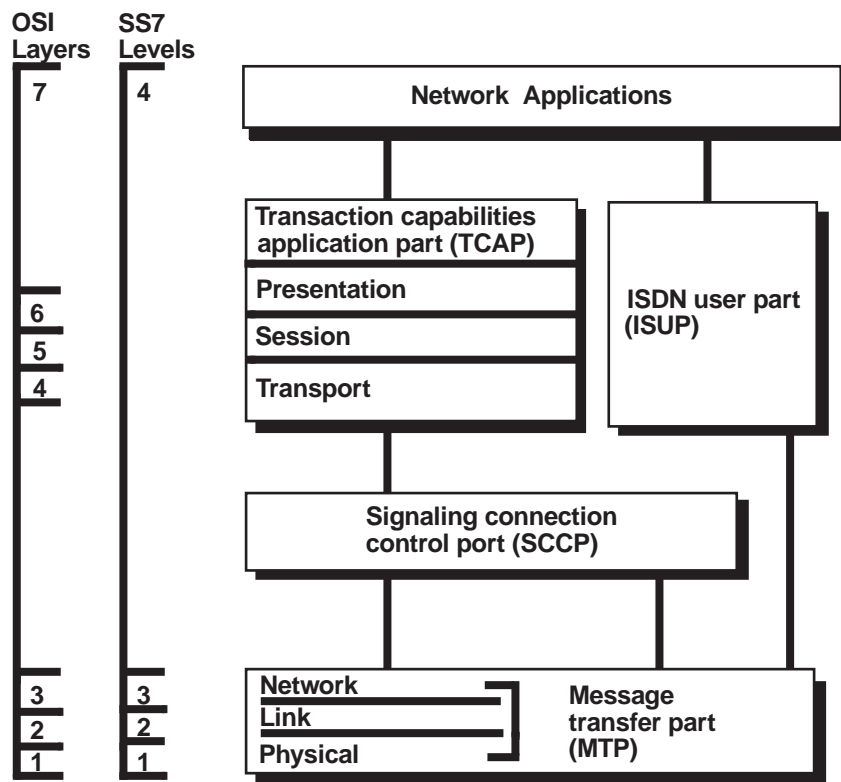
NOTE: SCCP is in OSI Layer 3 and SS7 Level 4

- **Layer 3** — Network Layer (3) transfers data using routing procedures and handles routing during failures. If the system needs reconfiguring as a result of a failure, this layer handles the reconfiguring procedures.

- **Layer 4** — Transport Layer (4) provides end-user to end-user transfer of information. This layer is similar to the Data Link Layer 2 in that it provides sequencing and error control to guarantee error free delivery of packets of data between end-users.

- **Layer 5** — Session Layer (5) coordinates the interaction between communicating application processes.

- **Layer 6** — Presentation Layer (6) transforms the syntax of the data into a form recognizable by the application process. For example, this layer may convert a data stream from ASCII to EBCDIC.

- **Layer 7** — Application Layer (7) the entry point for an application process to access the OSI environment.

SS7 layered model

SS7 is a message-based signaling protocol that segments into layers the interconnection and exchange of information that occurs between signaling points in a network.

SS7 is based on the *four-layer protocol* that is defined by the Consultative Committee on International Telephony and Telegraphy (CCITT). Signaling System 7 is related to the *seven-layer protocol* of the OSI reference model. The relationship between levels and layers is shown in the following list:

- **Level 1** — Equivalent to Layer 1, this defines the physical, electrical and procedural characteristics of the signaling data link and how to interface with it.

- **Level 2** — Equivalent to Layer 2, its purpose is to present an error free channel to Level 3. Major functions performed at this level are signal unit delineation and alignment, error detection and correction, signaling link failure detection and signaling message flow control.

- **Level 3** — Is a signaling network function that performs the functions of Layer 3 that do not involve the user. There are two major categories in this level: signaling message handling and signaling network management.

- **Level 4** — Performs the remainder of the functions of Layer 3 and the user parts, layers 4 to 7. This level handles call processing, trunk network management, and trunk maintenance.

SS7 modular structure

SS7 is modular in structure, see Figure 4-19. It consists of four functional levels for the interconnection and exchange of information among users:

- MTP (Message Transfer Part) — made up of Levels 1 through 3
- SCCP (Signaling Connection Control part) — included in Level 3

- TCAP (Transaction Capabilities Application Part) — Level 4
- ISUP (Integrated Services Digital Network User Part) (ISDN - User Part) — Level 4

Message Transfer Part

The Message Transfer Part (MTP) routes signaling messages between any pair of network nodes that rely on the transport capabilities of the MTP. The three levels of MTP: the signaling data link level, the signaling link function level, and the signaling network function level are equivalent to the OSI layers one (physical layer), two (link layer), and three (network layer), respectively.

- The physical level of the MTP defines the physical, electrical, and procedural characteristics for a 56 or 64 Kbps signaling data link that uses interfaces such as DS0A, V.35, and DS1.
- The data link level of the MTP ensures a secure signaling link between pairs of signaling points. This level provides signal unit alignment, error detection and correction, signaling link alignment, signaling link error monitoring, and flow control.
- The network level of the MTP performs logical address routing. This level also provides reliable signal transfer, even when signaling links or signaling points fail.

Signaling Connection Control Part

The Signaling Connection Control Part (SCCP) is situated above the MTP in the SS7 reference model. Together, the SCCP and level three of the MTP provide functions that are equivalent to layer three of the OSI model. The SCCP provides application addressing and management, keeps track of the status of applications, and lets the user know when an application is unavailable.

NOTE: Most of the specifications that are used by the MTP and SCCP are defined according to operating company requirements. The operating company defines these specifications through datafill.

SCCP services facilitate the transfer of circuit-related and noncircuit-related signaling data, as well as the monitoring and application availability. They also enhance those provided by the MTP, and together they create a Network Service Part (NSP) to make the application functional.

The operating requirements for the SCCP functions:

- minimizes the undeliverable messages sent from the SCCP into the SS7 network via the MTP to prevent unnecessary congestion.
- detect routing problems in the SCCP so that messages with return options can be directed to the appropriate application, rather than being lost at the MTP level.

- provide a flexible scheme for translating global titles (such as telephone numbers) for different applications into the SS7 address.
- Validates load-sharing across duplicate nodes such as signal transfer point.

Transaction Capabilities Application Part

The Transaction Capabilities Application Part (TCAP) provides a set of generic procedures for transaction-based applications. TCAP controls noncircuit-related information transfer between two or more nodes in a signaling network.

TCAP builds on the SCCP to provide a framework for a common approach to offering transaction-based services on the SS7 network. (For example, TCAP uses SCCP routing and translation capabilities to provide the functionality for supporting the transaction part of the database access service.) The framework consists of a set of procedures that are not specific to any particular service. Making use of such procedures avoids the inefficiency of having to tailor new ones every time a new application is created.

Typically, transaction capabilities are functions within the SS7 protocol for controlling the exchange of connectionless or noncircuit-related information between two or more signaling nodes over the SS7 signaling network.

Functionally, TCAP is divided into two parts—transaction and component.

The transaction portion identifies each TCAP message and ascertains which application process transaction its components belong to. Transaction association makes it possible to link a query to a response and to identify the context. As a result, a broader group of components—contained in one or more TCAP messages—can be interpreted.

The component portion enables an application process to invoke an operation in a remote application process and receive the response associated with it. A TCAP message may carry multiple components in any combination. Each component corresponds to one of the following operational protocol data units (OPDU):

- invoke—initiates a procedure
- return result—reports a successful transaction
- return error—reports a failed transaction
- reject—reports protocol errors

Integrated Services Digital Network User Part

ISDN User Part (ISUP) provides signaling, setting up, monitoring, and taking down SS7 calls on ISUP trunks.

The ISUP key protocol functions are:

- interoffice call setup, signaling, and basic call supervision
- basic maintenance for call processing

- enhanced office maintenance capabilities
- base for implementing networked ISDN

It is important to note that ISUP only supplies the capability to transport the information, and not the features that make use of the capability.

ISUP has two main functions—call processing and trunk maintenance.

Call processing involves the basic procedures of call setup and call takedown, as well as the handling of any irregularities that occur during call setup and takedown. As with other common channel signaling systems, call processing functions are carried out by exchanging messages that carry the information for call setup and call takedown over dedicated signaling links and the supporting signaling network.

Trunk maintenance operations are divided into two categories: automated system maintenance, and manual system maintenance.

Automated system maintenance operations are initiated automatically by system software. These operations can be triggered periodically, triggered from a predefined condition, or triggered directly from call processing software.

Manual maintenance operations are initiated at a maintenance and administration position (MAP) by maintenance personnel. These include functions such as manually busying a trunk, manually returning a trunk to service, or manually performing a trunk circuit test.

Mode of operations

Network planners and standards bodies have defined two modes of operation of SS7 for the U.S.:

- Trunk signaling mode—also known as connection-oriented signaling interoffice signaling mode (ISUP)—performs the normal trunk setup, supervisory and takedown signaling functions, and extends networkwide services that are currently available only to subscribers within a single office. Also serves as the network signaling transport for ISDN.
- Database query mode—also known as connectionless signaling (TCAP). Through online access to a database, this mode of operation allows multiple central offices to use a centralized database for user part data. The first application of this mode was E800 service.

Connection-oriented signaling

Connection-oriented signaling, also referred to as trunk signaling, is used to set up, monitor, and take down a call on an ISUP trunk using SS7 signaling.

Figure 4-20 — Mode of

**Connection-oriented
signaling
(trunk signaling)**

DMS
STP

Signaling
link

Signaling link

Originating
switching
office

Voice trunk

Terminating
switching
office

**Connectionless signaling
(Transaction services)**

SSP
(service
switching
point)

Signaling link

DMS
STP

Per-trunk signaling
(PTS) trunk

Signaling link

EO
(end
office)

SCP
(service
control
point)
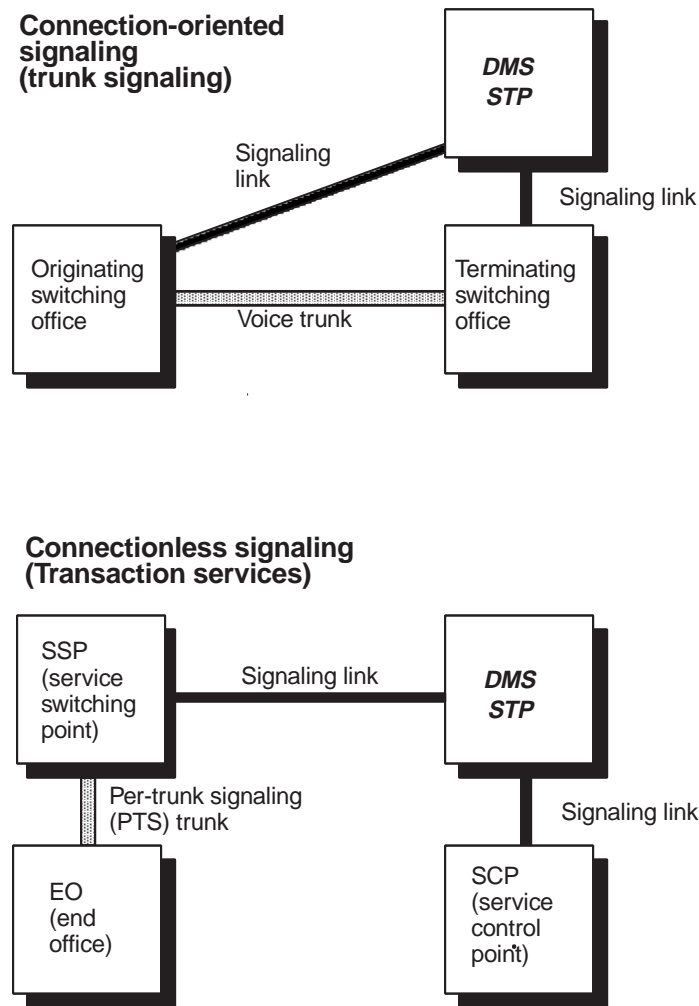
The upper part of Figure 4-20 illustrates an example of connection-oriented signaling. The signaling that is used to set up and monitor the call is routed from the originating switching office through a DMS-STP to the terminating switching office. Voice traffic is placed on a voice trunk that connects the originating switching office to the terminating switching office.

Connectionless signaling

Connectionless signaling, also referred to as transaction service, is the term used to define signaling that is not associated with the setup and takedown of an ISUP trunk call. For example, signaling that is used to access a database for 800 number translations and maintenance signaling messages between signaling points, is considered to be connectionless signaling.

The lower part of Figure 4-20 illustrates the use of connectionless signaling to access a database for the translation of an 800 number to a directory number and numbering plan area (NPA) code. The request for 800 number translation is passed through signaling messages from a per-trunk signaling end-office to a Service Switching Point (SSP).

The SSP routes the request through the signaling network to a Service Control Point (SCP) where the transaction is processed. The SCP returns the translated number back through the signaling network to the SCCP function in the SSP for final processing of the call.

Signaling methods

The common channel signaling method is largely dependent upon the node relationship in the SS7 network architecture. Signal messaging between nodes can be exchanged in any combination of two methods:

- associated signaling
- quasi-associated signaling

Associated signaling

In associated signaling, the signals pertaining to two switches are conveyed over a signaling link that directly connects the two SS7 nodes and related switched network.

The upper part of Figure 4-22 illustrates an example of associated signaling. The signaling link and voice trunk of a call both follow the same route between the originating and terminating switching offices.

Quasi-associated signaling

In Quasi-associated signaling, the signaling messages are conveyed over two or more link-sets in tandem. Messages pass through one or more signaling points other than those that are the origination and destination of the message. The path taken by a message through the signaling network is predetermined, and at a given point in time, fixed.

The lower part of Figure 4-22 illustrates an example of quasi-associated signaling. The signaling is routed from the originating node through a DMS-STP to the terminating node. Voice and data traffic is placed on a voice trunk that connects the originating switching office and the terminating switching office directly.

SS7 network architecture

The SS7 network architecture has evolved from a two node Signaling Point (SP) operation, during initial start-up phases, to multiple SP node systems. With the introduction of Signaling Transfer Point (STP) technology into the SS7 network architecture, all SS7 SP nodes may be interconnected into one large-scale dynamic common SS7 network.

Figure 4-21 — SS7 Network Architecture
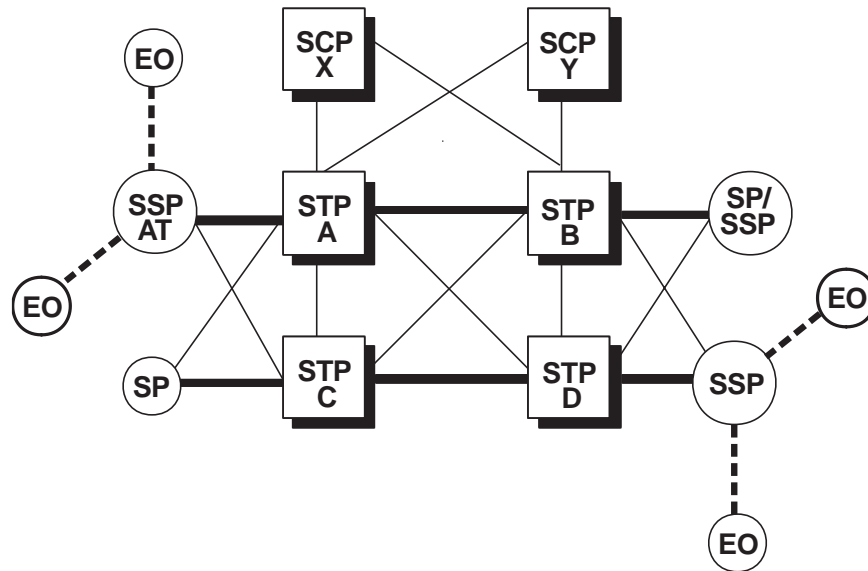
EO

End-office (class 5) with per-trunk signaling and homes on the SSP for SS7 functions

SP

Signaling Point, a node in the SS7 network with ISUP trunks (class 5 end-office)

SSP

Service Switching Point, access tandem or class 4 toll office, a node in the SS7 network with ISUP trunks. Accesses the SCP data base for advance services such as 800 service

STP

Signaling Transfer Point, a node in the SS7 network, provides the access to signal network between the various nodes of the SS7 network using packet switching technology (no ISUP trunks at STP).

SCP

Service Control Point, a node in the SS7 network, supplies the database for advance services such as 800 service and credit card validation.

An SS7 network consists of a number of switching and processing nodes that are interconnected by signaling links, see Figure 4-21. The size and complexity of a signaling network depends on the volume of traffic and the degree of redundancy that is required for the signaling paths between signaling points.

SS7 network elements

SS7 elements are arranged into system and network configurations. The minimum configuration (a two node system) would be two switching sites, provisioned for SS7

signaling, with an intra-SS7 type trunk group. Many sites may be combined into a network using STP and SCP elements.

Figure 4-22 — SS7 Signaling

Associated Signaling

Quasi-associated Signaling
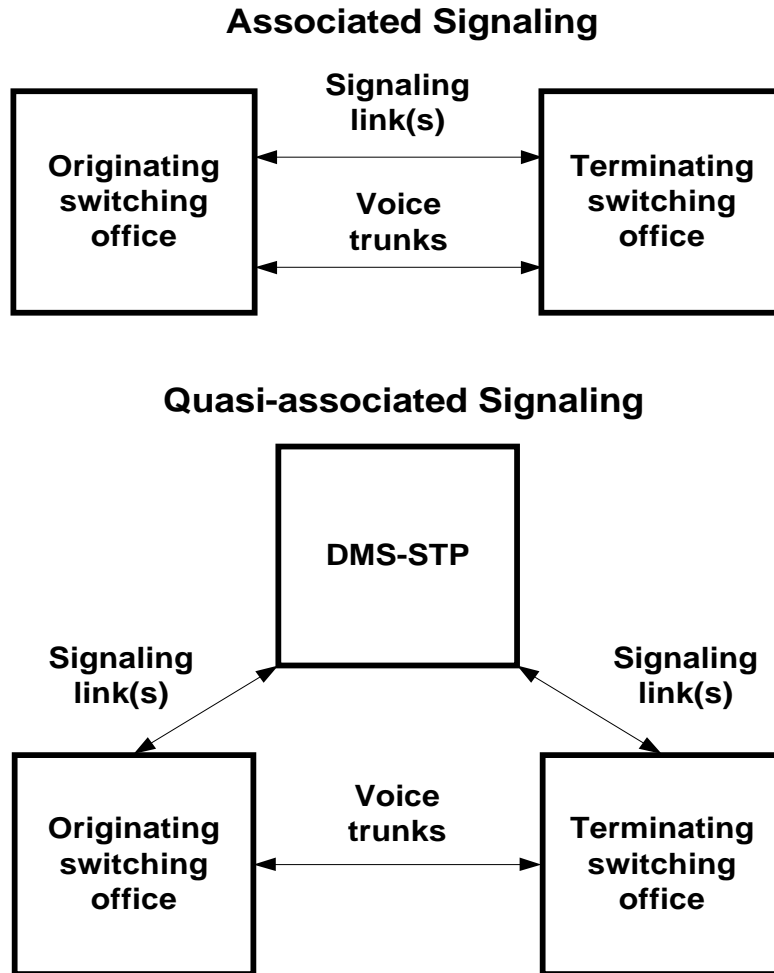
Application process — Application processes are end-users that communicate with other processes using SS7 and comply with the Transaction Capabilities Applications Part (TCAP) protocol. Application processes are identified by subsystem numbers resident at a service switching point. They can be queried, removed from service, and returned to service from the CCS sublevels of the MAP, see Figure 4-26 on page 4-173.

Inter-peripheral message link — Interperipheral message links (IPMLs) are nailed-up connections through the network, providing communication channels between the MSB7 and the DTC7 (that interfaces with voice trunks). An IPML consists of two network connections, called interperipheral connections (IPC). They

operate in a warm standby mode to avoid loss of information. The IPML uses channel 16 in the DTC7 to avoid contention with other trunks. The IPML may be connected to any channel in the MSB7. IPMLs are not used with Link Peripheral Processors (LPPs) that have replaced the MSB7 functions.

Integrated Services Digital Network User Part — ISUP is derived from Integrated Services Digital Network User Part. ISUP provides the signaling functions required to provide voice and data service in an SS7 network. It also provides interexchange signaling to support the normal trunk dialing and supervisory functions for interoffice trunks using SS7 protocol.

Link — A link is a communication channel between two adjacent signaling points. Depending on the type of network nodes that terminate each end of a signaling link (SL), there are specific designations for each type of SL configuration. Each of the various link types is described as follows:

- Access links (A-links) connect SPs, SSPs, and SCPs to home STP nodes. A-links are always installed in pairs, with one link assigned to each STP of the mated pair.

- Bridge links (B-links) connect mated STP pairs to other mated STP pairs, thus creating a B-link quad structure. The number of STP pairs that are used depends on STP capacity, subnetwork, network and internetwork traffic levels, company operating policies, and regulatory directives.

- Cross links (C-links) connect individual STP nodes to form mated STP pairs.

- Diagonal links (D-links) connect secondary STP pairs to primary STP pairs, creating a D-link quad structure. Secondary STP pairs are always connected to specific primary STP pairs. More than one secondary STP pair can be connected to a primary STP pair.

- Extended links (E-links) connect SPs, SCPs and SSPs to remote STP pairs.

- F-links connect SPs and SSPs to one another. The F-link does not use STP nodes and is considered an associated route.

Linksets — Linksets are a collection of links to be used as a group, each equally capable of carrying SS7 traffic between two adjacent point codes (PCs). Linksets identify the switching office to which they provide the signaling by the point code of the far-end node. Linksets can contain up to 16 links to provide a number of levels of redundancy.

Message Transfer Part — Message Transfer Part (MTP) is a software function (protocol) that serves as a transport system providing reliable transfer of signaling messages in correct sequence, without loss or duplication between the signaling points of the SS7 network.

Node DMS — A DMS node is a processing unit within a DMS switch (e.g., CC/CM, CMC/MS, MSB7, DTC7, LIU7, LPP).

Node SS7 — An SS7 node is a switching point within the SS7 network (e.g., DMS-STP). Each SS7 node is identified by a unique PC.

Nailed-up connection — Nailed-up connection (NUC) is a permanently assigned network connection that forms part of the message path between suitably equipped peripheral modules. Nailed-up connections are software connections made at a planned system load and maintained during a system reload.

Route — A route is a signaling path into the SS7 network that accesses a destination.

Routeset—Routeset is a logical grouping of linksets having the same destination point code (DPC). The office point code uniquely identifies the SP node within the network. Each office PC must have an assigned routeset. Up to six linksets may be assigned to a routeset.

Signal Connection Control Part — Signaling Connection Control Part (SCCP) is a software (protocol) function, an extension to the MTP. It provides connectionless signaling (customer database information) for advanced network services such as 800 service. The connectionless services supplied by the SCCP are divided into two protocol classes: basic protocol *Class 0* to deliver the data (packets) independently without the use of sequencing control, and enhanced protocol *Class 1* that guarantees, with a high level of reliability, that the data (packets) arrive correctly. Class 1 uses the properties of the MTP to transport data (packets) through the SCCP.

Service Control Point — The Service Control Point (SCP) uses DMS-SCP Super-Node hardware and is the SS7 network node that supplies the database transactions and routing data for advanced network services, such as 800 service and credit card validation. SCPs are accessed by other end nodes on the SS7 network, see Figure 4-23.

Signaling Points — SS7 end nodes are referred to as Signaling Points (SPs), and are connected to other SPs or to a pair of Signaling Transfer Points (STPs) by transmission links (TLs). An SP is any entity in a signaling network that is the origination point or the termination point for signaling information. Each signaling point has a unique PC associated with it. This enables messages to be individually addressed to each SP in the network.

Figure 4-23 — Nodes in an SS7
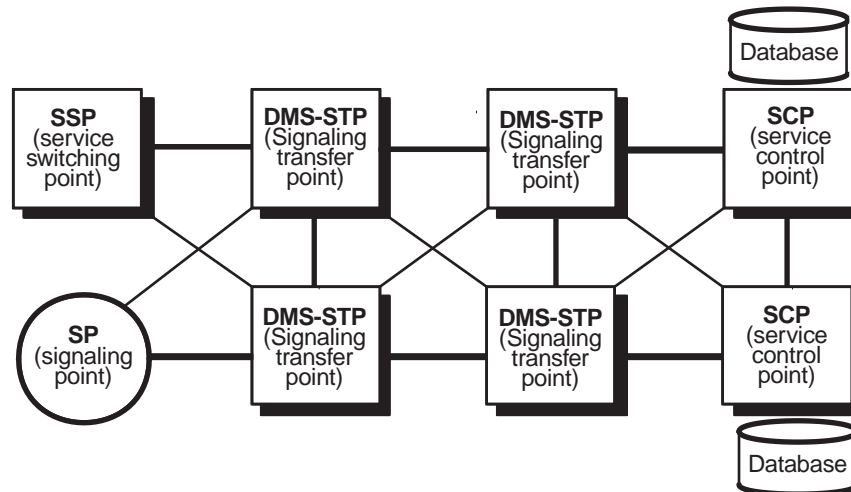
Service Switching Point — An end-office equipped with software features that provide the capability to query SCPs is called an Service Switching Point (SSP). SPs do not have this capability and rely on an access tandem (AT) to perform the function to launch database queries to access SCPs.

Signal Transfer Point — The Signal Transfer Point (STP) uses SuperNode hardware and is a node in the SS7 network. The STP is a highly reliable packet switcher that provides rapid transfer of information (signaling and database) between the various nodes in the SS7 network: SPs, SSPs, SCPs, and other STPs. This eliminates the need for interconnecting all the various SS7 nodes in a signaling network using dedicated signaling links.

The STP may also provide global title translation service for messages that are originated from end nodes and do not have the complete addressing or nodal status information about the other nodes of the network. STPs are usually deployed in mated pairs interconnected by transmission links. In the event of partial or complete failure of one STP, the mate STP is configured to provide uninterrupted message transfer for all connected SS7 nodes.

Signaling System 7 — Signaling System 7 (SS7) is the American National Standard Specification (ANSI) version of international CCITT Signaling System No.7 (CCITT SS#7).

Subsystem — Typical subsystems are Enhanced 800 service (E800) and Automated Calling Card Services (ACCS), and are identified at a point code by a Subsystem Number (SSN). These subsystems are software entities located at SS7 nodes and uses the Signaling Connection Control Part (SCCP) to send and receive messages across the SS7 network.

Local subsystem — A local subsystem is current application software at a DMS node. It performs functions within the processing part of the DMS node (DTC7, MSB7, LPP, LIU7, CM, MS, and CC.)

Replicate subsystem — Replicate subsystems are subsystems residing at different SS7 nodes that provide a backup for each other in case of failure at one of the SS7 nodes.

Transaction Capabilities Application Part — Transaction Capabilities Application Part (TCAP) is a software (protocol) function. It builds on the SCCP function that controls connectionless signaling in the SS7 network. TCAP provides the common protocol that contains message formatting, message content rules and message exchange procedures.

Transmission Link — Transmission link (TL) is the physical link, including the error-checking function that conveys the signaling and database messages between the various nodes on the SS7 network. The TL is also referred to as a signaling link or data link.

Voice Trunk — The voice portion of a trunk using SS7 signaling is basically a clear voice channel (DS0) on a DS1 carrier system. The signaling function, related routing, and switching of the companion voice channel is performed by the SS7 signaling system. Since this document discusses the SS7 signaling functions, the voice portion of the trunk has not been explained in any detail. However, to set up a serviceable end-to-end trunk, the two parts, signaling and voice, are united at the near and far-end nodes.

How nodes communicate across an SS7 network

All nodes on the SS7 network are interconnected using signaling links and signal transfer points. The quasi-associated signaling method facilitates the interconnection of all the nodes in the SS7 network, including alternate path protection. Associated signaling is used for high volume messaging between nodes with common interests. Associated signaling is not viable for networking.

All nodes and subsystems on the SS7 network are assigned a unique address called a Point Code (PC). The PC is embedded in the routing labels and directs the signaling message unit (SMU) to its destination. Routing labels are assigned by the MTP for signaling message units.

The routing of SS7 message signal units involves the logical application of signaling links and point codes into the following software functions:

- LINKSET — a set of links that are used as a group to carry signaling traffic between two nodes.
- ROUTE — a signaling path in the signaling network that access a destination
- ROUTESET — a logical grouping of routes from a node that has the same destination PC.

Part of the datafill for an ISUP trunk group identifies the routeset for carrying the signal message unit via a designated linkset to the destination point code. The foregoing is part of the translation process when an ISUP trunk group is selected that serves the same designated point codes.

Figure 4-25 on page 4-163 illustrates two examples of the SS7 network communications.

- Example "A" shows a route that consists of three linksets. The route originates from the SSP and terminates at the SCP. In addition, example "A" illustrates that a linkset consists of a set of links

- Example "B" shows two routes. Both routes originate from the same node and terminate at the same destination node in the network. Together, route "A" and route "B" form a routeset that originates from the same SSP and terminates at the same SCP.

How signaling messages are handled

Communication between nodes in the network takes the form of signaling messages that are formatted and transmitted by the node sending the message.

Signaling message format — Each signaling message contains a label. In the standard label, the portion used for routing is called the routing label. The routing label contains the following information:

- Originating Point Codes (OPCs) and Destination Point Codes (DPCs) that indicate the origination and destination points of the message

- a signaling link selector code that is used by the message routing function to distribute loading evenly

Figure 4-24 on page 4-162 illustrates the principal components of an SS7 signaling message. The routing label is part of the signaling information field (SIF). The standard routing label assumes that each signaling point in a signaling network is allocated a code according to a labeling code plan. Messages that are labeled according to international and national code plans are identified by the destination point code that is included in each message.

Message discrimination — Message discrimination is the process that determines if the signaling message has been delivered to its intended destination point. This decision is based on an analysis of the destination point code that is in the routing label of the message. If the signaling point to which it is delivered is the destination point, then the message is delivered to the message distribution function of the signaling point. If this signaling point is not the intended destination point, then the message is delivered to the routing function of the signaling point for further transfer on a signaling link.

Figure 4-24 — SS7 Message routing

Signaling information field

Signaling information octet

| MSU (message signal unit) | | SIF | SIO | |

SIF (signaling information field)

| User specific information | Routing Label |

Routing label

| | Signaling link selector code | Originating point code | Destination point code |

Originating point code

| Network Identification | Network cluster | Netwk cluster member |
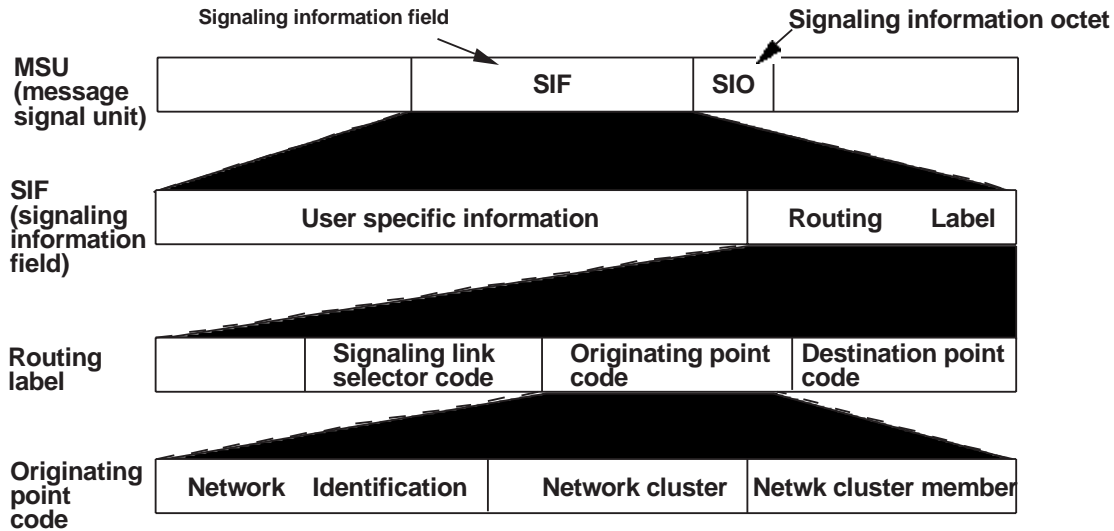
Message distribution — Message distribution is the process of analyzing the source indicator in the signaling message when it arrives at the destination point, then determining which user part the message is to be delivered to.

Message routing — Message routing involves the selection of an appropriate signaling link for each signaling message. The route a message takes is determined through a combined analysis of information that is contained in the routing label of a message, and of routing data that is provided at the signaling point.

Message routing is determined by a destination code and an additional load-sharing element that allows the signaling traffic to a particular destination to be distributed over two or more signaling links. This traffic distribution can be limited to different links within a linkset, or it can be applied to links in different linksets.

The route taken by a message with a particular routing label is predetermined and normally fixed at a given time. If failures occur in the signaling network, messages that would have taken a route that has failed are rerouted in a predetermined manner, under control of the signaling traffic management function at the MTP level.

Although there are advantages in using standard routes for messages that belong to different user parts, the service indicator that is included in each message provides the potential for using different routing plans for different user parts.

Figure 4-25 — Network communications
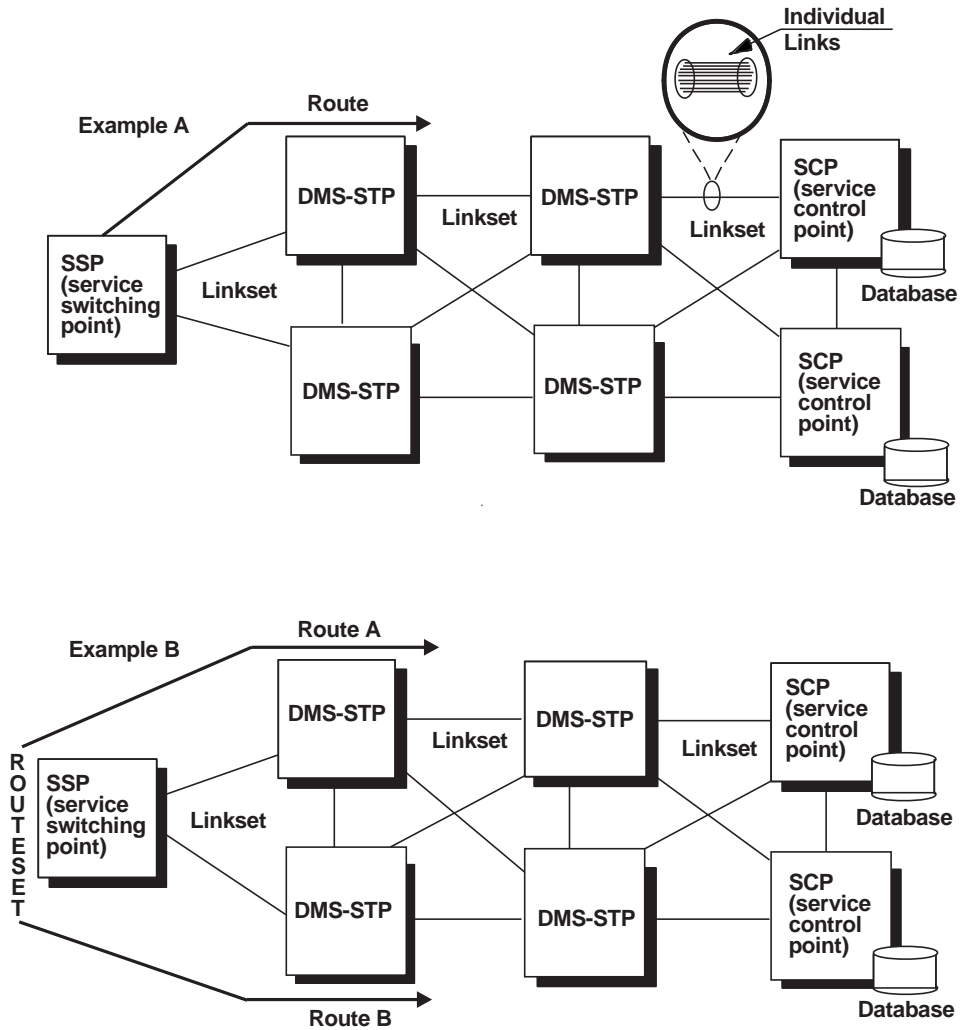
Example "A" shows a route that consists of three linksets. The route originates from the SSP and terminates at the SCP. In addition, example "A" illustrates that a linkset consists of a set of links

Example "B" shows two routes. Both routes originate from the same node and terminate at the same destination node in the network. Together, route "A" and route "B" form a routeset that originates from the same SSP and terminates at the same SCP.

How the SS7 network is managed

An SS7 network is managed through a set of network management functions that are divided between the Message Transfer Part (MTP) and the Signaling Connection Control Part (SCCP) of the SS7 protocol. The signaling network management functions provide the procedures that maintain signaling service by rerouting or controlling traffic due to congestion or failures in the network.

For STPs, operating companies can also control other network access to their SS7 networks and databases by using gateway screening.

Network management functions are described in the following:

- Message Transfer Part (MTP) management
- Signaling Connection Control Part (SCCP) management
- gateway screening

Message Transfer Part (MTP) management

Message Transfer Part (MTP) network management provides the procedures that maintain signaling service by rerouting or controlling traffic due to congestion or failures in the network.

MTP management is organized into three functions:

- signaling traffic management
- signaling link management
- signaling route management

Signaling traffic management — Signaling traffic management monitors the status of signaling links and routes. It takes appropriate actions to divert signaling traffic when failures occur, and to temporarily reduce traffic when congestion occurs.

Signaling link management — Signaling link management controls locally connected linksets. If changes occur in the availability of a local linkset, the signaling link management function initiates and controls actions aimed at restoring the normal availability of local links and linksets to the signaling traffic management function.

Signaling route management — Signaling route management maintains information on changes in the availability or the congestion status of signaling routes.

Feature "CCS7 MTP Routing Enhancements" is for SuperNode CCS7 LIU7-based link offices and maintains routing availability status of individual remote signaling points that have been datafilled as partial-point-code (PPC) routes. Specifically, this feature allows the DMS signalling points to maintain the route and routeset status for all members of a remote network cluster PPC route, in response to the following messages:

- Transfer Allowed (TFA)
- Transfer Restricted (TFR

- Transfer Prohibited (TFP)
- Transfer Cluster Allowed (TCA)
- Transfer Cluster Restricted (TCR)
- Transfer Cluster Prohibited (TCP)

Signaling Connection Control Part (SCCP) management

Signaling Connection Control Part (SCCP) management provides the procedures that maintain network performance by rerouting or controlling traffic due to failures or congestion in the network.

SCCP management is organized into three functions:

- point code status management
- subsystem status management
- traffic information management

Point code status management — Point code status management updates routing and translation tables based on the status of network failures, recoveries, or congestion that is provided by Message Transfer Part (MTP) indicators.

Subsystem status management — Subsystem status management updates routing and status tables based on the status of failures, withdrawal, congestion, or recovery of network subsystems. This allows alternate routing to backup subsystems in the network.

Traffic information management — Traffic information management procedures provide mechanisms for informing SCCP users of received traffic patterns.

Gateway screening

Gateway screening provides operating companies with the ability to control access to their SS7 networks and databases by other SS7 networks. By screening SS7 messages as they enter a STP, gateway screening permits an operating company to ensure that facilities and services can only be used by authorized network users.

Each SS7 message carries with it routing data, including DPCs and OPCs, global title translation (GTT) numbers, and information identifying the service the message is being used to access. By setting up combinations of screening criteria from the MTP and SCCP, the operating company can specify exactly what services can be accessed by any user of its network. Traffic originating from unauthorized sources, or attempting to use unleased services, is blocked from network access.

The specifications used for gateway screening are defined according to operating company requirements. Instructions for setting up these specifications through datafill are provided in NTP 297-8101-350, *DMS-100F SuperNode Signaling Transfer Point (STPBASE) Translation Guide.*

SS7 maintenance

SS7 maintenance described within this subsection, suggests a total SS7 network control and surveillance strategy, as opposed to a site or sectional maintenance strategy. Network control and surveillance procedures are essential for maintaining a high quality SS7 signaling network with no service interruptions.

The following SS7 maintenance topics are addressed within this subsection:

- SS7 Network Control Center (SS7/NCC)
- SS7 network maintenance overview:
  — SS7 maintenance tasks
  — CCS7 menu tasks
  — Signaling link fault scenarios
- Preventive maintenance & surveillance:
  — Alarms
  — Log reports
  — Operational measurements (OMs)
  — ISUP trunk continuity test (ICOT)
- Signaling link maintenance tests (SSP/STP):
  — Loopback & MTP BERT testing for signaling links
  — Data link transmission and stability requirements
  — Common Channel Signaling 7 Test Utility (C7TU)
  — Portable protocol analyzers
  — Signaling Link Marginal Performance Report (SLMPR)
- ISUP trunk maintenance & surveillance
- SPMS (SS7 application)
- SEAS Performance Indicators for SS7 Network
- Equal Access and CCS7
- ADJNODE table

SS7 Network Control Center (SS7/NCC)

Total redundancy with physical diversity is the cornerstone of SS7 common channel signaling reliability, and must be sustained to ensure uninterrupted service.

A focal point is required for maintaining the SS7 redundancy, since it may physically and functionally transcend existing regional and district maintenance and administrative boundaries. An SS7 network includes all Switching Points (SP), Service Switching Point (SSP), Signal Transfer Points (STP), mated pairs, and Service Control Points (SCP).

SS7 signaling is an intelligent type of network with built-in self-checking circuits, diagnostics, and related remedial actions to ensure signaling validity and completions. However, uncoordinated maintenance activity, including the digital transmission link, can trigger these features and negate the protective redundancy of the network.

All SS7 activity must be coordinated to preserve the SS7 network redundancy and reliability. This includes: preventive and corrective changes, extensions, rearrangements affecting the SP, SSP, STP, SCP, and digital line facilities used to derive the signaling links. This type of communications and coordination is required to prevent network congestion and potential switching office (SO) isolations.

The focal point for all this activity would be an SS7 Network Control Center (SS7/NCC) or other named center as defined by the operating company. For this subsection, the term "control center" will be used in place of where NCC and SCC would be applicable. The control center concept is a proven process and has been used for many years by operating companies for maintenance and administration of their toll and private line networks. The DMS-100F technology with its remote surveillance capabilities provides the tools necessary for the centralized SS7 Network Control functions.

Prevention of signaling network disruptions is a key objective of the control center. This is achieved by exploiting the DMS-100F surveillance features and related computer programs in a centralized operation. Another essential procedure in meeting this objective is the establishment of effective two-way communications between the control center and all the nodes in the signaling network, including related digital carrier facility maintenance groups.

SS7 service restoration is another key objective. This is a demand function, triggered by the SS7 alarm and surveillance features. When a fault occurs, it should be isolated to prevent further network degradation (e.g., bouncing links). The work activity would include: trouble identification, isolation, trouble restoration using spare digital facilities when applicable, sectionalization, repair, verification, and returning the faulty component to service.

Regardless of the personnel performing the testing and repair activity, the SS7/control center is in control and aware of the activities in progress and potential service impact for the network.

Plans should be developed for restoring SS7 service due to major carrier facility, STP, and SSP failures. These plans should be reviewed and tested periodically

Common channel signaling functions as one network, transporting trunk signaling and advance services information between all switching centers within its geographical boundaries. Interconnection with other SS7 networks extends SS7 signaling information to all telephone locations.

SS7 signaling is a means to an end, and as it performs, so does the trunk network connectivity of the switched network, and all its features.

The control center becomes part of an overall SS7 management organization responsible for performance, configuration, provisioning and security.

Reporting between the control center and the nodes would follow existing switch control organization procedures. Normally, this is between the SCCs and the NCC.

The size and complexity of the control center surveillance and management center would be governed essentially by the number of signaling links, degree of stability, volume of SS7 log messages, number of sites under surveillance, and the operational hours for the center.

Preferably, there is one control center *per network* with the required number of workstations and personnel to manage the workload.

If more than one control center is required for regional or workload purpose, establish subnetwork control centers and appoint one as overall authority for managing the SS7 network.

NOTE: STPs designated as signaling link control offices are prime for initiating restoration, fault locating, repair, and return to service. They should maintain a history of faults, disposition, initial BER testing, and maintenance readings for each link.

Control center functions and responsibilities

The control center for the SS7 network would have the prime responsibility for managing the SS7 network, and to ensure uninterrupted quality signaling between all nodes on the network. Key operations for managing the network are:

- Provide real time surveillance for all STP nodes and links.
- Identify signaling link failures, assess redundancy status, and if vulnerable, take action to sustain working link(s) by stopping any work activity on the working links until the failed link(s) have returned to service.
- Identify linkset failures that are jeopardy situations that might cause network congestion. Initiate action to sustain working links by stopping all work activity on the working links until the failed linkset has been corrected.
- Identify and resolve logical failures—such as Destination Point Codes (DPCs)—for specific nodes, subsystems, and remote subsystems. These are logical codes derived by datafill. They are critical situations causing an isolation— the SS7 network cannot complete to the point code.
- Identify routeset failures (critical service conditions) caused by MSB7/LIU7 equipment or linkset faults.
- Frequently follow-up on restoration progress for jeopardy conditions, and outages that have exceeded their expected restoration interval.
- Alert network management to jeopardy situations and provide status until corrected.

- Investigate DMS processor outages (MSB7/LIU7) as a jeopardy situation. Initiate action to sustain the working links that are associated with the MSB7/LIU7 that is in the simplex mode.

- Identify poor performance for links or equipment, and coordinate fault investigation.

- Coordinate maintenance activity requested by nodes. All routing activity should be performed outside the traffic busy hours.

- Provide a contact point for problems involving other SS7 networks.

- Validate signaling link facility diversity to ensure loss of a facility will not affect both links.

- Keep software current. Coordinate software loads and patches by staggering insertions for mated STP pairs.

- Establish plans for various emergency restoration conditions.

- Establish telephone number contact lists for key personnel (home and business), including interconnecting SS7 networks and 24 hour report center numbers.

- Insure personnel responsible for maintaining the SS7 network are properly trained. See the *Training* section within this manual and use the Advisor at www.nortelnetworks.com/advisor or a copy of the CD-ROM Advisor to see the courses for the CCS7/CLASS Curriculum.

- Verify that documentation supporting the SS7 network is easily accessible and current for the range of equipped software loads. This is especially important for recovery related documentation.

General responsibilities for all SS7 node locations

Ensure preservation of SS7 network redundancy by following these rules:

- Inform the control center of all work activity or scheduled activity on the signaling links or SS7 nodes. This includes such items as troubleshooting, routine maintenance, provisioning, equipment installation, PCL loads, and patches.

- Schedule all SS7 maintenance activity outside of traffic busy hours. Designate low traffic or out-of-hours periods for this work. Defer work until those time periods. Clear the scheduling of SS7 maintenance activities with the control center.

- For all signaling links, maintain facility and equipment assignments, including carrier test points and locations from node to node. Also, maintain telephone contact numbers for the various test locations.

- Perform fault testing and restoration activities with other nodes, including signaling link facilities.

- Inform the control center of threatening or abnormal service conditions, including any major outages.

- Perform signaling link surveillance using the Signaling Link Marginal Performance Report (SLMPR). Notify the control office of links with excessive faults. Remove them from service via the control center, initiate trouble sectionalization, clear, return to service, and notify the control center.

- Equip signaling link facilities with special service protection (SSP) devices to prevent accidental interruptions. This protection is applied at DSX type cross-connects, jack fields, and cable terminals. Also, equipment designations should indicate high priority service.

SS7 network maintenance overview

Maintenance is required for the following components of an SS7 system and network:

- hardware — there are two SS7 equipment configurations, the Message Switch Buffer 7 (MSB7) which is manufacture discontinued, or the Link Peripheral Processor's (LPP) Link Interface Unit for SS7 (LIU7). Each require specific hardware maintenance

- software functions — SS7 protocols (system operation)

- line facilities — data links that interconnect the SS7 nodes

- ISUP trunks — message trunk signaling (application layer)

The MSB7 hardware configuration involves the following components that are accessed from the PM level of the MAP for maintenance purposes:

- MSB7 (Message Switch Buffer 7)

- ST (Signaling Terminal)

- IPML (Inter Peripheral Message Link)

- DTC7 (Digital Trunk Controller 7)

The LIU7 for the LPP—is a replacement within SuperNode offices for the MSB7—is accessed for maintenance purposes from the PM level of the MAP, LIU7 sublevel.

The software function that provides the SS7 protocol is common, and is accessed for maintenance from the CCS menu level to seven sublevels as follows:

```
CCS7 menu      C7RTESET
C7LKSET        C7BERT (off C7LKSET)
SCCPRPC        SCCPRSS
SCCPLOC
```

The line facilities to derive the data link are accessed for maintenance from the LIU7 menu for SuperNode configuration, and from the CARRIER level off the TRKS level menu for the MSB7 configuration.

ISUP trunk testing and surveillance are described later within this subsection.

SS7 maintenance procedures

DMS maintenance procedures have been developed and customized for SP/SSP and STP equipment configurations using SuperNode. See NTPs 297-YYYY-543 thru 547 documents for CCS7 maintenance procedures. For the layer number (YYYY), see the 8101 layer for the STPBASE.

For additional supporting user interface information for the LIU7, LIM, and FBUS, see NTP 297-1001-592, *PM Maintenance Guide*.

For some SS7 network maintenance tasks, the customized procedures developed for the LIU7—which are system oriented—can be adapted to the MSB7 application.

Some of the following procedures in the NTPs can be used as is, or MSB7 PM input data may be substituted for the LIU7:

Administrative maintenance procedures:
- setting up the signaling link marginal performance report
- prioritizing CCS alarms
- changing table C7TIMER entries

Preventive maintenance procedures:
- routine maintenance procedures
- surveillance using the signaling marginal performance report (see "SLMPR" on page 4-215 within this subsection)
- running bit error rate tests (see "Signaling link maintenance tests" on page 4-192 within this subsection)
- testing F-bus taps

Corrective maintenance procedures:
- clearing CCS alarms
- clearing PM alarms
- replacing cards
- DMS SuperNode recovery procedures
- LPP recovery procedures for SSP applications
- interpreting and responding to logs
- activating an offline linkset
- activating links
- activating loopback on an NT9X78BA paddle-board
- activating loopbacks on an NTX6X55AB DS0A card (see "Signaling link maintenance tests" on page 4-192 within this subsection)
- checking for call completion
- estimating signaling link occupancy

- patching LIMs
- patching LIU7s
- replacing a cooling fan in a SuperNode cabinet
- returning a card or assembly for repair or replacement
- testing a LIM
- testing an LIU7
- downloading software to an LIU7
- downloading software to a LIM unit

Diagnostic maintenance procedures:

- performing a manual REX test for a LIM
- adding a LIM to the automatic REX test schedule
- scheduling an automatic REX test
- excluding a LIM from a REX test
- scheduling ISUP trunk audits
- setting up an ISUP per-call continuity test

CCS7 menu tasks

The CCS7 MAP level hierarchy and commands are recorded in Figure 4-26 on page 4-173. The CCS7 menu and sublevel functions are system and network applications that apply at all nodes. NTP 297-1001-531, *DMS-100F CCS7 Maintenance Reference Manual*, provides a description of the CCS7 MAP menu functions.

SS7 fault scenarios

Figure 4-27 on page 4-174 through Figure 4-30 on page 4-177 are example SS7 fault scenarios. They provide a list of alarm and log messages that are generated when signaling link failures occur. Also, the impact on the SS7 network messaging when links or equipment fail. The following graphical scenarios are provided:

Figure 4-22 Scenario 1 — a link failure in a linkset with one link

Figure 4-23 Scenario 2 — a link failure in a linkset with two links

Figure 4-24 Scenario 3 — two links fail in a linkset with two links

Figure 4-25 Scenario 4 — mated STPs — one fails

Figure 4-26 — MAP level SS7 hierarchy and

MAPCI

MTC
14 CCS

CCS
3 CCS7
14 QueryAlm

CCS7 MENU
0 Quit
2 DisAlm
3 C7RteSet
4 C7LkSet
5 SCCPRPC
6 SCCPLoc
7 SEAS
8 C7Router
16 C7MSUUER

C7LKSET MENU
0 Quit
2 Post_
4 Inh_
5 UInh_
6 Tst_
7 Bsy_
8 RTS_
9 Offl_
10 AbtDly_
11 NextLS
12 Next
14 QueryFlt
15 QueryUsr
16 QueryTrf
17 Act_
18 Deact_
Hidden Command
C7BERT

C7RTESET MENU
0 Quit
2 Post_
7 Bsy
8 RTS
9 Offl
12 Next
14 Queryflt

SCCPRPC MENU
0 Quit
2 Post_
7 Bsy_
8 RTS_
9 Offl_
13 SCCPRSS
16 TranTst_
18 QuerySS

SCCPLOC MENU
0 Quit
2 Post_
7 Bsy_
8 Rtr_
9 Offl_
12 Next
15 TesTSS
16 TranTst
17 Locate_
18 QuerySS

C7MSUUER MENU
0 Quit
2 Post_
3 Save_
4 SetSIO
5 SetDPC_
6 SetOPC_
16 Clear
17 IntMess
18 Screen_

C7ROUTER MENU
0 Quit
2 Post_
7 Bsy_
8 Rtr_
9 Offl_
12 Next
14 QueryRtr
16 QueryTrf

C7BERT MENU
0 Quit
4 Start
5 Stop
6 Query_
8 SetStop_
9 InjErr_
11 LFSLoop_

SEAS MENU
4 PVC
7 Bsy_
8 RTS_
9 Offl_
14 QueryFlt

SCCPRSS MENU
0 Quit
2 Post_
7 Bsy_
8 RTS_
9 Offl_
12 Next
16 TRANTST
18 QUERYSS

PVC MENU
2 Post_
6 Tst_
7 Bsy_
8 RTS_
9 Offl_
11 Next
14 QueryFlt

.

Figure 4-27 — Fault scenario 1 concerns a single link Y/Z failure in a linkset with one "A" link.
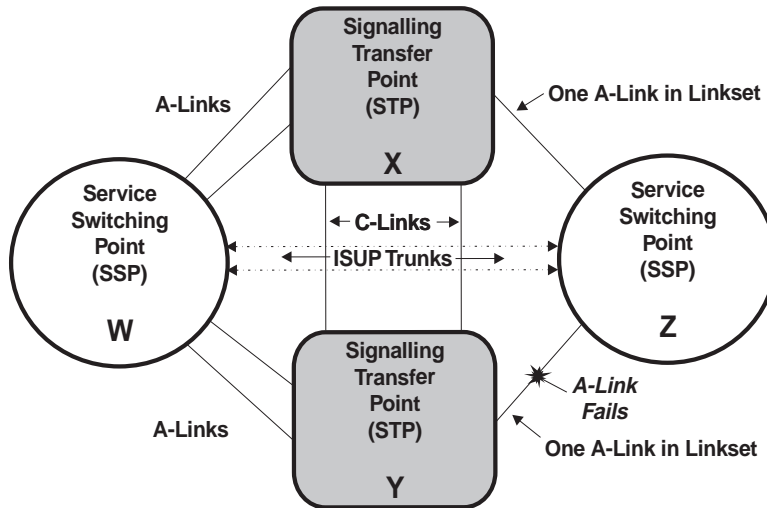
EVENT	NODE W AND X	NODE Y AND Z
1		LINK Y/Z fails
2	Alarms/Logs: ** CCS167 Route Restricted NOTE: CCS167 Route Restricted alarm and log notification are sent to every SS7 NODE when a linkset fails and causes a route restriction.	Alarms/Logs: ** CCS101 Link failure * CCS164 Link unavailable ** CCS175 Routeset restricted ** CCS167 Route restricted Possible PM/C7UP Logs, CCS198 SLMPR
3		All SS7 messaging diverted to links X/Z. Estimate link X/Z occupancy using C7LKSET command: QUERYTRF.
4	Action — network status information only since no other alarms or logs concerning specific links	Action at nodes Y and Z, control office prime: follow detailed CCS alarm clearing instruction. See NTP 297-8101-543 (STP node) and NRP 297-YYYY-543 (SP/SSP node) for alarm clearing procedures.
5	Recovery Logs: CCS166 Route allowed	Recovery Logs CCS102 Link Sync CCS163 Link available CCS155 Routeset available CCS166 Route allowed PM Logs

.

Figure 4-28 — Fault Scenario 2 concerns Linkset W/Y provisioned with two "A" links, and one fails.

EVENT	NODE W AND Y	NODE X AND Z
1	Two links fail in Linkset W/Y	
2	Alarms/Logs: * CCS101 Link failure * CCS164 Link unavailable Possible PM, C7UP Logs & CCS198 SLMPR	Alarms/Logs: Normally no logs or alarms with this scenario.
3	All SS7 messaging diverted to links W/X. Estimate link W/X occupancy using C7LKSET command QUERYTRF.	
4	Action — at nodes W/Y, control office prime: follow detailed CCS alarm clearing instructions. See event 4 with Figure 4-27 on page 4-174.	Action: network status information only, since no other alarms or logs concerning specific links.
5	Recovery Logs CCS102 Link Sync CCS102 Link Sync CCS163 Link available CCS163 Link available CCS155 Routeset available CCS166 Route allowed PM Logs	Recovery Logs: CCS166 Route allowed

Figure 4-29 — Fault Scenario 3 concerns Linkset W/Y provisioned with two "A" links, and both

EVENT	NODE W AND Y	NODE X AND Z
1	Two links fail in Linkset W/Y	
2	Alarms/Logs: * CCS101 Link failure (two logs) * CCS164 Link unavailable (two logs) ** CCS175 Routeset restricted ** CCS167 Route restricted Possible PM, C7UP Logs & CCS198 SLMPR	Alarms/Logs: ** CCS167 Route restricted. NOTE: CCS167 Route restricted alarm and log notification are sent to every SS7 NODE when a linkset fails and causes a route restriction.
3	All SS7 messaging diverted to links W/X. Estimate link W/X occupancy using C7LKSET command QUERYTRF.	
4	Action — at nodes W/Y, control office prime: follow detailed CCS alarm clearing instructions. See event 4 at Figure 4-27.	Action: network status information only, since no other alarms or logs concerning specific links.
5	Recovery Logs CCS102 Link Sync (two logs) CCS163 Link available (two logs) CCS155 Routeset available CCS166 Route allowed PM Logs	Recovery Logs: CCS166 Route allowed

Figure 4-30 — Fault Scenario 4 concerns a failure

EVENT	NODE W AND Y	NODE X AND Z
1		STP fails.
2	Alarms/Logs: * CCS101 Link failure * CCS164 Link unavailable (log reports to every link to failed STP X) ** CCS175 Routeset restricted ** CCS168 Route prohibited *** CCS154 Routeset unavailable ** CCS167 Route restricted Possible PM, C7UP Logs & CCS198 SLMPR	Alarms/Logs: ** CCS167 Route restricted. NOTE: CCS167 Route restricted alarm and log notification are sent to every SS7 NODE when a linkset fails and causes a route restriction.
3	All SS7 messaging diverted to STP "Y"	
4	Action: ensure A links to the working STP (Y) are not manual busy.	Action: critical situation, network in jeopardy with no redundancy. Top priority to restore STP and place online.
5	Recovery Logs CCS102 Link Sync (log for every link that restores) CCS163 Link available (log for every link that becomes available) CCS155 Routeset available CCS166 Route available CCS221 SCCP at remote PC performing subsystem status test local subsys CCS216 Remote subsystem available	

Preventive maintenance & surveillance

Preventive maintenance and surveillance procedures are necessary for SP and SSP nodes using MSB7 or LIU7 equipment.

The SSP maintenance and surveillance function may be performed locally or from a centralized location. SS7 maintenance and surveillance functions at an SSP can utilize some or all of the following tools:

- alarms associated with SS7
- log reports
- selected OMs
- OM thresholding
- Signaling Link Marginal Performance Report (SLMPR)
- ISUP trunk continuity test (ICOT)
- Switch Performance Monitoring System (SPMS)
- killer trunk (KT)
- automatic trunk transmission tests (ATT)
- CCS7 test utility (C7TU)

Before any SS7 maintenance is initiated, such as busying out equipment or links, contact your control center and advise them of the work to be done. Removing SS7 equipment or links from the network can cause signaling congestion or isolations.

The control center coordinates the work activity for the network and determines when all maintenance activities may be performed based on signaling load, and current network status. SSP maintenance activity is scheduled and performed during light traffic periods.

Alarms associated with SS7

The top level MAP MTC alarm banner displays the total system status, including SS7 signaling under CCS. The following SS7 alarms are listed in order of severity:

RSC	**CRITICAL**	**(ROUTESET)**
PCC	**CRITICAL**	**(SCCP point codes)**
SSC	**CRITICAL**	**(SCCP subsystem, e.g., 800 services)**
RSSC	**CRITICAL**	**(Remote Subsystem Critical)**
RSM	**MAJOR**	**(ROUTESETS)**
LKM	**MAJOR**	**(LINKSETS)**
PC	**MINOR**	**(SCCP point codes)**
SSMB	**SEAS**	**(Subsystem Manual Busy)**
SSTR	**SEAS**	**(Subsystem In-Service Trouble)**
SSSB	**SEAS**	**(Subsystem System Busy)**

The SS7 peripheral module hardware: MSB7, ST (STC), IMPLs, and DTCs are included in PM alarms.

The interoffice trunks using SS7 signaling links are included in the existing TRKS alarms.

The Multi-Protocol Controller (MPC) associated with the SEAS system is included in the existing IOD alarms.

NTP 297-YYYY-543, *DMS-100F Alarm and Performance Monitoring,* provides procedures for clearing CCS7 alarms.

Log reports

SS7 log reports are generated by the Logutil system using several log categories. The key log categories for SS7 are:

CCS — Common Channel Signaling (CCS) log reports for linkset and routeset management functions such as status, failures, and disruptions to service.

C7UP — CCS7 ISDN User Part (C7UP) are log reports for message trunks using SS7 signaling. Performance is monitored in relation to known message volume, unsuccessful attempts, and circuit availability.

PM — Peripheral Module (PM) logs for all peripheral hardware and software including MSB7, STC, IMPL, LIM, LIU7, and DTC used for SS7.

TRK — TRK logs include PTS and ISUP trunks, control hardware and software entities associated with trunks, peripheral circuit cards for digital carriers, and signaling links.

DDM — Distributed Data Manager (DDM) updates the data of many DMS nodes simultaneously.

NSC — Number Services Codes (NSC) reports on invalid data received by SSP, for enhanced 800 service.

SCP — Local subsystem management audits.

AUDT — Checks integrity of PM software, and attempts to correct errors when detected.

DFIL — Datafill (DFIL) reports on call cutoffs during call processing or debugging operations. Indicates a datafill error such as specifying more than the maximum number of digits for one stage of outpulsing. DFIL111, 122, 125, 126, and 133 logs are related to Common Channel Signaling Access Capability (CCSAC) datafill problems and action should be taken ASAP. Specifically, DFIL122 indicates missing datafill for table CKTDIGIT used for CCSAC. Use the TRAVER command to verify routing and see NTP 297-2101-500, *DMS-100F Equal Access Maintenance Guide* for further information on CCSAC.

DFIL108 through DFIL111 logs indicate datafill problems with Advanced Intelligent Network (AIN) calls that use the CCS7 network. See NTP 297-5161-500, *Advanced Intelligent Network Maintenance Guide* for further information on AIN and associated logs.

TCAP — Transaction Capabilities Application Part (TCAP) provides a common protocol for remote operations across the CCS7 network. TCAP100, 101, 102, 199, and 200 logs are associated with the Advanced Intelligent Network.

SS7 log management

Log messages are produced within the system to indicate various switching, signaling, and transmission events. SS7 log messages record events in the home office and far-end office, as well as critical SS7 network logs, as follows:

- Failures (links, synchronization)
- Information (self-test, transfers)
- Link & Routeset availability (MB, SYSB, Off-line, INHIB, congestion)
- Local Subsystem (can't reach, recovery)
- Far-end SS7 Processor Status (failure, recovery)
- Remote Point Code Status (can't reach, recovery)
- Remote Subsystems (can't reach, recovery)

NOTE: Suppressing SS7 log messages is not recommended—except for cases such as the C7UP105 log that is generated whenever a blank number is dialed.

Thresholding SS7 log messages is permitted—to the extent necessary—to manage the output from numerous sites in a centralized maintenance environment and to meet company performance objectives. During a transition to SS7 signaling, thresholding of certain SS7 log messages may be necessary for managing the higher log volume.

The log message groups (CCS, TCAP, C7UP, NSC, SCP, DFIL) associated with SS7 signaling must be added to table LOGCLASS. They should also be routed—using table TERMDEV—to the MAP position(s) responsible for that particular log activity.

The SS7 signaling system generates log reports during the many self-checks, including continuous packet transmission checks between the two nodes using digital line facilities. It is a continuous check and transient, marginal, and short duration troubles are recorded and stored within the buffers of the Logutil subsystem. CCS log report volume is affected by digital line faults.

Due to the increased volume caused by SS7—a workstation with features for storing, sorting, and thresholding log reports, including a dynamic visual status display, is essential for managing the log report volume in real time.

The log report volume can increase due to digital line faults detected by the inherent SS7 self-checking trouble detection features. This scenario is then compounded by centralizing the surveillance activity.

The addition of CCS7 type logs adds additional stress to the log system. Efforts are being made in design to reduce the number of logs and to better control the volume under an overload. As part of Nortel Networks design effort to reduce logs, some logs are being designed to provide a count of results instead of producing a number of logs. An example would be the C7UP123 log that replaces the C7UP100 or the C7UP300 log that is generated when audits are run on ISUP trunks in the Lockout (LO) state. The C7UP123 log can prevent an unnecessary large volume of C7UP100 or C7UP300 logs that might be generated during an office recovery or serious facility problem. The operating company has the option to control the use of the C7UP123 log by using the C7UP_RSC_LOG_THRESHOLD parameter in table OFCVAR.

During heavy SS7 log message conditions, the potential exists for losing log messages in the Logutil system. This is usually seen on logging devices as:

— **WARNING: 100 REPORTS NOT PRINTED**

For more information on how to manage the log report system and help prevent losing logs, see the "Log Message Administration" subsection within the *Office Administration* tab.

Table 4-15 lists the DMS-100 SSP/SP logs by subsystem, and identifies alarm class and log explanations. The NOTE column at the end of the table provides the following additional information when applicable: related OM registers, recommended log thresholding, and specific note references. Adjust the SS7 log thresholding as needed, after SS7 related troubles are cleared, after digital link facilities have stabilized, and after log volume drops to normal.

Table 4-15 — Index of DMS-100 SSP Logs

Log	Alarm Class	Explanation	OMs & Notes
Audit (AUDT) logs			
AUDT612	no alarm	A CCS audit discovered and corrected a mismatch in the link availability states between the CC and MSB.	
AUDT613	no alarm	A CCS audit discovered and corrected a mismatch in the linkset availability states between the CC and MSB.	
AUDT614	no alarm	A CCS audit discovered and corrected a mismatch in the routeset availability states between the CC and MSB.	

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
AUDT615	no alarm	A CCS audit discovered and corrected a mismatch in the route availability states between the CC and MSB.	
AUDT616	no alarm	A CCS audit discovered and corrected a mismatch in the link synchronization states between the CC and the ST.	
AUDT620	no alarm	A CCS audit discovered and corrected a mismatch in the link discard levels between the CM and the LIU7.	
AUDT622	no alarm	A CCS audit discovered and corrected a mismatch in the link discard levels between the CM and the LIU7.	
AUDT623	no alarm	A CCS audit discovered and corrected a mismatch in the routeset congestion levels between the CC and the MSB7.	
AUDT624	no alarm	A CCS audit discovered a link in a particular state for a period of time equal to at least the length of the audit cycle.	
AUDT626	no alarm	An SCCP audit discovered and corrected an integrity mismatch between the static data of the CC and of the MSB7.	
Common Channel Signaling (CCS) logs			
CCS101	minor	A CCS7 link has failed.	C7LINK1: C7ABNRFB, C7LKSYNU, C7EXCONG, C7LKFAIL, C7EXDLAY, C7EXERR
CCS102	no alarm	A link is aligned and ready for traffic.	
CCS103	minor	A CCS link synchronization failure occurred.	
CCS104	no alarm	The far-end of a CCS link has a processor outage condition.	C7LINK1:C7RPO
CCS105	no alarm	The far-end of CCS link recovered from a processor outage condition.	
CCS106	no alarm	A link has been deactivated manually.	
CCS107	no alarm	A test failed on a link.	C7LINK1: C7STLTFL, C7SLTFL

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
CCS109	no alarm	A CCS link reached the sync state but could not be nailed up.	
CCS151	no alarm	A routeset is in the off-line state.	
CCS152	critical	A routeset is manual busy.	
CCS153	critical	A routeset is system busy.	
CCS154	critical	A routeset is unavailable.	C7LINK2: C7RSFAIL, C7RSMANB
CCS155	no alarm	A routeset is available from an out-of-service state.	C7LINK2: C7RSUNAU
CCS156	no alarm	A link is in the off-line state.	
CCS157	minor or major	A link is manual busy.	C7LINK1: C7MANB
CCS158	minor	A link is system busy.	
CCS159	minor	A link is locally inhibited.	C7LINK1: C7LINH
CCS160	minor	A link is remotely inhibited.	C7LINK1: C7RINH
CCS161	no alarm	A local inhibit on a link has been removed.	C7LINK1: C7LUNINH
CCS162	no alarm	A remote inhibit has been removed from a link.	C7LINK1: C7RUNINH
CCS163	no alarm	A link is available for traffic.	C7LINK1: C7CBK
CCS164	minor	A link is not available for traffic.	C7LINK1: C7COV, C7LKUNAU
CCS165	no alarm	The office at the far-end did not obey the CCS7 signaling protocol.	
CCS166	no alarm	A route received a transfer-allowed signal from the network.	
CCS167	major	A route received a transfer-restricted signal from the network.	
CCS168	no alarm	A route received a transfer-prohibited signal from the network.	
CCS169	no alarm	A route received an unexpected signal from the network.	Threshold max. 10 messages
CCS170	no alarm	A routeset received an invalid message from the network.	Threshold max. 10 messages

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
CCS171	no alarm	A linkset received an invalid level 3 message.	Threshold max 10 messages.
CCS172	no alarm	A route received a transfer control signal from the network indicating a change in congestion level.	Threshold max 10 messages C7LINK2: C7RSCNGU
CCS173	no alarm	A transmission buffer of a CCS7 link is congested.	C7LINK2: C7ABATE1, C7ABATE2, C7ABATE3, C7ABATEV
CCS174	no alarm	A CCS7 message has an invalid destination point code.	
CCS175	major	A routeset is restricted.	
CCS176	no alarm	A ROUTESET Management (RSM) audit detected an inconsistency in link data.	
CCS177	no alarm	An RSM audit detected an inconsistency in link data.	
CCS178	no alarm	A change in office parameter H0H1_RCP.	
CCS190	no alarm	Summarized test statistics for C7BERT testing.	
CCS198	no alarm, unless office parm is set to YES	A Signaling Link Marginal Performance Report (SLMPR) is provided hourly.	See Note 3 C7LINK1: C7AUTOCO, C7NACKRX, C7SUERR
CCS199	major	A system restart caused a CCS7 link failure.	
CCS201	no alarm	An invalid SCCP message was received from the network.	C7SCCP: C7RTFAIL, C7RTFNTN, Threshold max 10 messages
CCS202	no alarm	An SCCP message with an invalid called-party address was received from the network.	C7SCCP: C7RTFAIL, Threshold max 10 messages
CCS203	no alarm	An SCCP message with an invalid calling-party address was received from the network.	C7SCCP: C7RTFAIL, Threshold max 10 messages.

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
CCS204	no alarm	An SCCP message destined for an unknown local subsystem was received from the network.	C7SCCP: C7RTFAIL, C7RTFVEQ, Threshold max 10 messages
CCS205	no alarm	An SCCP message was received from the network, but the SSP/SP has no translation tables for the required global title translation.	C7SCCP: C7RTFAIL, Threshold max 10 messages
CCS206	no alarm	An invalid SCCP message was received from a local subsystem.	Threshold max. 10 messages
CCS207	no alarm	The local SCMG subsystem has received an SCMG message with invalid data.	Threshold max. 10 messages
CCS208	no alarm	A remote point code is off-line.	
CCS209	no alarm	A remote point code is manual busy.	
CCS210	critical	A remote point code is system busy.	
CCS211	no alarm	A remote point code is available.	
CCS212	no alarm	A remote subsystem is off-line.	
CCS213	critical	A remote subsystem is manual busy.	
CCS214	critical	A remote subsystem is initializing.	
CCS215	critical	A remote subsystem is system busy.	
CCS216	no alarm	A remote subsystem is available.	
CCS217	no alarm	A local subsystem is off-line.	
CCS218	critical	A local subsystem is manual busy.	PM: PMUMBU, PMMMBU
CCS219	critical	A local subsystem is system busy.	PM: PMUSBU, PMMSBU
CCS220	no alarm	A local subsystem changes to in-service.	
CCS221	no alarm	SCMG at a remote point code is performing a sub-system status test.	Threshold max. 10 messages
CCS222	no alarm	SCMG has received a subsystem-prohibited message for a remote subsystem that is not in the routing tables for the SSP/SP.	Threshold max. 10 messages.

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
CCS223	no alarm	SCMG has received a subsystem-allowed message for a remote subsystem that is not in the routing tables for the SSP/SP.	PM: PMMMBU, Threshold max. 10 messages
CCS224	no alarm	SCMG has received an SST for the status of a local subsystem.	Threshold max. 10 messages
CCS225	no alarm	A remote point code has been removed from table C7NETSSN and is now unequipped.	
CCS226	no alarm	A message has been received from the network with an invalid global title in the called party address.	Threshold max. 10 messages
CCS227	no alarm	A message has been received from the network with an invalid global title in the calling party address.	Threshold max. 10 messages
CCS228	no alarm	A message that required global title translation resulting in an invalid network address for SCCP at an SSP has been received from the network.	Threshold max. 10 messages
CCS229	minor	A remote point code is in the in-service trouble state.	
CCS230	no alarm	An invalid message has been received from the network.	Threshold max. 10 messages
CCS231	major alarm	The status of a local subsystem changes to ISTB.	PM: PMERR
CCS232	no alarm	A local subsystem instance is taken OFF-LINE.	
CCS233	no alarm	A local subsystem instance changes to Manual-Busy.	PM: PMUMBU
CCS234	no alarm	The status of a local subsystem instance changes to System-Busy.	PM: PMUSBU, PMMSBU
CCS235	no alarm	The status of a local subsystem instance changes to In-Service.	
CCS236	no alarm	The status of a local subsystem instance changes to ISTB.	PM: PMERR
CCS237	no alarm	A request for removal from service by a local subsystem has been either granted or denied by its remote counterpart.	

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
CCS238	no alarm	An invalid coordinated state change control message has been received from the network.	Threshold max 10 messages
CCS239	no alarm	A local subsystem has made an invalid coordinated state change control request.	Threshold max. 10 messages
CCS240	no alarm	An invalid traffic mix information message has been received from the network.	Threshold max. 10 messages
CCS242	no alarm	SCCP cannot format a global title in the called party address of a message because the global title type name is not datafilled in table C7GTTYPE.	Threshold max. 10 messages
CCS299	no alarm	A trace of SCCP messages is provided.	Threshold max. 10 messages
CCS7 ISUP (C7UP) logs			
C7UP100	no alarm	ISUP has not received an acknowledgement message from a far-end office.	Threshold max. 20 messages
C7UP101	no alarm	ISUP has received an unreasonable message on the trunk indicated.	ISUPERRS: ISERRBAD, Threshold max. 20 messages
C7UP102	no alarm	A CCS7 connection has been released due to an abnormal condition.	IUPERRS: ISERRREL, Threshold max. 10 messages
C7UP103	no alarm	A circuit is blocked or unblocked.	Threshold max. 10 messages
C7UP104	no alarm	A group of circuits is blocked or unblocked.	
C7UP105	no alarm	An ISDN call attempt has failed because of an incomplete or invalid called number.	Threshold max. 10 msgs. See Note 4
C7UP106	no alarm	Problems have occurred because of a resource shortage.	
C7UP107	no alarm	Details for a continuity check test that has been performed on an outgoing trunk.	ISUPCONN: ISCONCOT, Threshold max. 10 messages

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
C7UP108	no alarm	No response has been received for a facility or information request message within a specified time.	Threshold max. 10 messages
C7UP109	no alarm	The state of an ISUP trunk has changed to match the far-end.	Threshold max. 10 messages.
C7UP110	no alarm	The far-end office had an incompatible protocol message format.	ISUPERRS: ISERRBAD, Threshold max. 10 messages
C7UP111	no alarm	An outgoing call attempt has failed due to trunk trouble.	
C7UP112	no alarm	A DMS call in progress has received an unexpected ISUP message.	
C7UP113	no alarm	An ISUP trunk had a maintenance problem.	
C7UP114	no alarm	ISUP has not received a far-end response to a release or reset circuit message before timeout.	
C7UP115	no alarm	ISUP message table has no space available to store group blocking or group reset circuit messages.	
C7UP116	no alarm	An ISUP trunk is blocked due to an outage on a DTC7 or digital carrier facility.	ISUPCKTA: ISCKTBLO
C7UP117	no alarm	An ISUP trunk is blocked due to the recovery of a DTC7 or digital carrier facility.	ISUPCKTA: ISCKTUBL
Distributed Data Manger (DDM) logs			
DDM100	no alarm	DDM has successfully transferred data to a PM.	
DDM101	minor alarm	DDM failed to transfer data to a PM.	PM: PMERR
DDM102	minor alarm	DDM failed to update distributed data for a PM.	PM: PMERR
DDM103	no alarm	DDM has successfully transferred a data table to a PM.	
DDM104	minor alarm	DDM cannot maintain data for a PM.	PM: PMERR
DDM105	no alarm	DDM has successfully transferred data to a PM and the distributed data is available in the PM.	

Table 4-15 — Index of DMS-100 SSP Logs (continued)

Log	Alarm Class	Explanation	OMs & Notes
DDM106	minor alarm	An audit of distributed data failed.	
DDM107	minor alarm	An attempt to retrieve OM data failed.	
Peripheral Module (PM) logs			
PM102	critical	Either an MSB7 or an ST7 is system busy.	PM: PMUSBU, PMMSBU, PMFLT, PMDRMBU, PMDRSBU, PMDRERR, PMDRFLT. C7LINK1: C7LPO
PM103	no alarm	Either an MSB7 or an ST7 is off-line.	PM: PMMSBU
PM104	no alarm	Either an MSB7 or an ST7 is unequipped.	
PM105	major	Either an MSB7 or an ST7 is manual busy.	PM: PMMMBU, PMUMBU C7LINK1: C7LPO
PM106	no alarm	Either an MSB7 or an ST7 is returned to service.	
PM128	minor	Either an MSB7 or an ST7 is in the in-service trouble state.	PM: PMMMBU, PMDRSBU, PMDRMBU, PMMSBU, PMMWXFR, PMSCXFR, PMSWXFER, PMUMBU, PMUSBU, PMMCXFR
PM181	critical	Either an MSB7 or an ST7 fault has been found.	PM: PMERR, PMFLT, PMINTEG, PMSCXFR, PMSWXFER,PMPSERR, PMPSFLT
Transaction Capabilities Application Part (TCAP) logs			
TCAP100	no alarm	A TCAP unit data message has been generated and contents are listed.	
TCAP101	no alarm	A TCAP unit data system message has been generated and contents are listed.	
TCAP102	no alarm	TCAP failed to send a reject component in response to a protocol error.	
TCAP200	no alarm	An originating TCAP message was not sent.	

NOTES:

1. For log information, see NTP 297-YYYY-840, *DMS-100F Log Reference Manual.* Also, see information on logs within in the *Introduction, Telco Notes & User Index* tab of this manual for new and changed SS7 logs.

2. Reference NTP 297-YYYY-814, *DMS-100F Operational Measurements* for detailed information on OM groups and their OM registers.

3. The Signaling Link Marginal Performance Report (SLMPR) description, implementation, and bogeys are described starting on page 4-215.

4. C7UP105 logs are generated when blank numbers are dialed within far-end nodes. This can cause an extreme number of C7UP105 logs to be generated with no importance to the originating office; therefore, it may be necessary to threshold or possibly suppress this log.

Operational measurements

Operational measurements (OMs) and supporting data for SS7 maintenance and surveillance activities are summarized in tables within the "Operational Measurements" subsection within the *Preventive Maintenance* tab.

The SS7 OM information within this subsection augments the OM information in the "Operational Measurements" subsection within *Preventive Maintenance* section of the MOM. SS7 OM bogey examples and customized class assignments can be found in the "Operational Measurements" subsection.

SS7 OM data covers all facets of the system, and provides information for key work functions such as: provisioning, traffic management, surveillance, and trouble isolation. For in-depth investigation, review the total OM package and select specific OM data for analyzing the current problem.

Another OM application is the policing of Message Signaling Units (MSUs) carried on the SS7 network—for the detection of corrupt data and unauthorized MSUs. These types of messages cause trouble reports that use up processing capacity, since the messages are discarded. The importance of this policing activity increases with the advent of interconnection with other carriers using SS7 signaling.

OMs for all facets of the SS7 system are collected in the following OM groups:

- C7GTWSCR records MSUs discarded at an STP by the gateway screening process because they were written by unauthorized users

- C7LINK1 records failures and recoveries for signaling links (key OM group for maintenance & surveillance)

- C7LINK2 records link and buffer congestion for signaling links (key OM for traffic measurements)

- C7LINK3 records MSU volumes at an STP. This group was established for SEAS

- C7LKSET records link and linkset failures, and outage intervals

- C7MTP records MSUs that are discarded by the MTP. This group was established for SEAS

- C7ROUTE records forced routing situations due to congestion (measurement of route performance)

- C7RTESET records routeset failures, errors & congestion. (may indicate switching center isolation)

- C7SCCP records volume of MSUs processed by the SCCP routing control

- ISUPCGRP records, by trunk group, the total of the individual trunk faults

- ISUPCKTA records for the office: blocking & unblocking message sent (all trunk groups)

- ISUPCONN records for the office: circuit availability and unsuccessful attempts (including called-party busy)

- ISUPERRS records for the office: all trunks with abnormal conditions, unexpected stops, and absences of acknowledgement messages. Used by maintenance personnel to track ISUP stability

- ISUPUSAG special study, counts ISUP trunk usage type by an application acronym

- NSC provides summary information for Number Service Calls (NSC). Indicates level of service provided by the SSP for NSC (800 service)

- NSCACG provides information on the effectiveness of Automatic Call Gapping (ACG) for NSC service

- TCAPERRS counts protocol errors detected by the Transaction Capabilities Application Part (TCAP) for each subsystem

- TCAPUSAG records TCAP messages, transactions, and components for each subsystem.

See NTP 297-YYYY-814, *DMS-100F Operational Measurements* for a complete description of all SS7 OM registers and a list of OM registers to OM groups cross-reference. A summary of the most common OM groups available for administering a DMS-STP is recorded in NTP 297-8101-350, *DMS-100F DMS SuperNode STP Base (STPBASE) Translation Guide*.

ISUP trunk continuity test (ICOT)

The ISUP per-call continuity test, when implemented, validates the voice or data transmission path of an ISUP trunk before the call is connected to the customer.

In SS7, signaling for call setup is not carried on the voice or data trunk; therefore, it is necessary to check the quality of the voice or data connection. On digital trunks this is verified by internal carrier maintenance using a continuity tone card (NT6X70) installed in DTCs or LTCs that contain ISUP trunks. On analog trunks, the voice or data path can be checked before connecting a call by connecting a tone and a receiver

to the originating end of the trunk. The terminating end is looped back to the originating end, thus enabling the originating node to validate the tone. If the tone passes, then the voice part of the call can be connected. If not, then another trunk is tried.

Datafill table TRKSGRP to implement ISUP continuity testing scheduled frequency, on a percent basis, for the trunk groups selected. See NTP 297-YYYY-350, *DMS-100F Translation Guide* for table TRKSGRP datafill and table LTCINV for the assignment of the NT6X70 continuity tone card.

ICOT testing requires substantial time to complete (60 ms to 3 sec.), a significant call processing factor. For an in-service office, running ICOT on 100% of the trunk groups could cause serious load problems. Therefore, to minimize this effect, the following ICOT testing scenario is suggested:

• During initial conversion or turn up of trunks, run the group(s) at 100%.

• Schedule ISUP trunks utilizing analog facilities and set ICOT for a minimum of 10%—in table TRKSGRP—for 2-way analog trunk groups. Also, setup ICOT tests on both ends to prevent glare.

• Normally trunks derived from digital carrier are not scheduled; however, DS0 trunk problems can occur and it is recommended that ICOT be performed to detect them.

Manual ICOT testing is done from the C7TTP level of the MAP on a trunk-by-trunk basis. The C7TTP level is accessed from the MAP TTP level.

Log messages C7UP107 and C7UP111 record the reason(s) for the ICOT failure(s). It is recommended that these logs be analyzed on a daily basis.

Since transmitter time-outs do not exist for ISUP trunks, and ICOT testing is on a percent basis, it is important to use other tools to detect trunk problems, such as: the killer trunk (KT) feature, periodic trunk maintenance (PRDTKMTC) OM reports, automatic trunk testing (ATT), and centralized automatic recording of trunks (CAROT).

NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide* provides a description of the ICOT test feature.

Signaling link maintenance tests (SSP/STP)

Loopback & MTP BER testing for signaling links

Testing DS0A signaling links using loopback test points, in conjunction with MTP BERT tests, provides a fast and effective means for trouble sectionalization of, near-end, far-end, or the interconnecting digital Data link facility. These loopback features are incorporated into NT's SS7 equipment and can be accessed from the MAP.

The SS7 loopback points are also equipped for remote operation using the DS0A bit stream and a unique looping address for each loop test point. At the node, where the remote loop is to be set up, a command, described later, must be activated from the LIU7 menu level of the MAP to effect the remote latching loopback instructions.

Remote loopback testing capability exists in various degrees for existing digital facilities and Data link services, generally under control of a control center. Remote loop access to the SS7 nodes and the digital facilities test points is usually an administrative responsibility of the Service Control Centers involved.

The usual scenario for troubleshooting a faulty link involves SS7 looping procedures, to prove the near and far-end node equipment meets requirements, using local loopbacks, and then remote loopback tests that includes digital facilities. When a fault is detected in a digital facility, it is referred to a control center for utilization of a spare span to restore service. The control center would sectionalize the fault using manual or remote loopback techniques. Once repaired and stabilized, the Data link would be returned to its assigned facility.

Sectionalization of marginal or soft faults on the signaling link requires the coordinated activities of the control center and the SS7 node. The SS7 node establishes a loopback to the far node, establishes Bit Error Rate Tests (BERT), identifies faults, and requests the control center to start systematically looping the line facilities from the far to near SS7 node. Determine from the BER tests—when the fault clears—what section(s) between the digital facility loop and the far-end node is failing.

All the foregoing activity should be cleared through the responsible control center prior to working on SS7 equipment/Data link facilities.

All DS0A loopback type tests and related BER tests are out-of-service tests that require the signaling link to be removed from service (busy-out and deactivate the link at both nodes).

Loopback and BERT test equipment

NTX839AA LPP Enhanced Maintenance & BERT — this feature package provides an MTP BERT feature test facility, a pseudorandom 2047-bit test pattern, *specifically for SS7 applications at an STP*. The path to be tested by the MTP BERT facility includes the LIU7 signaling terminal NT9X76AA, the data port paddle-board and associated Data link line facility. The C7BERT facilitates testing to a loopback point, as well as to other compatible BERT test facilities for DS0A and V.35 Data links, at speeds between 48 and 64-Kbps. The MTP BERT feature does not require any circuit pack changes to implement. MTP BERT cannot be run on pooled LIU7s. Access to C7BERT and MTP BERT is provided through a sublevel of the C7BERT MAP display. Inputting C7BERT on the command line of the C7LKSET MAP level, after a linkset has been posted, accesses the C7BERT sublevel. Figure 4-31 illustrates the MTP BERT test configuration. Table 4-16 and the related application information notes in Table 4-17 describe the test scenario.

NTX839AB LPP Enhanced Maintenance & BERT — this feature package provides an MTP BERT feature test facility and pseudorandom 2047-bit test pattern, *specifically for SS7 applications at an SSP using LPP equipment*. It has the same feature capabilities as described for the NTX839AA software package. Figure 4-31 on the next page illustrates the MTP BERT test configuration. Table 4-16 and the related application information notes in Table 4-17 describe the test scenario.

DS0A Loopbacks — this feature in the NTX839AB software package also includes a loopback test feature at an SSP or STP equipped with an LPP. The feature uses an enhanced NT9X78BA DS0A paddle-board in the LIU7 for the interface to the DS0A Data link transmission facility. The loopback features are controlled through MAP commands accessible from the LIU7 level. When enabled at the MAP, a loopback at this node can be operated by a remote request sent over the DS0A Data link being tested. Generally, remote requests would be initiated by digital facility control locations on the DS0A facility. The remote loopback feature uses a latching operation that ensures that the loopback path remains closed until a loopback release code is detected.

Figure 4-31   —   DMS-LIU7 MTP BERT test

**SS7 NODE
(SP/SSP/STP)**
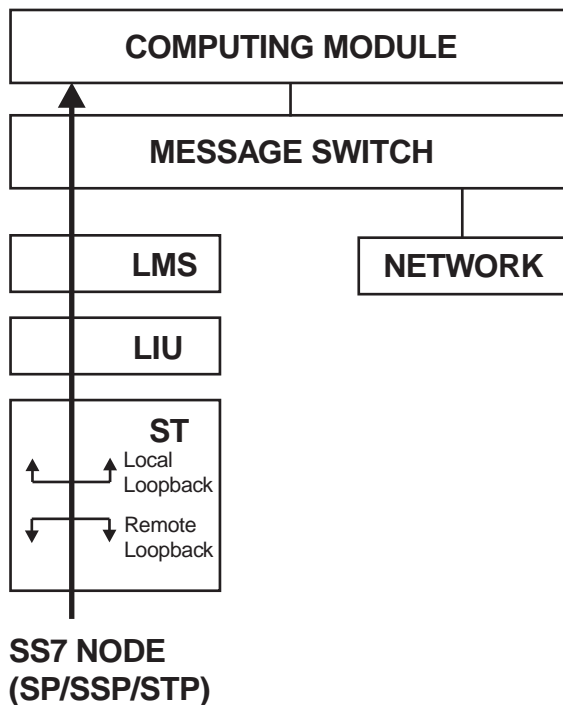
**NTX839AA MTP BERT access via LIU7 MAP menu
NTX839AB MTP BERT access via C7LKSET; C7BERT**

DS0A Loopback Modes (NT9X78BA) — for an STP or SSP using LPP/LIU7 equipment it provides the following three loopback modes—see Figure 4-32:

1. The remote mode loops data received from a DS0A signaling link through an NT9X78BA paddle-board and NT9X76AA signaling terminal card and back out on a DS0A signaling link. The data is looped back at the input of the NT9X76AA signaling terminal card.

2. The local mode loops data transmitted from the paddle-board output back into the paddle-board receive input.

3. The enable mode allows the control code scanning mechanism on the paddle-board to monitor and respond to any latching loopback control code that is received from a DS0A signaling link. When a valid control code sequence is received on a DS0A signaling link at the signaling terminal input, and enable mode is active, a remote loopback is established that loops the test pattern data back out on the DS0A signaling link output. Only one loopback mode can be active at a time.

NTX712AA CCS7 Data Port — this provides loopback test features at an MSB7 SSP using an enhanced NT6X55AB DS0A data port card in the DTC, which is the interface to the DS0A Data link transmission facility. The loopback features are controlled through MAP commands accessible from the CARRIER level via the TRKS level. When enabled at the MAP, a loopback at this node can be operated by a remote request sent over the DS0A Data link being tested. Generally, remote requests would be initiated by digital facility control locations on the DS0A facility.

Figure 4-32 — Loopback modes for the NT9X78BA paddleboard
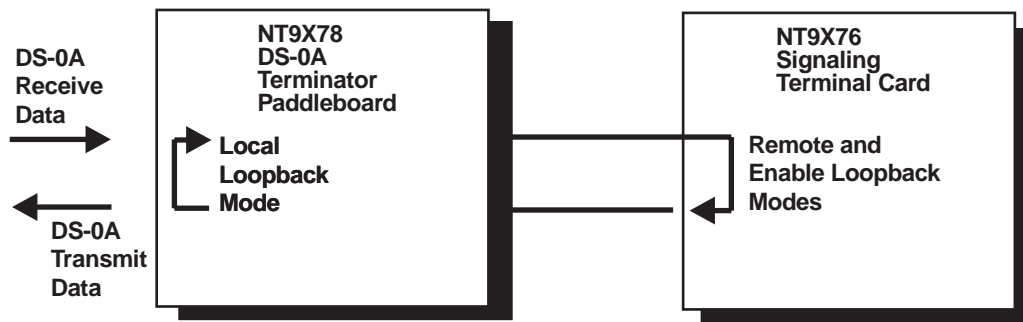
The remote loopback feature uses a latching operation that ensures the loopback path remains closed until a loopback release code is detected. Figure 4-33 illustrates the loopback test configuration. Figure 4-34 and the related application information notes (Table 4-17 on page 4-198) describe the test scenarios.

DS0A Loopback Modes (NT6X55AB) — for an SSP using MSB7 equipment provides the following three loopback modes—see Figure 4-33:

1. Remote mode loop, data received from a DS0A signaling link is resynced and looped back out on the DS0A link. These events take place in the NT6X55AB Data Port Card.

2. Local mode loop, data from the DS60 bus is looped back to the DS60 bus at the DS0 interface on the NT6X55AB Data Port Card.

3. Remote loopback enable, when set, a remote loopback initiated if it is remotely requested via the DS0A link. Until it is requested, all ones are transferred to ST on the MSB.

Figure 4-33 — Loopback modes for the NT6X55AB data port card
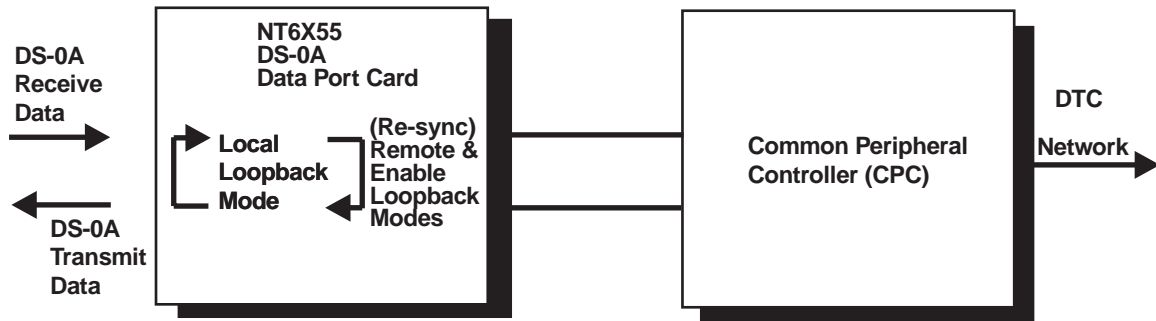
NTXE30AA MTP BERT Capability for SSP — this feature package provides an MTP BERT test facility, a pseudorandom 2047-bit test pattern, specifically for SS7 applications using MSB7 equipment. The C7BERT test facility is independent from the existing DMS-100 trunk BERT feature. The path to be tested by the C7BERT facility includes the MSB7 speech path, the network, the interface peripherals (DTC, LTC, DCM) speech path and associated digital transmission facility. The C7BERT facilitates testing to loopback points—as well as to other compatible BERT test facilities for DS0A and V.35 Data links—at speeds between 48 and 64-Kbps. This feature requires an enhanced NT6X66AC Signaling Terminal Card to handle the BERT pattern generation and reception. C7BERT cannot run on pooled ST7s. Access to C7BERT is provided through a sublevel of the C7LKSET MAP display (MAPCI;MTC;CCS;CCS7;C7LKSET;C7BERT). Table 4-16 on page 4-197 and the related application information notes describe the test scenarios.

Table 4-16 — SS7 Node to Node Loopback and BERT tests

WORK ACTIVITY	EQUIPMENT CONFIGURATION						OTHER
	STP		SP/SSP		SP/SSP		
	LPP	LIU7	MSB7	LIU7	MSB7	LPP	
	MTP BERT TEST	DS-OA LOOPBACK TEST POINT	DS-OA LOOPBACK TEST POINT	DS-OA LOOPBACK TEST POINT	MTP BERT TEST	MTP BERT TEST	
	------	NT9X78BA	NT6X55AB	NT9X78BA	NT6X66AC	------	
TEST SCENARIO TO ------>	NTX839AA	NTX839AA	NTX712AA	NTX839AA	NTXE30AA	NTX839AB	
LOOPBACK (NEAR/FAR) LOCAL MAP CONTROL **A**		SEE NOTE **A1**	SEE NOTE **A2**	SEE NOTE **A1**			
LOOPBACK (FAR) FOREIGN ENABLE (DS-0A ACTIVATION) **B**		SEE NOTE **B1**	SEE NOTE **B2**	SEE NOTE **B1**			
EXTERNAL LOOPBACKS (PHYSICALLY SET) **C**							SEE NOTE **C1**
MTP BERT TEST STP ------> SP/SSP **D**	SEE NOTE **D1**						
MTP BERT TEST STP <------> STP **E**	SEE NOTE **E1**						
MTP BERT TEST SP/SP <------> STP **F**					SEE NOTE **F**	SEE NOTE **F**	
MTP BERT TEST SP/SSP <------> SP/SSP **G**					SEE NOTE **G**	SEE NOTE **G**	

Table 4-17　—　Loopback and MTP BERT test applications

Notes A,B,C

Loopback Test Points

There are three methods for setting loopback test conditions:

- MAP control

- foreign control using the DS0A signal

- external (physically set.

Loopback test points in conjunction with MTP BER testing are used to identify and sectionalize signaling link faults. Several combinations of loopback and MTP BERT equipment configurations exist, these can be mixed in any combination to derive the required test scenario.

Note A1

DS0A loopback features for LIU7 equipment (NT9X78BA), are controlled locally from the MAP LIU7 menu level. It involves three possible loopback settings: *local* and *remote* for which descriptions follow, and *enable* that is described in B1.

Local Mode (near-end loopback set)

- Loops data transmitted from the NT9X78AA paddle-board output back into the paddle-board receive input—see Figure 4-32 on page 4-195.

- A local test for checking the home office equipment (NT9X78BA and NT9X76 cards) is performed when an MTP BER test has been established in the home node on the selected signaling link, and the local loopback mode is set (see applications D to G).

Remote Mode (far-end loopback set)

- Loops data received from a DS0A signaling link through an NT9X78BA paddle-board and NT9X76AA signaling terminal card and back out on the transmit side of the same DS0A link—see Figure 4-32 on page 4-195.

- The remote mode loopback test scenario is used to check the signaling link transmission facility up to the DS0A terminating card in the distant node. The remote mode loopback is set from the MAP LIU7 menu level at the far-end node.

Table 4-17 — Loopback and MTP BERT test applications

- For this remote mode loopback test scenario, assume you have just completed a satisfactory BER test using the local mode loopback previously described. Cancel the local mode loopback which restores the signaling link connectivity to normal. Call the far-end node and request them to set a remote loopback on the signaling link being tested. Restart your MTP BER to test the home office LIU7 equipment, the signaling link facility connecting the two nodes, and the far-end node NT9X78BA paddle-board end NT9X76 signaling terminal card.

- Similar MTP BER tests can be initiated by the far-end using local and remote mode loopbacks to confirm the fault and sectionalization findings.

Note A 2

DS0A loopback features, for MSB7 equipment configurations using a NT6X55AB DS0A card installed in a DTC, are controlled locally through MAP commands accessible from the CARRIER menu via the TRKS level. They involve three possible loopback settings: *local* and *remote* that are described below, and *enable* that is described in B2.

Local Mode (near-end loopback set)

- Loops data transmitted from the NT6X66AB data port card back into the receive input side. This loopback function in the NT6X55AB card takes place at the DS60 bus—see Figure 4-33 on page 4-196

- A local test for checking the home office equipment (ST7 part of MSB7, NUC part of DTC, and NT6X55AB), is performed when an MTP BER test has been established in the home node on the selected signaling link and the local loopback mode is set.

Remote Mode (far-end loopback set)

- Loops and resynchronizes data received from the DS0A signaling link. These events take place in the NT6X55AB dataport card.

- The remote mode loopback test scenario is used to check the home node, the signaling link transmission facility up to the DS0A terminating card in the distant node. The remote mode loopback is set from the MAP CARRIER menu level at the far-end node. For this remote mode loopback test scenario, assume you have just completed a satisfactory BER test using the local mode loopback previously described. Cancel the local mode loopback, which restores to normal the signaling link connectivity. Call the far-end node and request them to set a remote loopback on the signaling link being tested. Restart your MTP BER test checking from the home office MSB7 equipment (ST7 part of MSB7, NUC part of DTC, and NT6X55AB), the signaling link facility connecting the two nodes, and the far-end node to the data port card NT6X55AB.

Table 4-17 — Loopback and MTP BERT test applications

- Similar MTP, BER tests can be initiated by the far-end node using local and remote loopbacks to confirm the fault and sectionalization findings.

Note B1

The ENABLE command, part of the DS0A loopback feature, when set at the local MAP position, LIU7 menu (LoopBK E), conditions the remote loopback function, so that a foreign tester who has access to the DS0A line can activate the remote loopback feature. This requires specialized data link transmission test gear at the foreign test center.

ENABLE Mode (Far-end loopback set)

When enabled, allows the control code scanning mechanism on the paddle-board to monitor and respond to any latching loopback control code that is received from the DS0A signaling link. When a valid control code sequence is received on the DS0A signaling link (NT9X78BA paddle-board) and the enable mode is active, a remote loopback is established that loops the test pattern data back out on the DS0A output.

- This is an out-of-service test. Before the enable mode is activated, the signaling link must be removed from service. When it has been activated and the latching loopback code has not been received at this node, an all ones signal is normally generated back into the SS7 equipment.

- This feature permits remote signaling link trouble investigations by Data link maintenance personnel, controlled by the SS7 node (local or remote).

- Test scenarios involving the enable feature include out-of-service trouble sectionalization and trouble clearing conditions.

Note B2

Identical to B1, except for the hardware (NT6X55AB in place of NT9X78BA) and MAP access. For this arrangement access the CARRIER level for the loopback test features.

Note C1

DS0A loopback tests may be placed at external test points, other than the SS7 dataport terminating type cards. External loopback points would include equipment locations used to derive the Data link facilities, including digital cross-connect points. MTP BER test feature supports external and open ended test scenarios.

Again, these are out-of-service tests, the signaling link must be removed from service. The test scenario would be similar to those described in A1 and A2.

Table 4-17 — Loopback and MTP BERT test applications

CAUTION:
When setting up external loopback test points, especially when regenerative type hardware is ABSENT at the loopback point, cable lengths are a factor. The total cable length and test leads should not exceed those specified for the particular type of transmission protocol. Similarly, it applies to portable test set connections to external test points.

Notes D, E, F, G

MTP BER testing

The MTP BERT feature is dedicated to SS7 test applications. It is independent from existing DMS-100 switch and trunk BER test features.

MTP BER test features in conjunction with loopback test points are used to identify and sectionalize signaling link faults. Several combinations of loopback and MTP BERT equipment configurations exist. These can be mixed in any combination to derive the required test scenario.

The MTP BERT test feature NTX839AA applies to DMS-STP modes only. NTX839AB is an enhanced version that works with SP/SSP nodes for LIU7 equipment configurations. For a SSP/SP equipped with MSB7s, NTXE30AA provides the MTP BERT testing capability.

MTP BERT cannot run on pooled ST7 or LIU7 configurations; it must be under the basic allocation scheme.

MTP BERT test applications include:

- initial circuit order testing & verification
- fault identification
- fault sectionalization (near-end, far-end, digital line facilities)
- signaling link stability tests
- MTP BER test functions apply to both DS0A and V.35 signaling link line facilities

Figure 4-34 and Figure 4-35 on page 4-202 record the various MTP BERT test terminations. The basics are:

- loopback test points (internal/external)
- portable test equipment (MTP BERT compatible 2047 test pattern)
- ST7/LIU7 to ST7/LIU7 node to node testing

Table 4-17 — Loopback and MTP BERT test applications

Figure 4-34 — DS0A Loopback & MTP BER Testing — SS7 MTP BER Tests and Terminations
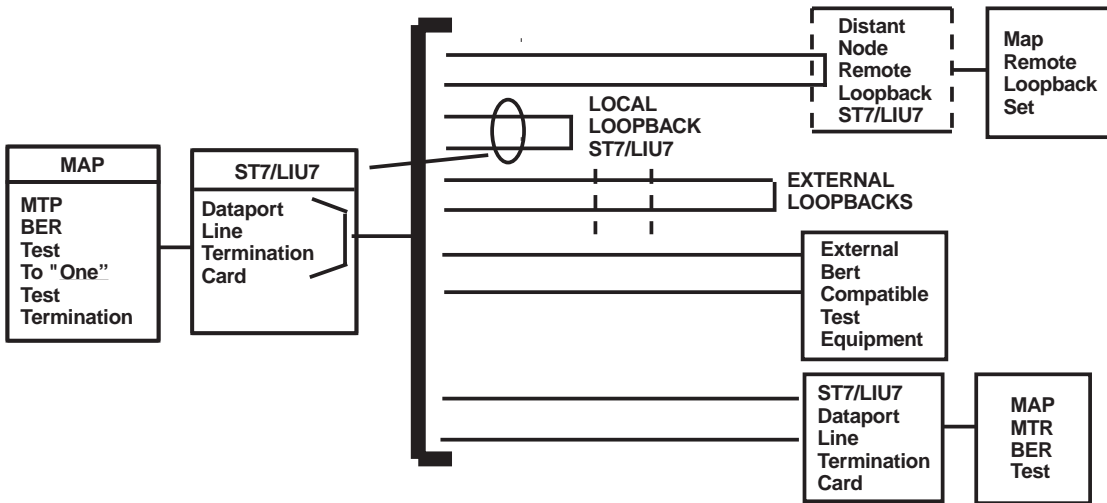
Figure 4-35 — DS0A Loopback & MTP BER Testing — Typical remote testing from a DDS
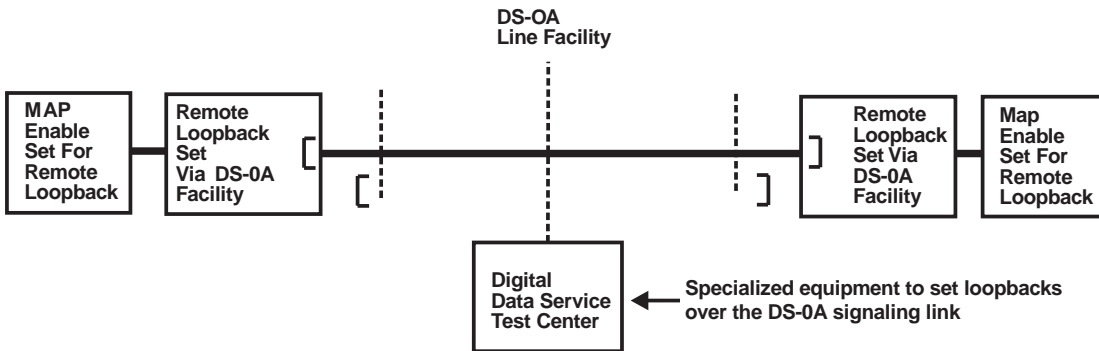
Note D1

Running a BER Test (NTX839AA) from STP to SSP Test Scenario 1

- STP establishes BER testing to the SP/SSP to investigate a signaling link problem. The following test scenario would work from an SSP to an STP if the SSP is equipped with the NTX839AB software package.

Table 4-17 — Loopback and MTP BERT test applications

Preparation and testing

- STP is equipped with MTP BERT (NTX839AA), DS0A loopback (NT9X78BA) and the SP/SSP is equipped with NT6X55AB Data link card.

- Obtain clearance from the control center to proceed with work activity and removal of the signaling link from service.

- Verify that the link to be tested is aligned at the C7LKSET MAP level.

- At each node, the link must be in-service and not allocated before placing in MANB state.

- At the SP/SSP, access the CARRIER level and post the NT6X55AB DS0A dataport card in the DTC.

- Set the loopback to R (remote).

NOTE: To use any loopback command, the carrier must be in MANB state.

- At the STP, access the LIU7 and post the LIU7 associated with the link to be tested (link must be in-service, but not running traffic).

- Invoke the MTP BER test ON.

NOTE: Cannot activate unless the LIU7 to be tested has been posted.

- A confirmation message is displayed indicating MTP BERT test is actively running (passed) or has failed.

- Verify MTP BER test is running by invoking the BERT QUERY command. A snapshot of the BER statistics is displayed—see Exhibit A.

- The MTP BERT can run for a maximum of seven days (BCS34 extended running time). Long runs are used for stability verification or investigating soft troubles. Minimum run time for a BERT trouble test is 10 minutes.

- During long BERT tests, use the BERT QUERY command and verify the operation periodically.

- The test is terminated by using the BERT STOP command. When the test is stopped, all the BERT cumulative statistics are displayed on the screen—see Exhibit A. Record data for current and subsequent analysis.

- Call the far node SSP to release remote loopback.

- If testing is complete, return link to service at both nodes, verify operation, and notify the control center. If testing is not complete, proceed with the additional tests that follow.

Table 4-17 — Loopback and MTP BERT test applications

Running a BER Test (NTX839AA) from STP to SSP Test Scenario 2

- STP establishes a local BER test to verify the LIU7 equipment. The local loopback is activated at the NT9X78BA paddle-board.

Preparation and testing

- Assume this test follows scenario 1, the link is still MANB.
- From the STP, access the LIU7 level, verify posted LIU7 is the link to be tested (must be in-service but not running traffic).
- From the LIU7 level, set loopback L (local).
- From the LIU7 level, invoke the BERT test "ON".
- A confirmation message is displayed (passed or failed).
- Verify MTP BER test is running by invoking the BERT QUERY command. A snapshot of the BER statistics is displayed—see Exhibit A.
- Run the test a minimum of 10 minutes or longer.
- Terminate the test using BERT STOP. The total statistics for the test are displayed—see Exhibit A below.
- If testing is complete, clear the local loopback.
- If testing is complete, return link to service at both nodes, verify operation and notify control center.
- A confirmation message is displayed indicating MTP BER test is actively running (passed or failed).
- Verify MTP BER test is running by invoking the BERT QUERY command. A snapshot of the BER statistics is displayed—see Exhibit A.
- The MTP BERT can run for a maximum of seven days (BCS34 extended running time).
- After 10 minutes, stop BER test and capture the BER statistics for test STP-X to remote loop at STP-Y.
- Notify STP-Y to clear the remote loopback.
- Test 2, at STP-X set local loopback.
- Start BER test & verify.
- After 10 minutes, stop BER test and capture the statistics for test STP-X looped locally.

Table 4-17 — Loopback and MTP BERT test applications

Exhibit A — MTP BERT Test results (statistics report and explanation)

The BERT statistics are displayed on the screen in this format:

Run Time	:000000161353	Err Free Secs	:000000156783
Tx Frames	:000000426800	Rx Sync Errs	:000000000000
Rx Bad Frames	:000000000000	Rx Frames	:000000426798
Rx Bit Errors	:000000000000	Rx Bits	:000003414384

Run time represents, in seconds, the length of time the test has been running.

Err Free Secs represents the total number of one-second intervals in which no errors were detected in the data stream.

Tx Frames represents the number of 2047-bit patterns that were transmitted. This counter is incremented in steps of eight.

Rx Sync Errs represents the number of times that the received 2047-bit pattern has changed position in time.

Rx Bad Frames represents the total number of 2047-bit frames that contained at least one bit error.

Rx Frames represents the total number of 2047-bit patterns that were received.

Rx Bit Errors represents the total number of bit errors that were detected.

Rx Bits represents the total number of bits that were received.

NOTE: Signaling link Bit Error Rate (BER) test criteria for circuit turn up is recorded in Table 4-18 on page 4-208.

- Test 3, repeat BER tests from STP-Y to remote loop at STP-X and capture BER data following previous steps.

- Test 4, repeat BER tests from STP-Y to local loop at STP-Y and capture BER data following previous steps.

- Analyze BER test data from the four tests to sectionalize trouble into near-end node, signaling link facilities, or far-end node and correct.

- When fault has been corrected, retest to validate.

- Verify all loopbacks are cleared and BER testing is off.

- Return link to service at both nodes, verify operation, and notify the control center.

Table 4-17 — Loopback and MTP BERT test applications

Note E1

Running a BER Test (NTX839AA) between STPs Test Scenario 3

- BER testing between two STPs to investigate a marginal signaling link problem. Since MTP BER testing is available at both nodes, four BER tests can be made to sectionalize the problem (see below).

STP-X   **STP-Y**

Test 1
Test 2
Test 3
Test 4
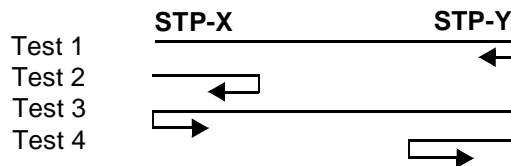
Preparation and testing

- STPs are equipped with MTP BERT (NTX839AA) and DS0A loopback cards NT9X78BA.

- Obtain clearance from control center to proceed with work activity and removal of the signaling link from service.

- Verify link to be tested is aligned at the C7LKSET MAP level

- At each node, the link must be in-service and not allocated before placing in the MANB state.

- At STP-Y, access the LIU7 level, and post the LIU7 that is connected to the link to be tested (must be in-service but not running traffic).

- Set LIU7 for remote loopback operation (NOTE: to use any loopback command, link must be in MANB state).

- Test 1, at STP-X, access the LIU7 and post the LIU7 associated with the link to be tested (link must be in-service, but not running traffic).

- Invoke the MTP BER test "ON" (will not activate unless the LIU7 to be tested has been posted).

Notes F & G

BCS34 extended MTP BERT testing capability to the SP/SSP nodes using either MSB7 or LIU7 equipment. Prior to this, MTP BERT testing facilities were only available at STP nodes. Also, the existing BER feature NTX839AA is updated to NTX839AB. Basically, the test scenario process stays the same. The important changes are:

Table 4-17 — Loopback and MTP BERT test applications

- MTP BERT is accessed from a menu level C7BERT that is provided through a sublevel of C7LKSET.

- Besides the existing commands, START, STOP, and QUERY, two additional ones have been added:

    — SETSTOP command is used for long-term MTP BER testing, up to one week from the current time. When the set/stop time has been reached, the BERT test is terminated and the results of the BER test are output as a CCS190 log.

    — REPORT command when activated, permits current MTP BERT data to be reported periodically to the log systems (CCS190 log message). The parameters are a minimum interval of 5 minutes and a maximum of 60 minutes.

Data link transmission and stability requirements

Highly stable data links are essential for provisioning reliable SS7 signaling links. Validate the circuit order acceptance tests for the facility to ensure the turn up performance criteria was met.

The data link bit error rate (BER) test is a node to node test and includes all T1 spans or equivalent digital facility, including dataport channel equipment required to derive the SS7 signaling link. The BER testing should be performed during busy hour load conditions.

Signaling links should be maintained at the BER criteria listed in Table 4-18 on page 4-208.

Use the resident MTP BER test feature to measure the DS0A and V.35 signaling link BER performance. However, it may require some additional considerations if the BER performance criteria are exceeded, since the signaling link is now terminated into the SS7 node equipment. The performance criteria stated in Table 4-18 are for the data link facility only. Therefore, when the BER performance criteria are exceeded, additional sectionalization testing is required to isolate the fault into the near-end, far-end or the digital facility. Loopback and BER testing scenarios are described in Table 4-17 on page 4-198 of this subsection.

Table 4-18 — Signaling link bit error rate (BER) test criteria

Digital Facility	Test Points	Test Time Interval	Performance Criteria	Notes
DS1	End to End	120 minutes	20 or less error-seconds	The normal DMS-100 criteria for T1CXR is BER greater than 1×10^{-6}
	Loopback far node	120 minutes	33 or less error-seconds	
DS-0A	End to End	10 minutes	0 error-seconds	Measured at dataport channel unit
	Loopback far node	10 minutes	0 error-seconds	
V.35	Local test	10 minutes	0 error-seconds	Verify V.35 port options in the DSU and paddleboard at both nodes to ensure compatibility
	DSU test	10 minutes	0 error-seconds	
	End to End	15 minutes	3 or less bit errors	
	Loopback far node	15 minutes	6 or less bit errors	

CAUTION:
For DS0A signal propagation considerations, the interconnecting cabling between the DS0A line facility termination (regenerative repeater, DSU) and the input to the SS7 Dataport card, the maximum length is 1500 feet of 24 gauge cable.

When testing DS1 BER performance, use the regular DMS BER test procedures described in NTP 297-1001-533, *DMS-100F Bit Error Rate Performance*, and NTP 297-1001-595, *DMS-100F Trunks Maintenance Guide*. Digital switch bit error performance (BERP) criteria is described in the "Network Maintenance" subsection within the *Preventive Maintenance* tab.

Upon successful completion of the signaling link circuit order and BER tests, proceed with a signaling link stability verification check at five consecutive 24 hour intervals. The objective is to place the signaling link in-service but at the same time unavailable for traffic. This scenario is possible during conversions and the stability check completed before the service date. Other arrangements may be possible using spare ST assignments and test data assignments. If the signaling link cannot be placed in-service with no traffic, consider using the MTP BER test setup for five days, and then running and evaluating the BER results to determine stability. Loopback and BER testing scenarios were previously described in Table 4-17 of this subsection.

NOTE: A test call is divided into time intervals of one second. A 10 minute test call has 600 seconds. A second is marked as an errored second if it has one or more errors during

that one particular second. A call could have none, one, or more errored seconds.
Derivatives are error free seconds (EFS) and percent error free seconds (PEFS).

During the stability verification run, record key operational measurements for the sig-
naling links under test for five consecutive 24 hour intervals and evaluate in 24 hour
increments. OM Group C7LINK1 captures the errors, failures, changeovers, and
usage for the signaling links levels 1 & 2 of the MTP. The OM registers to be evalu-
ated, and bogeys for the 24 hour intervals are shown in the following table

Table 4-19 — C7LINK1 group registers

C7Link1 Registers	24 hour Bogey	Notes
C7LKSYNU	8640	Total link usage time for 24 hours at a 10 second sample
C7LKUNAU	0	Total timelink unavailable for service in a 24 hour period. Measured in usage (CCS).
C7LKFAIL	0	Count of in-service link synchronization failures.
C7BYSON	0	Count of busy signal transmission starts, which is an indication of congestion
C7SUERR	40	Count of signaling units (SU) received with errors
C7NACKRX	9	Count of signaling messages incorrectly received at the far-end

Common Channel Signaling 7 Test Utility (C7TU)

There are two versions of C7TU:

- CCS7 Protocol Monitor Tool (PMT7)
- CCS7 Integrated Link Protocol Test Tool (ILPT7).

C7TU monitors CCS7 messages on the links, either MSB7 or LIU7 from the SSP,
STP, or SCP nodes of the DMS product line. C7TU is accessed from the CI level of
the MAP.

> **CAUTION:**
> Before using any C7TU commands, see TAM-1001-015, *C7TU User Guide* and review any **Danger, Warning,** or **Caution** messages.

CCS7 Protocol Monitor Tool (PMT7)

PMT7 allows the users to only monitor messages, and this is limited to 10 messages per minute. It has a limited command list and does not require a password to access.

CCS7 Integrated Link Protocol Test Tool (ILPT7)

ILPT7 allows the users to monitor, intercept, build, and send messages. Besides the commands that are included in PMT7 for monitoring, other commands are provided for creating and sending messages. In BCS34 the number of login users was reduced from 10 to two.

> **CAUTION:**
> Improper use of ILPT7 can seriously degrade CCS7 traffic capacities and may cause serious CCS7 traffic loss. Service and CCS7 message degradation may occur when ILPT7 is used on a high traffic link. The ILPT7 version of C7TU should only be used by experienced TAS or operating company personnel who understand the effects of using C7TU on a switch carrying live traffic. C7TU should only be used on low traffic links. To verify link traffic, post the links and use the QUERYTRF command on the C7LKSET menu level of the MAP.

C7TU involves two nonmenu directories for PMT7 and ILPT7 that are accessed from the CI level as follows:

```
CI: C7TU
```

```
CI: C7TU;C7TULINK
```

The C7TU access permits the following commands to be employed:

- C7TUREC specifies a device for saving C7TU reports
- C7TUPRT displays the reports saved with C7TUREC
- DPC query or monitor the state of a routeset(s)
- MSGCODE list of valid test message codes

Entering C7TU Directory gives the user access to the commands necessary to monitor links as well as set C7TU to monitor for specific messages.

The C7TUREL command permits the user to specify the log system to display C7TU messages as they occur, or to send all messages to a buffer.

The C7TUPRT command can then be used to display all the C7TU messages currently in the buffer. Should a large number of C7TU messages be expected, it is better to send the messages to a buffer rather than flood the log system. This avoids the problem of nonrelated messages not being printed due to the log system being overloaded with a large number of C7TU messages.

The DPC command allows the user to either monitor the state of a routeset or to query the current state of a routeset. In monitoring a routeset, any change in the routeset status is recorded.

The MSGCODE command is preset to allow the user to list the CCS7 message codes that can be monitored. If a message code is not listed using this command, the user is unable to use it in the MONITOR command in the C7TULINK sublevel.

C7TULINK

C7TULINK is a level in C7TU_PMT7 and C7TU_ILPT7 used to monitor specific message types on selected links. The PMT7 is limited to monitoring while the ILPT7 has additional commands to intercept, build, and send messages over the link.

The C7TU;C7TULINK command access permits the following commands to be used except for the limitation of PMT7:

ALTER	**alter the bytes in the built message**
BUILD	**build a message to be sent on a link**
DISPLAY	**display the built message**
DUMP	**display MATCH table in hex format**
HELP	**generate this text**
INTercept	**intercept MSB/ST messages**
MONitor	**monitor MSB/ST messages**
MASK	**mask out bytes in a monitor or intercept entry**
MATCH	**specify bytes to match on in a monitor or intercept mode**
QUIT	**exit C7TU LINK environment**
REMOVE	**cancel an intercept or monitor request**
RESTORE	**send the MATCH table entries to MSB**
SELECT	**select MSB7s and attributes**
SEND	**insert the message at ST interface**
STATUS	**display the status of the C7TU link environment**

The SELECT command allows the LIU7 log throttling to be set from one to 60 logs in the selected LIU7, and the STATUS command is enhanced to display the throttle setting for an LIU7.

Building SS7 test messages with C7TULINK

Entering the C7TULINK sublevel within ILPT7 allows users to build their own messages and send them on SS7 links. Once a built message is sent using the SEND command, the SS7 system will treat the message the same as any other SS7 message. This makes the command extremely useful for testing. However, caution must be used in using this command. Sending incorrect messages out onto the network may be detrimental to other nodes in the network or for the network itself.

The BUILD and ALTER commands modify the C7TU message table. This table allows a maximum of eight (8) entries and saves the complete SS7 message entered by the user. Messages are retained in the message table, even if the user should exit C7TU. The SEND command takes the specified message from the message table and

injects it at the given link. The DISPLAY command displays entries in the message table.

Monitoring SS7 messages with C7TULINK

C7TULINK sublevel provides the user with the ability to monitor for specific messages. This is done using the match table.

Following any changes to the match table (i.e., adding a new message to monitor for), the match tables in all in-service MSB7s or LIU7s are dynamically updated using the Distributed Data Manager (DDM). As soon as an in-service MSB7 or LIU7 has the updated match table, it starts screening messages according the table.

The match table allows for a maximum of eight (8) entries with a maximum length of sixteen (16) bytes per entry. C7TULINK only uses the first sixteen bytes of a message when compared against the match table. This is done in order to keep the real time impact to a minimum.

The MONITOR command automatically selects the next available entry in the match table when setting a match table entry. The match and mask bytes of the match table entry are determined by the MONITOR command, using the parameters specified by the user.

As an example, Figure 4-36 (dump 0) shows a MONITOR command that selects only signaling link test messages to a specific Destination Point Code (DPC) of network 1, cluster 2, member 3, and specific Origination Point Code (OPC) of network 4, cluster 5, member 6 with Signaling Link Selector (SLS) of 7.

Figure 4-36 — Making a match table entry

```
> MONITOR LINK LKSET1 1 IN ANSI LABEL NATL  0  1  2  3  4  5  6  7
                               SLTM  PARMS  01  10
> DUMP  0
C7TU MONITOR              SIO            DPC              OPC         SLS
NUM TYPE  DIR     NI      PR  SI      MEM  CLU  NET    MEM  CLU  NET
0   SLTM  IN      NATL    00  SNTS    003  002  001    006  005  004    07
          0   1   2   3   4   5   6   7   8   9   10  11  12  13 14 15
          —   —   —   —   —   —   —   —   —   —   —   —   —   — — —
Match:    00  04  00  00  82  03  02  01  06  05  04  07  11  10 01
Mask:     00  FF  00  00  FF  FF  FF  FF  FF  FF  FF  1F  FF  FF FF
```

If a user wishes to monitor all signaling link test messages from a specific OPC of network 4, cluster 5, and member 6 regardless of the DPC with an SLS of 7, the MONITOR command shown in Figure 4-37 (dump 1) demonstrates this.

Figure 4-37 — Monitoring for specific OPC

```
> MONITOR   LINK   LKSET1   1   IN   ANSI   LABEL   NATL   0   256   256   256   4   5   6 7
                                      SLTM   PARMS   01   10
> DUMP  1
C7TU MONITOR                 SIO              DPC                OPC            SLS
NUM TYPE  DIR       NI        PR   SI     MEM  CLU   NET      MEM    CLU    NET
1 SLTM    IN        02        00   STNS   000 000   000      006    005    004 07
          0    1    2    3    4    5    6    7    8    9    10   11   12   13 14 15
          —    —    —    —    —    —    —    —    —    —    —    —    —    — — —
Match:    00   04   00   00   82   00   00   00   06   05   04   07   11   10 01
Mask:     00   FF   00   00   FF   00   00   00   FF   FF   FF   1F   00   FF FF
```

Intercepting SS7 messages with C7TULINK

C7TULINK sublevel allows the user to intercept SS7 messages coming in off the link. By intercepting a message, the message is removed from the link and the SS7 system never sees it. Caution must be used with this command, since removing the SS7 message may have consequences for the node and for the network itself.

The INTERCEPT command uses the match table that is also used in monitoring messages. If an SS7 message is intercepted, a report containing the message intercepted is produced by C7TU.

The DUMP command is used to display the match table—see Figure 4-38. This displays for the user the criteria being used in interception.

Figure 4-38 — Showing a match table entry

```
> DUMP  2
C7TU INTERCEPT               SIO              DPC                OPC            SLS
NUM TYPE  DIR       NI        PR   SI     MEM  CLU   NET      MEM    CLU     NET
2 SLTM    OUT       02        00   SNTS   025  026   002      004  005  002   07
          0    1    2    3    4    5    6    7    8    9    10   11   12   13 14 15
          —    —    —    —    —    —    —    —    —    —    —    —    —    — — —
Match:    00   04   00   00   82   19   1A   02   04   05   02   07   21   10   01
Mask:     00   FF   00   00   FF   FF   FF   FF   FF   FF   FF   1F   FF   FF   FF
```

Table 4-20 lists the log messages generated by the ILPT7 feature.

Table 4-20   —   Summary of ILPT7 logs

LOG	EXPLANATION
C7TU101	A message coming in off the link has been matched to an entry in the C7TU match table.
C7TU102	A message from the LIU7/MSB7 onto the link has been matched to an entry in the C7TU match table.
C7TU103	A test message has been injected into the LIU/MSB7 so that it looks as if the message has come from the link.
C7TU104	A test message has been injected into the LIU7/MSB7 so that the message will transmit onto the link.
C7TU105	A test message should have been sent but was unsuccessful.
C7TU106	A message that C7TU is unable to interpret.
C7TU107	(not assigned)
C7TU108	A response to the request: query or monitor the status of a particular routeset.
C7TU109	A response to the Select command that records C7TU tracing ON.
C7TU110	A response to the Select command that records C7TU tracing OFF.

C7TU log reports

There are about 15 C7TU log reports that usually consist of a routing label followed by the S7 data in hexidecimal. The code can be broken down into various formats depending upon the message type. Reference NTP 297-YYYY-840, *DMS-100F Log Reference Manual* for details on the C7TU logs. For references to decode the hex format, see the American National Standards Institute document or the Telcordia Technical Requirements (TRs) documents.

C7TU User Guide

For a description of the C7TU commands, reference TAM-1001-015, *C7TU User Guide.*

Portable protocol analyzers

Portable protocol analyzers are specialized pieces of test gear, commonly used in packet switching technology for testing compatibility and fault location. Specialized portable protocol analyzers equipped with the SS7 feature may be used for testing the SS7 packet switching network.

Examples of test applications utilizing portable protocol testers are:

- compatibility validation when interconnecting to other vendor equipment or other networks
- identify datafill irregularities
- isolation of protocol problems on in-service links
- identification of hardware faults affecting a specific link
- effectiveness of gateway screening

NOTE: Initial signaling link transmission tests involve bit error rate testing techniques.

Portable protocol analyzers—with various features—are available from several manufacturers. Typical features are:

- monitors for specific message units
- formats and sends SS7 test messages
- collects and stores data strings
- retrieves/displays output to verify compatibilities
- executes test procedures via the link

For the selected test scenario, determine the signaling link involved, which becomes the test access point for the portable protocol analyzer.

> **CAUTION:**
> Testing with a portable protocol analyzer may affect the operation of the SS7 network, due to the insertion of signaling messages into the network. Protocol tests should be performed by competent personnel. Before starting any tests obtain authorization from the control center.

Signaling Link Marginal Performance Report (SLMPR)

The purpose of the Signaling Link Marginal Performance Report (SLMPR) is to provide real time signaling link surveillance for the identification of:

- signaling unit errors
- negative acknowledgments.
- automatic changeovers to alternate signaling links

This is achieved by measuring key OMs against preset bogeys and time intervals. The identified faults are recorded by individual link and related OM counts. In real time, when an OM count exceeds the bogey, an alarm and log message CCS198 is generated—providing that parameter C7_SLMPR_ALARM_ON has been set to "Y" in table OFCVAR. The SLMPR CCS198 log report is normally scheduled for hourly printout. SLMPR is present in offices with software package NTX041AB (CCS7 MTP/SCCP).

When SLMPR is in effect, it negates the need to place OMs C7SUERR, C7NACKRX, and C7AUTOCOV in OM thresholding. The backbone of SS7 perfor-

mance and reliability is the maintainability of the node to node signaling link facility, which includes the terminating data port cards and ST terminals. The signaling link portion of the network is trouble prone and accounts for the highest percentage of troubles in an SS7 network. In other common channel signaling systems, the signaling link accounted for 90% of all the troubles.

Use the SLMPR tool for real time SS7 link surveillance. It provides the following indicators—by link—to detect marginal performance and trouble:

SU data is derived from OM C7SUERR (OM Group C7LINK1), a peg count of Message Signal Units (MSUs) that were received in error because the MSU failed the checksum validation. The system tries again by retransmitting the faulty MSU. A 56 Kbps signaling link can transmit approximately 500 Signal Units (SUs), and receive another 500 SUs every second, complete with checksum validation. The signaling link continuously transmits and receives SUs. When the signaling link buffer is empty, a Fill In Signal Unit (FISU) is sent to fill in gaps between useful signaling messages so that link synchronization is maintained.

NACK data is derived from OM C7NACKRX (Group C7LINK1), which counts Negative ACKnowledgments (NACK) received from the adjacent node Signaling Terminal (ST). NACKs indicate the MSU data was corrupt when received and is retransmitted. NACK faults trigger the retransmission of the corrupt MSU, and during peak traffic conditions can contribute to congestion on the linkset.

AUTOCOV data derived from OM C7AUTOCOV (Group C7LINK1), which counts automatic changeovers. This indicates that SUs were diverted away from this signaling link to another because of a fault or congestion (system detected). An automatic changeover is any changeover that is not initiated by manual action.

The following assumptions are made when the SLMPR bogeys are set:

- Signaling links have met their acceptance and stability tests
- The SS7 conversion activity is complete and all known hardware, software, and facility problems have been corrected.
- The system is prone to detection of transient fault events due to the continuous self-checking tests. The bogey becomes the transient fault level, which when exceeded indicates a suspected fault.
- The bogey levels are severely affected by the stability and quality of the data links. For this scenario, assume the links have met BER test criteria.

The SLMPR-suggested bogey settings are:

	ONE HOUR	24 HOUR
SU	20	40
NACK	4	9
AUTOCOV	2	4

NOTE: The suggested bogey settings are for a *clean* network. During conversion or other transitional activity, higher bogey settings may be required.

Log message CCS198—see example below—records the results of the signaling link surveillance data processed by the SLMPR. This is an hourly report. The report can be programmed to record performance data for all links, or only links reaching or exceeding the threshold. This decision is made in table C7LINK.

```
CCS198              Jan 10  19:00:00 2636 INFO
 Signaling Link Marginal Performance Report
 Link  SU              NACK          AUTOCOV
 C7LKSET1 127                        8  3
 C7LKSET1 256                        21*1
 C7LKSET2                            6  1
```

A signaling link alarm can be associated with faults that reach or exceed the bogey thresholds set in the SLMPR, by setting parameter C7_SLMPR_ALARM_ON to "Y" in table OFCVAR. With the parameter set to "Y", when a signaling link reaches the threshold, a minor alarm sounds and the signaling link status changes from INSV to ISTB. Investigating the alarm by executing the QUERYFLT command—against the alarmed link—identifies the specific link that exceeds the SLMPR threshold.

Signaling link faults that extend across the hourly report interval may be included in the following hour's SLMPR report. This scenario can happen when the technician corrects the fault, but in the hour the fault was corrected SLMPR again reached the threshold. Following link repair it is recommended that the technician monitor, at a minimum, the next two hourly reports.

The following is an example of the data recorded in the SLMPR. In this example, the numbers under SU represent the signaling unit errors, the numbers under NACK represent the negative acknowledgments, and the numbers under AUTOCOV represent the changeovers to alternate signaling links. The numbers accompanied by an asterisk (*) are the numbers that have exceeded the threshold that is set in table OFCVAR.

Identifying signaling link faults:

- identify links with trouble indications that appear incidental (just exceeding the threshold and no previous history — include them in subsequent analysis)
- identify link(s) with high or chronic trouble counts previously identified on SLMPRs
- clear trouble investigation activity with the control center and obtain the necessary approval to proceed
- coordinate testing activity with the far-end node, busy out, and deactivate the link at each node

---

- proceed with the MTP BERT test using loopbacks to identify the fault at the near-end, far-end, or data link facility

- if the MTP BERT tests pass, run diagnostics on the MSB7/LIU7 peripheral equipment

- the sectionalization of an intermittent fault may require extended testing intervals

Setting up the SLMPR report

For procedures to set up the SLMPR see NTP 297-YYYY-544, *DMS-100F DMS Trouble Locating and Clearing Procedures*. For a signaling link to be included in the report, option SLMPR must be assigned to the signaling link—datafill field LINKOPT in table C7LINK.

ISUP trunk maintenance & surveillance

ISUP interoffice trunking uses SS7 protocol, which separates the signaling component from the voice and data component of the call. These two components are then carried on two different facilities. The signaling component is carried over the SS7 signaling network using packet switching protocol. The transmission facility used for the voice and data trunk does not change, only the signaling function has been removed from the trunk.

ISUP trunk testing is an SSP function (STPs do not have voice and data trunks). ISUP trunk maintenance involves two components: the message trunk and the SS7 signaling. Most of the existing DMS-100 routine maintenance and surveillance tools used for per-trunk signaling apply to ISUP trunking with SS7 signaling. Following are examples:

- trunk test position (TTP) access

- killer trunk (KT)

- automatic trunk testing (ATT)

- TRKS alarms (MAP alarm banner)

- trunk group status (STAT TRKGRP)

- trunk status (STAT TRKS)

- trunk log messages (C7TU logs)

- ISUP trunk continuity test (ICOT)

- periodic trunk maintenance (PRDTKMTC) report

- SPMS for SS7

Descriptions of all the tools listed above can be found within the *Preventive Maintenance* tab of this manual, except for "SPMS for SS7" which can be found in the *Performance* section of this manual.

Another trunk surveillance indicator is customer trunk troubles that are reported to the TOPS operator. The reports are then input into a switched analysis OSS system. Analyze the various summary output reports to identify poor performance trunk groups for actionable items.

ISUP trunk continuity test (ICOT), a test feature for trunks using SS7 signaling, validates transmission continuity before end to end use by the customer. ICOT is further described under "ISUP trunk continuity test (ICOT)" starting on page 4-191.

The effectiveness of detecting ISUP trunk faults using Focussed Maintenance has diminished due to the reduction in the Per-Trunk Signaling (PTS) trunk log reports. Many of the trunk faults that were counted in Focussed Maintenance were caused by malfunctions in the PTS component. Examples are: partial dial, mutilated digits, time outs, and more than two frequencies detected. Changing the signaling technology from PTS to SS7 negates these troubles and their related log messages.

Trunk calls that cannot be switched to their destination because of network congestion on voice and data trunks, or network signaling blockage are sent to treatment. Generally, this occurs at the originating office. This results in a higher reorder peg count for the originating node.

The voice and data message trunk component of an ISUP trunk is maintained using existing procedures for trunk access, administration, and transmission tests. The same routine trunk maintenance requirements persist: routine trunk transmission tests using the auto trunk tester, killer trunk surveillance, and periodic trunk maintenance report analysis.

Soft fault signaling problems are analyzed using killer trunk (KT), periodic trunk maintenance report (PRDTKMTC) and related trunk log reports. From analysis, determine if reports are isolated or if a visible trouble pattern can be identified. When a signaling trouble pattern has been identified, initiate the necessary testing and surveillance to sectionalize the trouble into the trunk part or SS7 signaling network and initiate remedial action.

Maintenance for the signaling component of the trunk involves two parts: surveillance of individual trunks for signaling faults, and the components that make up the common SS7 signaling network (MSB7/LIU7 equipment, related software, and signaling link facility between nodes).

Sectionalizing signaling faults identified by individual trunks involves a network approach, since hundreds of ISUP trunks pass their signaling information over common equipment and facilities using packet switching technology. The effect of some faults within the SS7 network generates trunk log reports against individual ISUP trunks such as: wrong signaling message, premature release (cutoff), demand continuity check test, and wrong trunk status. Threshold these types of trunk log reports, and set realistic bogeys and time intervals to separate the soft or transient faults from the hard faults. Network failures are generally accompanied by a flare-up of trunk log reports. Reference the "Index of DMS-100 SSP logs" table starting on page 4-181 within this subsection, for suggested thresholding values for C7UP logs.

When alerted by a trunk alarm threshold, observe the CCS alarm conditions and SS7 network status for indications such as: SS7 equipment outages, loss of links, blocked routes, and congestion—that may be causing the flare-up of ISUP trunk alarms. Initiate remedial action, the basic steps are: isolate the fault from the SS7 network, if possible restore service by using spare line facilities, sectionalize trouble to a maintenance responsibility, make repairs, test, return to service, and verify operation. Again, all SS7 network maintenance activity must be cleared with the control center.

The SS7 network also serves as the packet switch media for connectionless signaling (intelligent networking). 800 service, credit card validation service, and Custom Local Area Signaling Service (CLASS). These are examples of intelligent networking services using the SS7 network. Similarly, the signaling functions for the ISDN networking use SS7. These services can generate customer trouble reports that require a trouble investigation scenario similar to the one just described for ISUP trunks.

Trunk Test Position (TTP) access

SS7 trunks are maintained from the TTP, MON, MAN, and C7TTP levels of the MAP. Each of the commands at these levels is available, except for the following cases:

- At all MAP levels, the TST command supports only T100, T101, T102, T104, all T105 tests, T108, TCON, TCOT, and ICOT test lines, as well as trunk circuits
- At the TTP level, the LEVEL command supports access to only the MONitor, MANual and C7TTP sublevels
- At the MONitor sublevel, the CPOS command is not supported
- At the MANual sublevel, the SGNL command is not supported

SPMS (SS7 application)

See the *Performance* section and the "Performance monitoring for SS7" heading for supporting information on SS7 for SPMS.

SEAS Performance Indicators for SS7 Network

Signaling Engineering Administration System (SEAS) for SS7 management is comprised of two parts:

- SEAS Operational Support System (OSS), developed and distributed by Telcordia it operates on the customer's mainframe computer
- STP/SEAS interfaces located at the STP, developed by Nortel Networks to meet Telcordia compliance requirements. See NTP 297-5101-104, *DMS SuperNode STP Interface SEAS Reference Manual*, for SEAS operational descriptions

SEAS is a support system that provides the operating company with a centralized operating center—for administering its SS7 signaling network on a company or regional basis. The SEAS features are evolving in the following areas:

- Engineering
- Service Surveillance and Administration

- Network Management
- Network Maintenance Surveillance
- Recent Changes & Notification

The necessary data to support the SEAS activities is gathered from each STP in real time for alarms, log messages, and operational measurements—on a scheduled or demand basis. SEAS also provides the ability, on demand, to access the Command Interpreter level (CI level) for the selected STP, for SEAS related communication only (cannot reach the MAPCI level). This demand access feature to the DMS-STP is called the flow-through mode.

Figure 4-39 — SEAS Elements
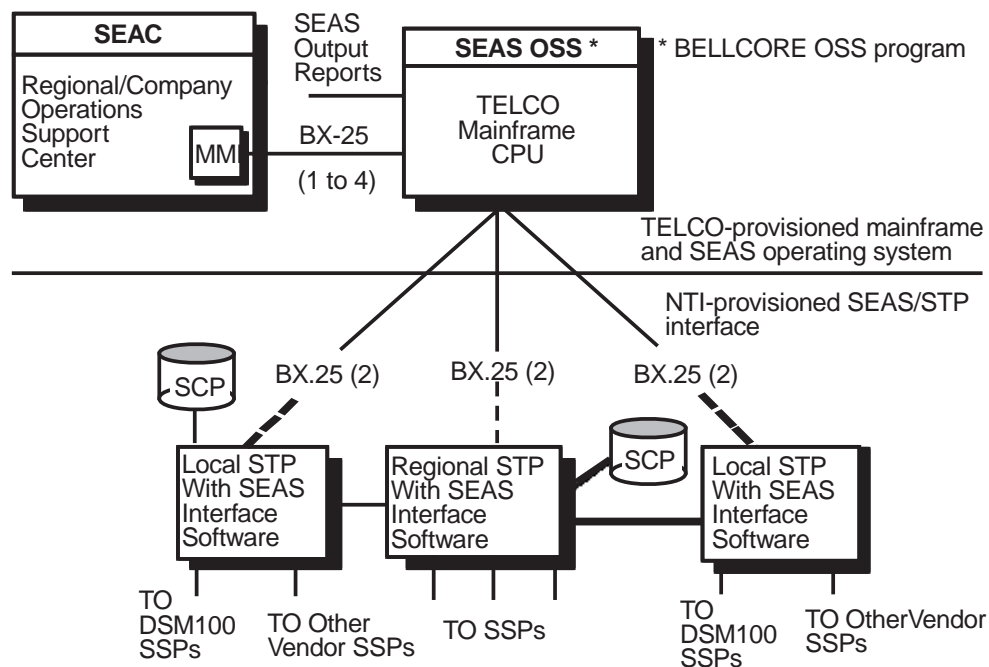
The elements of SEAS (see Figure 4-39) are:

- Each STP is equipped with a DMS-STP SEAS interface (software plus two Multi-Protocol Controllers (MPCs))
- Two X.25 data links between the SEAS mainframe and each STP
- STP activity (DDU storage volumes, office parameters, datafill tables)
- Operating company provided mainframe computer resource for the OSS that drives the SEAS and provides the Signaling Engineering Administration Center (SEAC) man-machine interface
- SEAS OSS software manufactured by Telcordia for the mainframe
- Additional data links and work station(s) when the SEAC is remote from the mainframe.

The input data to drive the SEAS OSS system is derived from each STP that makes up the SS7 signaling network. It involves gathering raw OM data from 53 registers located in six OM groups, and establishing three OM accumulating class assignments in table OMACC. NTP 297-5101-104, *DMS SuperNode STP SEAS Interface Reference Manual*, and NTP 297-YYYY-814, *DMS-100F Operational Measurements* provide the specific assignment and steps for establishing the OM input data for SEAS. See the "Operational Measurements" subsection within the *Preventive Maintenance* tab of this manual for specific details on the SEAS OM classes and customized register assignments.

Along with OM data, selected DMS-STP log reports are forwarded to the SEAS OSS system as follows:

- global-title-translation failure (see table C7GTWLKS for related log thresholding criteria)
- processor outage, alerting network management and maintenance personnel that a node adjacent to the DMS-STP is experiencing a processor outage
- termination of processor outage
- link set outage, informing network management and maintenance personnel that a link set is unavailable due to multiple link failures or a processor outage
- recovery from link set outage
- link congestion level increase, alerting maintenance personnel that congestion in a DMS-STP link transmission buffer has passed a preset threshold
- recovery from link congestion level increase
- near-end link management inhibit/uninhibit, providing reports on the status of DMS-STP Permanent Virtual Circuit (PVC) links

Equal access and CCS7

The Equal Access (EA) network links subscribers to the InterLATA and International Carriers (ICs), as selected on a per-call basis or through presubscription. Initially, EA used Multifrequency (MF) signaling; however, with the deployment of CCS7, CCS Access Capability (CCSAC) was offered. CCSAC provides interconnection to the switched network using CCS7 signaling with ISUP trunking. Software package NTXE13AA, CCS7 ISUP InterLATA connection EAEO (Equal Access End-office), provides this capability with the DMS-100F EO switch. NTXE14AA is the equivalent package for the DMS-100F Access Tandem (AT) switch

The following is a list of items to be aware of when implementing or troubleshooting EA with CCS7 in a DMS-100F office:

EA translation tables

Table CKTDIGIT has been added for EA within the end-office (EO) and access tandem (AT) office. Table OCCINFO, as well as many other existing tables, have changes when implementing EA with CCS7. See NTP 297-YYYY-350, *DMS-100F Translation Guide* for details and examples on datafilling both the EO and AT offices.

Protocol addition

An EXM (Exit Message) is sent from the AT to the EO when an EO to IC is via an AT office. This message from the AT to the EO provides the AT to IC Trunk Group Number and the carrier connect time and date.

Log messages

The DFIL122 log indicates missing datafill in the CKTDIGIT table. Logs DFIL145, 146, and 147 indicate problems with three and four digit Circuit Identification Codes (CICs). Be aware that C7UP102 log has an indication for EXM protocol problems.

Engineering parameters

The following parameters are associated with equal access:

- Parameter ISUP_SUBGRP_GLARE_AVAILABLE in the OFCOPT table, has to be set to "Y" for the subgroup yield method to work for IC trunk groups.
- If an equal access EO directly accesses an IC, then parameter ISUP_EAEO_DIRECT_ACCESS in table OFCOPT needs to be set to "Y".
- For those companies that have equal access with eight and 10 party Circle Digit (CD) dialing, the EA_WITH_CD parameter in the OFCENG table needs to be set to "Y" if the CD customers are allowed to dial 10XXX+direct dial calls. Also see parameter SPDD_DIGIT for setting of the CD for single party, two party, and four party lines.
- For those offices converting to, or using three and four digit CICs, then parameters EA_FOUR_DIGIT_CIC_STATUS and EA_TAB_CICSIZE4_OBSOLETE in table OFCENG, needs to be set according to individual office needs.
- The following additional parameters need to be set for equal access:
  - EA_TEST_CALL_SPILL (Table OFCVAR)
  - EA_OCS_AND_DP_OVLP_NEEDED (Table OFCENG)
  - EA_OCS_DIGCOL_METHODS (Table OFCENG)
  - EA_OVERLAP_CARRIER_SELECTION (Table OFCENG)
  - DEFAULT_CARRIER_OR_TREATMENT (Table OFCENG)
  - EA_LATANAME_IN_SERVORD (Table OFCOPT)
  - EA_REC_2ND_PRE_WK_TIME (Table OFCSTD)
  - EA_REC_1ST_PRE_WK_TIME (Table OFCSTD)

For details and supporting references for parameters, see NTP 297-YYYY-855, *DMS-100F Parameters Reference Manual.*

Glare detection for ICs

Glare detection for ICs is set within the TRKSGRP table for the IC trunk group by setting the SGRYLD and GLAREYLD tuples. Determine your company policy before setting. Reference NTP 297-YYYY-350, *DMS-100F Translations Guide* for details on the TRKSGRP table glare options.

Glare verification

Use the C7TTP level on the MAP and the CVTEST command to verify that the glare feature is properly datafilled for the IC trunk groups. See NTP 297-1001-531, *DMS-100F CCS7 Maintenance Reference Manual*, for detailed information on this test.

OM additions for equal access

OM registers were added in OM groups ISUPCGRP and ISUPUSAGE for equal access measurements. The ISCKTRAE register in the ISUPCGRP OM group counts the EXM time-outs in the equal access EO—time-out occurs when the EXM message is not received from the AT.

Equal access maintenance

For information about equal access maintenance, see NTP 297-2101-500, *DMS-100F Equal Access Maintenance Guide.*

ADJNODE table

Table ADJNODE (Adjacent Node) permits access to information regarding the type of software running in the adjacent node. Initially, documented information indicated that anytime an adjacent node updated to a new software that the ADJNODE table had to also be updated. In BCS34 the ADJNODE table was enhanced to clarify the meaning of the ADJNODE fields to help eliminate the possibility of the table being datafilled incorrectly, which could lead to network services not working between DMS nodes.

Table ADJNODE must be datafilled before tables TRKSGRP, ISUPDEST, TRK-MEM, CRTRKMEM, and after table TRKGRP. If an attempt is made to datafill the ADJNODE field of table TRKSGRP with a value that has not been entered in table ADJNODE, the entry is not allowed. Whatever name is given to the adjacent node will be used by table TRKSGRP.

It is recommended that the ADJNODE table be datafilled according to NTP 297-YYYY-350, *DMS-100 Translation Guide*.

ADJNODE restriction

Beware when datafilling the PRODUCT field with BELLCORESTD. The near-end node assumes that the far-end node can accept any protocol messaging if it complies to the Telcordia set of applicable standards. A situation can arise when the near-end complies with the latest version of a standard, and the far-end node complies with an earlier version of the same standard (i.e., the near-end node has an older software load than the far-end node). If a backwards incompatibility exists in transition from the old to the new standards version, a corresponding incompatibility could result in messaging between the two nodes. The operating company should administer their network with this potential problem in mind. One solution to potential incompatibility problems is to administer the ADJNODE table with the specific product type in the PRODUCT field, and then use the OPTIONS field to apply the applicable capabilities for the far-end node. Any backward incompatibility could then be controlled.

ENET Overview and Maintenance

ENET Overview

The SuperNode Enhanced Network (ENET) is a channel-matrix time switch that provides pulse code modulated voice and data connections between peripheral modules, and message paths to the DMS-bus components. The ENET is a single stage, non-blocking, junctorless time switch that provides a constant delay through the network. ENET replaces the current junctored network subsystems (i.e., DSNE, NT0X48).

ENET supports services requiring bandwidths greater than 64 Kbps. The architecture to support high-speed data services requires that ENET meet a low bit error rate standard of 10 to the minus 12th power ($1x10^{-12}$).

Functional systems of ENET

The ENET is composed of the following functional systems and supporting circuit cards:

- Processor and memory
    - NT9X13 Central Processing Unit (CPU)
    - NT9X26 Reset Terminal Interface (RTIF) paddle-board
- Clock and messaging
    - NT9X36 clock and message card
    - NT9X40 quad DS-512 fiber interface paddle-board
- Crosspoint
    - NT9X35 crosspoint circuit cards
- Transmission and interface
    - NT9X40 DS-512 fiber interface paddle-boards
    - NT9X41 DS-30 fiber interface paddle-boards
- Power
    - NT9X30 +5 volt, 80 amp power converter cards
    - NT9X31 -5 volt, 20 amp power converter cards

For a detailed description of the ENET circuit packs, see NTP 297-8991-805, *DMS-100F Hardware Reference Manuals.* For those that want more information on ENET circuit packs, see PLN 8991-104, *Provisioning Guides.*

ENET is housed in a standard DMS SuperNode cabinet with forced air ventilation. See the following figure for a general overview of the ENET location within the DMS SuperNode architecture.

Figure 4-40   —   Overview of the Enhanced Network (ENET) System within SuperNode
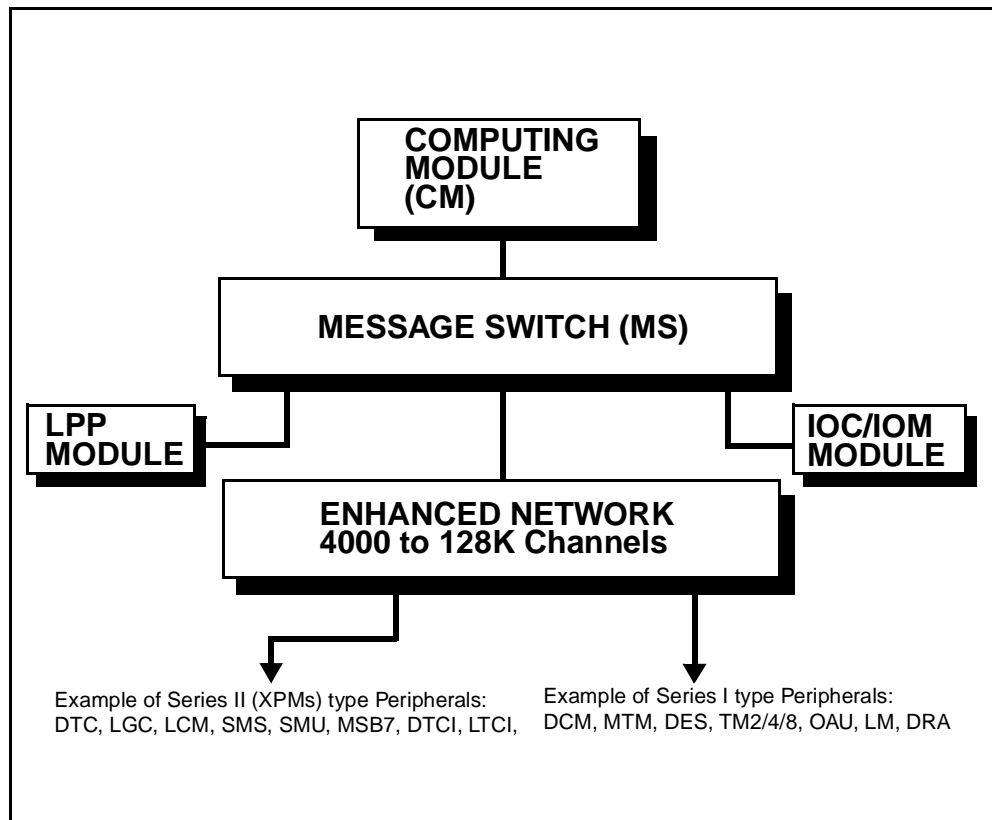
Peripherals

Series I peripherals interface the ENET using existing copper speech link cable group arrangements.

Series II peripherals (XPMs) interface the ENET using fiber speech links and require modification during an upgrade. The exception is the MSB7 and SMS modules that interfaces the ENET using copper speech links only.

ENET retrofit (upgrade)

An Enhanced Network (ENET) retrofit is the replacement of a Junctor Network Module within an inservice DMS SuperNode. The retrofit kits and rules are defined in PLN 8991-104, *Provisioning Guides.*

32K ENET

Higher Capacity ENET in NA006.

This software supports as hardware baseline the 16 megabytes of random access memory (RAM) first offered for ENET in NA004. The larger memory enables ENET to support all robustness and service features now available for the DMS SuperNode system, reducing the overall cost of ownership, while offering new revenue opportunities.

NOTE: The 16-megabyte ENET processor (NT9X13KA) is required for the ENET in the NA006 load and later.

New 32K ENET for DMS SuperNode SE in NA006.

This enhancement raises the limit on ENET channels for the DMS SuperNode SE and the Single Cabinet ENET to 32,000 channels (from the previous maximum of 16,000 channels). This permits greater flexibility and cost-effectiveness in configuring peripherals, lines, and trunks at DMS SuperNode SE offices.

NOTE: Engineering processes for the 32K ENET for the DMS SuperNode SE and Single Cabinet ENET became available in 4Q97.

Figure 4-41 — SN system architecture
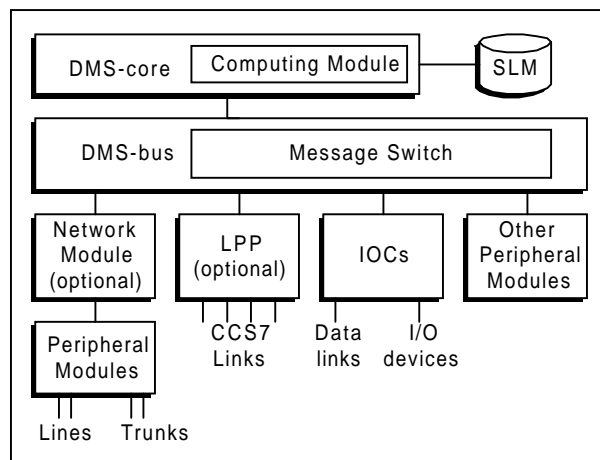
SuperNode SE

The DMS SuperNode SE (Small Exchange) is a single cabinet switch that provides the full range of DMS SuperNode features and services. The compact architecture supports at least 20,000 lines in typical applications. The SNSE is equipped with a 16K ENET—sometimes referred to as ENET16K—that features both planes on one shelf. The ENET16K architectural differences from the ENET require that the commands for the ENET MAP level and the ENINV table be modified.

The SuperNode SE switch can be configured with a 16K or a 32K enhanced network (ENET) and CCS7 link interface units (LIU7). The SuperNode switch can also be configured with a 64K or a 128K enhanced network (ENET). The ENET provides voice and data signal switching for nodes in the SuperNode SE switch and provides message routes to the MS.

The LIU7 provides CCS7 message processing.

Figure 4-42   —   SNSE system architecture
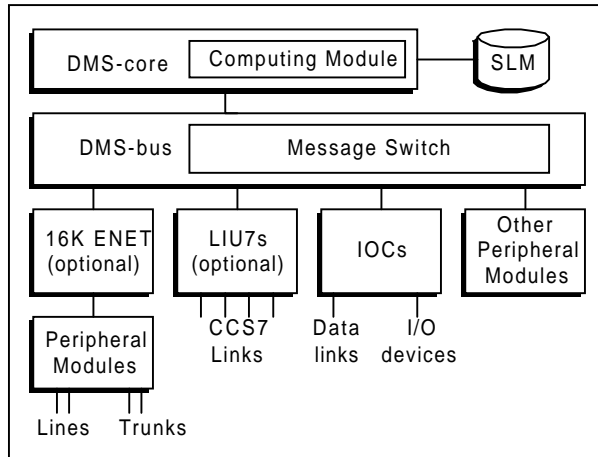
ENET software

NTXE01AA (Enhanced Network Switching Matrix Subsystem) is the software package required for all ENET operations. NTXF71AA (SuperNode Enhanced Messaging) is a prerequisite for this package.

Software package NTXP13AA (ENET Switch Path Diagnostics) enhances ENET maintenance by providing the ENET Integrity Check Traffic Simulator (EICTS) certification and Enhanced Network Fabric (ENETFAB) test capabilities for the ENET system. See "ENET maintenance tools" on page 4-238 for further information on EICTS and ENETFAB.

Datafill for ENET

The data tables that must be datafilled for an office equipped with an ENET are:

- Table MSCDINV (Message Switch Cards Inventory)
- Table PMLOADS (Peripheral Module Loads)
- Table ENCDINV (Enhanced Network Card Inventory)
- Table ENINV (Enhanced Network Node Inventory)

See NTP 297-YYYY-350, *DMS-100F Translation Guide* for the variables and options to datafill the tables for ENET.

ENET maintenance

The following topics summarize ENET maintenance and the supporting documentation that provides the necessary procedures to complete maintenance related tasks. The following areas are presented:

- ENET documentation
- ENET office parameters
- ENET logs
- ENET OMs
- ENET alarms
- ENET trouble locating and clearing procedures
- ENET recovery procedures
- ENET routine maintenance procedures
- ENET maintenance tools

ENET documentation

Prior to the evolution to PCL documents, ENET maintenance related documentation included several NTPs. With PCL, NTP 297-1001-591, *DMS-100F Network Maintenance* is the single source document to reference for ENET maintenance—some procedural type information is included in various other NTPs.

ENET office parameters

The office parameters associated with ENET are listed in the following table. The detailed information on any office parameter can be found in NTP 297-YYYY-855, *DMS-100F Office Parameter Reference Manual.*

Table 4-21 — ENET office parameters

Parameter name	Default values	Table	Activation
ENET_MAX_CHANNEL_GROUP	0	OFCOPT	immediate
ENET_AVAILABLE	N	OFCOPT	immediate

Parameter name	Default values	Table	Activation
NETFAB_DAILY_DURATION	4	OFCVAR	immediate
NETFAB_SCHEDULE_ENABLED	Y	OFCVAR	immediate
NETFAB_SCHEDULE_TIME	2	OFCVAR	immediate
NETWORK_ACTIVE	JNET	OFCOPT	immediate

NOTES:

1. Office parameter ENET_AVAILABLE must be set to Y before tables ENINV and ENCDINV can be datafilled, and the ENET MAP level can be entered.

2. The NETFAB (Network Fabric) office parameters—originally used with junctor networks—is also used with ENET. See ENET maintenance tools on Page 4-238 in this subsection, for further information on network fabric testing.

3. The NETFAB_DAILY_DURATION parameter provides the flexibility to run a test from one to four hours duration. The complete test takes over 10 hours which means running a minimum of three—four hour—nightly runs.

ENET logs

Following is a list of logs related to ENET—ECTS logs are described in "ENET integrity check traffic simulator (EICTS)" starting on Page 4-247. At the end of the list is an ENET log to ENET OM register association table that can be used as a maintenance reference.

Remember that for maintenance troubleshooting and fault analysis, logs run at a lower priority background level, while OMs count events at call-processing levels as the events occur. Even though the OM and log report software run at different priorities, the indirect association of the logs and OMs can help you analyze ENET performance.

ENET (Enhanced Network) logs are generated by a subsystem that provides information about computing module enhanced network maintenance. Most of the ENET3XX logs and the ENET700 log include the DS-30 equivalent pertaining to fiber links.

Most of the following ENET logs have been grouped into categories for quick reference:

ENET node logs

- ENET100 (MANB or SYSB to OK)
- ENET101 (OK to MANB)
- ENET102 (CBSY, SYSB, or OFFL to MANB)

- ENET103 (OK to SYSB)
- ENET104 (CBSY to SYSB)
- ENET105 (OK, MANB, or SYSB to CBSY)
- ENET106 (MANB or UNEQ to OFFL)
- ENET107 (OFFL to UNEQ)
- ENET108 (IsTb set or cleared)
- ENET110 (Node passed testing)
- ENET111 (Node failed testing)
- ENET700 (see "ENET other logs" below)

ENET system logs

- ENET112 (System RTS has failed)
- ENET100 (System RTS has passed)
- ENET114 (Parallel system recovery indication)

ENET REX test logs

- ENET120 (REX test error with BOOT file)
- ENET500 (REX test has been modified)
- ENET502 (REX test could not be performed)
- ENET503 (REX test has begun)
- ENET504 (REX test has passed)
- ENET505 (REX test has failed)
- ENET506 (REX test has been aborted)
- ENET507 (REX test incomplete because of error)
- ENET508 (REX test has passed)
- ENET510 (REX test started but stopped for reasons stated)
- ENET511 (REX test on a shelf has passed)
- ENET512 (REX test on a shelf has passed or failed with IsTb)
- ENET520 (REX matrix test started but stopped for reasons stated)
- ENET521 (REX matrix test has passed)
- ENET522 (REX matrix test has passed or failed with IsTb)

ENET card logs

- ENET200 (MANB or SYSB to OK)
- ENET201 (OK to MANB)

- ENET202 (CBSY, SYSB, or OFFL to MANB)
- ENET203 (OK to SYSB)
- ENET204 (CBSY to SYSB)
- ENET205 (OK, MANB, or SYSB to CBSY)
- ENET206 (MANB or UNEQ to OFFL)
- ENET207 (OFFL to UNEQ)
- ENET208 (IsTb set or cleared)
- ENET210 (Card passed testing)
- ENET211 (Card failed testing)
- ENET222 (Card fault(s) when node RTS)
- ENET230 (Crosspoint or interface card in wrong state)

ENET matrix logs

- ENET220 (Matrix passed testing)
- ENET201 (Matrix failed testing)

ENET peripheral-side link logs

- ENET300 (MANB or SYSB to OK)
- ENET301 (OK to MANB)
- ENET302 (CBSY, SYSB, or OFFL to MANB)
- ENET303 (OK to SYSB)
- ENET304 (CBSY to SYSB)
- ENET305 (OK, MANB, or SYSB to CBSY)
- ENET306 (MANB or UNEQ to OFFL)
- ENET307 (OFFL to UNEQ)
- ENET308 (IsTb set or cleared)
- ENET309 (OK, MANB, SYSB, or CBSY to peripheral-side busy)
- ENET310 (Peripheral-side (P-side) passed testing)
- ENET311 (Peripheral-side (P-side) and NETDIAG Control-side (C-side) hardware failed testing)

ENET control-side link logs

- ENET400 (Control-side (C-side) link fault)
- ENET401 (Control-side (C-side) link failed testing)
- ENET402 (Control-side (C-side) audit report)

ENET BERT logs

- ENET600 (BERT manual test started)
- ENET601 (BERT has completed)
- ENET602 (BERT has manually stopped)
- ENET603 (BERT has been aborted

ENET other logs

- ENET312 (PM message path switched from one link to another)
- ENET313 (Denied message path switching because of too many recent failures)
- ENET314 (Peripheral-side (P-side) link audit report)
- ENET315 (Peripheral-side (P-side) maintenance fault has been changed)
- ENET403 (Report of manual switch of reference links or by the system switch audit)
- ENET700 (This log is generated whenever a warning is issued, or should be issued by any of BSY, RTS, TST, OFFL, ABTK, LOADEN, LOADENALL, or ALARM commands. If the user uses the NOPROMPT option, the warning will not be issued at the MAP, but the ENET700 log is generated).

ENCP logs

ENCP (Enhanced Network Call Processing) logs are generated from a subsystem that controls processes involved in setting up connections between calling and called parties in ENET.

For the ENCP100 through ENCP105 logs, see "ENET integrity" later within this subsection.

ENCP131 indicates an ENET connection has been created that has overwritten an existing connection.

ENCP132 indicates an ENET connection has been created that has attempted to overwrite an existing connection.

ENCP133 indicates an ENET connection log audit has been performed. If the ENET connection control log is turned off, this log reports the number of logs that were not printed.

ENCP134 indicates an attempt has been made to reserve a previously created ENET path that is not connected in the hardware.

ENCP135 indicates an attempt has been made to reverse an ENET path that cannot be reversed.

ENCP136 indicates an attempt has been made to create an ENET connection for which the hardware is out-of-service in both planes.

ENCP143 indicates a discrepancy has been detected between connection control tables, specifically the nailed-up connection map and the connection map.

ENCP150 indicates a connection has been freed; however, there is a discrepancy between the stored information defining the freed connection and the physically freed connection.

For more detailed information on ENET logs and any action needed to be taken, see NTP 297-YYYY-840, *DMS-100F Log Report Reference Manual*.

ENET OMs

The following ENET Operational Measurement (OM) groups support ENET:

- ENETMAT (ENET matrix card group)
- ENETOCC (ENET CPU occupancy group)
- ENETPLNK (ENET peripheral-side link group)
- ENETSYS (ENET system card group).

Three of the ENET OM groups have several registers listed in the ENET OM to log association—see Table 4-22 on page 4-235. For detailed information on ENET OM registers and their relationship to the ENET log reports, see NTP 297-YYYY-814, *DMS-100F Operational Measurements Reference Guide.*

ENET alarms

ENET alarms are received, analyzed, and cleared from the MAP. Fault conditions in the ENET generate alarm codes that appear under the Net header of the MAP display. See Figure 4-43 on page 4-237 for an example of an ENET MAP display, and a list of alarm codes by priority.

To get to the ENET MAP level from CI, type MAPCI;MTC;NET. In place of typing in NET, you can also use ENET. In either case, you access the ENET level; however, the MAP level displays the NET above the command list instead of ENET. Also, other ENET displayed information on the MAP lets you know you are in ENET.

ENET trouble locating and clearing procedures

Alarm related ENET problems have procedures defined for finding and clearing the alarms in NTP 297-YYYY-543, 546, and 547 documents—for PCL loads and higher. Trouble isolation and correction procedures for ENET can be found in NTP 297-1001-591, *DMS-100F Network Maintenance.*

Problems that are related to ENET logs require the use of the "action to take" information in the log manual, and use of ENET related maintenance tools to locate and clear problems. Other problems related to bit error (data) reports from logs as well as customers require the use of the ENET maintenance tools to locate and clear problems. See "ENET maintenance tools" on Page 4-238 in this subsection.

A problem that may not generate an alarm could involve office parameters or datafill for the ENET tables. Verification for the correct office parameter values should be part of the trouble locating and clearing steps before verifying datafill for the ENET tables. Incorrect datafill for ENET tables could cause ENET not to recover after a system failure.

Table 4-22 — ENET OM to log association table

OM group	Register	Associated log
ENETMAT	ENCDERR ENMBCDU ENMBPBU ENMCDISO ENMCDPAR ENMPBISO ENMPBPAR ENOFCDU ENPBERR ENSBCDU ENSBPBU ENSCDISO ENSCDPAR ENSPBISO ENSPBPAR ENCDFLT ENPBFLT	ENET208 ENET201, ENET202 ENET201, ENET202 ENET201 ENET201 ENET201 ENET201 ENET206 ENET208 ENET203, ENET204 ENET203, ENET204 ENET203 ENET203 ENET203 ENET203 ENET203 ENET203
ENETPLNK	ENLKERR ENMBLKU ENMLKISO ENMLKPAR ENSBLKU ENSLKISO ENSLKPAR ENSPCHER ENLKFLT	ENET308 ENET301, ENET302 ENET301 ENET301 ENET303, ENET304 ENET303 ENET303 ENCP100, ENCP100, ENCP102 ENET303
ENETSYS	ENCALDND ENERR ENMBU ENMISOP ENMPARP ENSBU ENSISOP ENSPARP	ENCP136 ENET108 ENET101, ENET102 ENET101 ENET101 ENET103, ENET104 ENET103 ENET103

ENET recovery procedures

Two events that trigger an ENET system recovery are:

- a power outage

- a restart of the DMS core.

As stated previously, it is important that the ENET tables datafill is verified and corrected. The ENET system recovery will not be successful if the load file stored in table ENINV cannot be accessed for some reason. See NTP 297-YYYY-545, *DMS-100 Recovery Procedures* for ENET recovery procedures.

Figure 4-43 — ENET MAP display, including alarm codes

Alarm Class	Alarm Code	Description
Critical	Shiv	An ENET shelf is out-of-service
	CDpr	An ENET crosspoint card slot is out-of-service in both planes.
Major	CBsy	An ENET node is control-side busy.
	SBsy	An ENET node is system busy.
	SBCd	A non.system card is system busy.
Minor	MBsy	An ENET node is manual busy.
	MBcd	A nonsystem card is manual busy.
	CSlk	A control-side link is out-of-service.
	PSlk	A peripheral-side link is out-of-service.
	REx	An ENET routine exercise has been disabled.
Noalm	Istb	An ENET component has trouble, but is still in service.
	RExOff	A scheduled routine exercise has been disabled

```
         CM   MS   IOD   Net   PM   CCS   Lns      Trks       Ext   APPL
          .    .    .     .    .    .     .         .          .     .
  ENET
     0   Quit      ENET    System  Matrix   Shelf  0  1  2  3
     2             Plane 0   .       .             .  .  .  .
     3   QueryEN   Plane 1   .       .             .  .  .  .
     4   Locate
     5   Deload    ENET:
     6
     7
     8
     9
    10
    11   RExTst_
    12   BERT                         ┌─────────────────────────┐
    13   Integ                        │    Hidden Commands       │
    14   Pathtest                     │    ALARMCONNLOG          │
    15   System                       │    CPUDISP               │
    16   Matrix                       │    FINDSTATEENCLOCK      │
    17   Shelf_                        │    LOGFORMATMEMORY       │
    18                                 │    QUERYREXSHOWBLOC      │
         LV903                         │    ZOOM                  │
    Time 08:16 >                       └─────────────────────────┘
```

ENET routine maintenance procedures

Routine maintenance procedures are listed in NTP 297-YYYY-546, *DMS-100F Routine Maintenance Procedures*, which includes:

- preventing a dust buildup in an ENET cabinet
- replacing a cooling fan in an ENET cabinet
- returning a card assembly in Canada
- returning a card assembly in the United States
- taking an ENET image to an SLM disk
- testing power converter voltages
- testing wrist strap grounding cords

ENET maintenance tools

ENET uses the same maintenance tools (listed below) that were designed for the junctor networks; however, some of the MAP level menus have different names based upon the ENET architecture, and some of the commands have been moved on the various MAP levels. New BERT logs, BERT600 through BERT603, have been added, and the ICTS100 through ICTS105 logs are now ECTS100 through ECTS105 for ENET.

The following maintenance tools are used to diagnose faults in the junctor networks and the Enhanced Network (ENET):

- ENET Integrity
- ENET Pathtest
- Bit Error Rate Test (BERT)
- ENET Integrity Check Traffic Simulator (EICTS)
- ENET Fabric (ENETFAB)

Following is a summary of the maintenance tools and their application for ENET. It is recommended that the "Network Maintenance" subsection within the *Preventive Maintenance* tab be reviewed for maintenance tool processes, and a description of integrity and parity.

ENET Integrity

The Integrity (INTEG) MAP level is used to analyze errors that can occur along the speech links between Peripheral Modules (PMs) and the ENET. The integrity errors are reported through the following "information only" ENCP type logs.

An ENCP100 log is generated whenever an integrity fault is reported, and the connection has not been taken down. Both path ends of the connection are known, and the ENET hardware is checked to see that the connection is made. There are two possible formats for the ENCP100 log, one is for a path originated from the ENET Integrity Check Traffic Simulator (EICTS) and the other for a non-EICTS path.

When diagnosing faulty equipment, watch the plane, pair, slot, link, channel, peripheral module, active units, and terminal data in the ENCP100 log for reoccurrences. If the same piece of hardware keeps reappearing, run further tests on that equipment only.

If the "Diagnostics Submitted" field reads YES in the ENCP100 log, then further data has been submitted to the integrity buffer. See the "ENET Pathtest maintenance tool" on Page 4-242 in this subsection for further information on using buffer data for testing.

An ENCP101 log is generated whenever a peripheral module reports an integrity mismatch for a connection that has been terminated when the Integrity Fault Handler began its analysis of the report. Only one path end of the connection is known.

Compare ENCP101 and ENCP102 logs for a pattern to see if the sending (FROM) or receiving (TO) PM has appeared several times. Track the plane, ENET, card, link, and channel numbers in the ENCP101 logs for similarities. If the same piece of equipment, or connected pieces of equipment, appear in several ENCP101 logs over a period of time, use the ENCP102 log in conjunction with the ENCP101 logs to diagnose single-ended hits. Then watch for constant reoccurrences and similarities to narrow down the suspected hardware.

An ENCP102 log is generated after a diagnostic (i.e., a pathtest has run and lists the results of the test). Both path ends of the connection are known (that is, the sending and receiving end), and the ENET hardware has been checked to see that the connection is made. Diagnostics have been run on the faulty path. Save this information for future use in building patterns on intermittent problems. In BCS35, the amount of ENCP102 logs was *reduced* by not submitting a path test for trunks. The path test on a trunk is always aborted since the channel is reserved.

An ENCP103 log is generated each morning at 8:00 a.m. after an Integrity Fault Audit is run. It provides a summary of the number of integrity fault reports for the DMS switch, each ENET plane, and each ENET network. It also provides a list of all cards that have an excess of integrity faults and have been placed In-Service Trouble (IsTb). Pattern the hardware information list and set up maintenance tests using the commands on the PATHTEST and BERT levels.

An ENCP104 log is generated whenever a manual request is made to clear the counters. Use this as information for determining overall failures for the different ENETs and planes.

An ENCP105 log indicates the values of the integrity thresholds, PM thresholds, ENET integrity logs, or that ENET integrity audits have been changed.

ENET integrity MAP level
Access the INTEG MAP level at the CI by typing MAPCI;MTC;NET;INTEG, or choosing 13 on the Net MAP level.

Figure 4-44 is an example of the integrity (INTEG) MAP level display. Also included is a list of the INTEG level menu commands and a brief description of their use.

The FILTER command is used to *query* the integrity and parity threshold values or *alter* the parity. This throttling level determines the number of errors (faults) that are required in a ten second interval to invoke corrective activity by the PM (e.g., transfer to the other network plane and initiate diagnostics). Reducing the threshold value increases the trouble identification sensitivity, stimulating the need for trouble repair activity. As the parity error faults are cleared out of the networks and associated equipment, NET logs are reduced and service should improve. It is recommended to continue throttling the parity error threshold level until the lowest parity error rate is achieved, possibly one.

Field experience in the past has proven that changing the integrity value was of no help for improving networks, and in some cases when it was changed, caused unnecessary indications of problems that were not service affecting. Because of potential service problems with integrity parameter settings and related commands, the following steps were taken:

- in BCS33 the XPM_INTEGRITY_FILTER parameter in the OFCSTD table was removed
- integrity was set to a fixed value of 12 (previous default value for XPM_INTEGRITY_FILTER parameter that was removed)
- in BCS35 the hidden command SETINTEG was removed
- the capability to change the integrity value with the use of the FILTER command was removed in BCS35

Parity value settings using the FILTER command and the XPM_PARITY_THRESHOLD parameter will continue to be used for high-speed data certification, and should be used by companies to keep networks clear of problems.

Besides the changes with the FILTER and SETINTEG commands, changes to other ENET level commands and associated logs were made in BCS35 to enhance the ENET integrity fault handler and integrity user interface features. Enhancements to the ANALYZE and DISPLAY commands as well as the renaming of the CAPTURECCB to DISPCCB have been made. Log's ENCP100, ENCP101, and ENCP102 have been modified for display information and results.

For further details on the use of commands and supporting response examples for the INTEG level, see NTP 297-1001-591, *DMS-100F Networks Maintenance Guide.*

Figure 4-44 — INTEG level commands

```
        CM    MS     IOD    Net     PM    CCS    Lns    Trks    Ext    APPL
         .     .      .      .       .     .      .      .       .      .
INTEG
 0  Quit     ENET         System       Matrix      Shelf  0  1  2  3
 2                Plane 0        .            .            .  .  .  .
 3                Plane 1        .            .            .  .  .  .
 4
 5  Display_     Audit:   ON    Audit   time:  12:30   INTEGRITY  Logs:  ON
 6  Analyse_
 7  PMS_         INTEG:
 8  Filter_
 9   Thresh
10
11  Clear_
12
13
14
15
16  Logs_
17  Audit_
18  DispCCB
MAP 3
Time 17:41 >
```

INTEG level menu commands

Command	Description
ANALYZE	Analyzes and displays integrity statistics.
AUDIT	Turns the integrity audit on and off, and controls when it runs
CLEAR	Resets the integrity counters to zero, and empties the integrity path buffer
DISPLAY	Displays the integrity fault counters, or the path buffer contents.
DispCCB	Use to print the call condense block (CCB) info for the specified call.
FILTER	Queries the value of the XPM integrity and parity thresholds, and sets the value of the XPM parity threshold.
THRESH	Use to update, reset, or query the integrity count thresholds.
PMS	Displays the counts of the integrity faults on the PM ports connected to the ENET ports.
LOGS	Turns integrity logs on and off.

INTEG level non-menu level commands

Command	Description
CCBCAPTURE	Prints the CCB information for the call you specify.
SETINTG	Sets the value of XPM integrity thresholds.
THRESH	Updates resets, or queries the threshold values for crosspoint cards.

ENET Pathtest

The PATHTEST MAP level provides a means of performing fault isolation and integrity verification on the ENET components of a speech path.

Fault isolation is accomplished by running a path test along a one-way path through the ENET switching matrix.

If errors are detected during the run time of the test, a list of suspected faulty hardware is returned with the test results. These cards may be replaced, and the path test run again until it passes.

Path tests are generally run in response to the following problem indicators:

- integrity faults, indicated by the ENET integrity auditor. Path tests can be used to pinpoint the source of the integrity error, using information directly from the integrity buffer

- errors detected during the running of a network bit error rate test (BERT). A path test can determine if a faulty network component is the source of the error, using information directly from one of the BERT buffers

- any other user detected or system indicated suspect paths in the ENET switching matrix

The essential form of a path test is the insertion of data at an input point of the ENET switching matrix, and checking the integrity of the data that is returned at an output point. The input and output points are on ENLT link interface paddle-boards. The Pulse Code Modulation (PCM) channels used by the test are specified in the test definition.

The type of path over which the test data travels during the duration of the test is user definable. A path test may be used to test a connection through the ENET switching matrix, a connection through a peripheral module attached to the ENET, or both.

NOTE: The connection established by all types of path tests is a one-way connection; no looping back of the test data is performed. A two-way connection requires the use of another path within the switching matrix, making use of additional hardware components. This is not a supported option for an ENET path test.

Three types of path test are available for definition. These are listed below:

- NET — the internal network test option
- PSIDE — the ENET interface P-side test option
- LOOP — the ENET interface loop test option

NOTE: You may define and submit path tests that use the same path simultaneously. These tests are automatically placed in a queue and run sequentially.

NET test option

Use the NET test option to test a single one-way path through the ENET switching matrix. As illustrated in Table 4-45, this test inserts test data at a user specified originating end-point (F), and extracts this data at a terminating end-point (T). These end-points, or path tests, define a path through the ENET switching matrix

Figure 4-45 — NET test option

Crosspoint matrix

Insert data F

Test path

T
Extract data
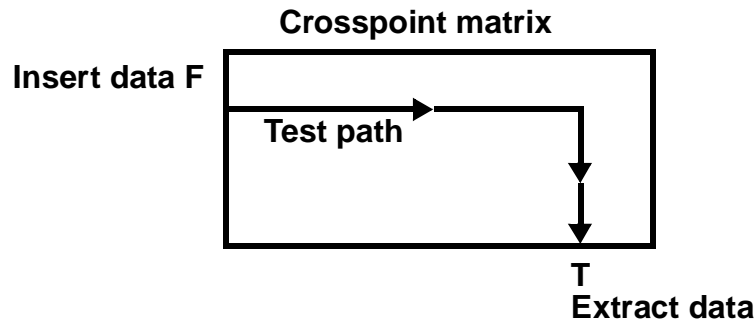
PSIDE test option

Use the PSIDE test option to establish a test path that travels over a link from an originating end-point on a link interface paddle-board, through a peripheral module with an XMS-based processor (XPM), and back over a link to the originating point.

As illustrated in Figure 4-46, this test inserts test data at a user-specified originating end-point (F). The data travels on the links to a peripheral module, and is returned for extraction on to the same point (F).

Figure 4-46   —   PSIDE test option

Crosspoint matrix

Test path   F

Insert data &
extract data

XMS-based peripheral
module (XPM)
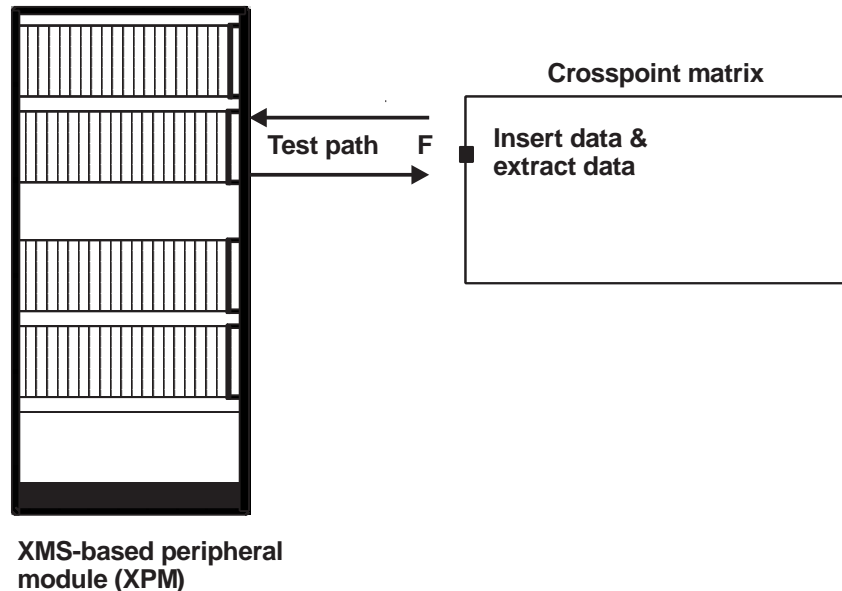
LOOP test option

Use the LOOP test option to test a complete one-way path, as monitored by the integrity auditor. This test includes both the path through the ENET switching matrix and the links through a peripheral module with an XMS-based processor.

As illustrated in Figure 4-47, this test inserts test data at a user specified originating end-point (F). The test data travels a path through the switching matrix, and is then inserted onto the links to a peripheral module, and returned for extraction at a terminating end-point (T).

Running tests may also be cancelled, if hardware components in the test path are required by a system maintenance action of higher priority. In this case, the path test resumes automatically when the higher priority process completes, and runs for the amount of time remaining at preemption.

When defining a test with a path type of PSIDE or LOOP, tests of all channels on a card, or of block connections are not supported.

When defining a PSIDL test, you must supply a path definition for the terminating path end, although it is not used for the path test.

Due to hardware limitations, the LOOP and PSIDE test options are not supported on older PMs.

Due to hardware limitations, running a path test using path ends on the same link is not a supported test option. The exception to this is the definition of a PSIDE test, where the originating and terminating path ends used by the test are the same.

Figure 4-47 — LOOP test option

Crosspoint matrix

extract data

Test path

Test path

F

Insert data

XMS-based peripheral module (XPM)
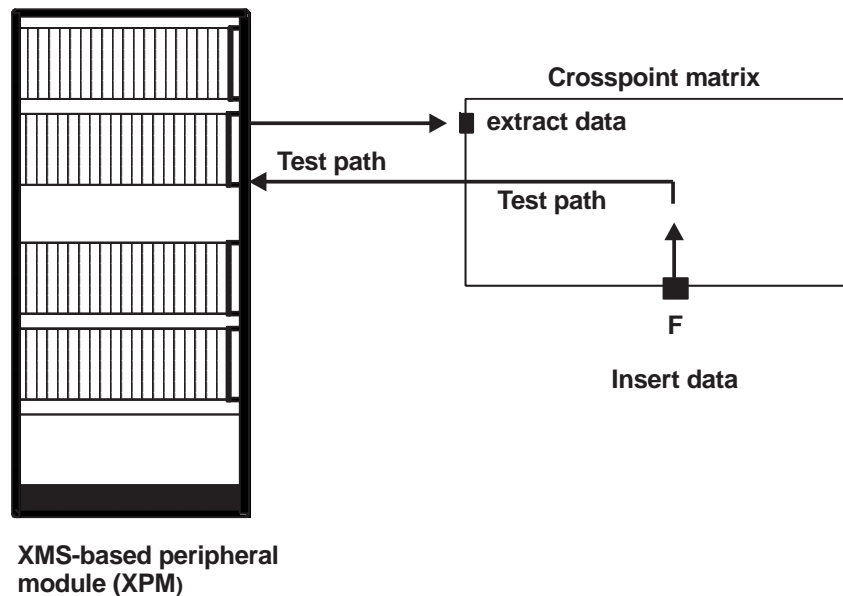
ENET PATHTEST MAP level

Access the PATHTEST MAP level at the CI by typing MAPCI;MTC;ENET;PATH-TEST or choosing 14 on the Net MAP level.

Figure 4-48 is an example of the PATHTEST MAP level display. Also, following the figure is a list of the PATHTEST MAP level menu commands and a brief description of their use. For further details on the use of the commands, command parameters and variables, and supporting response examples for the PATHTEST MAP level, see NTP 297-1001-591, *DMS-100F Networks Maintenance Guide.*

Bit Error Rate Test (BERT)

The ENET BERT level of the MAP provides a facility for you to perform network bit error rate tests.

The BERT level supports the definition of eight bit error rate test records. Up to five of these tests may be run simultaneously, facilitating the concurrent use of the BERT level by several users.

You can use a network BERT to measure the overall performance of the hardware components that make up the ENET switching matrix.

A network bit error rate test performs this function by establishing simultaneous, two-way, block connections over ENET speech paths, and measuring the bit error rates over these connections.

A block connection consists of a block of 511 pulse code modulation (PCM) channels, originating and terminating at the interface ports of an ENET link interface paddle-board. Examples of a block connection include a speech path over all the channels of a DS-512 fiber, or of one DS-30 cable. A DS-30 cable consists of 16 DS-30 links joined to a connector.

Transmission errors, or hits, are recorded when the measured error rate of a test path exceeds the allowable threshold specified in the test definition. These hits may be stored in one of eight BERT buffers, corresponding to the available test records. The system uses hit information to determine an overall performance rate for the ENET.

NOTE: The definition of a BERT on a single PCM channel is not a supported test option. The amount of time required to run such a test, using a reasonable target error rate, is unreasonable.

The connections established during a BERT depend upon the options used to invoke the test, and the user definition in the test record.

Figure 4-48 — ENET Pathtest MAP level

```
    CM    MS    IOD    Net    PM    CCS    Lns    Trks     Ext    APPL
    .      .     .     Istb    .      .      .      .        .      .

 PATHTEST          ENET        System   Matrix    Shelf   0   1   2   3
  0   Quit          Plane 0       .        .                .   .   .   .
  2   Post_         Plane 1       .       Istb             .   .   F   .
  3
  4   Define    PATHTEST  PENding   SUSpended   RUNning   FINished   ABorTed
  5   Info_                  00         00          00        00          00
  6   AltPath_
  7   AltTest_   PATHTEST:
  8   CpyBuf_
  9   CpyPath_
 10
 11   DispBuf_
 12
 13   Snapsht_
 14   Status
 15   Start_
 16   Stop_
 17   Clear_
 18   Reset_
          OPERATOR
  Time       12:11    >
```

Pathtest level menu commands

Command	Description
ALTPATH	Alters the path definition of a specified test record.
ALTTEST	Alters the test options of a test record.
CLEAR	Clears the information from a test record making it available for definition.
CPYBUF	Copies the path ends from an entry in the path saved buffer to a specified test record.
CPYPATH	copies the definition of one test record to another.
DEFINE	Defines the operational parameters of a path test record.
DISBUF	Displays the contents of the specified buffer.
INFO	Returns information on specified tests.
POST	Sets currently defined default path test record and accesses the Pathtest Post Record level.
RESET	Changes the state of test from finished or aborted to pending.
SNAPSHT	Copies entries from the specified buffer into the path saved buffer.
START	Submits a path test to run.
STATUS	Allows you to query defined tests by name or state.
STOP	Changes the state of a test from running to aborted.

> **NOTE:** Although supported by the software, BERTs are not generally used on a single entity smaller than a crosspoint card. This is because of the large amount of time that tests of this nature require.

Although the network BERT facility can indicate the presence of suspect hardware on a connection path, it is not useful for performing fault isolation on the individual hardware components of the ENET switching matrix that form the pad.

However, connections which you write to a BERT buffer in response to test hits may be imported at the PATHTEST level. Then they are used to perform fault isolation on the hardware components associated with the one-way paths making up the connection.

ENET BERT MAP level

Access the BERT MAP level at the CI by typing MAPCI;MTC;ENET;BERT or choosing 12 on the Net MAP level—see Figure 4-49 for an example of the BERT MAP level display. Also, following the figure is a list of the BERT level menu commands and a brief description of their use. For further details on the use of the commands, command parameters and variables, and supporting response examples for the BERT level, see NTP 297-1001-591, DMS-100F Networks Maintenance Guide.

ENET integrity check traffic simulator (EICTS)

ENET integrity check traffic simulator (EICTS), like the integrity check traffic simulator (ICTS) for the junctor network, is a tool for testing the integrity of network connections by setting up a number of connections which are monitored for integrity by the peripherals. EICTS and ICTS are most useful while live traffic is at a minimum. If EICTS or ICTS are still running at 7:00 a.m., it is stopped automatically by the audit.

The EICT is usually performed for the following reasons:

- routine maintenance

- monitoring of the integrity logs or network fabric (NETFAB) maintenance shows that the PM, slot, link or other hardware has reoccurring problems and you want to confirm the problem. The manual EICTS tests allow for more control when testing the system. For example, testing can be limited to specific hardware, or a specific time.

- to simulate an overload situation which should be performed jointly by Nortel Networks and the operating company.

    Note: The EICTS tool is not supported for the Spectrum Peripheral Module (SPM).

.

Figure 4-49 — ENET BERT MAP level

```
        CM    MS   IOD   Net  PM   CCS   Lns    Trks    Ext    APPL
         .    .    .     .    .    .     .      .       .      .
BERT
 0   Quit      ENET   System  Matrix   Shelf  0   1   2   3
 2   Post      Plane 0    .       .             .   .   .   .
 3   Display_  Plane 1    .       .             .   .   .   .
 4   Define
 5   Clear_    BERT  0      Observed       Elapsed      Percent   Optimum
 6   Start_                 Error Rate   Time (hhh:mm)  Complete  Error Rate
 7   STOP_                    10E-09         001:30         50      10E-09
 8
 9
10            BERT:
11
12
13
14
15
16
17
18
        MAP_4

Time 12:13  >
```

BERT level menu commands

Command	Description
CLEAR	Use this command to clear an entire BERT record, or a portion of the information in the record.
DEFINE	Use this command to initialize or modify a BERT record.
DISPLAY	Use this command to display information about the information in a BERT record or about the results of a BERT.
POST	Use this command to designate a BERT record as the current BERT.
START	Use this command to start a defined BERT.
STOP	Use this command to stop a BERT which is in the running state.

EICTS level

EICTS is accessed from the CI level of the MAP by typing in EICTS. The following commands allow you to set up EICTS to your specific needs:

EICTS Commands

Command	Description
EICTS	Use this command to enter EICTS.
ICLEAR	Use this command to take down all network connections and stop integrity scanning.
ICONFIG	Use this command to configure the network links on which you wish to set up connections.
IOPTION	Use this command to change the EICTS options.
IQUERY	Use this command to query the number of set up connections, the number of integrity failures, and the links used for EICTS connections.
IREFRESH	Use this command to initiate integrity checking to the original plane.
ISETUP	Use this command to set up the network connections.
ITRNSL	Use this command to translate an ENET shelf, slot, link and channel into a PM, circuit, channel, and terminal identification.

The following logs are associated with EICTS:

ECTS100 — Each time an EICTS connection has exceeded the integrity threshold (set with the ICPTION command) between audit cycles, an ECTS100 log is generated and the connection is cleared.

> **Action:** Once an ECTS101 log is generated, access the ENET level of the MAP and test the hardware recorded in the log.

ECTS101 — An ECTS101 is generated every half hour while EICTS is running to indicate how many cycles were executed. This log can be turned off with the IOPTION AUDIT command.

> **Action:** ECTS101 logs should be monitored as they are generated. If the number of connections cleared due to traffic starts to increase, turn EICTS off to prevent it from competing with call processing for network resources.

ECTS102 — An ECTS102 log is generated when the audit reaches the audit clear time (set with IOPTION command) and all EICTS connections are cleared.

> **Action:** This is an information log to indicate that EICTS has been deactivated, and that all connections have been cleared.

ECTS103 — The ECTS103 log is generated when the audit reaches the audit remake time (set with the IOPTION command). If the audit remake is turned on, the audit frees all connections and attempts to remake the same number of connections on the configured links, using different hardware.

> **Action:** This is an information log to indicate that EICTS has attempted to reestablish the EICTS connections.

Since the EICTS and ICTS basically work the same, see the "Network Maintenance" subsection within the *Preventive Maintenance* tab for a description of ICTS. Also described is how ICTS it is used with integrity, path, and network fabric testing.

For further details on the use of the EICTS commands, lists of parameters and variables, and supporting response examples for the pathtest level, see NTP 297-1001-591, *DMS-100F Networks Maintenance Guide.*

ENET fabric (ENETFAB)

The enhanced network fabric (ENETFAB) maintenance tool provides the ability to automatically test the call paths through the network modules of the switch.

The ENETFAB test is similar to the EICTS test. ENETFAB uses the EICTS package to systematically test the entire office while EICTS runs the configuration you define. The ENETFAB can be started, stopped, suspended, or resumed manually. See parameters NETFAB_DAILY_DURATION, NETFAB_SCHEDULE_ENABLED and NETFAB_SCHEDULE_TIME listed within Table 4-21 on page 4-229 under "ENET office parameters" within this subsection.

ENETFAB is accessed from the CI level of the MAP by typing in ENETFAB. The following commands allow you to set up ENETFAB to your specific needs:

ENETFAB Commands

Command	Description
ENETFAB	Use this command to enter the ENETFAB increment.
RESUME	Use this command to resume scheduled testing if it has been suspended.
START	Use this command to start a manual test.
STATUS	Use this command to provide the test status and a summary of the test results.
STOP	Use this command to stop a currently running manual test.
SUSPEND	Use this command to suspend a currently running scheduled test.

The following logs are associated with ENETFAB:

ECTS105 — The ECTS105 log is generated each morning at 8:00 a.m. to display the results of the previous night's network testing. Use the ECTS105 log and the Pathtest test tool to diagnose any error paths to determine the faulty hardware.

> **Action:** This is an information log to display test results. Error paths can be diagnosed using pathtest. The error paths are stored in an integrity fault buffer and can be displayed at the ENET INTEG level of the MAP.

ECTS106 — The ECTS106 log is generated when one complete network fabric test has attempted to test 100% of the network hardware. The ECTS106 log provides an indication of the number of faulty connections. It can also be used to estimate the time it takes to completely test all the networks.

> **Action:** This is an information log to display test results of the previous complete test of the office network hardware.

As EICTS was to ICTS, the ENETFAB maintenance tool is basically the same as the network fabric (NETFAB) maintenance tool that was developed for the junctor network. Since the ENETFAB and NETFAB basically work the same, see subsection "Network Maintenance" within the *Preventive Maintenance* tab for a description of NETFAB.

Datapath Overview and Maintenance

Datapath overview

Datapath, a trademark of Nortel Networks, is a system for providing direct, circuit-switched narrowband digital data transmission through a DMS switch over existing telephone networks. Public and private network connectivity is also provided by Datapath.

Datapath transmits data up to 64-Kbps for synchronous and 19.2-Kbps asynchronous over a standard, nonloaded, twisted two-wire subscriber loop. Datapath serves end users outside its normal range of 5.5 Km (3.4 miles) through DMS remote peripheral modules and channel banks. However, Datapath service can be extended up to 160 Km (100 miles) from the switch by using a remote DMS switch or a datapath extension (DPX) channel unit that is installed in a channel bank. Digital trunks that are used for Datapath must not have echo cancellors or digital pads. Modems are required when the route of the data call contains an analog section or is through an analog switch, or when a data unit (DU) has to communicate with other terminal equipment.

Provisioning Datapath type line cards, appropriate Datapath software feature packages, and resident test feature programs are prerequisites for establishing Datapath service. However, before satisfactory service can be provided, the switch network and XPMs must be groomed to a parity threshold of *one* using the FILTER command and the resident network and XPM test features. See the "Network maintenance subsection within the *Preventive Maintenance* tab for a description and use of the tools for network grooming and preventive maintenance.

Datapath software requirements

Besides needing few hardware components, Datapath also has minimal software requirements. Datapath requires the Meridian Digital Centrex Basic (NTX100AA) software package as a prerequisite for providing service through a DMS-100 central office. The appropriate bit error rate testing (BERT) software package should also be resident in the central office for maintenance purposes. Table 4-23 lists the additional software packages for implementing Datapath.

Table 4-23 — DataPath Feature Packages

Feature-Package Name	Ordering Code	Status
Datapath Basic	NTX250AA	Required
Modem Pooling	NTX251AA	Required for access to devices connected to the network through analog loops and modems.
Datapath Extension	NTX259AA	Required if Datapath service is extended through a channel bank and a Datapath Extension card.

Datapath hardware requirements

Basic Datapath services for a computer or other data terminal equipment requires three hardware components:

- the appropriate meridian data unit (MDU), terminal interface unit, or control unit interface connected to the data terminal equipment (DTE) or IBM 3270 Cluster Controller
- a data line card (DLC) installed and datafilled in the DMS-100
- a nonloaded twisted-pair wires between the DMS-100 and the data communications equipment (DCE) located at the customer's premise

Meridian data units

Meridian data units (MDUs) are microprocessor based data communications modules that provide an all digital data transmission loop to a DMS-100 office. The DMS-100 provides switched access to any computer or data terminal connected to the public switched network. The MDU is installed between the computer or data terminal, and a standard two-wire telephone loop that terminates at the DLC in the DMS-100. There are two types of data units, RS-232C or V.35.

MDUs have controls and indicators for selecting options, features, and diagnostic self tests. MDUs transmit on the two-wire loop using time compression multiplexing (TCM). TCM is described later. See NTP 297-2121-226, *Datapath Data Unit Installation and Maintenance* for further information.

Data line card

The NT6X71AA/AB/AC Data Line Card provides the interface between an MDU at the customer premises and a DMS-100 over a single pair of wires. A DLC occupies two vertical slots in an LCM line drawer. The DLC provides two types of full-duplex channels between the MDU and the DMS-100:

- 64-Kbps data channel

- 8-Kbps signaling channel

For detailed information on the NT6X71AA/AB/AC DLCs, see NTP 297-8991-805, *DMS-100F Hardware Description Manual.*

Datapath loop

Datapath provides circuit-switched data transmission services on DMS-100F switches using several loop access technologies:

- two-wire loop up to 18K feet (time compression multiplex (TCM))

- four-wire loop up to 4K feet (RS422)

- computer PBX interface (CPI) that uses T1 CXR lines

NOTE: See Figure 4-50 below for various Datapath loop configurations.

Figure 4-50 — Various datapath loop configurations

AILC	- Asynchronous Interface Line Card	DIU	- Digital Interface Unit	PAD	- Packet Assembler/Disassembler
AILU	- Asynchronous Interface Line Unit	DLC	- Data Line Card	RLCM	- Remote Line Concentrating Module
AIM	- Asynchronous Interface Module	DPX	- Datapath Extension	TCM	- Time Compression Multiplexing
CB	- Channel Bank	DTI	- Digital Trunk Interface	TIF	- Terminal Unit Interface
CPI	- Computer-to-PBX Interface	DTU	- Data Terminal Unit		
CUIF	- Control Unit Interface	DU	- Data Unit		

Time compression multiplexing

Time Compression Multiplexing (TCM) was chosen as the vehicle to provide data transmission capability on long loops for both synchronous and asynchronous data rates up to 64-Kbps. The following equipment configuration is required:

- Line Concentrating Module is XPM type

- Digital Line Card (DLC) requires two adjacent slots
- two-wire nonloaded loop (maximum length of 18K feet and maximum loss of 45 dB at 80 KHz)
- data unit (DU) at customer (HSD/LSD DU or CUIF)
- loop transmission rate of 160 Kbps that provides
    — 64-Kbps full duplex channel for customer data
    — 8-Kbps full duplex channel for signaling and control

Time compression multiplexing was selected because of the following major design considerations that enable Datapath to deliver efficient, cost-effective data communication service:

- full-duplex (bi-directional) transmission
- loop length of up to 18,000 ft. (22- or 24-gauge wire) or 14,000 feet (26-gauge wire), at a loss of 45 dB
- transmission over mixed-gauge loops (in the presence of bridge taps)
- reduction of loop engineering requirements
- reduction of bit error rate

T-link rate adaption protocol

T-link is a full duplex byte oriented protocol designed to transfer either synchronous or asynchronous data over a digital circuit at DTE data rates of up to 64-Kbps. To ensure communications compatibility, Nortel Networks developed the T-link rate-adaption protocol.

T-link protocol applies to all switched Datapath configurations. Data transmitted from a DU is formatted according to the T-link protocol. Data on the TCM loop can only be received by another DU or DLC. However, after the same data is switched into the 64-Kbps PCM stream in the DMS-100F switch, it can be received by any circuit supporting the T-link protocol.

T-link maps all other terminal data rates it encounters into 56-Kbps for uniform transport through the switch and today's digital network. The facility must remain dedicated to T-link for the duration of the end-to-end communication, since there is a continuous flow of messaging over the circuit. The T-Link protocol ensures compatibility between the communicating DTE prior to the start of data transmission. Calls proceed as follows:

- the calling and answering units are synchronized
- the identifiers for rate-adaption protocol are exchanged
- transmission parameters (asynchronous, synchronous, bit rate, clock type) are exchanged
- once data-terminal compatibility is ensured, data transmission begins

T-link error correction

When the user transmits data rates of 9.6-Kbps or less, the extra unused bandwidth is used for forward error detection. The T-link protocol transmits each piece of data several times (three times for asynchronous and four for synchronous) and uses a majority vote on the received data. Data at higher rates than 9.6-Kbps is transmitted only once.

User data at the lower speeds is rate adapted to 56-Kbps or 64-Kbps by using byte repetition and padding with signal bytes. Therefore, within the Datapath system, all data is transmitted at the 56- or 64-Kbps rate.

Datapath protocols

Datapath protocols are procedures for providing a transparent digital communication pipe to the two end user devices for exchange of data. Datapath protocols define how calls are to be set up, end-to-end transport of data, how maintenance messaging is handled, and other items. Built in rate adaption and handshaking protocols free the user from having to know and set transmission parameters for each call.

These protocols consist of three main parts:

- physical level (TCM and RS422 loop transmission)
- signaling level (control messages between site and DMS-100F)
- data rate adaption (use Nortel Networks T-link protocol)

DU-DMS signaling

The signaling protocol level carries connection control messages between the user, the Data Unit (DU), and the DMS-100F switch in an orderly manner. These control messages are exchanged over the 8-Kbps full duplex signaling channel derived from the TCM facility. When RS422 facilities are used, direct communication with the DMS-100F ends at the asynchronous integrated line card (AILC).

Messages between the Data Unit and the DMS-100F are called DU-DMS, examples are:

- switch to DU
  - operate key feature lamps
  - enable or disable speaker
  - control loopback testing
- DU to switch
  - originate a call
  - terminate a call

Handshake protocol

Each DU-DMS message is 16 bits. The transport protocol for sending and receiving DU-DMS messages over the 8-Kbps signaling channel is called full duplex hand-shaking protocol (FDHP). It provides error detection (via checksum), error correction (via retransmission), and flow control.

RS422 physical interface

The RS422 physical interface fills a need for an inexpensive means of providing a loop technology for asynchronous ASCII terminal users. The technology used for the RS422 (protocol) type link is essentially 5 volt transistor-to-transistor logic. It provides data transmission capability over short loops up to 4K feet. The RS422 technology does not use a DU at the customer's premise. The following equipment configuration is required:

- Line Concentrating Module (LCM)
- asynchronous interface line card (AILC) that requires two adjacent slots
- four-wire nonloaded loop of up to 4K feet
- asynchronous interface module (AIM) operated from 110V AC or asynchronous interface line unit (AILU) powered from DTE
- AIM and AILU convert RS422 to RS232 input interface
- RS422 loop facility directly interconnects some DTEs
- Asynchronous RS422 data rates from 110-bps to 19.2 Kbps are supplied

> **CAUTION:**
> AILC line cards consume more power per slot than the normal voice line card. Limit concentration to 10%—6 data lines per 64 slot line drawer.

Computer PBX interface

Computer PBX interface (CPI) essentially provides 24 channels of data service to one location using one T1 interface, instead of the more costly 24 individual DUs. Each of the 24 channels provides for a full duplex 56-Kbps data channel and an 8-Kbps signal channel. Otherwise, it is similar in operation to the two-wire loop TCM configuration.

Datapath DIALAN service

Datapath DMS Integrated Local Area Network (DIALAN) service provides integrated voice/data access for DMS-100 subscribers over existing voice lines and the public switched telephone network. This service provides the capability to simultaneously connect a telephone and a personal computer (PC) or ASCII terminal at the customer's premise, to a DMS-100 switch using an existing two-wire facility. See NTP 297-2121-227, *Datapath DIALAN Service Installation and Maintenance*, for further information on DIALAN.

Datapath extension

The access range of DLCs can be extended by serving the customer from any one of the DMS-100F remote modules such as: RLCM, RSC, LBR, and OPM. The full range of Datapath features become immediately available to these remote switching locations.

Where no remote modules exist, Datapath service can be provided using a datapath extension (DPX) card in the DE-4E or D4 channel bank at the remote location. The DPX feature extends Datapath service beyond the normal reach of the host switch and its remotes.

Datapath 3270 Network Switched Access

Another application of TCM loop technology is switched access for various IBM 3270 type terminals. The service that provides this is called "Datapath 3270 Network Switched Access Service." This is done by replacing the coaxial cable interconnection with a terminal interface (TIF) device with a twisted pair connected to a rack mounted control unit interface (CUIF), which is extended by twisted pair to the DMS-100F DLC termination. A similar arrangement is required at the host computer.

The 3270 Network Switched Access can be configured for two kinds of operation, switched and nonswitched. Both configurations allow the reduction of coaxial cable, yet maintain flexibility in the design of the network terminals.

For further information, see NTP 297-2121-225, *3270 Networks Switched Access Installation and Maintenance*.

Keyboard dialing

Datapath provides keyboard dialing (KBD) capability for the IBM 3270 type terminals. It can be implemented in the following three ways:

- Nortel Networks symbolic KBD asynchronous protocol
- Hayes asynchronous KBD protocol
- CCITT V.25 bits on synchronous automatic calling (SAC)

Modem pooling

Modem pooling is an arrangement that permits a Datapath service to convert to a non-Datapath service (analog). This arrangement requires a modem unit and Datapath DU connected together through an RS232 interface. The loop side is connected to two line equipment numbers (LENs). Connection is made through the DMS-100 by calling the assigned telephone numbers. An automated method for performing this function is through a feature titled "Automatic Modem Insertion." Automatic modem insertion is a process that inserts an outbound modem pool element into the call path of a Datapath call (without manual intervention by the end users). The main purpose of this feature is to enhance speakerless DUs that must use outbound modem pooling during the call. For further information on modem pooling, see NTP 297-2121-223, *Modem Pools Installation and Maintenance*.

Datapath references

The following Nortel Networks documents provide additional DMS-100F Datapath information:

- NTP 297-2121-100, *Datapath Guide to Documentation*
- NTP 297-2121-103, *MSL/DMS-100 Asynchronous Access General Description*
- NTP 297-2121-182, *Line Engineering Rules and Procedures for Two-Wire Loops*
- NTP 297-2121-203, *MSL/DMS-100 Asynchronous Access Installation*
- NTP 297-2121-223, *Modem Pools Installation and Maintenance (BCS35 and up)*
- NTP 297-2121-224, *Modem Pools Installation and Maintenance (up to BCS34)*
- NTP 297-2121-225, *3270 Networks Switched Access Installation and Maintenance*
- NTP 297-2121-226, *Data Unit Installation and Maintenance*
- NTP 297-2121-227, *Datapath DIALAN Service Installation and Maintenance*
- NTP 297-2121-228, *Datapath 3270 Network Switching Access with 3194 Distributed Function Terminals Support*
- NTP 297-2121-303, *MSL/DMS-100 Asynchronous Access Operations and Testing*

Datapath Maintenance

The purpose of this subsection is to summarize the key DMS-100F resident test features and applications available for Datapath maintenance. Also provided is the Datapath maintenance strategy to be used for the switch network, loop testing, and switch-to-switch testing.

Datapath testing

Datapath services are fully integrated into the DMS-100 Family maintenance structure. The DMS-100 provides diagnostics and bit error rate tests (BERTs) that isolate a fault to the smallest replaceable component. The MAP of the DMS-100 switch is the focal point for Datapath maintenance. From the MAP, maintenance can be carried out by manual request, as part of a regularly scheduled routine, or by the system in response to self-detected faults.

Loop testing

Physical electrical tests can be conducted from the LTPMAN level of the MAP to determine the resistance and capacitance of the data transmission loop.

Means for testing the data transmission for continuity and error rate from the customer's site is provided by a data looparound feature within the switch. Once a user

dials the looparound access code, the DU transmit path is connected to its receive path within the network of the DMS-100 switch. Once the looparound is accessed and activated, the DU *connect* lamp flashes when the baud rate of the monitor is different from the baud rate of the DU under test. When the baud rate is the same, by adjusting if necessary, then the *connect* lamp will light steady. BER testing can then be performed from the customer's site. See BERT below for performing BERT from the switch side.

Status testing

The external status of Data Line Cards and Meridian Data Units can be examined from the MAP terminal. Various tests can be accessed from the MAP to detect, isolate, and identify facility failures or faults. The command SUSTATE on the LTPMAN level determines how a DLC, AILC, or MDU is set, which facilitates changes to incorrectly configured equipment.

The DU is equipped with a pushbutton switch in the faceplate that activates the unit's self-test feature. It also provides loopbacks at the TCM tip and ring, and at the RS232-C interfaces.

When an LCM finds a DU that does not respond to messages, it initiates a series of diagnostics to determine whether the fault lies within itself, the bus interface card (BIC), or the line card. If the diagnostics indicate that the fault lies with the line card, and the diagnostic flag is not set against it, a LINE204 line card fault log report is output. The line is then flagged as being suspect, and may be scheduled for an extended diagnostic.

DPX testing

All normal Datapath loopback and BERT features are functional with the DPX channel banks. In addition, each DPX channel unit has a self-test capability.

Datapath audit

Datapath audits check the DU/DLC synchronization status. It searches for DUs that are in the CPB state but are not synchronized with their DLC. Such calls are disconnected and a log report generated.

Bit error rate testing (BERT)

Provisioning an integrated bit error rate test (IBERT) line card (NT6X99) provides the bit error rate testing (BERT) capability in the DMS-100. BERT provides a simple means of testing Datapath loops and does not require external test equipment. Any possible faults on the loop are easily isolated through loopback testing. Loopbacks can be set at various points along the line: at the switch, on the DLC, on the loop, or in the subscriber's equipment.

BERT can be performed using the LTPDATA level of the MAP. Three commands on this level allow the connection of external test equipment to a DU for BERT on that unit, as well as monitoring of any data call on the DMS-100. The commands are:

- EQUIP command which reserves DU monitor(s) and a test line for use with the CONNECT command
- CONNECT command which connects a specified line to the currently posted line with the option of simultaneous DU monitor connections
- LOOPBK command which activates one of the loopback points of the currently posted line. This causes the data transmitted from the switch to be sent back to the switch for testing purposes

In Figure 4-51, IBERT transmits a bit pattern through the network, out onto the line being tested, receives the pattern from the point where the loopback was set, and compares the pattern received with the pattern transmitted. The results of the loopback tests pinpoint where the fault might lie. IBERT can be used to test the Meridian Data Unit/19, Meridian Data Unit/64, 3270 Switched Access Service interface unit (TIF or CUIF), and any Meridian Data Unit served by Datapath Loop Extension.

Figure 4-51 — IBERT Loopbacks

DMS-100

DLC   a

IBERT

Meridian Data Unit

Data Terminal Equipment

Maintenance and Administration Position

LEGEND:

a — 64-kbps loop-back at the Data Line Card
b — 64-kbps loop-back at the Meridian Data Unit
c — loop-back at the RS-232/V.35 interface to the Meridian Data Unit
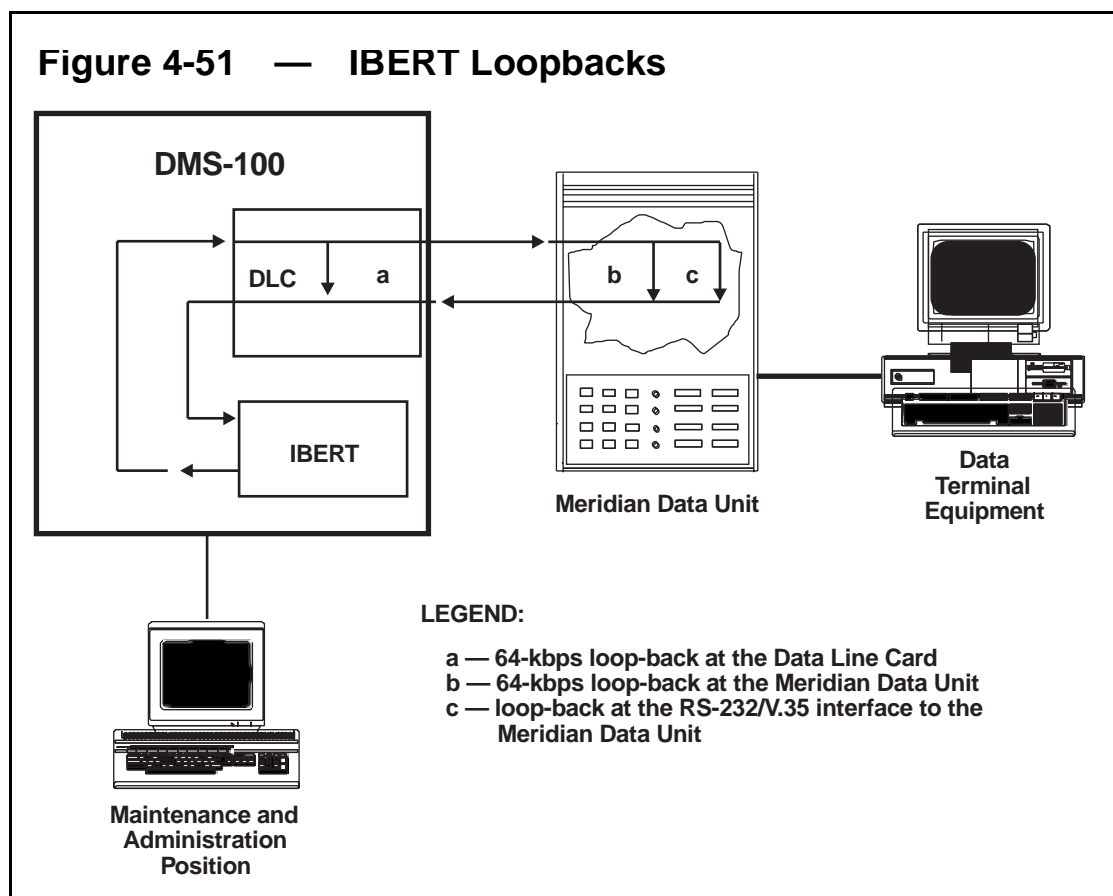
For more detailed information on Datapath line testing, see NTP 297-1001-594, *DMS-100F Lines Maintenance Guide*.

Datapath maintenance strategy

Datapath maintenance strategy consists of the utilization of the various resident maintenance features within the switch to perform preventive and corrective maintenance for Datapath. The following is an overview of the features and troubleshooting tests for performing Datapath maintenance strategy:

Station and line card testing features

- audits to detect missing synchronization between the DU and DLC
- call processing detected troubles and related diagnostics
- automatic line testing (ALT), including the DLC line card
- data looparound
- bipolar violation (BPV) count for a posted line(s)
- DU monitor
- DU Silent Switchman dialable feature
- DU dialable Station Ringer Test feature
- integrated bit error rate testing (IBERT)
- LTP, LTPMAN, LTPDATA, and LTPLTA for Datapath
- MAP metallic jack access (loop tests)

Network and XPM switch testing features

- integrity check traffic simulator (ICTS)
- XPM bit error rate testing (XBERT)
- bit error rate performance (BERP)
- NETPATH fault testing
- network fabric (NETFAB) testing
- NETINTEG analysis tool
- BERT for Trunks testing
- switch BER indicator for Trunks
- interoffice monitoring (DU call interswitched)

The above network and XPM test features work equally well for all types of DMS-100F switches, and when applied, can improve the switch performance. Figure 4-52 is a block layout of the various Datapath maintenance and network grooming tools.

Datapath preventive maintenance

Datapath preventive maintenance automatic detection activities for the station loop and DLC are derived from audits and call processing error indicators. Preventive maintenance routine tests for the network involves scheduling and running NETFAB. Preventive maintenance routine tests for trunk facilities involve the use of the BERT

for trunks and automatic trunk testing (ATT) features. Automated BERT for trunks can be scheduled on trunks derived from DS0 channel testing just as other net loss and noise tests can be made.

The maintenance features are effective on a stand alone basis; however, each feature is enhanced when used in conjunction with the others. For example, NETFAB failures can be further diagnosed to the specific pack problem using the NETPATH feature.

For more detailed information on the use these features, see the "Network Maintenance" subsection within the *Preventive Maintenance* tab of this manual.

Datapath corrective maintenance

Corrective maintenance actions are initiated by a technician as a result of a customer trouble report, a machine generated audit, or a diagnostic test. The technician determines the tests required to verify, sectionalize, and correct the trouble condition based on the trouble report information, history, and subsequent test actions. Figure 4-53 and Figure 4-54 are flow diagrams of typical steps for troubleshooting the loop and customer equipment, and includes DMS-100F switch reports.

Datapath loop troubleshooting from MAP

The following tests are available for troubleshooting the loop access facilities from the MAP:

- an IBERT test can be initiated from the LTPDATA level of the MAP for the specific line in trouble. It measures the transmission quality of the subscriber data loop (expressed in *bit error rate* terms). The MAP can be used for sectionalizing troubles by setting loopbacks at various points along the loop to determine the faulty part

Figure 4-52 — Datapath Maint. & Network Grooming Tools

```
┌──────────────┐  ┌──────────────┐  ┌──────────────┐  ┌──────────────┐  ┌──────────────┐
│  NETFAB      │  │ ICTS TESTING │  │  BERP        │  │  IBERT       │  │ BERT ROUTINE │
│ ROUTINE      │  │              │  │ ROUTINE      │  │  TEST        │  │ TRUNK TESTING│
│ TESTING      │  │              │  │ TESTING      │  │              │  │              │
└──────────────┘  └──────────────┘  └──────────────┘  └──────────────┘  └──────────────┘

 LOG'S ICTS105                         BER                                   ATT LOG
  & ICTS106      LOGS GENERATED     PERFORMANCE                            GENERATOR
 SUMMARY REPORTS                   REPORT SUMMARY


                          ◄─►              ◄─►
                                                 ┌──────────────┐
                                                 │    XBERT     │
                                                 └──────────────┘

┌──────────────┐  ┌──────────────┐
│ ENET NETPATH │  │ JNET NETINTEG│   XPM FAULT LOCATER     DATAPATH        TRUNK FAR END
│ FAULT LOCATER│  │ FAULT LOCATER│                         LINE FAULT       TEST FAULT
└──────────────┘  └──────────────┘                        LOCATER          LOCATER
```
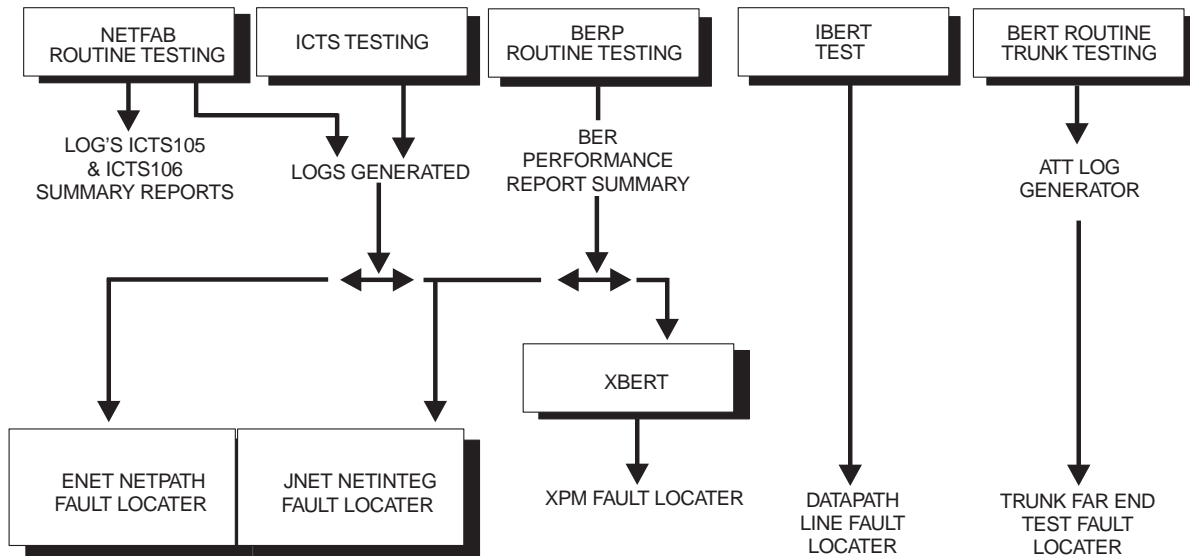
- a bipolar violations overflow (BPVO) test can be initiated from the MAP on the specific line under test. The BPVO is the count of bipolar violations (measurement of transmission improvement) exceeding a predefined threshold

- a data unit monitor test can be initiated from the MAP on the specific line under test. The test monitors the selected data call in progress. This monitor feature may also be used to connect external bit error rate testing equipment. For the monitor and test feature, two DUs and DLCs are required

- automatic line testing (ALT) can be initiated from the MAP on the specific line under test to perform long or short diagnostic tests on the DLC

- metallic test access (MTA) can be initiated from the MAP on the specific line under test. It allows the related subscriber loop to be tested via a direct metallic connection using the metallic access bus. This direct metallic test arrangement allows for high frequency test signals, current, and voltage to pass through to the subscriber loop

- loop testing MAP commands at the LTP, LTPMAN, and LTPLTA levels can be used for testing Datapath lines. When testing a Datapath loop, and an invalid command is entered, a warning message appears on the MAP screen to alert the technician. NTP 297-1001-594, *DMS-100F Lines Maintenance Guide*

Datapath loop troubleshooting from DU

The following tests are available for troubleshooting the loop access facilities from the customer's premises:

Figure 4-53 — Loop/station report troubleshooting steps
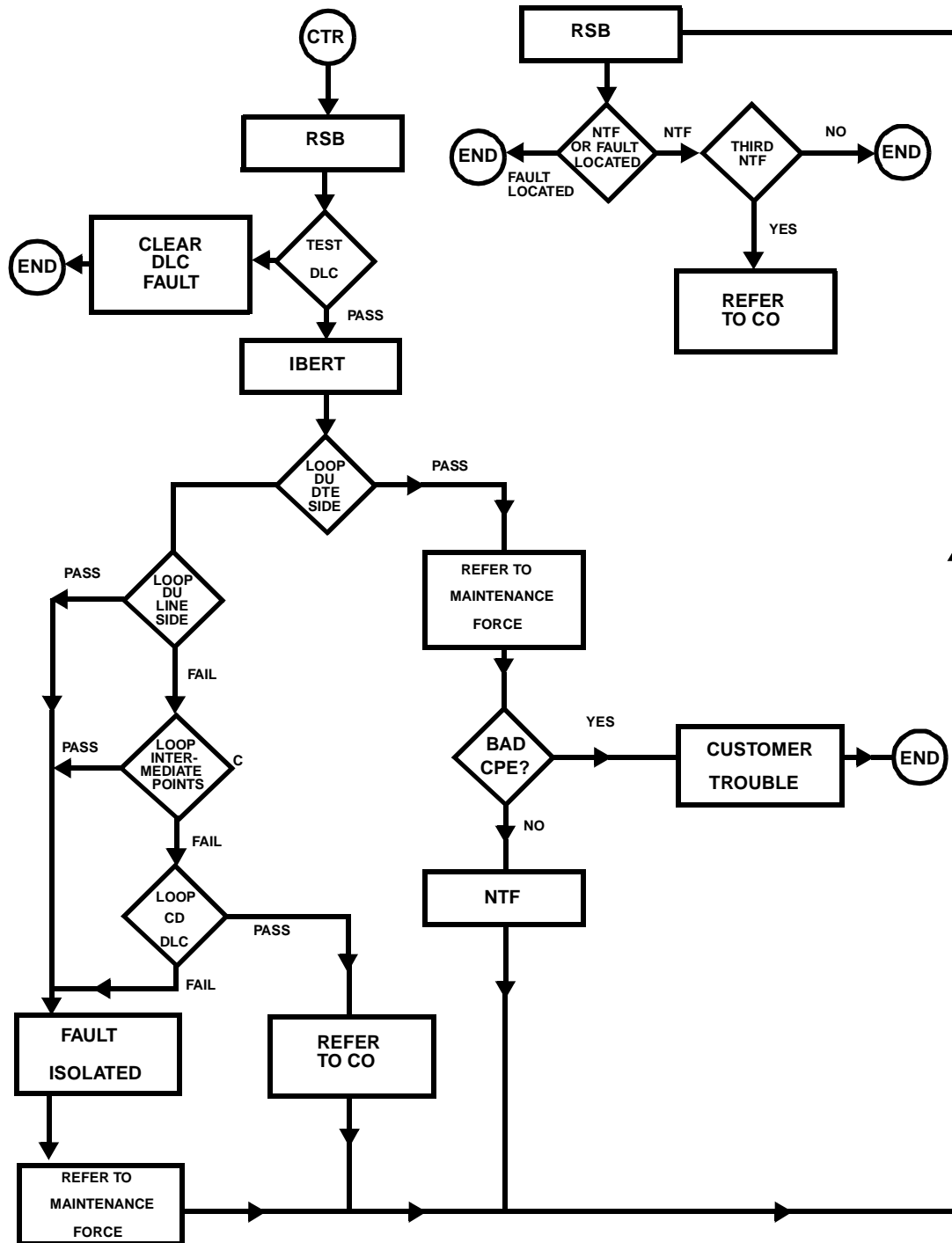
- data looparound test can be initiated from the DU at the customer's site using the normal Datapath call to the looparound test line number. This test verifies Datapath continuity to the DMS-100F, since the transmit is looped back to receive path in the switch (the DU *connect* lamp should be lit). For this data looparound test feature, datafill tables IBNXLA and NCOS that are described in NTP 297-YYYY-350, *DMS-100F Translation Guides*

- the dialable Silent Switchman feature test can be initiated from the DU at the customer's site. This operates the cutoff relay in the DLC to open the tip and ring so that the loop conductors can be tested from the station end

- the station ringer test (SRT) can be initiated from the DU at the customer's site. SRT tests the hardware of the DU by following a specific test sequence that is described in NTP 297-1001-594. The technician at the customer's site has seven minutes to perform the station tests before the loop returns to normal (idle condition)

DIALAN troubleshooting and correcting faults

Troubleshooting and correcting procedures for Datapath DIALAN service are provided in NTP 297-2121-227, *DMS-100F Datapath DIALAN Service Installation and Maintenance*. The procedures identify the trouble down to the following major component level:

- customer site equipment
- a two-wire facility
- the customer's Integrated Voice and Data Module (IVDM)
- an IVDM in the DMS-100 switch
- a voice line card (VLC)
- a personal computer or ASCII terminal
- an asynchronous integrated line card (AILC)

3270 troubleshooting and correcting faults

Testing, troubleshooting, and corrective action for IBM 3270 network switched access equipment can be found in NTP 297-2121-225, *DMS-100F Datapath 3270 Network Switched Access Installation and Maintenance.* The troubleshooting section of this document describes some of the problems that might be encountered during installation or during normal operation.

Testing, troubleshooting, and corrective action for IBM 3270 network switched access equipment with 3194 distributed function terminals can be found in NTP 297-2121-228, *DMS-100F 3270 Networks Switched Access with 3194 Distributed Function Terminals Support Installation and Maintenance*.

Data unit troubleshooting and correcting faults

Testing, troubleshooting, and corrective action for rackmount and desktop DUs can be found in NTP 297-2121-225, *DMS-100F Datapath 3270 Network Switched Access Installation and Maintenance.*

Figure 4-54 — Switch report troubleshooting steps
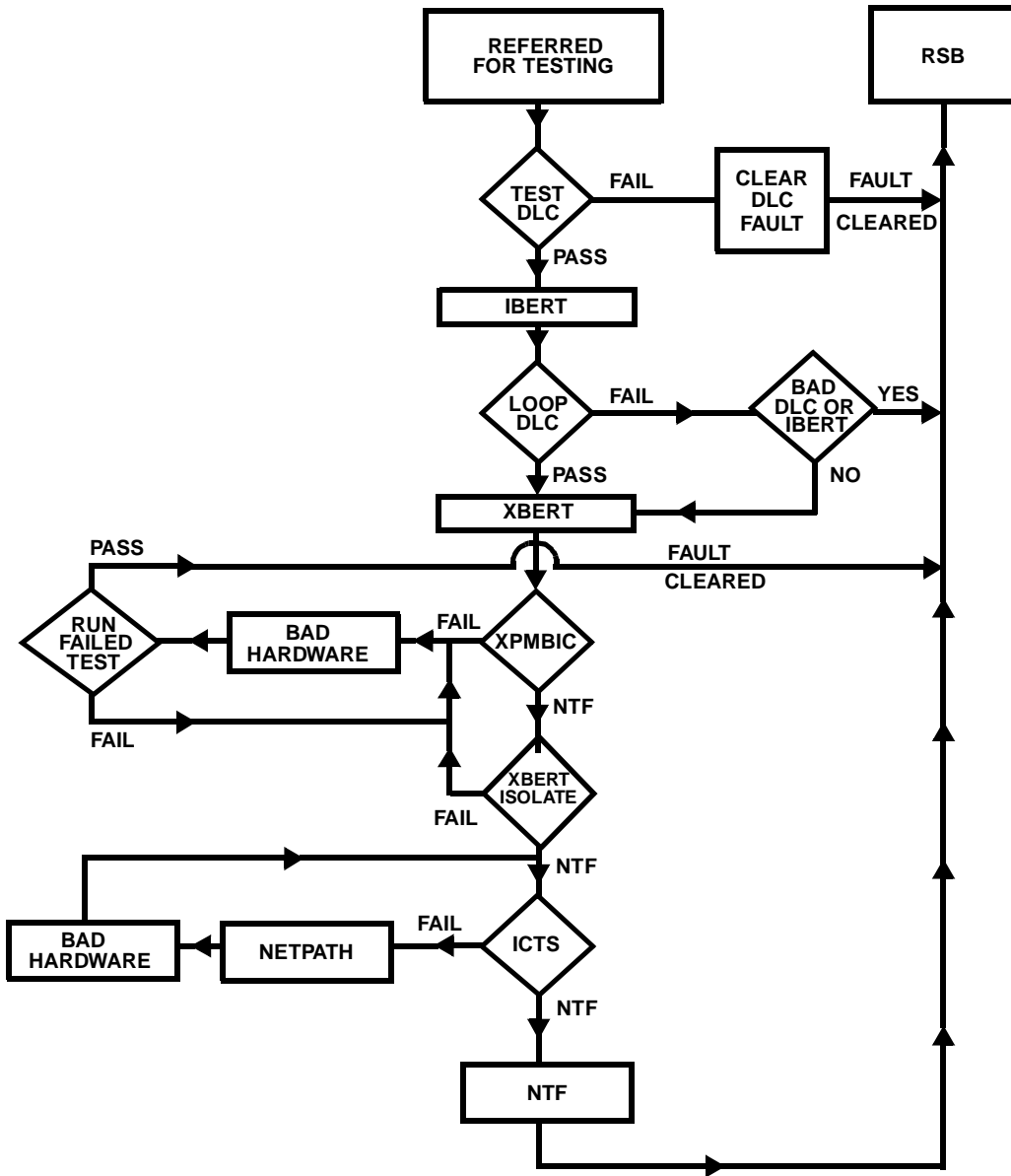
MDC Overview and Maintenance

This subsection provides an overview of Meridian Digital Centrex (MDC), and maintenance related information for MDC business sets and attendant consoles. To locate supporting information on MDC, refer to the more detailed documentation referenced within this subsection.

MDC overview

Prior to the introduction of Meridian Digital Centrex, the Integrated Business Network (IBN) environment existed to provide business customers with special features. Meridian Digital Centrex was announced around 1986 to replace the IBN terminology. However, since the IBN term was already established, both terms are used interchangeably.

MDC refers to the Meridian Digital Centrex software packages that were developed for the IBN environment. The various features within the MDC software packages allow operating companies to provide their business customers with special services.

MDC provides a set of efficient, low-cost voice and data services for businesses of all sizes. The services originate within the DMS-100F switch and use the standard phone lines already installed in a business. Whether installed in a large established business or a start-up enterprise, MDC gives all the advantages of a sophisticated PBX without the following <u>disadvantages</u>:

- PBX equipment purchase and installation
- PBX maintenance and repair cost
- spare parts for PBX
- building floor space
- air conditioning and electricity
- backup power
- insurance for PBX
- software and hardware updates

MDC features

MDC offers a variety of features that meet today's business needs. The recommended document to reference for MDC features is NTP 297-YYYY-350, *DMS-100F Trans-*

lations Guides. This document provides complete descriptions and datafill for the MDC features, including system, attendant console, station, and business set features. A variety of information on DMS-100 MDC can be found in the yellow/black 500XX documents that were first published in 1992. Supplement documents have since been published.

Meridian business sets

If the customer currently uses 2500-type telephone sets, they can be kept in an MDC network. However, to make the most of the MDC features, the customer should use the Meridian business sets with single key access to advanced features.

The Meridian business set—previously called a "P-phone"—and sometimes known as an electronic business set (EBS), is provided through the Nortel Networks M5000-Series of sets. They provide a variety of features and are described in the following documents:

- NTP 297-2011-200, *DMS-100F Business Set General Description, Installation, and Maintenance*

- NTP 297-2011-201, *DMS-100F Meridian M5009 Basic (9 Button) Business Set Description, Installation, and Maintenance*

- NTP 297-2011-202, *DMS-100F Meridian M5112 Handsfree (12 Button) Business Set Description, Installation, and Maintenance*

- NTP 297-2011-205, *DMS-100F Meridian M536 36 Button Add-On Description, Installation, and Maintenance*

- NTP 297-2011-206, *DMS-100F Meridian M518 18 Button Add-On Description, Installation, and Maintenance*

- NTP 297-2011-211, *DMS-100F Meridian M5209 9 Button Business Set with Alpha-Numeric Display Description, Installation, and Maintenance*

- NTP 297-2011-212, *DMS-100F Meridian M5312 Handsfree (12 Button) Business Set with Alpha-Numeric Display Description, Installation, and Maintenance*

- NTP 297-2051-104, *DMS-100F Meridian Digital Centrex Simplified Message Desk Interface Setup and Operation*

Business set records and reports

Line card records

The following is information required to support business set repair activity:

- All business sets must be identified on the face plate with a unique number for each set.

- A station record (line card) must be available to the trouble repair center, to include the following

  — station number

— primary directory number

— Line Equipment Number (LEN)

— cable(s) pair(s)

— user's name

— key assignments (pickups)

— record of trouble history

Trouble report information

Customer reports must include the following:

- station number

- location

- complete description of problem

    — Only one set?

    — What was the last action?

    — What time did the problem occur?

    — What number(s) were you connected to?

    — What number did you call?

    — Does this problem occur on all calls?

    — Where did the call come from?

    — What buttons did you operate?

MDC maintenance

For MDC technical support, call 1-800-251-1758 (option 7).

Business set testing using LTP

Verify that the set and modules are responding for each software condition assigned.

Log on the maintenance administration position, then proceed through the MAP levels below in sequence.

1st Level	MAPCI
2nd Level	IMTC
3rd Level	LINES
4th Level	LTP
5th Level	LEVEL;LTPDATA;SUSTATE

ADDRESS   0 1 2 3 4 5 6 7

DATA FILLED **X**- - -   - - - **X**   = Data filled for one main business set.

RESPONDING - - - - - - - -   = Switch sees no response from the field (improper signal from the set) due to set options.

ADDRESS   0 1 2 3 4 5 6 7

DATA FILLED**X** **X** - - - - - -

RESPONDING   **X** - - - - - - - -   = Under address 1 indicates the switch has software assigned, but the add-on module is not responding.

NOTES:

1. When an address (0-7) has a (**X**) under it, it indicates the following:

Data Filled

Address 0	Main line business set in software
Address 1	First add-on module in software
Address 2	Second add-on module in software
Address 3	Third add-on module in software

Responding

Address 0	A business set in the field has been placed and appears to be working
Address 1	The first module is in place and responding
Address 2	Second add-on module is in place and responding
Address 3	Third add-on module is in place and responding

2. When an address (0-7) has a dash (-) under it, then there is either no software assigned or the station equipment is not being recognized by the switch.

3. Addresses 5-7 are used only for business set extensions or other electronic set. Further action may be required based on the following conditions:

- Not data filled, but field is responding
    — Check station records
    — Check set options
    — Is there supposed to be something in the field or is the software missing?

- Data filled, but no response from station equipment
    — Check set power
    — Check set options
    — Run diagnostics
    — Run line test

Line diagnostic tests

Perform a line diagnostic test on the assigned station LEN. The following indications may be received:

```
*LINE 101 APR01 12:00:00 2112 FAIL LN_DIAG
LEN HOST 03 0 14 24 DN 7811999
DIAGNOSTIC RESULT  No Response from Peripheral
ACTION REQUIRED  Check Peripherals
CARD TYPE  6X21AC
```

Other actions required may include some of the following:

- change line card
- check facilities
- transhybrid
- flux cancel
- FEMF (foreign voltage on the line)

A line test of facilities on the assigned LEN may result in the following indications being received:

LNTST

TEST OK

	RES	CAP	VAC	VDC
TIP	999K	0.050μF	0	0
RNG	999K	0.050μF	0	0
TIP TO RNG	999K	0.050μF	0	0

(1) The tip and the ring should have the same reading.

(2) Not cross connected at the mainframe would result in a reading:

       T   0.010μF

       R   0.010μF   (This is close to reality)

       T-R   0.010μF

(3) No set connected across the tip and ring would result in a reading:

       T   1.50μF

       R   1.50μF (This reading is dependent on cable and length)

       T-R   1.50μF

(4) An open on the ring side of the line would result in a reading:

       T   2.055μF

       R   1.005μF (This reading would depend on cable length)

       T-R   1.005μF

(5) An open on the tip side of the line would result in a low cap reading on that side of the line.

(6) A reading under VDC (foreign DC voltage) of over one VDC across the T & R, T to GND, or R to GND should be investigated. See NTP 297-2011-180, *DMS-100F Meridian Business Set Line Engineering* for this requirement.

(7) Readings under the RES header should be 999K unless there is either a ground condition or shorted condition on the line. Typical examples:

	RES	CAP	VAC	VDC
TIP	.240K	0μF	0	0
RNG	.240K	0μF	0	0
TIP TO RING	.600K	0μF	0	0

Would indicate a short across tip and ring.

	RES	CAP	VAC	VDC
TIP	999K	0.094μF	0	0
RNG	999K	0.010μF	0	0
TIP TO RING	999K	0.010μF	0	0

Would indicate an open ring lead on the line.

	RES	CAP	VAC	VDC
TIP	.225K	0.000μF	0	29V
RNG	999K	0.000μF	0	0
TIP TO RING	999K	0.000μF	0	29V

Would indicate a ground on the tip lead on the line.

Based on any of the test results above, repair action should be taken to resolve the problem.

See Exhibit A starting on the following page for line card diagnostic failure reports and possible causes.

EBS testing

The CKTTST command, used in the automatic line testing (ALT) program, can be used to test electronic business sets (EBSs), data units (DUs), asychronous interface modules (AIMs), and IBERT applications.

The feature, "Retain EBS Volume Setting During Maintenance" in software package NTX106AA, allows the volume setting for an EBS to be retained during maintenance. This is accomplished by using the metallic test unit (MTU) to keep the EBS powered up while the cutoff relay on the EBS line card is being operated.

Switch room repair activity

Failures testing toward the switch should result in one of the following corrective actions:

- Replace bad line card.
- Correct cross-connect problem on MDF.
- Correct MDF protector problem.
- Correct balance network problem or padding.
- If trouble is affecting more than one LEN or stations that have LENs in the same LCM, then refer the trouble to the switch repair technician.

Exhibit A — Line card diagnostic failure reports and possible causes

Line cards show activity on LOGUTIL whenever the LCM is busy or RTS

a) Check the ACT signal CONN D pin 18; miswiring may cause this response.

White noise

a) Bad NT6X51, NT6X52, or line card.

b) Can be caused by the next card slot being empty. You may have to powerup extra LCMs to put a load in the empty card slots.

Cards skipped during an ALT run

a) Bad NT6X54.

b) Bad NT6X47 in the LGC.

c) Cards in the PLO state.

Permanent lock out (PLO)

a) Bad drawer (NT6X05), NT6X54, or line card.

b) Broken CLK pulse wire to connector pin 24.

Ringing failure

a) Bad line card, NT6X54, NT6X51, or NT6X30.

b) RG switch settings.

c) RG contacts need cleaning.

d) RA/RB fuses not in the frame.

Battery fuse

a) Sloppy RB fuse holder.

b) Line card switch not set correctly.

c) Bad line card.

d) Bad control cable in the line drawer.

Drawer fails all cards

a) Bad line card in own drawer or in MATE drawer.

b) Broken wire(s) in drawer connector bundle.

c) Bad NT6X48 in LGC.

d) Bad solder connection at fuse holder.

ALT aborted

a) Check the LTU. Busy the first LTU in the MTM so that the ALT grabs the second LTU.

b) Check the LGC. Do a SWACT and restart the ALT. If it runs, then suspect the NT6X48 in the LGC.

Exhibit A — Line card diagnostic failure reports and possible causes (continued)

Drawers clicking

a) Bad DS3O cable.

b) Check the FP signal in connector D, pins 21 and 22. These have been found cut.

Voltage detect before ring

a) Check at LTPLTA level with LTA out. T&R should be 0. Release the card and check the CO3 and CO4 connectors. The wires on pins 12 and 32 must be GR/W. Pins 22 and 42 must be W/GR. These have been found reversed.

PAD dB

a) Check gauge of jumper wire between TB2 and TB3. Gauge 22 fails various cards in LCM.

TRANSBYBRID

a) Bad line card in MATE drawer.

b) Bad NT6X54, NT6X52, or line card.

SV1 stuck before ringing

a) Bad line card in MATE or OWN drawer.

No voltage detect after ring

a) Check for RB fuses in fuse holders.

b) If using a NT6X18, check tables LNINV and LENLINES for proper assignment.

c) Possible reversal of RG connector pins 25 and 26.

d) Possible miswiring on MTA connector (CO3 and CO4). TIP and RING have been found reversed.

e) Possible broken wires between shelves. SLOT 2, pin 2Q, shelf 4 and SLOT 2, pin 2Q, shelf 21 have been found broken.

Flux cancel

a) Bad LTU or MTA vertical.

b) Bad line card.

c) Bent or broken pin behind line card.

d) Check MTA connector. Pin 49 should be at slant corner of hood. LCM connectors have been found installed upside down.

e) Broken solder connection on fuse holder

f) Loose mini-bar MTADRIVER cable.

g) TIP and RING shorted inside the FSP panel at the MTA connector. Look for pinched wires.

Exhibit A — Line card diagnostic failure reports and possible causes (continued)

Loop detect

a) Perform VDC test on one card at LTPLTA level. Test a card in both halves of the bay to help narrow down the possibilities. If problem is in LCM 0, use connector CO3; in LCM 1, use connector CO4. If problem is in DRAWERS 10-19, check pins 32 and 42. Pull 48v fuses until the voltage disappears to locate the problem drawer. Replace fuses and pull line cards one at a time until the voltage disappears to locate the problem line card. You can also remove the drawer from the bay, and using the TIP and RING reference point on the line drawer itself, scan the pins to locate the bad line card that has a continuous tone.

NOTE: Keep in mind that you may have more than one shorted line card.

b) At LTPLTA level, the *resistance* test shows 50 ohms. Using the above method, and pins in MTA connector, attach the meter on the appropriate pin. Once again, pull the 48v fuses and watch for a fluctuation in resistance. Check the drawer connector for a wire that might be sticking through the insulation.

DCC - BIC looparound

a) Bad NT6X52, NT6X54 (any drawer), line card, or NT6X51 (either unit).

b) Bent pin behind NT6X54 or line card in drawer connector.

c) Bad drawer.

d) Bad NT6X30.

e) NT6X54 not properly seated in a drawer other than the drawer being called out.

f) Drawer connector not properly seated.

g) Check solder connection on fuse holder.

h) Check position on DS30A cable on LCM and LGC. One pin makes a lot of difference.

i) Check pins in the drawer connector for voltage and continuity to backplane.

Found PIN 26 did not have a +4.8v; crimped wire in the connector.

Found PIN 13 of connector C and PIN 14 of connector D did not have +15v; lead broken off of the capacitor.

Found DCLK pulse wire broken between the drawer connector and the backplane.

j) NT6X30 RG connectors need cleaning.

k) Cut wires found in the drawer connector cable bundle.

Be careful of the bundle getting caught between the line cards and the backplane when the drawer is shoved in.

NOTE: Every time a line card is replaced, a balance (BAL) test should be performed. The BAL test automatically sets the balance network in the line card to provide transmission balance between the four-wire side of the switch and the two-wire loop. If possible, the BAL test should be performed in the off-hook state for a more accurate measurement. This can minimize subscriber reports of noise, echo, garbled, hollow, hum, too loud, and can't be heard. BAL test is located off the LTPMAN and LTPLTA levels of the MAP.

Station and cable repair

Problems that are tested and proved to be beyond the main distribution frame (MDF) should be referred to the field repair forces. The following actions should be taken by the field repair technician:

- Verify with the user that the reported problems match the equipped station set. Review with the user the problem they experienced from that set.

- If any of the following troubles are identified, then the cable pair and cross-connects should be inspected and corrective action taken (i.e., change bad pair, reterminate, rerun):

    — FEMF on tip or ring

    — open on either tip or ring

    — shorted tip and ring

    — split pair

- Inspect station wiring and jacks, and repair as required.

- Ensure that business set switch settings are correct for station configuration.

- Perform station ringer test three times. Replace set if the set fails any test. The station ringer test (SRT) is described next.

- Check business set power.

- Refer outside problems are to the field repair forces. Examples are:

    — feeder cable trouble

    — defective station equipment

- Verify that problem is not the result of an in-progress service order, refer to service order group if that is the case.

- Ensure that a previous trouble report has not been taken and scheduled for corrective action.

> **⚠ CAUTION:**
> If the set requires any internal access (i.e., switch settings, cords changed), extreme caution should be taken. The business set is subject to static discharge and improper handling may result in permanent damage.

Station ringer test

The station ringer test (SRT) circuit tests the hardware of MDC business sets, and can be performed by the installer or repairman at the site with no involvement of the maintenance personnel, provided the switch is equipped with the necessary software package.

Circuit test

MDC Circuit Test Enhancement feature G0063 in software package NTX106AA, IBN Business Set Features, adds a *circuit test* check to the end of the station ringer testing sequence. This test confirms the ability of the set and line card to transmit and receive messages correctly and adherence to the message protocol.

These additional testing steps and the following notes are described in NTP 297-1001-594, *DMS-100F Line Maintenance Guide* under "Keyset station ringer test":

- The circuit test portion of the station ringer test may fail on a business set or data line if any keys on the set are depressed while the test is running.

- The amount of time the station ringer test waits for a reply for the circuit test portion of the test from the peripheral depends on the number of messages to send:

1-10 messages:	waits	30 seconds
11-20 messages:	waits	60 seconds
21-30 messages:	waits	90 seconds
31-40 messages:	waits	120 seconds
41-50 messages:	waits	150 seconds

- In heavy traffic, these wait times may not be long enough for the peripheral to complete the circuit test and send the results back. The results are returned and displayed when the peripheral has completed the circuit test.

Test setup

With the handset on hook and all LCD indicators off, press a loop key and dial the seven digit access code. Normally, this is the number 57, followed by the last five digits of the phone (or line) directory number from which the call is originated. However, the first two digits may differ, depending on telephone company preferences. If the last five digits are incorrect (i.e., incompatible with the directory number of the line), a reorder tone sounds and the call will have to be reoriginated. If all digits are correct, then all LCD indicators at the main set should light up. The test can now proceed in

accordance with NTP 297-1001-594, *DMS-100F Line Maintenance Guide.* This NTP also describes the complete station ringer test sequence.

If add-on modules are present, repeat the necessary steps for each strip of numbers of each module.

The only messages not tested are *turn on/off hands free control* and *open/close echo mode*. They are not used by call processing.

Display screen test

The "LTS" switch (S3) on the NT4X20AB/AF display set circuit board has two toggles. When looking at the circuit board with the telephone inverted, the left-hand side toggle (LT0) operates the test function, and the right-hand side toggle (LT1) operates the notepad function. When the display screen is to be tested for proper functioning, toggles must be set as given in the following text. When the set is to be returned to operating mode, both toggles must be in the off position.

Notepad Mode

In this mode, display screen responses (receive simulation) to input can be verified without the need to access switching equipment. The dial pad and volume control keys are switched to *local* mode and are used to enter alphanumeric data directly into the display. To call up this verification feature, set the notepad toggle (LT1) to on, while leaving the test toggle (LT0) in the off position.

In notepad mode, each dial key has four characters associated with it. As soon as a dial pad key is depressed, the first character in the sequence for that key appears at the cursor position (flashing block character). Holding the key down causes the next character in the sequence to appear after approximately half a second, and so on. This continues and the character sequence repeats itself until the key is released. Once a character has been entered on the screen, the cursor automatically advances to the next position. The cursor can also be manipulated by operating the volume control. Volume up moves the cursor one space back and volume down moves the cursor one space forward. If the volume key remains depressed for half a second, the cursor progresses to the next location and continues to do so at a rate of 8 characters per second until the key is released. Normal volume control functions are inhibited in the *notepad* mode.

Receive mode

In this mode, a single transmission of the notepad buffer is forced. Transmission of the notepad buffer begins at the cursor location (display or display image cursor) and continues until the end of the display. Characters are interpreted in pairs after the cursor position as the hexadecimal representation of the message to be transmitted. For example, to transmit message 60 H, enter 60 into the notepad positions 30 and 31, and backspace the cursor to position 30. Set the LT0 toggle of the S3 switch to on. Transmission over the T & R leads begins when LT0 is set, and continues while the LT1 toggle remains in the on position.

This verification feature permits a switch simulation when communicating in a closed loop with another MDC business set.

Semi-transparent monitor

In this mode, the set acts as a semi-transparent message monitor by displaying messages sent over the tip and ring leads from another set, in two-character hexadecimal representations. To access this mode, the LT0 toggle must be set to on, and the LT1 toggle must be set to off. This may be used to check proper character transmission over the tip and ring leads.

MDC attendant console

This part of the subsection provides telephone operating company personnel, or SL-100 maintenance personnel, with an overview of the MDC Attendant Console, and some of the installation and maintenance requirements for the console. It is suggested that NTP 297-2031-100, *DMS-100F Attendant Console OA & M* and NTP 297-YYYY-350, *DMS-100F Translation Guides* be referenced when performing work activities with the MDC Attendant Console.

Overview

Where a medium or large size business requires a dedicated call-handling attendant, then the MDC Attendant Console and corresponding MDC features can fill those needs.

The console is a self-contained unit equipped with various keys and lamps used to activate or display the associated MDC features that work with the unit. Also, the console is equipped with a speaker and headset jacks, including volume controls, to alert the attendant. A connector on the base of the unit provides all the power and signal connections. See Figure 4-58 on page 2-297 at the end of this subsection for a block diagram that shows the connection of the MDC Attendant Console to the DMS switch.

The NT4X09BB Meridian Services Attendant Console, Phase 2, replaced the Nortel Networks Integrated Business Network Services Phase 1 Attendant Console (rated manufacture discontinued). It provides the following enhancements:

- electrostatic discharge improved to 15 KV
- static mat requirements
- double headset operation
- reset
- IEC standard
- operational testing

The NT4X09BB console provides the customer with attendant-controlled service on premises. It transmits data to the switch at 300 baud and receives the data from the switch at 1200 baud. Trunks and lines are not tied directly to the console. Instead, the attendant is involved only in one call at a time, and only long enough to complete or

otherwise dispose of a call. The console uses up to six loops to gain access to calls routed to it.

The console operates over a standard telephone wire loop with a maximum loop-length of 4,877 m (16K ft.). The recommended DC resistance is 1300 Ohms with no greater than 8 dB loss at 1 KHz.

The console has two modes of transmission, normal and DTMF. The modes are controlled by a console DTMF on/off key equipped with an LED indicator.

NOTE: For effective performance there should be no bridge tap on the line.

Installation

The outside plant requirements for the voice circuit are:

Two wire Impedance	900 ohms
DC Resistance	441 +/- 22 ohms
Transmit Gain	2 dB nominal
Volume Control	-15 dB to -2 dB
Sidetone	-9 dB to +4 dB

It is recommended that data loops meet the requirements of data lines, specifically:

• Slope-Frequency Response — 3 dB at 404 and 2804 Hz, compared to loss at 1004 Hz

• Loop Noise Level — 59 dBrnC

• Impulse Noise — no more than 15 counts in 15 minutes, tallied at a level above the threshold of 6dB below the received data level

• C Notched Noise — ratio of 1004 Hz tone signal to C notched noise meets or exceeds 24 dB

LEN assignments

The MDC Attendant Console is connected to a LCM/RLCM/RLM/LM via three Type A Line Cards; one for voice, and two for transmitting and receiving Frequency Shift Keying data from the switch.

To minimize impact on consoles during peripheral module controller takeovers and take backs, all three LENs (Line Equipment Numbers) should be assigned to the same LSG (Line Sub Group) in the same LCM or RLCM, or the same LD (Line Drawer) in the same LM or RLM.

The assignments should be made horizontally (not vertically) in the LSG or LD, for administrative reasons. Since all three console lines are assigned to one PM controller, the console only reacts to one PM controller malfunctioning, rather than to two or three controllers spread over different PMs. The single LCM, LM, RLCM, or RLM may be placed on a *priority* list for monitoring by maintenance personnel.

For protective redundancy, MDC Attendant Consoles serving the same customer group or customer subgroup should not be assigned to the same peripheral (LM, LCM, or LGC).

In the case of an LM or RLM, the line card used for all three LENs is NT2X17AB. In the case of an LCM or RLCM, an NT6X17AD line card is used for all three LENs.

MDF special safeguard protection

To protect the attendant console from electrical interference, the main distributing frame near the DMS and the distributing frame located at the customer's premises (if applicable) should contain special safeguard protection (SSP) on all console voice and data lines. SSP protection involves placing red plastic tags on exposed MDF contacts, to warn maintenance staff of the sensitive nature of the circuits.

Dmodems

Digital modems (Dmodems) support the attendant console receive and transmit data lines. The Dmodems reside in MTMs.

Two adjacent circuit packs comprise a four-port Dmodem unit. The NT3X02AA TOPS Control Processor circuit pack is always to the left of the NT3X03AA TOPS Digital Signal Processor circuit pack. The NT3X02AA is always in an odd-numbered slot, while the NT3X03AA is always in an even-numbered slot. They cannot be assigned to an NT2X58AA MTM type shelf. If assigned to an NT2X58AU MTM type shelf (MTM for Digital Recorded Announcement, DRAM), they are restricted to slots 15 and 16. Dmodems are datafilled in table DMODEM—see NTP 297-YYYY-350, *DMS-100F Translation Guides.*

Three-port conference circuits

The NT1X31AA Three-Port Conference Circuit provides the attendant console with three-way calling. Six circuits are located on the circuit pack. The two adjacent slots to the right of the N1X31AA must be left blank, but the circuit pack may be mounted in slot 16 of the MTM.

As a substitute, the NT3X67AA Six-Port Conference Circuit may be used instead. The NT3X67AA may be used as two three-port conference circuits, or as a single six-port conference circuit. The same slot rules as those for the NT1X31AA circuit pack apply.

Three-port conference circuits are data filled in table CONF3PR and six-port conference circuits are data filled in table CONF6PR (unless they are assigned as three-port conference circuits in table CONF3PR).

NOTE: When an MDC Attendant Console is placed inservice from a MAP, a DMODEM and a three-port conference circuit become dedicated to that console. They are not released until the console is busied out.

Tone cards

The NT3X68AC Tone Card provides tones to MDC subscribers. There are no special plug-in requirements for NT3X68AC circuit packs.

Tones are declared in table TONES.

Cabling

There are no special requirements for the attendant console between the distribution frame on the customer's premises and the console itself. However, if the loops pass through an electrically noisy environment (e.g., electric motors, fluorescent lamps), then shielded cable should be used. One site whose console loops run past fluorescent lamp fixtures changed to shielded cable—console performance improved significantly. The site has about 55 feet of Belden #93334, type 605-15PR. Each pair is wrapped in foil and has a third bare conductor with each pair.

Electrostatic discharge

Electrostatic discharge (ESD) has been found to cause some attendant consoles to fail. In Phase II of the attendant console, the electrostatic discharge protection of the console has been significantly increased, virtually eliminating the need for ESD mats.

Environment

NTP 297-2031-100, *DMS-100F Attendant Console OA & M*, specifies the following environmental requirements for attendant consoles to meet all performance and reliability parameters:

- Operating temperature 4°C to 38°C (40° to 100°F)

- Nonoperating temperature -4°C to 49°C (-4°F to 140°F)

- Operating relative humidity 25% to 55% (noncondensing)

- Nonoperating relative humidity 10% to 95% (noncondensing)

The area an attendant console resides in should be monitored during the heating season to ensure the above conditions are met. When operating at low humidity levels below 30%, additional measures to control ESD may be required.

Power supply

To ensure proper operation, MDC Attendant Consoles require a power supply of 1.2 amps at -48VDC +/- 10%. Each console consumes 15 watts maximum.

Consoles within 600 cable feet of the supporting PM are powered directly from the PM Frame Supervisory Panel (FSP) over a fourth twisted pair.

Consoles more than 600 cable feet from its supporting PM require a separate power supply. PYLON (PYLON is a trademark of Pylon Electronic Company) power supplies are commonly used. No more than two attendant consoles should be attached to a single power supply. Note that it was found during field tests that removing the

power supply ground strap (producing a floating ground) did not change console failure rate.

Further information on PYLON power supplies and the strapping and testing requirements can be found in NTP 297-2031-100, *DMS-100F Attendant Console OA & M*.

MDC Attendant Console data tables

The following tables are required for the MDC Attendant Console:

- IBNLINES
- ATTCONS
- CUSTCONS
- FNMAP
- WCKCODES
- ICIDATA
- CUSTHEAD
- SUBGRP
- DMODEM
- CONF3PR/CONF6PR
- TRBLCODE

See NTP 297-YYYY-350, *DMS-100 Translation Guides* and NTP 297-2031-100, *DMS-100F Attendant Console OA & M*, for supporting information and examples on the tables required for MDC Attendant Consoles

Maintenance

Once a week, post each MTM at the MAP PM level and perform an inservice test:

```
>MAPCI;MTC;PM
>POST MTM <MTM __ number>
>TST
>QUIT
```

Dmodems should be added to the ATT schedule. They should be tested daily and if any fail, they should be replaced. The results of this testing must be examined daily.

Even though manual tests can be run on the NT1X31AA Three-Port Conference Circuits (CF3Ps) from the TTP level of the MAP, the CF3P conference circuits should be scheduled to run daily by the Automatic Trunk Test (ATT). The results need to be examined daily and circuit pack replacement carried out as required. NTX001AA G0060 enhances the test to provide two-way transmission tests between all ports on the bridge (3/6 port).

To ensure detection of PM troubles that may affect console operation, the PM REX test must be scheduled. These include LM, LCM, RLCM, LGC, DTC, and other

types. The REX test may be enabled by parameters LCDREX_CONTROL and
NODEREX_CONTROL in table OFCVAR.

MDC Attendant Console diagnostics

The diagnostics listed in this section shall be performed during a low traffic period
when attendant consoles are not in use, as they involve busying out the console under
test. These tests should be performed bi-weekly: typically, early Monday morning.

Dump table ATTCONS in the following manner:

```
>TABLE ATTCONS
>SEND <printer __ name>
>LIST ALL
>SEND PREVIOUS
```

You now have a list of all MDC Attendant Consoles datafilled on your DMS switch.

Using the following commands post the first console to be tested at a MAP:

```
>MAPCI;MTC;LNS;LTP;IBNCON
>POST L <site> <LEN> L
```

Where <site> and <LEN> are one of the console's LENs in table ATTCONS. The
<site> applies only if the host PM is an RLM or RLCM. The <LEN> is the Line
Equipment Number, consisting of <frame> <module> <drawer (for LM, RLM) or
LSG (for LCM, RLCM)> <line __ card>. The "L" (lines) option at the end of the
command requests all lines associated with the console be posted.

The MDC Attendant Console and its lines should now be posted. Note the DMO,
DEM, and CF3P numbers from the display. If the *state* of the console is CPB (Call
Processing Busy), post another console. If it is not CPB, then continue as follows:

```
>BUSY
```

If the state of the console is CPB and the customer group has given permission to
work on the console, ensure console has been unplugged before proceeding.

```
>FRLS
```

If FRLS does not work, try the following command and try commands FRLS or
BUSY again.

```
>AC <console __ CLLI> RESET
```

Now perform diagnostic tests on the console and its voice and data loops:

```
>SEIZE
>DIAGNOSE
>RELEASE
```

Go to the LTP level and test all three line cards associated with the console:

```
        >LTP
        >POST <site __ name> <LEN> L
```

```
>BUSY
>DIAGN
>RTS
```

Diagnose the Dmodem and CF3P circuits (identified when the console was first posted) by following the commands listed in parts of this document.

After all problems have been cleared by following the card lists displayed, then return the console back to service:

```
>LNS;LTP;IBNCON
>POST L <site> <LEN> L
>RTS
```

Maintenance guidelines summary

Frequency	Operation
Ongoing	Watch for MDC Attendant Console alarms Check MDC Attendant Console state Monitor IBNXXX Logs
Weekly	Test MTM Test Dmodems** Test CONF3 Circuits** Test LGCs* Test LCMs or RLCMs* Test LMs or RLMs*
Bi-weekly	Test MDC Attendant Consoles
Monthly	Measure power supply voltages

    *   Test these PMs using REX Test
        See the *Preventive Maintenance*
        section of this manual for scheduling.

    ** Test CONF3 Circuits & Dmodems
        using ATT. See the *Preventive Maintenance*
        section of this manual for scheduling.

Console go-no-go tests

The console is equipped with a "console test key" that allows for a go-no-go tests initiated from the keys on the console. See NTP 297-2031-100, *DMS-100F Attendant Console OA&M*, that provides a table of procedures for performing these tests.

MDC Attendant Console power supply tests

On a monthly basis, visit the consoles (including those consoles fed from FSPs). Measure DC voltage with a DMM (Digital Multi-Meter). It should be 48 volts +/- 2.4

volts. Measure and chart AC voltage at the same points, and from each point to ground. It should remain constant from month to month.

Headsets

Experience with headset brands and substitution of handsets for headsets, has led to the following recommended sets:

- Plantronics Starset II Headset
- Plantronics Supra Headset
- Nortel Networks Type G Handset

When a second headset is used with the NT4X09AF or AG console for training or other purposes, then the volume control will need to be adjusted after inserting or removing the second headset.

If using headsets or handsets other than the recommended above, and customers complain about the transmit volume, then a transmit gain strap can be used to adjust the transmit volume. For instructions see "Transmit gain strap adjustments" in NTP 297-2031-100, *DMS-100F Attendant Console OA&M*.

MDC Attendant Console logs and OMs

There are four logs that support the MDC Attendant Console: IBN101, IBN102, IBN103, and IBN104. Operational measurements (OMs) for the console are found in the ACSYSTR, ACRTS, ACTRBL, and ACTAKEDN OM groups. See the following "Troubleshooting techniques" for further information on IBN logs and console OM groups.

A good description of both the logs and OMs for the console can be found in NTP 297-2031-100, *DMS-100F Attendant Console OA & M*. The relationship of console logs to OMs can be found in NTP 297-YYYY-814, *DMS-100F Operational Measurements*. Also, for those using the Switch Performance Monitoring System (SPMS), see NTP 297-1001-330, *DMS-100F SPMS Application Guide* for information on the ATTCNERR index that measures MDC Attendant Console errors.

Troubleshooting techniques

Alarms

For craft personnel to quickly detect console problems, establish additional alarms using the OM Threshold feature described in the *Preventive Maintenance* section of this manual. Select key OMs for the OMTHRESH table from the list of console OMs listed in "MDC Attendant Console OMs" on page 4-290.

IBN log description

IBN logs, for the most part, are console logs. Detailed explanations of these logs may be found in NTP 297-YYYY-840, *DMS-100F Log Report Manuals*.

Analyzing and charting IBN logs

To check IBN logs for console problems, enter the following at a printer terminal:

```
> LOGUTIL
> OPEN IBN
> WHILE (BACK) ()
> QUIT
```

A history of IBN logs should be output. Skim the printout for *repeated offending* consoles, Dmodems, and CF3P circuits. One handy way of analyzing logs is to focus attention on IBN103 return to service (RTS) logs. Identify the console, Dmodem number, PM, etc., and chart the information in a format like the log analysis chart at the end of this subsection. The fields of the chart are as follows:

DATE:	Date of IBN103 log.
TIME:	Time IBN103 log output
GRP:	Customer group abbreviation (points to common outside plant or remote power supply problem).
CONS:	Last two numbers of console CLLI.(Console number).
CAUSE:	Cause of console being placed in MANB state, per immediately preceding IBN logs.
DMODEM:	Dmodem number, output with logs (by examining the chart, it should point to intermittent Dmodems, or a fault MTM)
PM:	PM that attendant console is homed on. (see summary chart) (points to PM load or controller problems, or to RLM/RLCM carrier problems)
COMMENTS:	Analyzer's remarks (e.g., "LCM HOST 0 1 reloaded at 0745").

Now, given a chart of IBN103 logs (as per the sample log analysis chart at the end of this subsection), the analyzer may pick out the poorest performing consoles and intermittent or faulty hardware and circuits. These items may then be tested thoroughly and replaced accordingly. If the cause is not apparent, get the date and time of the IBN103 log and look at the adjacent system logs from the log printer for possible causes (e.g., RLCM carrier bipolar violations (BPV) causing a console connected to the RLCM to go down). If analyzed every couple of days in this manner, attendant console failures should be reduced to acceptable levels.

Console SWERRs

Sometimes an attendant console causes a SWERR (software error). At times when this happens, an IBN log is output to indicate that a console is in trouble, but posting each console at the MAP IBNCON level reveals nothing. One cause is if an MTM has been busied out for maintenance action, or has gone system busy for some other reason. Consoles using Dmodems or CF3Ps in the busied out MTM will be left in an

uncertain state, even though posting the consoles may show them to be unplugged or CPB (call processing busy).

At a printer terminal execute the following command:

>LOGUTIL;OPEN IBN;FORWARD <number or ALL>;QUIT

Look for other similar logs, up to several hours previous. Once the console has been identified, and with the customer's permission, busy and return to service the console from the IBNCON level. This usually cures the problem; however, if it does not help, contact your next level of support.

Operational measurements (IBN OMs)

Operational measurements (OMs) may be used to identify problem areas in the DMS that may affect attendant console performance. For example, executing:

>OMSHOW LMD ACTIVE

will point to a malfunctioning LCM if the NORIGATT field is compared to the ORIGBLK and TERMBLK fields. OM group PM2 may also help in pointing to malfunctioning PMs.

The IBNAC OM group identifies the customer, subgroup, console, and 17 registers to record in real time the various console operator's work function activities, such as: position busy, headset plugged in, calls placed on hold, and originating calls.

MDC Attendant Console OMs

Operational measurements for the console have been enhanced. Selected maintenance MDC console OMs are summarized below with a brief description of the registers within each group. From this summary, select key MDC console OMs for tracking performance. You can also use the registers with the OM Threshold feature to alarm and analyze various problems on a real time basis.

The following registers in OM group ACSYSTR measure shortages of console related resources:

ACDMOVFL	shortage of digital modems
ACCF3POV	shortage of conference 3-ports
ACDMFL	various Dmodem related reasons
ACCF3PFL	various CF3P related reasons
ACEXOVFL	shortage of AC extension blocks
ACDATAER	datafill error
ACERR	summary of OM counts (Group ACTRBL)
ACFLT	summary of OM counts (Group ACTAKEDN)

The following registers in OM group ACRTS contain peg counts related to attendant console return to service attempts:

ACRTSMAT	manual RTS attempts
ACRTSSAT	system audit RTS attempts
ACRTSNOR	no response from AC
ACRTSCC	circuit confusion

ACRTSIL	integrity lost
ACRTSNWB	network blockage
ACRTSCHC	channel congestion
ACRTSCRL	AC circuit put out-of-service
ACRTSCAR	carrier failure
ACRTSSE	system error

The following registers in OM group ACTRBL measure console errors not serious enough to take down the attendant console:

ACTRCC	circuit confusion
ACTRPFO	parity, framing or overrun error
ACTRRES	AC has reset
ACTRCARF	carrier failed
ACTRSYS	console system error
ACTRDMFL	bad dmodem message
ACTRCTRL	circuit released
ACTRSERR	console software failure
ACTRSFLT	call lost on the AC
ACTRCLFR	call lost due to AC take down
ACTRCNR	no response from AC

The following registers in OM group ACTAKEDN count errors that can cause a console to be taken out-of-service:

ACTDCC	circuit confusion
ACTDINLO	integrity lost
ACTDINKY	AC generated invalid key codes
ACTDPFO	parity, framing or overrun errors
ACTDRES	AC reset
ACTDCARF	carrier failed
ACTDSYS	console system error
ACTDDMFL	bad Dmodem message
ACTDCTRL	circuit released
ACTDSERR	console software failure
ACTDMAN	console force released manually
ACTDAUD	console system force release
ACTDCNR	no response from console

Individual console OMs

The "IBN Attendant Console OM on an Individual Console Basis" feature in software package NTX856AA provides for the generation of OM reports for individual customer MDC Attendant Consoles. The OM information is available in real time using the INACOM (Individual Attendant Console OM) level of the MAP, or the normal OM log reporting routine.

To access the INACOM level, type MAPCI;IBNMEAS;INACOM from the CI level of the MAP. The following figure is an illustration of the INACOM level of the MAP.

Figure 4-55 — INACOM level of the MAP

```
 CM    MS    IOD     Net  PM   CCS      Lns       Trks   Ext   APPL
  .    .    .      .    .    .      .      .      .      .

                  Customer Group      Subgroup          Consol * NS  *
INACOM|           START TIME:   yyyy/MM/dd      hh  :   mm   ss.sss     day
0    Quit         |
2                 |  IACLDN   :  IACINTRP    :      IACDIAL0    :
3    Select_      |  IACXFRAT:  IACCFW       :      IACRECAL    :
4                 |  IACSPCL  :  IACQTOTL    :      IACHLD      :
5                 |  IACORIG  :  IACEXTD     :      IACPOSBY    :
6    NextSG       |  IACAUTH  :  IACLDN1     :      IACLDN2     :
7    NextCON      |  IACLDN3  :  IACLDN4     :      IACLDN5     :
8                 |  IACLDN6  :  IACLDN7     :      IACLDNR     :
9    QLDN         |
10                |
11   StartOM      |
12   StopOM       |
13                |
14                |
15                |
16                |
17                |
18                |
 _____|
Time:  hh  :   mm   >
```

Console summary chart

To aid in troubleshooting, prepare an *attendant console summary chart* by compiling data extracted from DMS tables. To dump a table, follow this example at a printer terminal:

>TABLE CUSTHEAD

>LIST ALL

>QUIT

Dump tables to fill in the following chart fields:

CHART FIELD	TABLE
Customer Group	CUSTHEAD
Console CLLI	ATTCONS
Directory Number	(QLEN LENs from ATTCONS)
LEN	ATTCONS
Host LGC (if applicable)	LCMINV

A sample at the end of this subsection shows how handy this chart can be in times of emergency and nonemergency troubleshooting.

IBNCON MAP level

The quickest way to check an attendant console is to post it.

> **MAPCI;MTC;LNS;LTP;IBNCON**

> **POST L <site> <LEN> L**

   or

> **POST G <CLLI>**

   or

> **POST S <state> (see below for states)**

The state will be on the right hand side, about halfway down the screen. Possible states are as follows:

CODE	STATE	DESCRIPTION
NRDY	Not Ready	The Attendant Console has been un-plugged and is currently going through a 60-second time-out period. No call processing activity or maintenance activity (except Force Release) can occur.
CPB	Call Processing Busy	The Attendant Console is jacked in and is in-service. Call processing can take place. Console cannot be seized for maintenance purposes.
SZD	Seized	The attendant Console has been seized for maintenance activity by operating company personnel. A digital modem has been allocated, and maintenance activity can take place. Call processing can not occur.
UNJK	Unjacked	The Attendant Console is in service, but the headset or handset has been un-plugged and the 60-second time-out has occurred. Neither call processing nor maintenance activity can take place.
OFFL	Off Line	The Attendant Console is hardware and software equipped, but is not in-service. Call processing cannot take place.
MB	Manual Busy	The console has been removed from service by the tester using the command FRLS. Call processing cannot take place.
SB	System Busy	The Attendant Console has been re-moved from service by system maint-

enance action.

UNEQ	Unequipped	The Attendant Console has not been software equipped (data filled).
DEL	Deloaded	A temporary state assigned to an Attendant Console, upon completion of call processing, if maintenance personnel have requested the console while it was in the CPB state.

ACMON MAP level

The ACMON (Attendant Console Monitor Display) displays information about a specified console at MAP. The information is updated every four seconds on the MAP. To access the ACMON MAP level, type in MAPCI;IBNMEAS;ACMON at the CI level of the MAP. The following figure is an illustration of the ACMON MAP level.

Figure 4-56 — ACMON level of the MAP

```
CM     MS   IOD      Net      PM    CCS     Lns        Trks    Ext   APPL
 .      .    .        .        .      .       .           .      .      .

   ACMON         CLLI            CUSTGRP         SUBGRP     AC STATE
                 ATTKDKA         COMKODAK          0         UNJK    *NS*
0  QUIT
2                CONF:           CF3P            110          DM:  DMODEM 13
3  SELECT_
4                AC FEATS:       WILDCARD        IBN FEATS:    3WC
5                                PARK
6  NEXTCON
7                MSGCNT:    7                    RESENT:    C
8
9                           **LOOP INFORMATION**
10
11
12               LOOP        SRC                DEST            STATE
13               1:CKT   INMF   15              DN   6137227005  ACT
14               2:DN    6137221235             DN   6136211235  HLD
15               3:DN    6139995132                              HLD
16               4:                                              IDL
17               5:                                              IDL
18               6:                                              IDL
                 ACMON:
Time:   hh  :  mm
```

Attendant console debugging tools

TID-1001-004, *Attendant Console Software Debugging Tools*, provides three commands used to investigate software problems associated with consoles in the field or in a captive office environment. The commands are MT (Message Trace), QQ (Query Queues), and AC (Attendant Console trace).

> **NOTE:** Only Tier II personnel trained in DMS-100F software should attempt to utilize these commands.

This document is available to those companies that have a Technical Information Agreement (TIA) with Nortel Networks.

References

Table 4-24   —   Sample attendant console summary chart

Customer Group	Console CLLI	Directory Number	LENS (In/Out/Talk)	Host LCG
City of Toronto	Z1T013011	555-7000	HOST 01 1 10 00 HOST 01 1 10 01 HOST 01 1 10 02	1
City of Toronto	Z1T013021	555-7000	HOST 01 0 07 01 HOST 01 0 07 02 HOST 01 0 07 03	0
Toronto Transit	Z1T029011	555-2000	EGLT 24 0 15 29 EGLT 24 0 15 30 EGLT 24 0 15 31	5
Toronto Transit	Z1T029021	555-4000	DUFF 13 0 03 01 DUFF 13 0 03 02 DUFF 13 0 03 03	7

Table 4-25   —   Sample IBN log analysis chart

(Key on IBN103 logs with Return To Service (RTS))

Date	Time	GRP	CONS	Cause	DMODEM	PM
5/24	0805	GOC	51	System Error	17	HOST 0 1
5/24	0805	CBC	30	System Error	12	HOST 0 3
5/24	0804	GOC	51	System Error	8	HOST 0 1
5/26	1206	GOC	21	MB/no response	5	HOST 0 1
5/26	0940	GOC	11	System Error	4	HOST 0 1
5/26	0932	GOC	31	System Error	6	HOST 3 1
5/26	1536	GOC	41	Integ Lost	7	HOST 4 1

Figure 4-57 — Attendant console cable/pin assignments
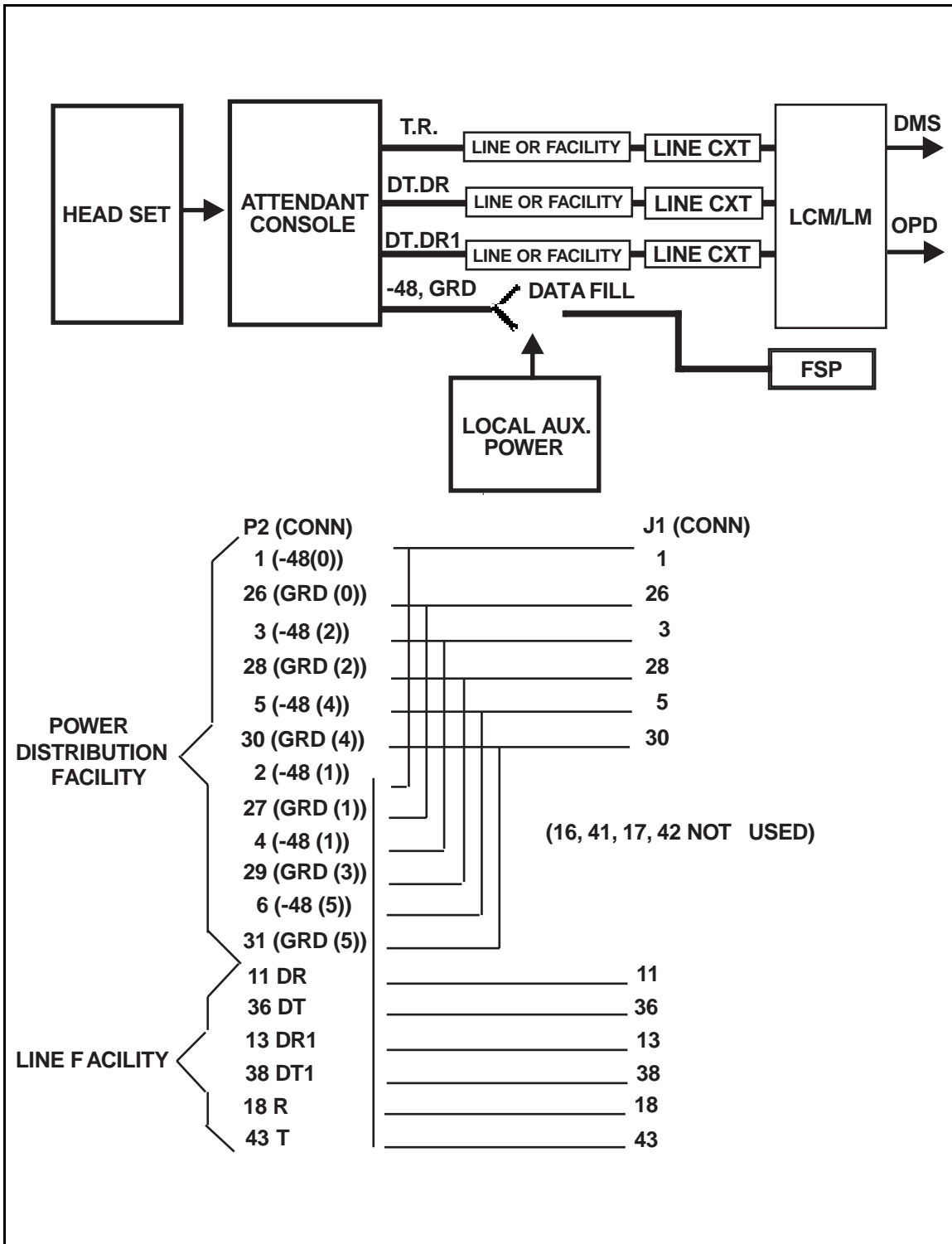
Figure 4-58 — Attendant console/DMS block diagram
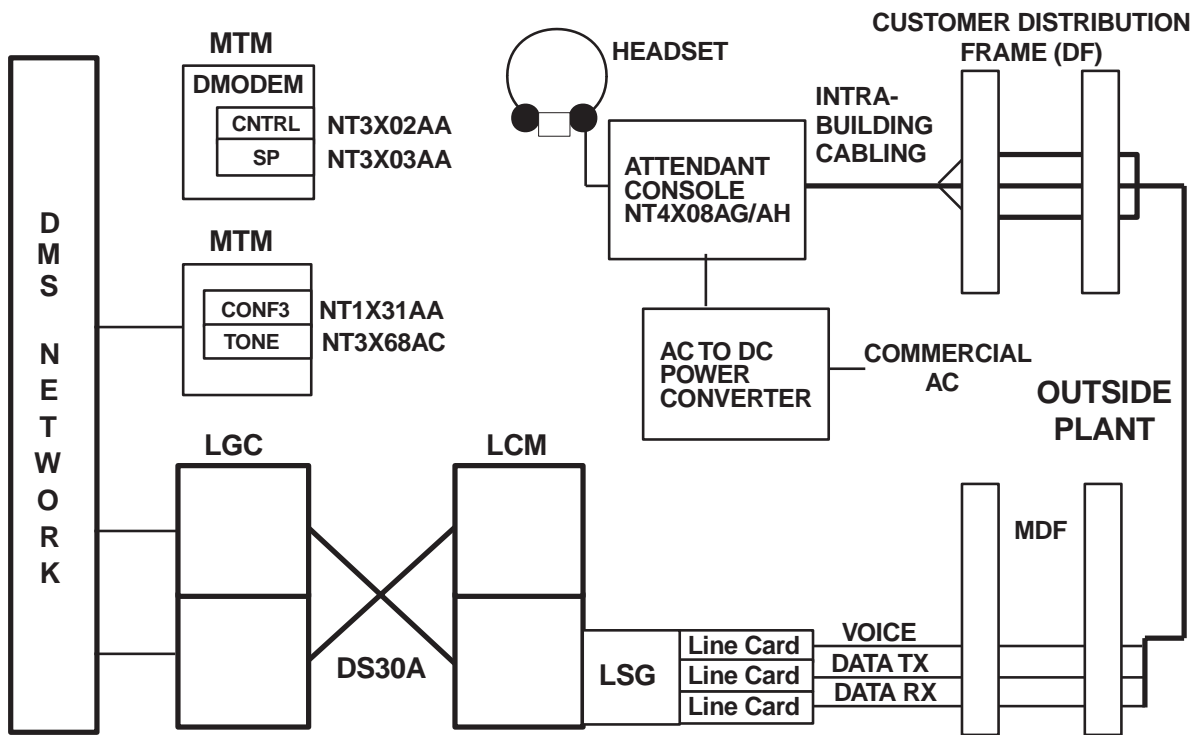
RSC Overview and Maintenance

This subsection provides an overview and maintenance related information for the Remote Switching Center (RSC). For more detailed information, including advanced troubleshooting, see NTP 297-8221-550, *DMS-100F Remote Switching Center Maintenance Manual.* For additional information on the Cabinetized RSC or RSC-Sonet, see PLN-8991-103, *Engineering Manuals* or PLN-8991-104, *Provisioning Guides.* Other information for RSC-Sonet can be found in NTP 297-8261-550, *RSC-SONET A Maintenance Manual* or NTP 297-8281-550, *RSC-SONET B Maintenance Manual.*

RSC overview

The largest member of the remote family is the Remote Switching Center (RSC). It is comprised of a Remote Cluster Controller (RCC), one or two Remote Maintenance Modules (RMMs), and up to nine LCMs. The RSC uses hardware that is common to that of the DMS-100 Family System host office. The RCC is based on the LGC. The LCMs associated with the RSC use the same line cards as in the host office.

The main component of an RSC is the remote cluster controller (RCC). The Remote Cluster Controller (RCC) is a remote Line Trunk Controller type peripheral controller module in a RSC. It can support Line Concentrating Modules, digital trunks, and Remote Line Concentrating Modules (that is, remotes off of a remote). RCCs are connected to a Line Trunk Controller or to a Digital Trunk Controller by means of DS1 C-side links. RCCs may be equipped with Emergency Stand-Alone (ESA).

The RCC with Peripheral Life Upgrade Strategy (PLUS) provides a universal processor (UP) for all units at the RSC. The RCC is supported by a host line group controller/line trunk controller (LGC/LTC).

Advantages of RCC with PLUS

Advantages provided by RCC with PLUS are:

- replacement of five cards with one UP card in each unit of the RCC, resulting in overall reduction of power consumption
- increase of RCC memory from 5 Mb to 8 Mb, with a potential expansion of up to 16 Mb
- increase in real time capacity

- downloadable firmware, electrically erasable programmable read only memory (EEPROM), on the NTMX77 card. This card is equipped with two FLASH EEPROMs, or banks, which are two 256 Kbyte programmable chips. These FLASH EEPROMs allow operating company maintenance personnel to load the firmware independently of the random access memory (RAM) load on a manually-busied (ManB) RCC, or a ManB unit of the RCC, when using the following command strings:

  > LOADPM PM CC FIRMWARE

   or

  > LOADPM UNIT unit_no CC FIRMWARE

Figure 4-59 on page 2-300 is a functional block diagram, showing the four sections which make up the RCC PLUS:

- Host communications section
  — NT6X72AA Host Link formatter Card
  — NT6X50 DS1 Interface Card

- Processor section
  — NTMX77 Unified Processor and Memory Card

- Speech Bus complex
  — NT6X72 Host Link formatter Card
  — NT6X69 Message Processor Card
  — NT7X05 Peripheral Loader Card
  — NT6X78 CLASS Modem Resource Card
  — NT6X92 Universal Tone Receiver Card
  — NT6X44 Time Switch Card

- Peripheral communications section
  — NT6X44 Time Switch Card
  — NT6X48 DS30A Interface Card
  — NT6X50 DS1 Interface Card

Host communication cards

The following cards translate between the 16 host DS1 ports and the parallel speech bus:

- NT6X50 DS1 Interface Card — provides the two-way voice and message interface between the 24-channel, bipolar, serial bit stream of the DS1 links and the 32-channel serial bit stream of the NT6X72 card.

- NT6X72 Link Formatter Card — converts the sixteen 32-channel serial bit stream of the NT6X50 to the 512-channel parallel speech bus and vice versa. The 512 speech channels are added to the 128 internal channels.

Figure 4-59 — Functional block diagram of RCC with XPM PLUS
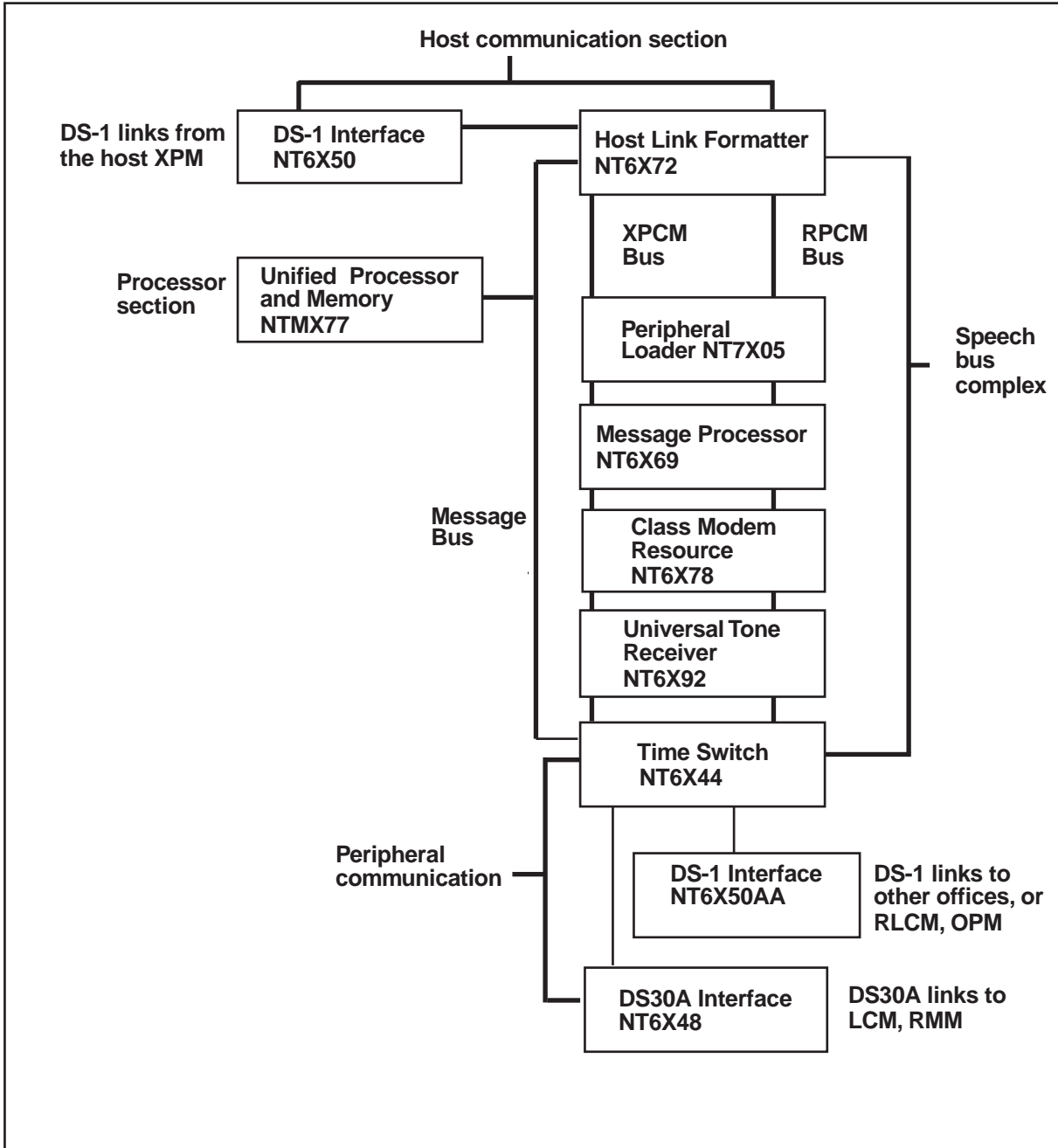
Universal Processor (NTMX77)

The Universal Processor (UP) replaces the NT6X45, NT6X46, and NT6X47 cards in each RCC shelf. The UP provides increased memory and real-time capacity, expandable memory, and decreased power consumption.

NOTE: Filler face cards (NT0X50) are located in slots 08 through 12, previously occupied by the NT6X45, NT6X46, and NT6X47 cards.

Speech bus cards

The speech bus is actually two speech buses, send (XPCM) and receive (RPCM). Following are the cards on the buses:

- NT7X05 Peripheral Loader Card — provides local storage of XPM loads and images in a nonvolatile, nonmechanical-based memory card.

  XPM peripheral loader (XPL), provides the ability to reduce XPM simplex time by allowing XPM software loads to be transferred to the XPM and stored locally within an XPM unit while the unit is in-service. This allows replacing an existing loadfile with a newer loadfile. During the process of replacing a loadfile, the last image is still available for recovery actions if required. The local storage mechanism is the NT7X05 circuit pack. The software is later transferred by instructing a XPM unit to load itself from the NT7X05 card, with the enhanced LOADPM command, while manually-busy (ManB).

- NT6X69 Message Processor Card — interfaces and processes signaling and control messages between the RCC and the CC.

- NT6X79 Tone Generator Card — provides tones, this card is only provided with the AA version of the NT6X69, in all other versions of the NT6X69, the tones card is onboard.

- NT6X92 Universal Tone Receiver Card— identifies and processes pulse code modulation (PCM) tones for the 30 channels on the parallel speech bus.

- NT6X44 Time Switch Card — concentrates the 20 peripheral-side (P-side) ports to 16 central-side (C-side) ports and allows service circuits to be shared among all ports and channels.

- NT6X72AA Host Link Formatter or NT6X72AB Remote Link Formatter — serial to parallel and parallel to serial conversion, network message interface, shelf clock generation, raw T1 clock generation, time slot mapping, looping unused C-side channels for intracalling, and transparent A/B bit mapping.

- NT6X78 CLASS Modem Resource Card

  The NT6X78 custom local area signaling service (CLASS) modem resource (CMR) card supports Calling Number Delivery (CND) and other CLASS services. The CMR card provides the Analog Display Services Interface (ADSI) protocol to transmit CLASS data between the CC and ADSI compliant customer premises equipment (CPE).

  The NT6X78AB, the NT6X69AD, and the NT6X92BB cards are required for compliancy with ADSI protocol. ADSI protocol supports CLASS features that provide display-based information, such as deluxe spontaneous call waiting iden-

---

tification (DSCWID), to subscribers with ADSI-compatible customer premise equipment (CPE). For further information on the ADSI protocol and DSCWID, see NTP 297-8221-550, *Remote Switching Center Maintenance Manual.*

Peripheral communication cards

The following cards translate between the 20 P-side ports and the parallel speech bus:

- NT6X44 Time Switch Card — translates between the parallel speech bus format and the NT6X48 and NT6X50.
- NT6X50 DS1 Interface Card — provides the interface to DS1 links that connect to other offices, remote line concentrating modules (RLCM), or outside plant modules (OPM).
- NT6X48 DS30A Interface Card — provides the interface to LCMs and RMMs.

Speech and message paths in the RCC

The following figure specifies the speech and message paths of the RCC. Refer to Figure 4-60 on page 2-303, while reading the following paragraphs.

NOTE: The parallel speech bus consists of a transmit PCM bus (XPCM) and a receive PCM bus (RPCM).

Intermodule communication

For the RCC to work effectively, there must be adequate communication between the RCC units so that, for example, the inactive unit can take over call processing if necessary. RCC units communicate over the intermodule communication links (IML). There are two IML links, one connecting NT6X69 cards (at 64 kb/s) and the other connecting NT6X45 cards between each unit (at 19.2 kb/s). The NT6X69 link allows general interunit messaging, such as updating call processing information in the inactive unit. The NT6X45 exchanges call processing data.

RCC to host communication

The RCC communicates with the host over message links 0 and 2. If both links fail, the RCC cannot communicate with the host, and emergency stand-alone (ESA) is enabled.

RSC maintenance

Basic maintenance support for the RSC includes:

- Low-level types
- Office data management
- MAP
- I/O system
- Messaging

Figure 4-60 — RCC speech and message paths

Host communication section

DS-1 links from the host XPM — DS-1 Interface NT6X50 — Host Link Formatter NT6X72

XPCM Bus — RPCM Bus

Processor section — Unified Processor and Memory NTMX77

Peripheral Loader NT7X05

Speech bus complex

Message Processor NT6X69

Message Bus

Class Modem Resource NT6X78

Universal Tone Receiver NT6X92

Time Switch NT6X44

Peripheral communication

DS-1 Interface NT6X50AA — DS-1 links to other offices, or RLCM, OPM

DS30A Interface NT6X48 — DS30A links to LCM, RMM

- Maintenance aspects
- Speech aspect
- BST/RTS/OFFLINE
- Loading
- Tests/audits
- SWACT (SWitch ACTivity
- DS1 maintenance
- P-side modes

SWACT

The RSC provides the capability for warm SWACT in the RCC so that established calls are preserved in an activity switch between mate units. Messaging between the RSC and the CC passes through the Channel Supervision Messaging (CSM) hardware of the LGC. The CSM hardware of the LGC keeps the Master Processor (MP) of the LGC aware of connection data in the RSC. This awareness allows CSM to survive SWACT of the LGC, it allows warm SWACT of the LGC.

DS1 maintenance

DS1 maintenance on P-side ports of an RCC is identical to that provided for an LGC. However, an RCC has DS1 maintenance on its control side links, which interface as remote links with DS1 maintenance of the peripheral side of the host. For additional information on DS1 maintenance, see the "Carrier Maintenance" subsection within the *Preventive Maintenance* tab of this manual.

P-side modes

P-side modes allow maintenance on DS1 links connected to the control side of the RCC. Most functions provided are similar to those currently available in DS1 maintenance for peripheral side DS1 links. The functions are called by the CC, either by itself or in response to MAP maintenance commands. The maintenance functions provide four capabilities:

- enable/disable monitoring of DS1 circuit physical presence
- enable/disable maintenance monitoring of DS1 circuits
    — monitoring slips within elastic maintenance store of a DS1 circuit
    — counting all occurrences of lost frame pulse
    — monitoring levels of bipolar violations
    — monitoring remote alarm indicator
    — monitoring local alarm
- access the counters and status of DS1 circuits
- monitor the DS1 link of an inactive unit

Remote maintenance module

The RMM is a shelf module derived from the MTM consisting of:

- A single control card
- An optional group codec card
- Two power converters
- Up to 14 service circuit cards

A maximum of two RMMs may be provisioned at an RSC site, each occupying one shelf in the RSC bay. At least one RMM is recommended at each RSC site to perform diagnostic tests. Service circuit cards include scan, signal distribution, metallic access, metallic network, and line test unit. The RMM contains its own processor that performs scanning of the service circuits, test trunks, and alarm service circuit packs. The major differences between the MTM and the RMM are as follows:

- MTM DS-30 ports are replaced with DS-30A ports, which allows connection of the RMM to DS-30S links from the RCC
- MTM input/output protocol is replaced with DMS-X protocol. This enhances the reliability of the RMM by rendering it less vulnerable to noisy DS-1 link message corruption

The RMM is supported as a separate node off the peripheral side of the RCC. It is treated, for messaging and maintenance, as a stand-alone peripheral. RCC peripheral side links 0 and 1 are dedicated to the RMM. These two links cannot be datafilled otherwise.

RSC equipment maintenance

The maintenance of all RSC modules is integrated into DMS peripheral module maintenance performed at the MAP:

- LCMs, including their line cards and ringing systems
- RMMs and associated service circuits
- RSC control equipment and associated interfaces to LCMs, RMMs, and DS-1 links

The RSC MAP level looks like the LGC level with a few differences based on the RSC remote location and the C-side DS-1 links. All commands available to the LGC are available to the RSC with the addition of ESA commands.

Automatic and manual line testing

The RMM line test service circuits are used by the ALT diagnostic. RMMs operate with ALT as ALT is currently implemented. No changes or additional commands are required. See the "Line Maintenance" subsection in the *Preventive Maintenance* tab of this manual for details on line testing.

Automatic maintenance

When fault conditions occur, the remote switching system and DMS initiate system actions (such as audits) to find the fault and correct it automatically. If manual intervention is required, the appropriate trouble indicators are explained in NTP 297-8221-550, *Remote Switching Center Maintenance Manual*.

Essential line service for the RCC

Essential line service (ELN) for nodes off of an RCC requires essential service protection (ESP) and guaranteed dial tone (GDT). ESP is a CC feature that treats all originations equally until they reach the CC. If ESP is active, ELN originations are placed at the top of the origination queue. A call origination requires a call condense block (CCB). If an ELN call arrives and there are no CCBs available, the CC will steal a CCB from the oldest nonessential call origination. The nonessential line is treated as if it never had a CCB, and is discarded. If the queue is full and made up entirely of ELN lines, incoming ELN originations are discarded. Discarded ELN and non-ELN calls are handled by GDT; if the subscriber stays off-hook, the subscriber eventually receives dial tone.

ESP is activated at the MAP terminal with the ESP ON command.

Operational measurements (OM) keep track of the number of originations from ELN lines, the number of times an ELN origination had to steal a CCB, and the number of times that an ELN received delayed dial tone because no CCBs were available.

ELN for the RCC

The preferential handling of ELN lines applies to the RCC as well as the CC. ELN lines are placed at a higher priority in RCC call processing, and when the RCC cannot process all incoming calls, ELN lines receive priority over non-ELN lines.

How ELN is activated

Since ESP call processing occurs in the RCC, both the CC and RCC must have the same knowledge about lines ELN capabilities. The CC stores this knowledge in its data store, while the RCC stores it as static data. The following examples show how the CC and RCC receive the same data about a line:

- The RCC is in-service and ESP is ON.

  — If the RCC is in-service and ELN is added to an LCM line, the CC sends a message to the RCC. The RCC updates its knowledge automatically, activating ELN for that RCC line. Also, if ELN is deleted from a line, the CC sends a message to the RCC telling it to remove it from the LCM line.

- The RCC is manually busy and ESP is ON.

  — If ELN is added, the line configuration is not updated in the RCC until the RCC is returned to service. As part of the return-to-service sequence, static data is downloaded and, once the RCC is back in-service and processing calls, lines with ELN receive preferential treatment. Also, if ELN is removed, the RCC does not update

its configuration until it is returned to service. The state of ESP (OFF or ON) is not affected by any type of restart.

NOTE: Refer to the XPM Operational Measurements Reference Manual, for information on how calls are prioritized and which OMs track call traffic when the RCC enters overload.

Examples of CC versus RCC overload

With ESP, both the RCC and the CC process calls on a queue basis. These priorities are important when either the CC or the RCC enters overload. During overload, the CC and RCC work together. When the RCC becomes overloaded the RCC throttles new work for itself, and when the CC becomes overloaded the RCC throttles work for the CC. The following examples show how ELN calls are handled when either the CC or RCC goes into overload:

- When the CC enters overload:
    - Non-ELN traffic is throttled and placed in the last-in first-out (LIFO) queue. Some of these calls eventually reach the CC, while others are dropped and then handled by GDT.
    - ELN traffic is sent immediately to the CC, even though the CC is in overload. The CC puts ELN calls at the front of its first-in first-out (FIFO) queue.
- When the RCC enters overload:
    - ELN line originations have priority over non-ELN lines.

Overload indicators (PM128, QUERYPM)

When the RCC enters overload, a PM128 (RCC is ISTb) log is generated with the following message:

PM Overloaded

At the PM MAP level, posting the RCC and entering the command QUERYPM FLT generates the same message (PM Overloaded).

NOTE: The EXT104-108 logs, produced when ESP is turned on or off, are no longer produced. Also, the tuple ESP_ALARM has been removed from table SFWALARM.

When overload occurs, operating company personnel should immediately collect all relevant OMs that track the amount and types of traffic from the RCC. In some cases, the RCC enters overload because of a maintenance problem, such as network faults. In other cases, the overload relates to an under-engineering of the RCC configuration. Therefore, OM reports should be forwarded to both maintenance and engineering personnel for analysis.

Routine exercise test

A routine exercise test (REX) test includes a series of tests performed on an XPM unit, ideally initiated daily by the system scheduler or manually by operating company personnel. The REX test combines the diagnostic and functional routines available on XPMs. Results of the REX test can be divided into four classes:

- not performed
- passed
- failed
- aborted by manual action (that is, maintenance action with the FORCE parameter or with the ABTK command from another MAP terminal with the XPM posted)

All four classes generate a log or display a message at the MAP terminal. Only passed and failed REX tests are stored in the maintenance record. Failure reasons are available only for failed REX tests.

The sequence of events performed by the REX test state machine (or controller) is enumerated as follows:

1. Test the inactive unit (includes InSv tests only).

2. SysB the inactive unit.

3. RTS the inactive unit. This includes out-of-service (OOS) tests only.

4. Wait for superframe and data sync to be achieved.

5. Perform a pre-SWACT audit.

6. Perform a warm SWACT.

7. Maintain call processing capability on previously active unit.

8. Perform a post-SWACT audit.

9. SWACT back to previously active unit if necessary.

10. SysB the newly inactive unit.

11. RTS the inactive unit.

12. Wait for superframe and data sync to be achieved.

13. Run InSv diagnostics (TST) on the newly active unit.

14. Run InSv diagnostics (TST) on the inactive unit.

The REX test state machine (controller) actions are shown in the following figure, REX test state machine actions. If a REX test fails, a PM600 log is generated. The PM600 log initiates a major alarm for the XPM that failed the REX test. The major

alarm appears at the MAP terminal under the PM banner at the top of the MAP display.

If an InSv or OOS diagnostic test fails, the REX test failure reason includes the mnemonic (an easy to remember abbreviation) of the diagnostic that failed and the unit that failed (0 or 1).

The PM600 log details the start time of each step the REX test executed, the unit affected by the REX test step, and the failure reason. REX test steps included in the log after the failed step are recovery actions the REX test initiates as a result of the failure. The unit number is included only if the REX test action is unit specific (BSY unit, RTS unit, TST unit, sync) and not an action affecting the node (SWACT, BSY both units). The log's supplemental data consists of a card list and a mnemonic of the failed diagnostic.

The QUERYPM command and the QUERYPM FLT and TST REXCOV QUERY command strings contain information about the last REX test. Both manually and system initiated REX tests store and display a new date, time, and status (passed or failed) in the REX test maintenance record. Passed means that the REX test completed with no errors. Failed means that the REX test did not complete because of an error. This information is available through the QUERYPM and TST REX QUERY commands. If the REX test fails, the user either performs a manual RTS, a manual REX test, or an automated REX test to return the XPM to service from ISTb.

A REX test maintenance record is stored for each XPM containing the following information:

- REX test scheduler, if the XPM is in the system
- date, time, and result (passed or failed) of the last REX test
- failure reason, diagnostics failures, and a list of faulty cards (if applicable), if the last REX test failed
- date and time of prior failed REX test
- date and time of first passed REX test following prior failure

NT6X69 audit

The NT6X69 card processes messages from both the C-side and P-side speech bus. Messages between the units are also included in the speech bus interface. To communicate with the UP, the NT6X69 interrupts the UP process. An audit determines if an interrupt occurred. The NT6X69 sent messages to the UP. If an interrupt did not occur, the audit looks for incoming messages. If the audit twice detects incoming messages and an interrupt does not occur, the audit causes the RCC to drop activity. In this case, a PM181 log is generated and an ISTb RCC occurs.

This audit regularly checks peripheral protocol (PP) sanity in order to detect faulty PP circuitry. It also diagnoses faulty NT6X44 phase comparators, thus preventing synchronization losses that can cause carrier slips. It checks both InSv and OOS states. In

order to prevent interference with channels in use, this audit operates only on the C-side maintenance channel.

UTR diagnostic enhancements

Universal tone receiver (UTR) in-service (IS) and out-of-service (OOS) diagnostics perform the following tests on tone quality boundary conditions, which could result in undetected faults:

- twist test
- frequency deviation and noise test
- total power offset test

Both IS and OOS diagnostics exist for the UTR. The OOS diagnostic is a comprehensive test of the UTR board typically run on a return to service (RTS) of the peripheral unit. It can be invoked from the DIAG level of PMDEBUG or from the PM MAP level by testing the unit.

The IS diagnostic is a limited test of the UTR board that is run while the peripheral unit is in-service. It is invoked by the diagnostic driver approximately every seven minutes. It can be also invoked from the DIAG level of PMDEBUG or from the PM MAP level by testing the unit.

The operating range of the UTR for MF tone reception is set close to the expected value of the MF tones. This allows tone quality boundary conditions for MF tones to be simulated. DTMF tones cannot be tested directly. They are tested by the MF testing. The following tests enclose the expected value of the MF tones and simulate all boundary conditions:

- twist — The operating range is changed from -11dB with a power level range between -27dBm and +12dBm, to between -7.5dBm and +12dBm with a twist of no more than +/-1.25dB. Frequency deviation is detected as a decrease in power level.

- frequency deviation and noise — The total power offset range is from -1.0dB to +1.0dB. The power level range is reduced to -7.5dBm to +12dBm. Since the expected value of the tones is in the new operating range, all tones generated should be detected and reported.

- power level increase — The operating range is between -5.75dBm and +12dBm. Since the expected value of the tones is not in the new operating range, the tone generated during this test should not be detected or reported.

The combination of the above tests effectively reduces the operating range around the expected value of the tones enough to simulate the boundary conditions not tested by the original UTR diagnostic.

Audit of the IML links

This audit runs sanity tests on the intermodule message links (IML) links to ensure that data passed on those links is not lost or corrupted. It runs on both the inactive and

Figure 4-61 — REX test state machine actions

```
Start
┌──────────────────────┐     ┌──────────────────────┐     ┌──────────────────────┐
│ Test the inactive unit│───▶│ SysB the inactive unit│───▶│ RTS the inactive unit │
│  (InSv tests only)    │     │                      │     │ (out-of-service tests │
└──────────────────────┘     └──────────────────────┘     │      only)           │
                                                            └──────────────────────┘
                                                                       │
                                                                       ▼
                                                            ┌──────────────────────┐
                                                            │ Wait for superframe  │
                                                            │ and data sync to be  │
                                                            │     achieved         │
                                                            └──────────────────────┘
                                                                       │
                                                                       ▼
                                          (See note 1)      ┌──────────────────────┐
                                                            │ Initiate a pre-SWACT │
                                                            │ audit to determine if│
                                                            │ a SWACT should be    │
                                                            │     requested        │
                                                            └──────────────────────┘
                                                                       │
                                                                       ▼
                                          (See note 2)      ┌──────────────────────┐
                                                            │ Initiate a warm SWACT│
                                                            └──────────────────────┘
                                                                       │
                                                                       ▼
┌──────────────────┐     ┌──────────────┐              ┌──────────────────────┐
│ PM600 log is     │◀───│ SWACT back   │◀─────────────│ Initiate post-SWACT  │
│ output identifying│    │ to originally│              │ audit of newly active│
│ the REX failure  │     │ active unit  │              │      unit            │
│ reason           │     └──────────────┘ (See note 3) └──────────────────────┘
└──────────────────┘                                              │
       ▲  ▲ ▲ ▲                                                   ▼
       │  (A)                                         ┌──────────────────────┐
                                                      │ SysB the newly       │
                                                      │ inactive unit        │
                                                      └──────────────────────┘
                                                                 │
                                                                 ▼
                                                      ┌──────────────────────┐
                                                      │ RTS and SysB the     │
                                                      │ newly inactive unit  │
                                                      └──────────────────────┘
                                                                 │
                                                                 ▼
                                                      ┌──────────────────────┐
                                                      │ Wait for superframe  │
                                                      │ and data sync to be  │
                                                      │     achieved         │
                                                      └──────────────────────┘
                                                                 │
                    SWACT                                        ▼
                    passes                              ┌──────────────────────┐
┌──────────────────┐     ┌──────────────┐              │ Perform InSv         │
│ SysB the inactive│◀───│ Perform a    │◀─────────────│ diagnostics (TST) on │
│ unit after       │     │ recovery warm│              │ the newly active unit│
│ recovery failure │     │ SWACT        │              └──────────────────────┘
└──────────────────┘     └──────────────┘                        │
                                                                 ▼
                                              ┌──────┐  ┌──────────────────────┐
                                              │  A   │◀─│ Perform InSv         │
                                              └──────┘  │ diagnostics (TST) on │
                                                        │ the newly inactive   │
                                                        │       unit           │
                                                        └──────────────────────┘
                                                                 Finish
```

Note 1: Pre-SWACT audit failed
Note 2: SWACT failed.
Note 3: Post-SWACT audit failed.

active units. If a fault is detected, the active in-service unit reports the fault to the CC. When a fault is detected on the IML link(s), the following occurs:

1. The link is closed.

2. The RCC status changes to ISTb.

3. The RCC units no longer communicate over the links, a warm SWACT cannot occur.

4. A PM128 log is generated.

5. At the RCC level, the command QUERYPM FLT contains the following message:

   NON-CRITICAL HARDWARE FAULT

Message links (links 0 and 2) and DS1 maintenance

Message links between the RCC and the LTC are always links 0 and 2. If a maintenance request to busy either of these links is entered from the LTC peripheral side MAP level, the DMS responds with a warning that such action could take the RCC down by severing communication between the RCC and the CC. A maintenance person can override this warning if maintenance must be performed on the link.

The link state is particularly important to overall peripheral sanity when the peripheral is remote and the link is supporting messaging to the remote host. To ease maintenance in the remote peripheral, DS1 maintenance reacts to a limited set of detected events by generating log messages. The following detected events aid peripheral maintenance software in some decision making, such as the SWACT:

- card removed
- local alarm entered
- local alarm cleared
- remote alarm detected
- remote alarm cleared

Messaging links are maintained in the same manner as any other links when DS1 maintenance is enabled. They are subject to the same scanning, filter times, alarms, and reporting as any other link. The only unusual treatment these links receive is extended DS1 maintenance.

Extended DS1 maintenance utilities and routing procedures subject message links to continuous scanning, whether or not DS1 maintenance is enabled. On each C-side DS1 message supporting link, in all applications except the DRCC inter-RCC IRlinks, a permanent looparound connects the outgoing side of channel 12 to the incoming side of channel 16. This looparound allows the DMS to respond with a warning when a maintenance request is entered to busy a message link between the RCC and the LTC. The idea is to prevent the DS1 circuits from remaining in a state

that cuts off the remote peripheral from its host, unless this action is clearly needed. This warning exists only when DS1 maintenance is enabled on a message link.

RSC recovery procedures

NTP 297-8221-550 contains the recovery procedures for the DMS-100 Remote Switching Center (RSC). These procedures are used by maintenance personnel to return to service an RSC from a completely out-of-service condition, including Emergency Stand-Alone (ESA).

RSC alarm clearing procedures

NTP 297-8221-550 contains the alarm clearing procedures for the DMS-100 Remote Switching Center (RSC) and the DMS-100 RSC with Peripheral Life Upgrade Strategy (XPM PLUS). These procedures are used by maintenance personnel to clear alarms as they appear at the maintenance administration position (MAP). An alarm is the stimulus indicating the procedure that is to be used to clear the trouble. Procedures are named to correspond with the alarms as they appear at the MAP, and are arranged in alphabetical order.

RSC card replacement procedures

NTP 297-8221-550 contains card replacement procedures for the Remote Switching Center (RSC). These procedures are used by maintenance personnel to remove and replace hardware modules. Unless these procedures are part of verification or acceptance procedures, use them only when instructed to do so by some other maintenance procedure, such as an alarm and performance monitoring.

RSC trouble locating and clearing procedures

Trouble locating and clearing procedures are provided in NTP 297-8221-550 and is intended for use by maintenance engineering and field maintenance personnel who already have a basic knowledge of the DMS-100 Family of switches and of the Remote Switching Center (RSC). It is not to be used by operating company personnel who need specific, step-by-step procedures when performing maintenance tasks.

Advanced trouble locating procedures

Advanced trouble locating procedures are used when normal troubleshooting procedures do not clear a fault. For the remote cluster controller (RCC), advanced troubleshooting is often needed when a technician performs a PMRESET several times and a failure message is produced each time. When this occurs, the PMDEBUG tool is used. Refer to the PMDEBUG Users Guide for more information.

Under normal circumstances, a faulty component is busied and tested. As a result of this testing, the MAP (maintenance and administration position) terminal displays a list of cards. The card at the top of the list often is the cause of the component problem. Once the problem card is replaced, the faulty component is tested again. If the component passes this test, it is returned to service (RTS) and the troubleshooting procedure is completed.

However, if normal troubleshooting procedures do not restore a component to service, advanced troubleshooting procedures are required. Experienced operating company personnel use MAP responses from unsuccessful troubleshooting attempts to formulate a maintenance strategy. Alternatively, advanced step action procedures can be used to repair a component fault.

See NTP 297-8221-550 for RSC advanced troubleshooting procedures—including powering up and powering down the RSC.

DRAM & EDRAM Maintenance

Maintenance and diagnostics testing

NTP 297-1001-527, *DMS-100F DRAM and EDRAM Guide* describes the DRAM and EDRAM maintenance and operating procedures. The following topics are covered in this NTP:

- Understanding DRAM and EDRAM
- DRAM and EDRAM hardware
- DRAM and EDRAM software
- Understanding DRAM and EDRAM planning and engineering
- Determining service requirements for DRAM and EDRAM
- Ordering DRAM and EDRAM
- Planning DRAM and EDRAM expansion
- Understanding DRAM and EDRAM translations
- Understanding DRAM and EDRAM administration
- Evaluating DRAM and EDRAM performance factors
- Using OMs to evaluate DRAM and EDRAM performance
- DRAM and EDRAM tracking work sheets
- Recording on DRAM and EDRAM

EDRAM

A single-slot EDRAM circuit pack (NT1X80AA) provides the capabilities of a fully configured DRAM shelf. The EDRAM is a stand-alone peripheral module (PM) with its own DS30 link interface. It is plugged into one of the trunk slots (5 through 16) of the maintenance trunk module (MTM) or service trunk module (STM) with the DS30 cable connected directly to the backplane pins of the associated slot. EDRAM hardware integrates MTM and DRAM control and memory. Central control PM loader software is based on existing XMS-based peripheral module (XPM) utilities that permits the downloading of data (loadfiles from either a tape or disk) using the message channel of the DS30 link on both network planes.

NOTE: One EDRAM card provides the same functionality as one DRAM shelf provisioned with NT1X76 PROM or NT1X77 RAM memory.

EDRAM DS30 links

Since the EDRAM is a stand-alone PM, it has its own pair of DS30 links for connecting to both planes of the network module (NM). Therefore, it communicates with the central control/central message controller (CC/CMC) directly via the message channel of the DS30 link. The DS30 cable for the EDRAM can be plugged directly into the pins at the back of the MTM/DRAM backplane at the slot corresponding to the position of the EDRAM. The other end of the cable is terminated at the peripheral speech link (PSL) panel mounted on the speech link connecting (SLC) frame or at the enhanced network (ENET) depending on office requirements. The direct link means that the EDRAM appears twice on the MAP display. It appears as a PM since it is directly connected to the network, and it also appears as a trunk like the DRAM.

Maintenance considerations

Digital Recorded Announcement Machine (DRAM) and Enhanced Digital Recorded Announcement Machine (EDRAM) corrective maintenance need only be done when faults such as hardware or speech record failures occur. Hardware failures are recognized by a DRAM diagnostic routine programmed into the software. Speech faults can be detected automatically by storing checksums of speech record segments that are monitored continuously by the controller card, or by listening to the announcements.

The EDRAM differs from the DRAM in that it possesses the characteristics of both a PM and a trunk in one circuit pack. Diagnostic and self-tests can be carried out manually from the PM or TTP levels of the MAP, and both in-service and out-of-service tests are supported. Test results are displayed at the MAP terminal and detailed in system log reports. MAPCI commands for EDRAM are the same as those for DRAM. Maintenance tasks at the PM and TTP level use the same approach as standard maintenance procedures. The EDRAM is posted as a digital trunk module (DTM) at the PM level.

The self-test routine is a regular maintenance procedure used by the DMS-100F front end processor whenever a fault is suspected. The results from the DRAM unit self-test is used to diagnose the suspected fault.

NOTE: Ensure that the DRAM card is listed in table DRAM by the same code as the actual corresponding card on the shelf.

Posting the DRAM/EDRAM

The DRAM/EDRAM can be posted by using either of two commands from the TTP level of the MAP.

```
>POST G DRAM 1 0
```

```
>POST TM MTM 2 0
```

NOTE: The CTLR card of a DRAM group, always circuit zero on the MTM of the DRAM group, cannot be busied unless all the physical circuits associated with it are also busied, because these circuits need the controller to function.

Each circuit is referred to as a DRA trunk. The first circuit, that is, DRA trunk 0, is reserved for use by maintenance or for RAM recording.

CAUTION:
Removal of the CTLR card destroys the contents of the NT1X77AA RAM card. All phrases must be erased from the RAM memory cards using the DRAMREC utility before removing the CTLR card. Refer to RAM card description. List table ANNMEMS to determine the memory cards associated with the CTLR card being tested. The cards are those with HDWTYPE = DRAM on the same MTM as the CTLR card.

DRAM diagnostic test

The DRAM diagnostic test has four parts:

- DRAM installation diagnostic test—run if the DRAM is in the installation busy (INB) state. The controller, the memory cards, and the channels of the DRAM are checked.

- DRAM in-service diagnostic test—run if the DRAM is not INB. (This is a subset of the DRAM installation diagnostic). The in-service checks of the controller, the memory cards, and the channels are run.

- DRA memory card diagnostic test—each memory card is separately tested.

- DRA trunk diagnostic test—a single-trunk test for a DRA trunk.

NOTES:

1. The DRAM/EDRAM diagnostic test is run from the TTP or ATT level of the MAP.

2. When inservice diagnostic tests are carried out on the MTM containing the DRAM/EDRAM, a dedicated channel is required to connect the trunk test-tone circuit to the MTM.

3. The channel is set up in table TRKMEM as:

>TERM102T 2 0 A MTM 3 29 (assuming the DRAM/EDRAM resides on MTM 3; however, any outgoing trunk can be used)

4. When a diagnostic test is done, the trunk is posted at the TTP level and returned to service.

5. When a 30-channel office is involved, one channel is lost.

6. In-service diagnostics should be avoided during busy hours because of the required dedicated DRAM/EDRAM channel and increased overhead on the DRAM/EDRAM control-

ler. If diagnostics must be done during peak DRAM/EDRAM use, then invoke diagnostics on the individual DRAM cards, rather than doing a controller card test.

7. The DRAM/EDRAM diagnostic test causes the DRAM/EDRAM to stop playback if it is in progress. Playback can be restarted, if desired, by using the PLAYBACK command.

Diagnostic test responses

When a diagnostic test is done on the DRAM/EDRAM, one or more of the following type messages can be displayed to indicate the results:

- CKT NOT PART OF DRAM/EDRAM
- CTLR PROM/RAM FAULT
- DRA SET SCAN FAILED
- DRAM/EDRAM NO RESPONSE
- MEM CARDS XXXXXXXX
- PCM LOOPBACK FAULT

Posting a DRA memory card

A memory card can be posted by using a command such as the following from the TTP level of the MAP:

>POST G DRAM 2 5

NOTES:

1. MEMORY CARD is a PROM, RAM, or EEPROM card.

2. A double-density card is equivalent to two single-density memory cards. If both members of the double-density card are datafilled, they require two consecutive even member numbers (for example, 0 and 1, 4 and 5).

> **CAUTION:**
> Before removing an NT1X77AA RAM card, use DRAMREC to erase all phrases that have been recorded on the card.

Memory card diagnostic test responses

When a diagnostic test is done on the memory card, one or more of the following messages can be displayed to indicate the results.

- CARD NOT PROM MEMORY
- CARD NOT RAM MEMORY
- CARD NOT EEPROM MEMORY
- CKT NOT PART OF DRAM
- DRAM/EDRAM NO RESPONSE
- DRAM/EDRAM PORT 0 IS BUSY

- H/W & S/W MISMATCHED
- PCM LOOPBACK FAULT
- TEST TONE FAILED (RAM CARD)
- TEST TONE FAILED (PROM CARD)

DRA diagnostic testing

Posting a DRA announcement trunk

A DRA trunk can be posted by using a command such as one of the following from the TTP level of the MAP:

>POST TM MTM 2 21

>POST G VCA 2

DRA diagnostic test responses

One or more of six possible responses are displayed when a diagnostic is done on the DRA.

- CKT NOT PART OF DRAM/EDRAM
- DRAM/EDRAM - NO RESPONSE
- DRA PORT - NO RESPONSE
- DRA SET SCAN FAILED
- PCM LOOPBACK FAULT
- TEST TONE FAILED

DRAM/EDRAM commands (for recording)

The DRAM/EDRAM commands form part of the CI increment DRAMREC. They are used to inform the system of the prerecorded phrases in PROM and to record phrases in RAM and EEPROM. The increment can be entered by typing DRAMREC at the CI level. Entering ABORT as an operand stops the prompting and prevents execution of the command. To exit the increment, enter QUIT. See NTP 297-1001-527, *DMS-100F DRAM/EDRAM Guide* for a complete description of the DRAM/EDRAM commands. A quick reference for these commands are provided in the TAM-1001-018, *DMS-100F Quick Reference Guide.*

Helpful hints on DRAM/EDRAM operation

In some DMS installations, the MAP terminals are in areas with background noise that may affect recording quality. One solution is to record from a quieter location (recording may be on any trunk). If the site does not contain a MAP terminal but is in viewing range of one, a technician at the MAP can signal when the recording will begin. The DRAM/EDRAM always pauses a couple of seconds before giving the prompt tone.

Many of the commands in the recording and backup facilities have optional card parameters. Their use is not recommended, since leaving them out allows the system to make the most efficient use of storage space.

The optional parameters are provided only for those users who wish to dedicate memory cards to a specific use at the possible expense of storage space.

Use the phrase structure of announcements to save recording space. A phrase that is common to two or more announcements needs only to be stored once. However, be sure that the announcements sharing the phrase are recorded in the same voice.

The phrase structure allows the definition of announcements to be changed while the announcements are in use. For example, the phrase "Have a happy and safe holiday" could be recorded in RAM. The phrase could be included in a standard announcement during the Christmas season simply by adding it to the phrase list in Table DRAMTRK. The remainder of the announcement does not have to be recorded again. The seasonal greeting is just as easily removed when no longer desired.

When constructing multitrack announcements, try to make the tracks as close to the same length as possible. This is important, so that the subscriber does not hear a lengthy silence between tracks. If it is difficult to equalize the different languages segments, place different languages on the same track.

A bilingual announcement, for example, could have all the prime language phrases and the first second language phrase on the first track, and all the remaining second language phrases on the second track.

Multilingual announcements do not have to be multitrack. The entire announcement may reside on a single track if it is short or infrequently used.

Multitrack organization can be used whenever the announcement is long. Consider a 30-second announcement with text and phrases so arranged that it can be divided into two 15-second groups of phrases. The first group can be placed on track 1, and the second on track 2. Since the first track is always heard first, the announcement phrases are always played in the correct sequence. The maximum waiting time for the announcement is 15 seconds. The traffic capacity of the announcement is the same as two separate announcement trunks with one track each.

If the announcements are implemented as two one-track members, the maximum subscriber waiting time is anywhere from 15 to 30 seconds. The two-track method must have both tracks functioning; however, the two-member method can function with only one member, but at reduced capacity. Therefore. long announcements provide better service when implemented as multitracks.

The reliability of any announcement can be increased by placing members on different DRAM/EDRAM units. Use the display command to ensure that the component phrases are stored on both DRAMs/EDRAMs. Spreading announcements makes critical announcements less vulnerable to individual equipment failures. Announcements

can be spread over both electromechanical and DRAM/EDRAM by placing trunks on both machines.

If you use the REPEAT command from directory SYSDIR to diagnose the DRAM/EDRAM, use it with the SLEEP command. This allows the DRAM/EDRAM trunks to release before the next diagnostic starts. When insufficient time is allowed, an incomplete diagnostic produces a log. For a complete description of the REPEAT command, see NTP 297-1001-822, *DMS-100F Commands Reference Manual*.

DRAM/EDRAM proactive routine maintenance

Operating companies and Nortel Networks recommend that DRAM/EDRAM recordings be monitored for quality on a monthly basis—see NTP 297-1001-527, *DMS-100F DRAM/EDRAM Guide,* which describes DRAM/EDRAM maintenance and operating procedures.

DRAM/EDRAM OMs

The following ANN OM group and registers could be helpful with trouble locating of DRAM and EDRAM problems.

Table 4-26   —   Key DRAM/EDRAM OMs for maintenance and surveillance

OM Group	Register	Measurement	Related logs/notes
ANN	ANNATT	announcement attempts	
	ANNOVFL	calls routed to recorded announcement but fail to connect (route to ANNOVL.)	LINE138 and TRK138 can be analyzed for calls routed to treatment
	ANNMBU	announcements manual busy (usage count)	
	ANNSBU	announcement system busy (usage count)	TRK106
	ANNTRU	announcement traffic usage	

MPC Maintenance

Multi-Protocol Controller (MPC)

A general-purpose card that allows data communications between a DMS-100 Family switch and an external computer (for example, between a central office (CO) billing computer and a DMS-100 Family switch). The MPC card resides on the I/O controller (IOC) shelf. MPC card protocol software is downloaded from the DMS-100 CPU and then used to support software routines for Data Packet Network (DPN) communications.

MPC MAP level access

The MAP terminal provides maintenance access to the MPC through the Command Interpreter (CI).

The following MAPCI command provides access to the MPC card and link status level:

>MAPCI;MTC;IOD;IOC n1;CARD n2

NOTE: n1 is the IOC shelf number as identified by data table MPC; n2 is the IOC card number—the card number is a result of taking the value given to the IOCCT field in table MPC divided by 4.

A sample of the MAP display response is illustrated by Figure 4-62 on page 2-323. In this figure, the AP subsystem display area shows port status of IOC 3, and gives the status of MPC, IOC card 8.

In the sample display, the user line displays SYSTEM, BOARD, LINK0, LINK1, LINK2, and LINK3.

NOTE: Only LINK2 and LINK3 are assigned for TOPS applications.

Status possibilities under MAP display item for SYSTEM are READY, NOTREADY, OFFL (Offline), ManB (Manual Busy), or SysB (System Busy). In the sample, the status shows SysB.

Status possibilities under the BOARD, shown as cccc in the MPC MAP display (Figure 4-62) are:

- APPLIP (Application In Progress),
- COMACT (Communications Active),
- COMIDL (Communications Idle),
- DNLDED (Downloaded),
- DNLDIP (Download In Progress),
- NOLOAD (No Load),
- OFFL (Offline),
- UNKWN (Unknown if MPC downloaded).

LINK status possibilities, as depicted by kkkkkk in the MAP display, are CBSY (C-side Busy), DISABLD, ENABLD, ENBLIP (Enabling In Progress), MBSY, OFFL, SBSY, UNEQ, and UNKNWN (link state unknown). For link1, a N/A means Not Applicable because link1 is equipped with an EMPC NT1X89BA circuit pack.

Menu commands, numerically listed on the left side of the display in Figure 4-62 are provided for MPC maintenance testing and control purposes. A brief summary of the MPC menu commands are described later within this subsection.

Figure 4-62 — MAP display for MPC card

```
CC      CMC      IOD     Net     PM      CCS      Lns     Trks    Ext     EIO

 •        •      nMPCOS   •       •       •        •        •       •        •
MPC
 0      QUIT     IOD     IOC      0   1   2   3   4
 2      _link_           STAT     •   •   •   •   •
 3      _ALL_
 4      Listdev_  DIRP:    •    XFER:         •     CDR:  •   DPPP:  •
 5                DPPU:    • NOP:        •
 6      Tst
 7      Bsy_    IOC  CARD   0    1    2    3    4    5    6    7    8
 8      Rts_     3   PORT 0123 0123 0123 0123 0123 0123 0123 0123 0123
 9      Offl_        STAT ___ ___ ___ ___ ___ ___ ___ ___ ___
10      Qmode        TYPE
11              Card 8 Unit        0
12                User     SYSTEM BOARD LINK0  LINK1 LINK2 LINK3
13      Qmpc_       Status   SysB    cccccc   UNEQ  N/A  kkkkkk kkkkkk
14      Qlink_
15      Qconv_
16      Revive_
17      Downld_
18
   OPERATOR

Time
```

MPC card fault recovery

The MPC software contains several maintenance procedures for recovering from most errors. Following is a description of the system run procedures.

Error processing

Because the goal of the MPC is to offload the DMS CC, it handles error processing when possible. The protocol specifies the recovery mechanism to be tried for various errors. If a remote DTE does not respond to a request, and a specified number of attempts are exhausted, the link is disabled and CC protocol support is notified. Both CC and peripheral processor recovery are then invoked.

For X.25 packet level errors, the MPC resets the specific conversation. Any state changes are specified in a report to the CC.

For maintenance action requested of the card, the MPC subsystem supplies maintenance procedures that are entered automatically. The following events cause the maintenance system to invoke this procedure:

- a manual or automatic restart
- system busy of the card
- addition or deletion of a card using table editor tool
- issuance of any MAP command related to maintenance action

Maintenance audits

A periodic maintenance audit is performed on all cards in the DMS to determine whether the cards are functioning properly. The response or lack of response to a query status message determines the sanity of each MPC card. If an MPC is determined to be functioning improperly, it is made system busy. This maintenance audit process also handles maintenance messages and periodically resets internal fault counters.

Manual and automatic resets

The MPC card can be reset manually or automatically. Internal commands exist to reset the MPC. These commands effectively disable the IOC bus interface, preventing the card from initiating unnecessary transfers between itself and the CC while the card is in an insane state. Occasionally, faults may arise from the failure of the MPC card to recover. In this situation, an MPC alarm is generated. The MPC also resets itself when an extreme voltage dip occurs. The MPC monitors the voltage level on its internal power bus and automatically resets itself if the voltage drops below a specified threshold. An extreme voltage drop causes the card to be system busied. When the card is returned to service, the CC checks whether the software is intact and, if necessary, reloads the software—see "MPC card replacement warning" on Page 4-325.

MPC alarm clearing procedures

When an MPC is taken out of service, an alarm is posted under the IOD header of the MAPCI. There is an IOD alarm shown in Figure 4-62. The alarm, nMPCOS under IOD, indicates that n number of MPC cards are out of service, where n equals the quantity of Multi-Protocol Controllers. Fault analysis would include reviewing log reports as well as MAP testing of the MPC to isolate problems. For a brief summary of alarms, see Table 4-27 on the next page. See NTP 297-1001-590, *DMS-100F Input/Output Device Maintenance Guide* for a list of MPC card and link states.

MPC card replacement

> WARNING The supply voltage on a DMS shelf can be affected when any card is inserted or removed while the shelf power converter is active.

The effect is a temporary change in voltage level. The magnitude of the change in voltage is dependent on the inrush and steady-state current drawn by the card, with the inrush current having the greatest effect. The inrush current typically is required to charge filter capacitors in the power circuitry of the card, and the steady-state current is the normal operating current drawn by the card.

For most DMS equipment, this effect does not impact the operation of other devices on the shelf. However, the MPC card has larger filter capacitors in its power circuitry than other cards, and as a result, draws a higher inrush current when inserted. This higher inrush current can cause a significant change in the IOC shelf voltage level that could possibly corrupt data or program store, or alter internal logic states on any other inservice card in the IOC.

Table 4-27   —   MPC alarms

Alarm	Indication	Meaning	Action/clearing
MPCOS	The word MPCOS, preceded by a number under the IOD header of the MAP indicates the presence of a multiple protocol controller major and minor alarm.	One or more multiple protocol controllers is out of service.The number that precedes MPCOS indicates how many are out of service.	1. Access MAP IOD level 2. Access the status display and menu for the affected IOC. 3. Access the card display and menu for the MPC card with one or more P-side busy ports.and proceed to step 4. 4. Look for the following indications:
	If you find...	then...	see...
	FSP under EXT label in system status display	a possible FSP power fault exists	External Subsystem NTPs
	SysB under SYSTEM header for MPC card	the MPC card is system busy due to one or more of the following: MPC card is defective MPC file cannot be downloaded to MPC because filename is not correct or file is unavailable.	the system busy MPC sub-procedure Table (following page)
	Offl or ManB under SYSTEM header for MPC card	the MPC card is offline or manual-busy	the office log. or ask other personnel to determine why.

MAP maintenance IOC level, MPC sublevel

The MPC level is accessed from the IOC level by entering the command MPC n or CARD n for the assigned MPC card.

For the MPC, the term *conversation* applies to logical link activity between two systems through which data transmission occurs. Conversation does not refer to voice transmission (talking) or to the establishment of a voice link for call processing. The term board is used synonymously with card.

The commands that can be accessed from the MPC sublevel of the MAP are listed below.

Table 4-28 — MPC alarms - system busy

Alarm	Action/clearing:		
MPCOS SysB	1. Busy the MPC. If any conversations that use the controller are in progress the system will reject the BSY command. Ask users to log off then try to busy the MPC again 2. Attempt to return the MPC to service. If the attempt fails note the MAP response and proceed as below:		
	If...	then...	do the following...
	the message FAILURE IN DIRECTORY SEARCH appears	the download file cannot be found	Check that the filename is correct in table MPC field DLDFILE. Ensure that file is on the storage device.
	the message REQUEST FAILS appears	the MPC card may be defective	Replace the NT1X89 MPC card. If the problem persists gather logs MPC101 through MPC106 and get help

BSY command

This sets the state of the MPC card to Manual Busy (MBSY). Options for the BSY command allow for maintenance on individual links of the MPC card, as well as the card itself. Individual links, all links, the card and all links, or the card only can be busied.

A busy command is effective only for an Offline (OFFL), System Busy (SBSY), or inservice (READY/NOT READY) state. Also, if FORCE is not specified, a busy command succeeds only when there are no conversations in progress. While busy, the MPC card handles no conversations.

DOWNLD command

This manually downloads software from the CC to a selected MPC card.

LISTDEV command

This displays a list of all MPCs.

OFFL command

This changes the status of the MPC card as displayed by the command LISTDEV to Offline (OFFL). Options for the offline command allow for maintenance on individual links of the MPC card as well as the card itself. Individual links, all links, the card and all links, or the card only can be set to offline. The offline state can be set only

from the manual busy state. The MPC card status changes to unequipped (state UNEQ) if the card is deleted by the table editor and is offline.

QCONN command

This queries the following information about an MPC conversation. MAP display headings are shown in parentheses.

- MPC number (MPC)
- Link number (L)
- Logical channel number (LCN)
- Status of MPC conversation (STATUS)
- MPC conversation number (CCC)
- Security number of the conversation (SEC)
- Parameter device or directory entry for MPC (PARDEV)
- Input indicator (INP)
- Number of files opened on the conversation (OPEN)
- Application owner of conversation (OWNER)

QLINK command

This queries system configuration parameters for a specified MPC.

QMPC command

This displays the current status of the MPC card, MPC download file, each of the four links on the MPC card, and the OM tuple that correlates to the MPC.

QNODE command

This displays data about the node that is connected to the MPC.

REVIVE command

Revives one or more MPC application processes: ALL, SDADY, APPLN, PROC-NAME, and PROCESSID.

The command, REVIVE should be used under exceptional conditions only. Logs MPC101 and MPC106 indicate process error conditions under which the command should be used.

The SDADY process must be running properly before attempts to revive all other processes are initiated. As a result, SDADY is always the first process the command REVIVE attempts to affect. Because the state of the SDADY process is critical to revival of all other processes, special messages noting the state of the SDADY process are produced when the command REVIVE ALL is attempted.

If the SDADY process cannot be revived, processes running under MPC software control continue to operate, provided no error conditions are encountered. If these

processes encounter error conditions while the SDADY process is down, they cannot be revived. In addition, no new processes can be initiated while the SDADY process is not running.

MPCGDADY can be used as a process name, but is treated as an UNKNOWN PROCNAME. Data for MPCGDADY is kept separate from other processes.

RTS command

This places the MPC card in service after testing. Options for this command allow for maintenance on individual links of the MPC card as well as the card itself. Individual links, all links, the card and all links, or the card only can be returned to service.

A return to service command is effective only when the state of header SYSTEM or LINK is MBSY.

During the test the card's status is displayed as RTS. If the test fails, the card is not returned to service. If the test is successful, the state is OK.

If the test determines the card is not downloaded, the following steps occur:

- The card is marked as needing a download.
- The card is put in service.
- The card is marked NOT READY on the MPC display.
- A download is initiated.

TST command

This tests the displayed MPC by ensuring that the card is communicating properly with the CC. The TST command also checks whether the MPC has been downloaded, and if it has, checks the sanity of that software. Please note that a full TST command causes the card to perform full tests. It also erases the downloaded file so that the card requires downloading.

MPC nonmenu commands

The nonmenu commands do not appear on the IOD level menus, but may be entered as if they were listed on the menu. The nonmenu command MPCCOPY is listed below.

MPCCOPY command

This translates download files for the MPC.

MPC log reports

The following situations can generate MPC log reports:

- a software event in the software subsystem that prevents normal operation of MPC functions

- a controller condition in the software subsystem that could prevent normal operation of protocol support functions
- the CC requests information on a problem in the MPC PP software; a possible PP failure occurred
- trouble during an audit that could prevent normal operation of MPC functions; a possible PP failure
- the MPC card, or links, change state
- certain commands are entered at the MAP level altering MPC status

MPC log reports are summarized in NTP 297-1001-590, *DMS-100F Input/Output Device Maintenance Guide.* For a complete and detailed description of MPC and related logs, see NTP 297-YYYY-840, *DMS-100F Logs Reference Manual.*

MPC OMs

Table 4-29 lists the MPC OM groups and registers for maintenance and surveillance. Table 4-31 lists the key MPC LINK OM groups and registers for maintenance and surveillance. For a complete list of registers see NTP 297-YYYY-814, *DMS-100F Operational Measurements* or NTP 297-1001-590, *DMS-100F Input/Output Device Maintenance Guide.*

Table 4-29   —   MPC OM Groups and Registers

OM group	Register	Measurement	Related logs/notes
MPCBASE	MPCNSSBU	times MPC node system busy	MPC904
	MPCNSMBU	times MPC node manual busy	MPC903
	RESETL2	number of line resets on link 2	MPC102, if link protocol problem.
	RESETL3	number of line resets on link 3	MPC102, if link protocol problem.
	CONVERR	conversation rests on links 2 & 3	MPC102
	LOSTMSGS	messages incoming to CC that cannot be delivered to proper address	MPC102
	BDAPPERR	peripheral traps on the board	MPC103
MPCFASTA	LLNKXFRD	logical link unavailable when output attempts fail (an indication of link stability)	
	FAOUTFLD	output fails due to lack of internal resources (may indicate application or protocol software problems)	

Table 4-31 — MPC LINK OM Groups and Registers

OM group	Register	Measurement	Related logs/notes
MPCLINK2 MPCLINK3	L2PABORT	aborted frames on link.	parity and framing errors
	L2PSYNC	loss of carrier or `clear-to-send' (CTS) lost	carrier detect (DCD) and CTS signal during modem configuration
	L2PDOWN	seconds physical layer spends to enable link while MPC is in RTS.	number of seconds to enable modem control.
	L2PHWERR	h/w exceptions during operations on the link.	hardware interface process exception.
	L2LSETUP	number of times a link setup sequence executed	
	L2LDISC	link disconnects sent & received	
	L2LDOWN	link down time due to no response from remote level 2 software	
	L2LACKTO	unacknowledged message from the remote	
	L2LXMIT	frames sent to a remote	data messages sent to the remote.
	L2LRXMIT	frames resent because remote did not receive	
	L2LLVIO	MPC messages perceived by the remote as invalid	
	L2LRVIO	invalid remote messages received at the MPC.	
	L2MSGLST	number of incoming messages lost on MPC link	for asynchronous protocol only.

AIN Overview and Maintenance

AIN overview

Advanced Intelligent Network (AIN) is a set of software feature packages located in the computing module (CM). It allows switch call processing capabilities to use operating company provided databases placed at service control points (SCP). The SCPs determine how AIN calls should proceed for further call processing. Queries and responses between the SuperNode switch equipped with AIN features and the SCP use CCS7 protocol. AIN allows operating companies to implement their own features and to make these features available across public and private networks. For an overview of CCS7, see the "SS7 Overview and Maintenance" subsection within this tab of the MOM.

AIN operation is transparent to the subscriber. The majority of calls through the network access traditional functions that are standard features of the switch software. An AIN Release 0.1 call signals the need for additional instructions through the use of trigger detection points (TDP) and triggers. Information about the TDP and triggers can be found in NTP 297-5161-021, *AIN Essentials, Service Implementation Guide* or NTP 297-5161-022, *AIN Service Enablers, Service Implementation Guide*.

AIN architecture

AIN consists of a number of switching and processing nodes that are interconnected by signaling links. The size of an AIN network is dependent on the services offered and the traffic handling capacity required; however, the basic block concept of the system is the same for installations from a metropolitan area to a regional operating company.

The basic network components of AIN are the SCP, SSP, network access point (NAP), and signaling transfer point (STP). AIN Release 0.1 using Nortel Networks supplied central office (CO) equipment is supported only for the DMS SuperNode switch; however, Nortel Networks does not currently provide an SCP that is capable of providing AIN services. With this exception, the DMS SuperNode switch can provide a unified equipment solution for each of the AIN network members. The individual building blocks of the AIN architecture are represented by various DMS-100 SuperNode office configurations. Because core equipment and operations are the same regardless of the node's function, administration and hardware support of AIN are the same for all AIN facilities. See Figure 4-63 for a block diagram of the typical AIN Release 0.1 architecture.

Figure 4-63 AIN Release 0.1 network components

Adjunct = "SCP" like device
IP = Intelligent Peripheral
NAP = Network Access Point
SCE = Service Creation Environment

SCP = Service Control Point
SMS = Service Management System (OA&M)
SSP = Service Switching Point
STP = Signal Transfer Point
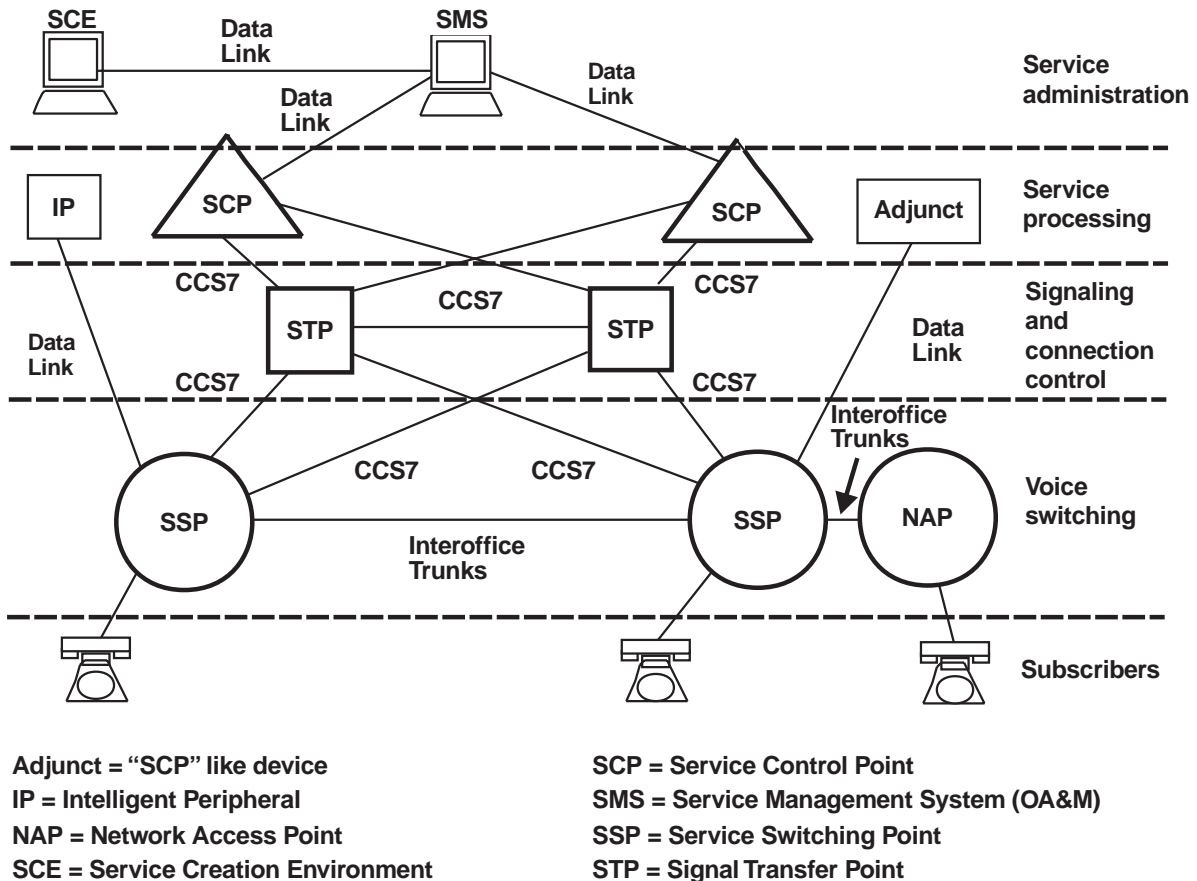
Following is a description of the primary blocks of the network:

- SSP — the end office (EO) responsible for formulating the transaction capability application part (TCAP) query to the SCP for subscribers connected directly to it or connected to subtending NAP. Upon detecting an AIN call, the SSP stops the processing of the call until a response to the query with routing information or other information (for example, play announcement, collect digits, or other) is received from the SCP. Upon receiving a response from the SCP, the SSP routes the call to the appropriate EO based on information received from the SCP in the response message.

  The SSP can be an equal access end office (EAEO) or an access tandem (AT). If the SSP is an AT, it needs DMS-100, 200 software.

- SCP — an application database that contains service control logic instructions and associated information required to provide AIN services to the subscriber. Once the SCP receives the query from the SSP, it determines the service to be provided to the subscriber and returns the necessary processing information to the SSP for action. In addition, the SCP may provide a tool kit from which telephone companies can create and customize services using the service creation environment (SCE).

- Adjunct — provides similar functions as the SCP, but it is directly connected to an SSP through a high-speed interface. Consequently, the adjunct can support services requiring fast response to certain user requests. For AIN, the adjunct is available for lab use only.

- STP — a switch responsible for routing CCS7 messages to the appropriate SCP or EO, based on global title translations (GTT). In some network configurations, the STP may be combined with the SSP. The STP cannot be the source of the user generated messages.

- Service management system (SMS) — enables the provisioning and administration of AIN services.

- SCE — provides tools for creation and customization of services that reside in the SCP.

- Intelligent peripherals — have the ability to exchange information with an end user, such as voice announcements and dual-tone multifrequency (DTMF) digit collection.

- NAP — an EO that supports AIN functionality but does not have SSP capability to access the SCP directly using the CCS7 TCAP messages. AIN call requests are routed to an SSP using multifrequency (MF) or integrated services digital network (ISDN) user part (ISUP) messages for the SSP to initiate an SCP query. AIN calls originating from a NAP are always routed to an SSP.

AIN is a service control architecture that is engaged during basic call processing when a designated condition is encountered. The condition may be that a certain event has occurred and that prespecified conditions are satisfied. Once engaged, predefined logic using a common set of service independent functions directs subsequent call processing actions. After the switch sends the query and the response is processed, the call proceeds; however, post query and post response feature interactions may be affected by the responses received.

Any network information that has been received by the AIN SSP prior to the query is retained by the SSP while the call process is suspended awaiting SCP instructions; however, this information may be overridden by responses received from the SCP. If not overridden by responses received from the SCP, this information continues with the call after the successful reception of a routing response. Some examples of such network information are calling number, calling name, and redirection information.

AIN operation

A typical AIN call progresses through the network and follows this basic route:

1. Triggering — After an AIN call is placed by the subscriber, the DMS SuperNode switch with AIN features determines that the call needs special AIN handling.

2. Querying — The SSP stops processing the call and assembles and launches TCAP requests to the SCP database.

3. Post-querying — Once the SCP database returns the response message to the SSP, the subscriber may trigger again or be asked by the SCP to continue, to authorize termination, or to disconnect the call; or the AIN call processing may be completed, routed, and given information for automatic message accounting (AMA) billing or queries for additional input by the SSP using the instructions from the SCP.

Figure 4-64 illustrates a simple AIN call flow through the network to completion.

Figure 4-64   —   AIN call progression example
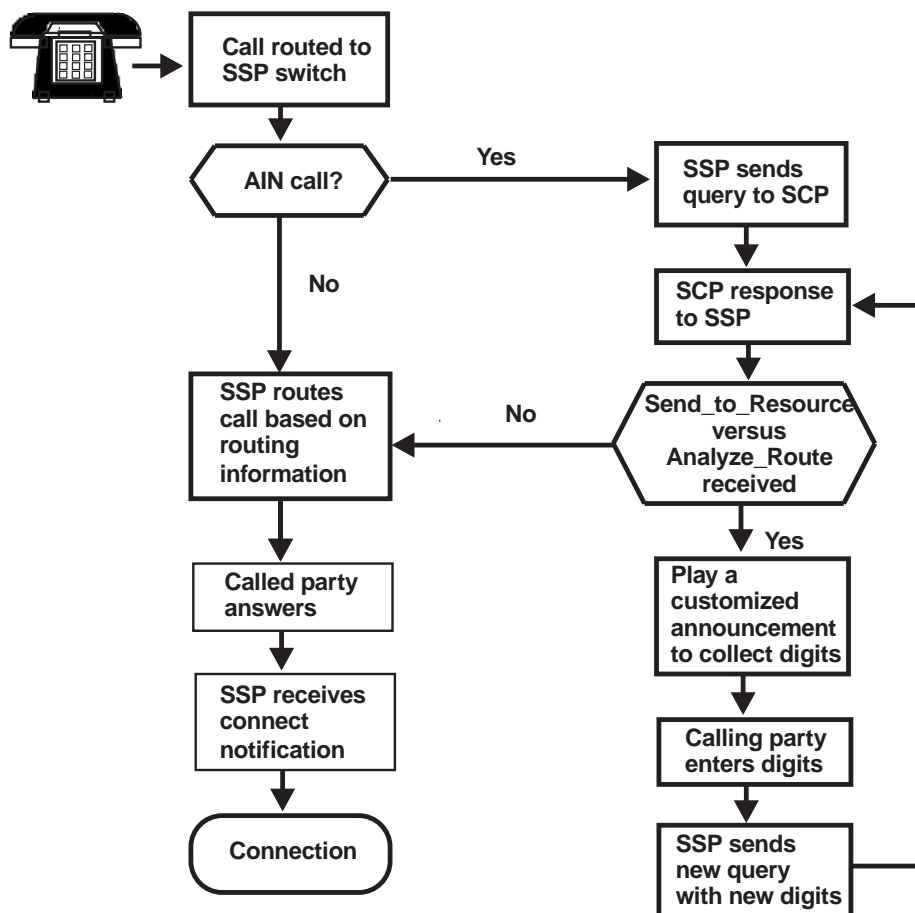
AIN maintenance

Because AIN is primarily a software product, there is no manual maintenance that can be performed. Any manual maintenance would be performed on components that affect AIN and not on AIN itself. For a list of manual routine tasks that can be performed for the SuperNode product, see the "Routine Tasks" subsection within the *Preventive Maintenance* tab of this manual.

Analysis of a switching system is based on a combination of maintenance and traffic indicators. These indicators denote the state of the system and assist in identifying actual or potential service problems.

To assist in an analysis of the grade of service provided and of AIN performance, an extensive set of measurements is provided by the DMS-100 switch operational measurements (OMs) associated with provisioning and administration can be used to determine if adequate software and hardware resources are provided. In addition, maintenance measurements, along with log reports, provide data that are used to evaluate AIN performance and the impact on system performance.

Maintenance support for AIN can be found in NTP 297-5161-510, *AIN/LRN-LNP Maintenance Guide.* Besides providing an overview for AIN maintenance, the NTP provides trouble locating and clearing procedures examples and first level and advanced troubleshooting support.

AIN commands

TRAVER

The translation verification (TRAVER) command can be used to diagnose AIN translation datafill problems. Examples are provided within NTP 297-5161-021, *AIN Essentials, Service Implementation Guide* or NTP 297-5161-022, *AIN Service Enablers, Service Implementation Guide* and NTP 297-5161-510, *AIN/LRN-LNP Maintenance Guide.*

TSTQUERY

The TSTQUERY command enables the user to test AIN by sending and receiving messages to and from the SCP without placing a telephone call. This enables the user to ensure that the AIN service is fully operational before it processes telephone calls.

C7TU

The C7TU test utility can be used to monitor messages going over links to the database and back. C7TU provides testing of CCS7 features but is also password protected. This can be used for troubleshooting, and monitoring and interpretation of messages from the SSP and SCP. See the "SS7 Overview and Maintenance" subsection within this manual for more information on this tool. Also see TAM-1001-015, *C7TU User Guide* for more detailed use of the tool.

AINTRACE

This command enables maintenance personnel to trace AIN messages by line/trunk. Users can select desired TIDs (Terminal Identifiers) tracing. Related TCAP messages in hexadecimal along with TID and time stamp are stored in a buffer and can then be displayed. Dynamic Packet Trunks (DPTs) can be traced as well.

Through the AINTRACE CI (Command Interpreter), the user selects TIDs by specifying DN (Directory Number), LEN (Line Equipment Number), Dynamic Packet Trunk (DPT) agent, or trunk group name and member number. The selection CI command is similar to CallTrak. Up to ten selected TIDs are added to a list. The user can also remove TIDs from the list. After selecting TIDs, the user can set AINTRACE to start tracing. Tracing must be stopped to add or remove TIDs from the list. A buffer stores the message information which includes the TID, time stamp, and hex TCAP message. The buffer can hold two hundred messages. The user can use CI commands to do the following:

- display all messages captured

- display only the most recent message in the buffer

- step backward and display the messages specified by the step value

- clear the buffer contents

For more information on the AINTRACE command, see NTP 297-5161-510, *AIN/LRN-LNP Maintenance Guide*.

AIN logs

Several AINXXX, AUDXXX, AUDTXXX, LINEXXX, TRKXXX, TRAPXXX, SWERRXXX, CCSXXX, as well as CCS7 TCAPXXX logs can be used for troubleshooting AIN. Since a severe network condition can generate a large volume AIN logs within a short interval, many AIN related logs are only generated once within a five minute interval. However, a total count for the five minute period is maintained within the SUPPRESSED field of those logs. Not generating a log for every event helps to prevent overloading the logging buffers unnecessarily.

A table in NTP 297-5161-510 contains a list of AIN and TCAP logs along with information on the cause of the log report and the recommended maintenance response. Addition details on the logs can be found in NTP 297-YYYY-840, DMS-100F Log Report Reference Manual.

AIN operational measurements

For an overview of AIN related OM groups and their registers, see "Operational measurements" within NTP 297-5161-510, *AIN/LRN-LNP Maintenance Guide*. For an overview of operational measurements, see the

SDM Overview and Maintenance

SDM overview

The fault-tolerant SuperNode Data Manager (SDM) is a high-performance UNIX-based processing platform that supports DMS SuperNode operations, administration, maintenance, and provisioning applications.

The SDM fault-tolerant platform uses Motorola technology, and includes the following elements:

- PowerPC 604 family microprocessor
- fault-tolerant (FT) hardware
- IBM AIX 4.1.4 operating system
- SDM resident base and application software developed by Nortel Networks

Figure 4-65, "SDM position in the DMS SuperNode system" shows the position of the SDM within the DMS SuperNode system. The fault-tolerant SDM is connected to the message switch (MS) using four DS512 fiber links from two DS512 interface modules. Each DS512 interface module is equipped with two ports that connect over separate links to the two MS planes. These links maintain communication to the MS if a link fails or if one side of the MS is unavailable. External hardware is connected to the SDM through modems using serial ports or through the operating company LAN using a built-in Ethernet interface.

Figure 4-65 — SDM position in the DMS SuperNode system
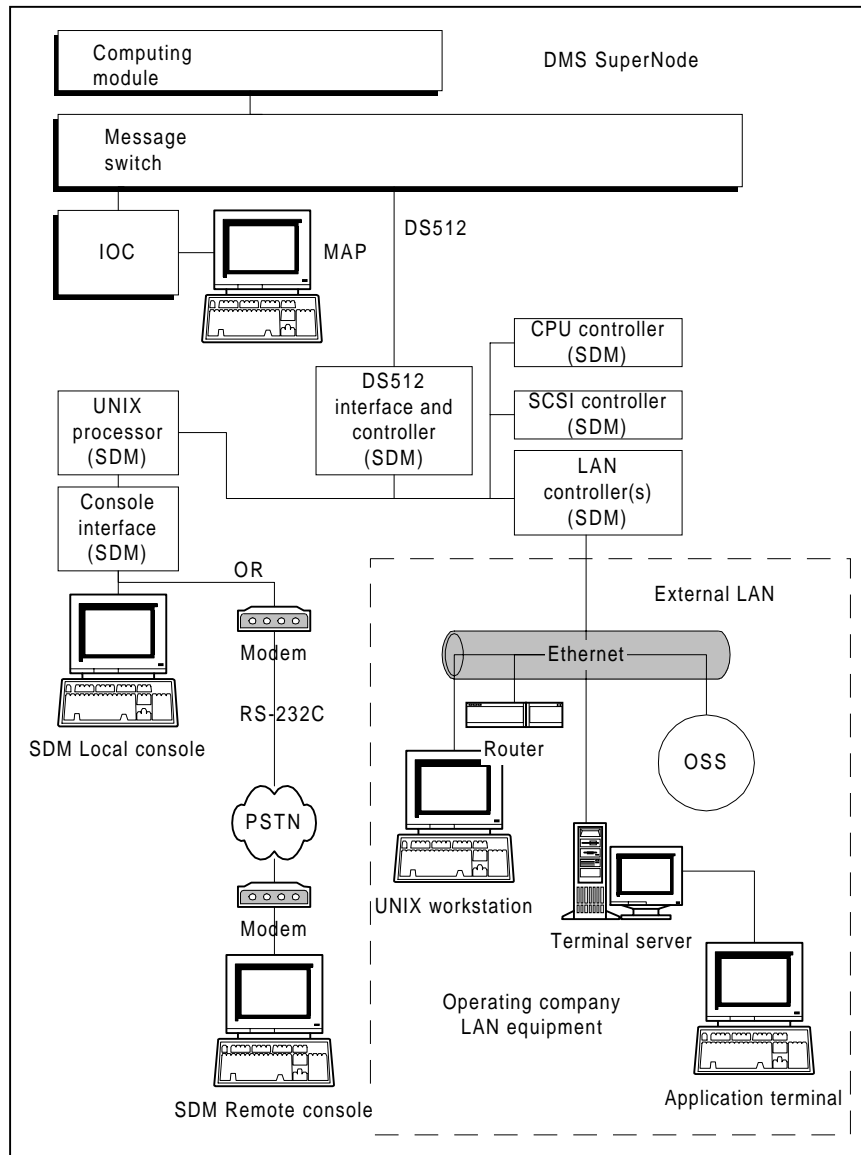
SDM reference documents

297-5051-300, *DMS-100 Family SuperNode Data Manager SuperNode Billing Application Application Guide*

297-5051-303, *DMS-100 Family SuperNode Data Manager User Guide Platform Software Upgrade*

297-5051-304, *DMS-100 Family SuperNode Data Manager Upgrade Guide*

297-5051-350, *DMS-100 Family SuperNode Data Manager Translations Guide*

297-5051-543, *DMS-100 Family SuperNode Data Manager Alarm Clearing and Performance Monitoring Procedures*

297-5051-801, *DMS-100 Family SuperNode Data Manager SuperNodeBilling Application Alarm and Performance Monitoring Procedures*

297-5051-840, *DMS-100 Family SuperNode Data Manager Log Report Reference Manual*

297-5051-900, *DMS-100 Family SuperNode Data Manager Simplex User Guide*

297-5051-904, *DMS-100 Family SuperNode Data Manager Enhanced Terminal Access User Guide*

297-5051-905, *DMS-100 Family SuperNode Data Manager ASCII Terminal Access User Guide*

297-5051-906, *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*

297-5051-912, *DMS-100 Family SuperNode Data Manager User Guide Exception Reporting*

297-5051-913, *DMS-100 Family SuperNode Data Manager Secure File Transfer User Guide*

297-5051-914, *DMS-100 Family SuperNode Data Manager DDMS and GUIDE Installation and Administration Reference Manual*

For more SDM document references, please refer to 297-8991-001, *DMS-100 Product Documentation Directory.*

Maintenance interfaces

There are two maintenance interfaces for the SDM:

- the MAP (maintenance and administration position) accessed from the CM
- the SDM maintenance interface accessed from the SDM

The MAP is the primary access point for maintenance activities. The SDM maintenance interface is the secondary access point for maintenance activities. Maintenance activities must normally be performed at the MAP interface. When connectivity to the CM is not available, the SDM maintenance interface provides access to most maintenance activities that would normally be performed at the MAP interface.

MAP-based SDM maintenance

A dedicated SDM maintenance subsystem is provided at the MTC APPL level of the MAP display which allows you to do the following:

- determine the node state and operating condition of the SDM

- alter the state of the SDM for maintenance purposes

- determine the status of connectivity from the CM to the SDM

- reboot or halt the SDM

- alter the state of SDM hardware

- determine the status of SDM applications, including any faults currently affecting applications, by using the QuerySDM command (See "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 for more information.)

- determine the status of the SDM operating system, including any faults currently affecting system software resources, by using the QuerySDM command. ("SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 for an overview of MAP-based maintenance capabilities.)

The MAP display is used to maintain the SDM if the CM is communicating successfully with the SDM. If the SDM and the CM are unable to communicate due to a fault on the SDM, use the SDM maintenance interface to diagnose, and clear the problem.

See the procedure "Maintaining the SDM using the MAP interface" in Chapter 2, "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 for an overview of MAP-based maintenance capabilities.

SDM maintenance based on the SDM maintenance interface

The SDM maintenance interface can be accessed by the following methods:

- using a remote or local VT100 terminal console port

- telnet from the operating company LAN (telnet must be enabled)

- using the optional ETA application from a remote workstation The SDM maintenance interface provides the following maintenance capabilities:

- control and maintenance access to all maintenance capabilities normally available through the MAP interface (including state change and monitoring capabilities) when connectivity to the CM is not available

- control and maintenance of SDM hardware

- control of individual SDM application software packages

The Log Delivery application delivers all DMS logs that are available from the LogUtil utility.

Maintaining the SDM using the MAP interface

The primary access point for maintaining the SDM is the dedicated SDM maintenance subsystem in the MAP interface. The SDM subsystem is a sublevel of the application (APPL) subsystem in the MAP interface. The MAP command and display structure for the SDM is similar to that provided at other MAP levels.

Commands at the SDM level allow you to do the following:

- monitor and alter the state of the SDM
- determine the state of the DS512 interface associated with the SDM
- query status information on the SDM system, application software, and hardware location
- access the Platform sublevel which allows you to monitor and alter the state of the SDM devices

Use the MAP interface to maintain the SDM when at least one of the communication links between the computing module (CM) and the SDM is in service. If all of the links are out of service, the SDM is isolated and maintenance must be performed using the RMI, described in the section "How to maintain the SDM using the remote maintenance interface" in Chapter 2, "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

Figure 4-66, on page 4-342 "SDM MAP level" shows an example of the SDM level of the MAP display. The display shows the SDM node state, the number of links out of service, any current maintenance actions, and provides an SDM-specific command set. Fault conditions related to the SDM are reported in the maintenance and APPL alarm banners. In Figure 4-66, the maintenance banner is the top most banner which appears in all MAP displays. The APPL alarm banner is below the maintenance banner. It appears only in the APPL level and its sublevels.

In Figure 4-66, the SDM is InSv. Using the command set provided, you can obtain additional details about the condition of the SDM to isolate and resolve faults.

Figure 4-66   —   SDM MAP level

```
CM        MS        IOD        Net        PM        CCS        Lns        Trks        Ext        APPL
.         .         .          .          .         .          .          .           .                     .
SDM                            OAMAP                 SDM        SWMTC SDMBIL
 0 Quit . . . .
 2 _
 3         SDM 0 InSv        Links_OOS: .
 4         <Maintenance message text area>
 5 Trnsl
 6         <scrolling text area>
 7 Bsy
 8 RTS
 9 OffL
10
11
12
13
14 QuerySDM
15 Locate
16
17
18 Platform
  USERID
Time 19:48 >
```

Monitoring SDM-related alarms at the MAP display

The MAP displays SDM alarms under the APPL header of the maintenance level alarm banner and the SDM header of the APPL level alarm banner.

Figure 4-67, "SDM alarms on the Maintenance banner" shows an example of an SDM alarm under the APPL header of the maintenance level alarm banner.

Note: Power-related faults on the SDM also trigger a frame supervisory panel (FSP) alarm under the external (Ext) header. The modular supervisory panel (MSP) also provides an audible alarm, and visual indications on the cabinet and at the end of the aisle.

Figure 4-67 — SDM alarms on the Maintenance banner

	CM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	**APPL**
	.	.	.	.		.	.	.	.	**SDM** *C*
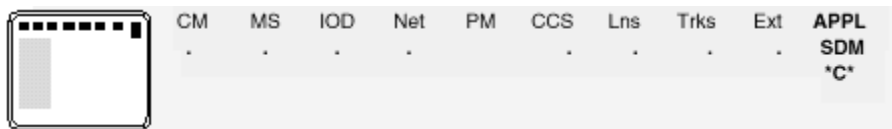
Table 4-32, on page 4-343 identifies and explains the SDM alarm severity symbols that appear in the Maintenance banner. These alarm symbols also appear in the maintenance banner of the RMI.

Table 2-3, "SDM alarms at the MAP alarm banners" in Chapter 2, "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 lists the following various maintenance level alarm values:

- alarms associated with the SDM
- SDM node states that trigger the alarms
- meaning of each combination of alarm and node state

The SDM node states appearing at the MAP display, represent the CM view of the state of the SDM. The SDM state at the MAP display is the true state of the SDM whenever the communication link between the SDM and the CM is functioning.

If the communication links between the SDM and the CM are not functioning, the operating condition and local state of the SDM are unknown to the CM. In this case, the CM designates the SDM as SysB, with a communication fault, as described in table 2-3 in Chapter 2, "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906. Under these conditions, the SDM state displayed at the MAP interface and the local node state of the SDM (as it appears on the RMI) may be mismatched.

Table 4-32 — SDM alarm symbols

SDM alarm severity symbol	Explanation
	minor alarm or no alarm
M	major alarm

SDM alarm severity symbol	Explanation
C	critical alarm
Note: There is no symbol for minor alarms.	

Refer to Chapter 2, "SDM maintenance overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 for more information.

Using SDM commands at the MAP display

The SDM MAP display is accessed at the SDM level of the MTC APPL level. The following table describes the commands available at the SDM MAP level.

Table 4-33   —   SDM MAP level commands

Command name	Command purpose
QUIT	The QUIT command is the standard SDM level menu command used to exit the current MAP level.
TRNSL	The TRNSL command displays the link address information for the links between the MS and the SDM.
BSY	The BSY command sets the SDM to manual busy (ManB) state.
RTS	The RTS command returns the SDM to service from the manual busy (ManB) state.
OFFL	The OFFL command sets the SDM to offline (OffL) state from the manual busy (ManB) state. Executing the OFFL command disables communications between the CM and the SDM.
QUERYSDM	The QUERYSDM command provides a variety of information about the status and configuration of the SDM.
LOCATE	The LOCATE command provides a list of hardware modules installed on the SDM and their physical location.
PLATFORM	The PLATFORM command provides access to the SDM platform level for the SDM device-level fault isolation and resolution functions.
REBOOTSDM	The REBOOTSDM command is a non-menu command that reboots the SDM.
HALTSDM	The HALTSDM command is a non-menu command that halts the SDM.

Using the Trnsl command

Trnsl displays the link address information for the DS512 links between the MS and the SDM. When Trnsl is executed, the following information is displayed:

- the SDM number, domain, and port

- the MS number, card, and port

- the link status and messaging condition

- whether C-side (MS) or P-side (SDM node control) actions are in progress

Using the Bsy command

Bsy sets the SDM to manual busy (ManB) state. The system response to the Bsy command depends on the status of the communication link between the CM and the SDM:

If the CM and the SDM are communicating successfully, the CM sends the Bsy command to the SDM. If the SDM is in service, you receive a yes/no prompt. This indicates that executing the Bsy command causes a service interruption (all applications running on the SDM shut down). Executing the command changes the state of the SDM at the MAP display to ManB, changes the local state of the SDM (as it appears on the RMI) to ManB, and shuts down all SDM applications.

If the CM and the SDM are not communicating, the CM cannot send the Bsy command to the SDM. The CM view of the SDM state (as it appears at the MAP display) changes to ManB (NA) or ManB/The SDM is not responding. This state depends on the reason for the communication problem. The local state of the SDM (as it appears at the RMI) and its operating condition are unaffected by the Bsy command. However, when CM-SDM communications are restored, the SDM aligns to the current CM view of its state.

You can set the local state of the SDM to ManB when the CM and the SDM are not communicating. However, the Bsy command must be executed at the RMI, which shuts down any applications that are running.

When the SDM is in OffL state, the CM sets the SDM state to ManB and enables CM-SDM communication. The CM then sends the Bsy command to the SDM.

The Bsy command has the options Force and Nowait. The Bsy command with the Force option overrides the following commands that are in progress:

- RTS
- RTS Force
- Bsy

The Nowait option is the standard DMS MTC command parameter used to return command entry capability immediately. That is, you can continue to enter other commands while the system is executing the Bsy command. Refer to logs output to determine the progress of the Nowait option.

Using the RTS command

RTS returns the SDM to service from manual busy state. The system response to this command depends on the status of the communication link between the CM and the SDM:

If the CM and the SDM are communicating successfully, the CM sends the RTS command to the SDM. If the command executes successfully, the SDM is returned to ser-

vice. If there are no faults on the SDM, the state of the SDM changes to InSv at the MAP interface, and at the RMI. If faults exist, the SDM state is ISTb.

If the CM and the SDM are not communicating, the CM cannot send the RTS command to the SDM. The CM view of the SDM state (as it appears at the MAP display) changes to SysB (NA) or SysB/The SDM is not responding. The state depends on the reason for the communication problem. The local state of the SDM (at the RMI) and its operating condition are unaffected by the RTS command. However, when CM-SDM communications are restored, the SDM aligns to the current CM view of its state.

To perform a local return-to-service of the SDM when CM-SDM communications are down, the RTS command must be executed at the RMI.

The RTS command has the options Force and Nowait. The Force option invokes a forced return-to-service of SDM applications. Use the Force option with caution. It ensures the state change takes place, however, all errors (IP mismatch) are ignored and checks are bypassed. The Nowait option is the standard DMS MTC command parameter used to return command entry capability immediately. That is, you can continue to enter other commands while the system is executing the RTS command. Refer to logs output to determine the progress of the Nowait option.

NOTE: When the SDM or one of its applications or services is returned to service from a manual busy (ManB) state, the state of the SDM may move to in-service (InSV) briefly, then to in-service-trouble (ISTb) for a few minutes, and finally back to InSv.The ISTb state is the result of the application not being fully capable of supplying service during initialization. For example, if the Operations Measurements application is not yet InSv, the Exception Reporting application will be ISTb.

Using the QuerySDM command

QuerySDM provides information about the SDM, as follows:

- QuerySDM with no additional parameters displays the status of the SDM as seen from the MAP display, its IP address on the CM side, and its physical location as defined in table SDMINV. The slot number is always blank. This information is displayed regardless of the state of the CM-SDM communication link.

- QuerySDM FLT displays information about SDM software and device faults. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning. Stopped processes are not displayed when the node is in ManB state. The following information is included for device faults:
  - alarm severity
  - the faulty component
  - time stamp of the last SDM state change
  - the faulty module, its product engineering code (PEC), and location

— other devices on the faulty module and their state
— reason text that describes the fault (if available)

If there are no faults on the SDM, and the SDM is in service, QuerySDM FLT displays the message "No local SDM fault to report".

- QuerySDM LOADS displays the version and state of software installed on the SDM. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.

- QuerySDM STATUS displays local SDM alarms (application software, LAN connectivity, system software, and CM connectivity). QuerySDM STATUS also shows all hardware devices on the SDM, and their states. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.

- QuerySDM CONFIG displays the following configuration data related to the SDM:

    — connectivity information
    — DCE configuration
    — operating company LAN configurations
    — platform type
    — system and logical volume threshold values
    — system variable settings

This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.

Error messages for QuerySDM with the FLT, LOADS, CONFIG, or STATUS options are generated for the following reasons:

- The request to the SDM cannot be sent because there are no available DS512 links.

- The CM timed out before the command complete message was received from the SDM.

- The SDM is not responding.

- The SDM is in the OffL or unequipped state.

- Messages could not be sent to the SDM for the following reasons:

    — The node maintenance process could not obtain a CM-side message transport service (MTS) endpoint.
    — The node maintenance process could not obtain an SDM-side MTS endpoint.

- The maximum number of simultaneous SDM commands has been exceeded. Try the command later.

- An unexpected software error was encountered.

In addition, error messages are generated for QuerySDM FLT for the following reasons:

- The MS has indicated that the SDM is a minor, major, or critical babbler. That is, the SDM node is sending too much information before receiving acknowledgements:

  — When the MS indicates that the SDM is a minor babbler, the state of the SDM on the CM is set to ISTb. An APPL SDM minor alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL SDM minor and major".

  — When the MS indicates that the SDM is a major babbler, the state of the SDM on the CM is set to SysB. All links are maintenance open. Applications can no longer communicate between the SDM and the CM. An APPL SDM-major alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL critical".

  — When the MS indicates that the SDM is a critical babbler, the state of the SDM on the CM is set to SysB. All links are closed. Applications can no longer communicate between the SDM and the CM. An APPL SDM critical alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL SDM critical".

Using the Locate command

Locate displays location information about the SDM hardware modules and the devices they support. The following information is displayed when this command is executed:

- the type of module, its location (including chassis and slot number), and PEC

- devices on the module

The SDM must be in ManB or higher (InSv, SysB or ISTb) state to execute this command successfully. The Locate command can only be used if the CM-SDM communication link is up. Error messages are displayed for the following reasons:

- There is no communication route to send the locate request to the SDM.

- The CM has timed out before receiving a command complete message from the SDM.

- The SDM is not responding.

- The SDM is in the OffL or unequipped state.

- Messages could not be sent to the SDM for the following reasons:

  — The node maintenance process could not obtain a CM-side MTS endpoint.
  — The node maintenance process could not obtain an SDM-side MTS endpoint.

- The maximum number of simultaneous SDM commands has been exceeded. Try the command later.

Using the Platform command

Platform displays state information on the SDM software components, hardware modules, and devices. The following information is displayed when this command is executed:

- SDM application and software state (APPL)
- SDM LAN connectivity state (LAN)
- SDM system software state (SYS)
- CM connectivity state (CON)
- hardware device states. A state is displayed for a hardware device on domain 0 (D0) and domain 1 (D1).

The Platform command can only be used if the CM-SDM communication link is up. Error messages are displayed if the CM-SDM communication link is down or the Platform MAP level could not be allocated.

The following commands are available from the Platform level:

- QUIT is the standard menu command used to exit the current MAP level.
- TRNSL displays information on the state of the CM to SDM connecting links.
- BSY is a menu command that sets the requested SDM hardware device to a manual busy (ManB) state. The command has one optional parameter:

    — The FORCE option is the standard DMS MTC command parameter used to force the state change. Force works even if the change will cause a service outage. Use the Force option with caution. It ensures the state change takes place, however, all errors (IP mismatch) are ignored and checks are bypassed

> **CAUTION: Possible service interruption**
> Using the FORCE option with the BSY command may cause a possible service inter-ruption. BSY with the FORCE option overrides any commands in progress.

Error messages for BSY with the FORCE option are generated for the following reasons:

- The command could not be executed because of lack of SDM resources.
- The CM timed out before the command complete message was received from the SDM.
- Execution of the command was canceled because the user chose abort or a negative response to a confirmation prompt.
- The hardware device is already in a ManB state.
- The command could not be executed due to an abnormal condition or because communications with the SDM are down. The reason is described by one of the following error messages:

    — The SDM is Unequipped

— The SDM is OFFL
— No communication route to the SDM
— No SDM C-side MTS address
— No SDM P-side MTS address
— The SDM is not responding
— Maximum number of SDM command users exceeded

- RTS is a menu command that returns the requested hardware device to service from a manual busy (ManB) state.

- The QuerySDM command provides a variety of information about the status and configuration of the SDM. See the section, "Using the QuerySDM command" on Page 4-346 for more information.

- Locate provides a list of modules and devices installed on the SDM and their physical location. See the section, "Using the Locate command" on Page 4-348 for more information.

Using the RebootSDM command

RebootSDM is a non-menu command that is used to reboot the SDM. It can only be executed if the node state is ManB and the links are available.

NOTE: Reboot message

When a RebootSDM command is issued, the following message may appear on the SDM's local console during the reboot:

Board Configuration Data Failure

Ignore this message. It is not service-affecting.

Using the HaltSDM command

HaltSDM is an unlisted menu command that halts the SDM. It can only be executed if the node state is ManB and the links are available.

CAUTION: Possible loss of service If the RebootSDM or HaltSDM command is used on an SDM/FT system while there is a loss of power to the ICM on D0 of the main chassis (ICM 0), the system will not recover from the reboot. A loss of power can be caused by the removal of the power cable, turning off the circuit breaker in the MSP, or a faulty ICM 0. Restore power to ICM 0 and perform a reboot.

Using the SDMRLogin command

SDMRLogin is a non-menu command that allows root and maint (maintenance) users to log in to the SDM from any MAP CI level.

NOTE: When you execute an SDMRLogin session from the CM to the SDM as a root or maint class user, the system puts you in a restricted shell. SDMRLogin is used to

---

perform local maintenance activities. If you need to perform other operations that require root user privileges, log directly into the SDM as the root user.

To log into and execute commands in the SDM refer to *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906. There are many complex commands and references in the NTP, refer there for more information.

SDM Log Delivery

The Log Delivery application, included as part of the base software platform on the SDM, delivers user-defined streams of DMS SuperNode logs and SDM fault-tolerant platform and application logs to one or more of the following:

- up to 30 operations support systems (OSS), by TCP/IP links from the SDM to the operating company LAN
- up to 30 UNIX files stored on the SDM

A maximum of 30 Log Delivery output devices can be commissioned (the sum total of TCP/IP links and UNIX files cannot exceed 30).

The Log Delivery application cannot be used to deliver logs generated by DMS SuperNode processors other than the CM and the SDM. Logs from other processor types may continue to be delivered by the standard input output controller (IOC) log devices by datafilling a valid IOC log device name for each required processor type in table RLOGDEV.

For more detailed information please refer to *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

Routine maintenance recommendations

Nortel Networks recommends that you perform the following activities as part of the SDM routine maintenance strategy. Some tasks can be performed by maint class users, while others require root user permission for accessing the SDM.

Maintenance user tasks

The following activities require maintenance user permission:

- Check dial-up access to SP0 on the CPU personality module by periodically dialing into the SDM from a remote VT100 terminal and logging in to the RMI. This ensures that the RMI is readily available for maintenance purposes.
- If your system is configured with a local VT100 terminal, connected directly to SP0 by a null modem, log in to the RMI periodically to ensure it is readily available for maintenance activities.
- Clean the SDM tape drive after the first 4 hours of tape movement of a new cartridge, and then after each 25 hours of use, using the appropriate cleaning tape (Hewlett-Packard part number 92283K or equivalent). For more informa-

tion, see the procedure "Cleaning the SDM DAT drive" in "SDM maintenance procedures" within *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

Root user tasks

The following activities require root user permission:

- Backup the SDM software and data as required. Refer to the "SDM system administration overview" in *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906 for more information.

- Monitor log files in the /var/adm directory for system or security abnormalities.

Fault reporting

Only SDM faults with the current highest priority are visible at the MAPCI SDM display. SDM faults are also visible at the RMI, and by status LED indicators provided on the SDM hardware. Power-related and thermal-related SDM problems are also reported by the EXT alarm, and by the office alarm system.

SDM hardware replacement procedures

For more detailed information on detailed SDM hardware replacement procedures please refer to *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide, 297-5061-906*. Each procedure contains the following:

- explanatory and context-setting information
- summary flowchart
- step-action instructions

Upgrading the CPU controller module

For more detailed information on upgrading the CPU controller module please refer to *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

OSSDI

The Operations Support System Data Interface (OSSDI) Command Specification provides a description of the user interface to the DMS Data Management System (DDMS). The OSSDI defines a message protocol used between the Operations Support System (OSS) and the DDMS. The OSS uses OSSDI commands to provision table data on the DMS-100 switch. These OSSDI commands also are used by the OSS in the administration of the DDMS provisioning system. The DDMS system

returns OSSDI responses after processing a command. These OSSDI commands and responses are OSSDI messages.

This topic is beyond the scope of this document. Please refer to *DMS-100 Family SuperNode Data Manager OSSDI Technical Reference Manual*, 297-5051-915.

SDM applications

There are some new and existing applications that work with SDM.

Multi-Application OAM&P Platform

- Fully redundant and fault tolerant platform
- High Speed Interface to DMS OAM&P data and Applications

    —MAP
    —Billing
    —Service Activation
    —Surveillance
    —Performance Monitoring

OM Delivery

High Speed OM Delivery via Comma Separated Value

- Provides for the storage of the DMS OMs on SDM
- Allows for user definable OM Group Profiles based on:

    —Selected OMs
    —Polling frequency (5 Min. or DMS Office Transfer Period of 15/30)
    —Number of records per file

- Secure FTP to PC or WorkStation

    — Comma Separated Value (CSV) file format for spreadsheet application

Eventure

Eventure is a distributed, web-based fault, performance, and accounting record management product which adapts and adds value to the Nortel Networks SuperNode Data Manager.

- Collection & Storage

    — fault, performance & accounting

    — from one to many SDMs

    — unified web interface

- Analysis

    — Filter

— Summarize

— Display

— Integrated online help

EADAS via TCP/IP

TCP/IP interface with NTM / DC OSS

- Provides a common open interface between DMS / SDM and NetMinder or any Network Traffic Management / Data Collector OSS to reduce Telco's operating costs and will avoid unnecessary delay during upgrade

- Provides high-speed interface (Ethernet (10M) vs. X.25 (56Kbps)). Allows telcos to lower mtce cost and reduces reliance on Datakit

- Direct connection to NetMinder from SDM will improve reliability (Traffic Management data will not depend on DC OSS)

SMDR

SuperNode Billing Application

- Provides near real time delivery of SMDR

- Provides flexible routing of Records

- Provides high-speed SMDR Deliv.

- Provides a single application for AMA and SMDR

XA-Core Overview and Maintenance

XA-Core overview

Introduction

The XA-Core type of DMS-core has three main modules of shared memory (SM), processing element (PE), and input/output processor (IOP).

The DMS-bus processes and sends messages to nodes in the SuperNode and SuperNode SE switches. The DMS-bus has two load-sharing message switches (MS).

The DMS-link allows the DMS-core and DMS-bus to communicate in the SuperNode and SuperNode SE switches. The DMS-link is the software structure which does signaling standards for the public network.

Figure 4-68 shows the system architecture of the XA-Core in a DMS SuperNode switch.

Figure 4-68 — **XA-Core in a DMS SuperNode switch**
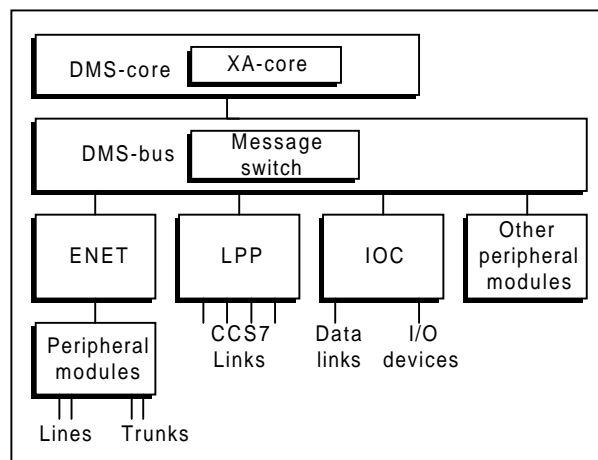
Processor and memory

The processor and memory controls call processing, configuration, and maintenance of the switch. The processor and memory include the following circuit packs:

- processor element (PE) circuit packs (NTLX02)
- input/output processor (IOP) circuit packs (NTLX03)
- shared memory (SM) circuit packs (NTLX14)

File system

The XA-Core has a logical file system (LFS) and a fault tolerant file system (FTFS). The LFS does not depend on the device type. An LFS-to-FTFS interface gives the LFS access to the FTFS volumes. The interface transfers LFS operation requests into FTFS operation requests. The FTFS provides the following to XA-Core:

- volume directories and the capability for directories in a hierarchy structure with path names
- a configuration for disk cache
- extent-based system for disk files
- application registration for file system event notification

In-service spares

All installed spares in XA-Core are in an in-service mode. XA-Core automatically places the spares into replacement use for other equipment that goes out of service. Replacement of equipment that goes out of service requires no manual maintenance action. XA-Core has hot insertion and removal of circuit packs and packlets.

Reset control

The reset control provides a utility for a local or remote reset of the XA-Core. The reset control displays the status of total XA-Core processing. The reset control also has command interpreter (CI) capability but no display of menu-type levels of the maintenance and administration position (MAP). The reset terminal interface (RTIF) is an interface to a display terminal for reset control. The RTIF can be a local or a remote terminal. A remote RTIF terminal can connect through a modem to the XA-Core. The RTIF interface protocol for the XA-Core are as follows:

- RS-232 (local or remote)
- RS-422 (remote)
- current loop (local)

The RS-232/RS-422 serial interface packlet (NTLX08) contains the reset capability in an XA-Core shelf. An XA-Core shelf has two NTLX08 packlets for reset control (one packlet is a backup for the other packlet).

XA-Core status information of the reset control display indicates the following:

- heartbeat on operation of the switch

- status during a boot or reset
- information on RTIF hardware
- results of diagnostics and tests when power is applied
- node name of RTIF

Figure 4-69 — XA-Core to MS port connections for DMS SuperNode
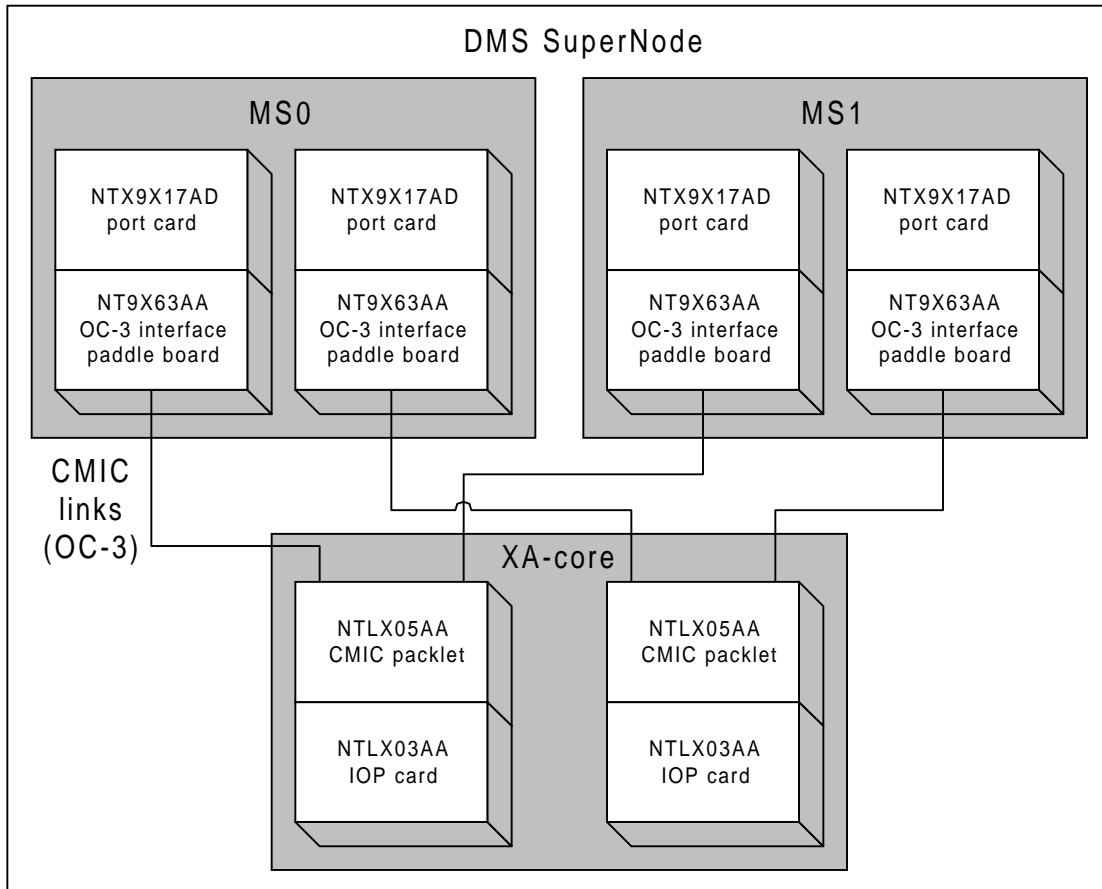
Visual indicators on circuit pack

Each XA-Core circuit pack and packlet has visual indicators on the faceplate. The visual indicators are light-emitting diodes (LED). These LEDs are indicators of the status of the circuit pack or packlet for removal. All the LEDs on all circuit packs and packlets of the XA-Core shelf illuminate in response to a MAPlevel command INDI-CAT with parameter TESTALL. The parameter TESTALL checks the LEDs for correct illumination. The status indicators are:

- Red LED illuminated indicates you can remove the circuit pack or packlet safely (circuit pack is not in service). The red LED can also wink instead of illuminate. The red LED winks in response to a MAP level command INDICAT activated for a circuit pack or packlet.

- Green LED illuminated indicates you cannot remove the circuit pack or packlet safely (circuit pack is in service).

- Amber LED illuminated indicates a loss of primary feed or link signal to the circuit pack or packlet. The amber LED is only on the SIM circuit packs and the CMIC/RTIF packlets. The amber LED is on the SIM circuit pack for loss of one or more power feeds to the SIM circuit pack. The amber LED is on the CMIC/RTIF packlets for loss of one or more link signals.

Live-inserted circuit pack

Maintenance activities can insert and remove XA-Core circuit packs from a live slot of an XA-Core shelf. The design of a non-contact midplane permits the live insertion and removal of XA-Core circuit packs. A non-contact midplane has electrical connections completed by the effect of electric and magnetic field coupling in the circuit path. An exception to the live insertion and removal of circuit packs is the NTLX12AA shelf interface module (SIM) circuit pack. Remove power from the SIM circuit pack only before the insertion or removal of the SIM circuit pack. To remove power from the SIM circuit pack, turn off all three circuit breakers on the faceplate of the SIM circuit pack. XA-Core also permits the live insertion and removal of packlets.

This section describes the cards and packlets for the eXtended Architecture Core (XA-Core) of the DMS SuperNode and DMS SuperNode SE switches. Refer to the *XA-Core Reference Manual*, 297-8991-810, for additional information on XA-Core cards and packlets.

DMS SuperNode and SuperNode SE XA-Core card and packlets descriptions

The XA-Core shelf has cards and packlets located in front and back slots of the XA-Core shelf. The cards and packlets are field replaceable units (FRU). Each of the cards and packlets has a product engineering code (PEC) for an identifier.

A card is a circuit pack that inserts into a slot on the XA-Core shelf. XA-Core has three basic types of cards:

- memory cards
- processor cards
- power interface cards

The communication link between the cards is the extended architecture interconnect (XAI). The XAI is a network of links found in the midplane. The midplane is a printed circuit board (PCB) that is like a backplane. The XA-Core shelf has the midplane located in the center of the shelf between the front and back slots for cards and packlets. The midplane is a non-contact midplane. A non-contact midplane has electromagnetic field couplers and connector pins for card connections to the midplane. These couplers connect through the effect of an electromagnetic field from one pair

of circuit tracks to another pair. A voltage on a transmit pair of circuit tracks induces a small voltage pulse on a receive side of another track pair. Each coupler has a small transmitter and antenna embedded in the midplane circuit tracks. The non-contact midplane allows card insertion and removal in a live state of electrical power.

A packlet is a circuit pack that inserts into a slot on the input/output processor (IOP) card. XA-Core has two basic types of packlets:

- mass storage packlets
- external communication packlets.

Preventive maintenance

This section describes preventive maintenance methods for the eXtended Architecture Core (XA-Core) in the DMS SuperNode and DMS SuperNode SE switches. This section lists the preventive maintenance procedures for routine maintenance that operating company personnel can perform. This section also describes the automatic maintenance performed on the XA-Core by the support operating system (SOS) of the switch.

This section includes the following subsections:

- Routine maintenance procedures list the preventive maintenance procedures in the *XA-Core Maintenance Manual*, 297-8991-510.
- Automatic maintenance describes the system-run processes that detect, repair, and report problems.
- System recovery controller (SRC) describes the control of recovery activities by the SRC.
- Split mode of XA-Core describes the split mode of XA-Core into two sides.

Routine maintenance procedures

Routine procedures if performed according to a schedule, prevent faults in both the hardware and the software of the switch. Refer to the *XA-Core Maintenance Manual*, 297-8991-510 to find the procedures.

The XA-Core preventive maintenance procedures include the following:

- How to allocate test volumes on XA-Core disk drives
- How to allocate test volumes on XA-Core digital audio tape (DAT) drive packlets
- How to change XA-Core routine exercise (REx) intensity
- How to check and adjust the time of day (TOD) clock of XA-Core
- How to clean the XA-Core digital audio tape (DAT) drive
- How to copy an office image from XA-Core disk to tape

How to perform light-emitting diode (LED) maintenance

- How to replace XA-Core cooling unit filters
- How to restore an office image from XA-Core tape to disk
- How to return an XA-Core circuit pack, packlet, or assembly to Nortel Networks
- How to schedule automatic image taking for XA-Core
- How to schedule digital audio tape (DAT) drive maintenance in XA-Core
- How to test wrist-strap grounding cords in XA-Core

The *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511 provides the detail instructions required to perform the XA-Core routine procedures.

Automatic maintenance

The XA-Core provides automatic maintenance through the following activities:

- processor bus matcher
- Audits
- Routine exercise (REx) tests
- System recovery controller (SRC)

Processor bus matcher

The processor bus matcher is in the RHINO processor which is an enhanced version of the high-speed instruction prefetcher path optimizer (Hippo) containing 512 Kbytes of on board SRAM.

Audits

Audits are background processes that the switch runs to monitor the state of the XA-Core. Audits of software provide background processes that check the accuracy of applications and of resource data. Audits of hardware provide diagnostic tests of hardware. Audits run for both in-service and out-of-service conditions of hardware. The in-service diagnostics of audits prevent isolation of the circuit pack or packlet under test. An in-service diagnostic checks hardware except when the hardware is under normal operation of the software. The out-of-service diagnostics of audits are complete tests of a circuit packs or packlets. Separate diagnostic tests of hardware are in the audits or in the routine exercise (REx) tests but normally not both.

Routine exercise (REx) tests

Routine exercise (REx) tests are maintenance tests that the switch runs to check the state of the XA-Core. REx tests of software check the accuracy of software applications and of resource data. REx tests of hardware identify hardware failures before an

outage or performance degradation occurs. The correction of hardware failures that REx tests identify prevents an outage or performance degradation. The system REx (SREx) test controller has software that runs the REx tests for automatic execution at time intervals. The SREx tests run on the complete switch. SREx tests run when the CPU occupancy for CallP + Maintenance is less than 40%. Software table REX-SCHED defines the time intervals for SREx tests. Table REXSCHED also provides the ability to enable or disable separate REx tests. A REXTST command at the MAP terminal can request a manual REx test on part of the XA-Core when required. A RExTst indication appears on the MAP display when the switch executes a REx test.

REx diagnostic tests

The REx tests perform diagnostic tests of hardware under two conditions. REx tests perform diagnostic tests on hardware that is in service and out of service. The in-service diagnostic tests of REx tests check all XA-Core functions and hardware that the XA-Core audits have not checked. The in-service diagnostics of REx tests prevent isolation of the circuit pack or packlet under test. The out-of-service diagnostic tests of REx checks fault detection of XA-Core hardware through error insertion. Error insertion for an out-of-service diagnostic on hardware requires the circuit pack or packlet to be in isolation. The out-of-service diagnostic of a REx test is not a complete test like the out-of-service diagnostic of an audit. An out-of-service diagnostic of a REx test checks hardware except when the hardware is under normal operation of the software.

REx tests have no check of the IDPROM of a circuit pack against software table PEC-INV. A check of the IDPROM occurs automatically in XA-Core during the addition of the circuit pack to the shelf.

The SREx tests run automatically each night, normally at the default time of 1:30 a.m. Normally on Wednesday, the full SREx test runs. On all other nights of the week, the base SREx test normally runs. Entries in software tables can modify the schedule for SREx tests. The entries for REx schedule are in table REXSCHED and office parameter NODEREXCONTROL of table OFCVAR. Refer to the procedure, "How to change XA-Core REx intensity" in *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511.

Before the REx test begins, the switch automatically checks the dedicated stability threshold counters. The stability threshold counters perform a monitor of parity fault counts of the static random access memory (SRAM). If there are too many SRAM parity faults in a determined time before the request for a REx test, the switch responds as follows:

- The MAP displays a warning and confirmation prompt when a manual request for a REx test is not good. The manual REx test can abort or can execute.

- The switch aborts the beginning an automatic REx test at the planned time and generates a log report. The log indicate the reason for no REx test. When two automatic REx tests that follow one another cancel in one day, a RExSch minor alarm occurs.

A monitor of the switch stability continues during a REx test. The switch aborts the REx test when a mismatch, trap, link closure, or restart occurs during a REx test.

REx test classes

REx tests are available in groups called classes. The classes of REx test are as follows:

- PE
- SM
- IO
- BASE
- ALL
- FULL

The classes of REx tests have the following differences:

- PE class of REx test is:
  - A REx test on a processor element (PE) circuit pack of an XA-Core that is a different PE circuit pack for each REx test performed.
  - The REx tests are out-of-service tests.

- SM class of REx test is:
  - A REx test on a shared memory (SM) circuit pack of an XA-Core that is a different SM circuit pack for each REx test performed.
  - The REx tests are out-of-service tests.

- IO class of REx test is:
  - A REx test on an input/output processor (IOP) circuit pack and related packlets of an XA-Core. The REx test is on a different IOP circuit pack and related packlets for each REx test performed.
  - The REx tests are out-of-service tests.

- BASE class of REx test is:
  - A REx test while in service on all PE circuit packs, SM circuit packs, IOP circuit packs, and related packlets of an XA-Core.
  - An image test performed.
  - By default, BASE REx tests run each day of the week except Thursday.

- ALL class of REx test is:
  - A REx test while in service on all PE circuit packs, SM circuit packs, IOP circuit packs, and related packlets of an XA-Core.

— A REx test while out of service on a different PE circuit pack, a different SM circuit pack, and a different IOP circuit pack (with related packlets) of an XA-Core. The circuit packs and packlets are different for each REx test.

- FULL class of REx test is:
    — A REx test while in service on all PE circuit packs, SM circuit packs, IOP circuit packs, and related packlets of an XA-Core.

    — A REx test while out of service on a different PE circuit pack, a different SM circuit pack, and a different IOP circuit pack (with related packlets) of an XA-Core. The circuit packs and packlets are different for each REx test.

    — An image test performed.

    — By default, FULL REx tests run each Thursday of the week.

REx test results report

When there is a REx test, the switch generates log report XAC415 to indicate a pass or failure of the REx test. The switch issues a RExTst minor alarm under the XAC header of the alarm banner when the REx test fails. Log report XAC415 reports on a REx test failure to indicate the following:

- reason for REx test failure
- category
- list of hardware detected for possible problem

When a system REx test cannot complete, the switch generates a failure reason. The following conditions of the switch prevent the system REx test from completing:

    — can not interrupt another maintenance activity in process
    — system resources not available to run the REx test (recommend REx test occur during low traffic periods)

When a REx test fails, another REx test that passes is the only way to clear the RExTst minor alarm. For the detail instructions to clear the RExTst minor alarm, refer to the chapter, "Expert problem solving procedures" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511. Also refer to the Alarm and Performance Monitoring Procedures for detail instructions to clear the RExTst minor alarm.

When a system REx test cannot start on two daily attempts that follow one another, the switch issues a RExSch minor alarm. The RExSch minor alarm appears under the XAC header of the alarm banner. A system REx test cancels because faults exceed the thresholds monitored by the switch. The switch monitors thresholds for stability faults to identify repeating problems. Entries in software tables list the values of the thresholds.

Indications of automatic test results

The following indicators warn operating company personnel of the results of automatic maintenance tests.

- alarms

- logs

- operational measurements (OM)

Operating company personnel can monitor the indicators for directions and patterns. When monitored, operating company personnel can detect and correct small problems before the small problems become larger problems.

For detail information about clearing alarms, refer to the chapter, "Problem solving charts" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511. Also, refer to Alarm and Performance Monitoring Procedures section of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511.

Refer to the chapter, "Logs" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511 for additional information about logs. Also, refer to the *Log Report Reference Manual*.

Refer to the chapter, "Operational measurements" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511 for additional information about OMs. Also, refer to the *Operational Measurements Reference Manual*.

System recovery controller (SRC)

The system recovery controller (SRC) controls recovery activities in the switch. The SRC arranges the recovery of switch nodes in the correct sequence. The SRC recovers a node after recovery of other nodes that the node requires for correct recovery. The SRC plans the recovery activities to reduce the period of the outage.

The SRC makes several recovery attempts when a node cannot recover. The SRC makes more detail analysis with each recovery attempt. If needed, the SRC reloads a node's software and return the node to service. This reload of a node's software occurs when required because the node is out of service during the reload.

The SRC also controls recovery activities on switch nodes outside of the XA-Core module.

The SRC performs the following functions:

- SRC dependency manager controls the correct sequence of recovery of the switch nodes

- SRC group manager arranges switch nodes together in groups for broadcast loading when required

- SRC concurrent activity manager balances the amount of recovery work with other switch activities

- SRC starts recovery applications and monitors each step of the applications for quick completion

SRC activation

The following events make active the SRC to query and when needed, begin the recovery activities:

- warm restart of the XA-Core
- cold restart of the XA-Core
- reload restart of the XA-Core
- loss of software load in a peripheral module (PM)
- manual RESTART SWACT, ABORT SWACT, or NORESTART SWACT of the XA-Core

A restart restores the software of the support operating system (SOS) of the switch to a state that has stability. The reset terminal interface (RTIF) indicates the completion of a restart. The shape of the cursor on the RTIF display changes every second to indicate a completion of the restart. This change of the cursor shape for each second indicates basic operation of the SOS.

Split Mode of XA-Core

The XA-Core splits into two sides during an image test. The image test checks the sanity of the switch's software within the shared memory (SM) circuit packs of the XA-Core. The split XA-Core has an active side and an inactive side. The image test cannot start and split the XA-Core if one SM circuit pack only is available to the active side. The active side needs a minimum of two SM circuit packs for the XA-Core to split. Each side of the split XA-Core has one copy of the software image. The image test occurs on the image copy of the inactive side. Each side of the split XA-Core has one processor element (PE) circuit pack. The XA-Core has an ImgTst minor alarm displayed on the MAP during the image test. The image test runs manually by the Image command at the XACMtc level of the MAP. The image test also runs automatically for the base and full REx tests.

The split mode of XA-Core also can occur when the XA-Core is in an upgrade operation. The XA-Core has an Upgrade minor alarm displayed on the MAP during the upgrade operation.

Problem isolation and correction

This section describes the resident tools used to problem solve fault conditions on the eXtended Architecture Core (XA-Core). The XA-Core is on the DMS SuperNode and SuperNode SE switches. For information on nonresident tools, refer to the *Technical Assistance Manuals*.

Diagnostic tools

This section describes the following diagnostic tools:

- alarms
- DMS monitoring (DMSMON) tool
- log reports
- maintenance manager's morning report (AMREPORT)
- OM-log-alarm cross reference charts
- operational measurements (OM)
- Sherlock
- switch performance monitoring system (SPMS)
- TRAPINFO

Alarms

Alarms are the main indicators of problems with the system. Alarms provide information about the following types of problems:

- equipment failure
- equipment that operates at a performance degrade
- equipment reached defined capacity level of the operating company
- full or partial system sanity
- software errors
- automatic recovery attempt that is unsuccessful
- reboot that is not authorized
- auto transfer to standby
- inability to transfer from a fault condition to standby
- loss of communication between entities or subsystems
- loss of ability to store operational information (data exceeds threshold)
- failure of inter-node transmission
- loss of communication with operation support systems
- power distribution failure
- security violations
- fire and intrusion

Three levels of severity divide the alarms:

- minor
- major

- critical

A minor alarm means a problem that does not cause a loss of service. Examples of minor alarm conditions include the following:

- conditions that may lead to a major alarm if not corrected
- one piece of a pool of equipment that has been busied
- service degradation that has fallen below a threshold of an operating company

A major alarm means that one-half of a duplicated system is out of service. The major alarm may cause a loss of service. There is no backup if another fault occurs on the active system. A switch generates a major alarm when service degrades below a threshold of an operating company.

A critical alarm means a problem that causes a loss of service. Examples of critical alarm conditions include the following:

- loss of call processing capability (dead system)
- partial or full loss of system sanity
- service degradation that has fallen below a threshold of an operating company

Each alarm has a log report for reference. The log report give more detailed information about the problem than the alarm.

XA-Core system alarms appear under the XAC header of the MTC level of the MAP. Refer to the chapter, "Problem solving charts" in *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511. The chapter, "Problem solving charts" has a list of all XA-Core alarms, possible causes, and where to find information on how to clear each alarm. Also refer to *XA-Core Maintenance Manual*, 297-8991-510 for more detailed information about the alarm system.

DMSMON

DMSMON monitors changes in operation when operating company personnel change a release load. DMSMON formats the information into a report for manual or automatic generation.The type of information in the report includes the following:

- counts of internal events (e.g. warm and cold restarts) and downtime information
- system trap information
- counts of log reports
- hardware counts (configuration information)

Refer to the *DMS Family Commands Reference Manual*, 297-1001-822, for additional information about the DMSMON tool.

Log reports

Log reports are a primary source of information about the components of the XA-Core. Some logs can isolate a problem to a single component. Other logs help to identify problems attributed to more than one component.

Log reports include the following information:

- severity of the log report (represented by the number of asterisks)
- type of log
- time and day
- suspected problem
- list of suspected cards

For information about the XA-Core related logs, refer to the "Logs" chapter of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511.

Maintenance manager's morning report

AMREPORT provides a 24-hour summary of performance, administrative, and maintenance information. The AMREPORT information helps maintenance programs for correction and prevention of problems. The switch produces AMREPORT as a log report that includes the following information:

- switch performance information
    — SPMS indicators
    — call processing performance
    — processor element (PE) occupancy
    — network integrity
    — peripheral module (PM) switch of activity (SWACT) information
    — software performance: trap and SWER counts
    — footprint (FP) and OM log counts
    — information on SWACT of XMS-based peripheral module (XPM)
- scheduled test results
    — automatic line test (ALT)
    — automatic trunk test (ATT)
- switch operations
    — image dump results
    — patch summary
    — outage indicators
    — integrity check of table data

— unscheduled XPM REx test

Refer to the *Digital Switching Systems DMS-100 Family Maintenance Managers Morning Report*, 297-1001-535, for additional information about AMREPORT.

OM-log-alarm cross-reference charts

The chapter, "Problem solving charts" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511 contains a set of three charts. The three charts show the cross-reference of OMs, logs, and alarms. Each chart uses a key indicator of an OM register, log, or alarm as a starting point. The key indicator references the associated indicators of OM registers, logs, or alarms. A key indicator (e.g. OM register) of a cross-reference shows the associated indicators (e.g. log and alarm).

Operational measurements

Operational measurements (OMs) provide load and performance information. The OMsystem controls collection, display, and report generation of OMdata for the operating company.

Refer to the chapter, "Operational measurements" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511 for additional information about XA-Core related OMs.

Sherlock

Sherlock is a data collection tool for immediate use after a service outage. Sherlock automatically collects the data required to analyze the cause of the failure. Only one person can use Sherlock at a time.

Sherlock initiates a set of parallel processes that collect all the data available for the specified type of service failure. Sherlock sends the data to a series of temporary files. A person cannot access or control the data except if the person stops the Sherlock process before data collection completes.

Once data collection completes, Sherlock creates data and console files on a specified storage device. Sherlock also erases the temporary files. The data file name is SHRKyyyymmddhhmmss(Z). The Z means the file is a compressed file. The name of the console file is SHERLOCK$OUT. The console file contains all the messages and responses sent to the terminal. The console file also contains some additional messages (e.g. time stamps).

Refer to the *DMS Family Commands Reference Manual*, 297-1001-822, for additional information about how to use Sherlock.

Switch performance monitoring system

The switch performance monitoring system (SPMS) monitors all areas of switch operation and outputs regular reports on performance. The reports show different points of view.

The base for SPMS reports is the index values of OMs that the switch generates. The time covered in the SPMS report ranges from 0.5 hour to one month. This range of time provides a monitor of day-to-day events and of a longer period of switch performance.

Plans for the switch performance index use SPMS results for administration purposes. The operating company can use the overall office performance index, any section of lower-level indexes, or both. SPMS consists of three sections as follows:

- service section
- maintenance performance section
- provided resources section

Refer to the *Switch Performance Monitoring System Application Guide*, 297-1001-330, for additional information about SPMS.

TRAPINFO

TRAPINFO displays information about software traps. TRAPINFO gets information from the log utility and displays the information in one of several formats.

Refer to the *DMS Family Commands Reference Manual*, 297-1001-822, for additional information about the TRAPINFO tool. Also see the procedure, "How to respond to an XATrap alarm" in the chapter, "Problem isolation and correction" of *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511.

Overview of card replacement

XA-Core Maintenance Manual, 297-8991-510 describes SuperNode and SuperNode SE (SNSE) XA-Core circuit pack (CP) and packlet replacement procedures. Each replacement procedure description provides the following information:

- application information
- common procedures
- summary flowchart
- step-action instructions

Application information

The Application information section describes when to use the procedure. The Application information section also lists the versions of the CP or packlet.

Common procedures

The Common procedures section refers you to another set of instructions located elsewhere in the documentation. The common procedures describe how to perform related maintenance activities.

Summary flowchart

The summary flowchart shows the primary activities, decision points, and paths to correctly replace the CP or packlet. Use the summary flowchart to preview the replacement activities and to prepare for the replacement procedure.

Step-action instructions

The step instructions are a sequence of activities that describe how to replace a CP or packlet. The instructions also provide examples of MAP command syntax and MAP terminal responses.

On occasion, a step instruction can refer to a common procedure or to another document. After completion of the common or related procedure, return to the original point in the step-action instructions and continue.

Please refer to *XA-Core Maintenance Manual*, 297-8991-510 for more information on card replacement.

Recovery procedures

XA-Core Maintenance Manual, 297-8991-510 describes how to perform recovery maintenance procedures on the DMS SuperNode (SN) and DMS SuperNode SE (SNSE) XA-Core (XAC).

Each procedure contains the following sections:

- Application
- Interval
- Common procedures
- Action

Please refer to *XA-Core Maintenance Manual*, 297-8991-510 for all detailed recovery procedures.

Extended Architecture Core (XA-Core) highlights

New, scalable XA-Core processor.

The VToA Application employs a Nortel Networks XA-Core computing module.

Based on the PowerPC Reduced Instruction Set Computing (RISC) processor, the XA-Core houses up to 16 processor elements and input/output processors in a multi-processing environment employing an advanced shared memory technology.

Though grounded in the latest computing technology, XA-Core only requires a minimal DMS-100 hardware change before deployment.

Many DMS SuperNode components- examples include the DMS-Bus, the Link Peripheral Processor, and the Enhanced Network (ENET)-are compatible with XA-Core.

The deployment of XA-Core in the DMS-100 system offers the following benefits:

- Reduced cost of ownership
- With simplified "plug-and-play" provisioning of processor elements, input/output processors, and memory, this processor enables the network provider to make incremental capacity adjustments easily and cost-effectively.
- A fully provisioned XA-Core is projected to have six times the capacity of a DMS SuperNode Series 70 processor-with dynamic load balancing between all processor elements.
- The life cycle of XA-Core components is significantly extended over the current single-processor architecture. Instead of completing an upgrade by replacing the entire processor set, new XA-Core components can be simply added alongside existing investments.
- With the XA-Core, spare processors can be used to share the call-processing load as well as for "hot" backup. Instead of remaining in standby mode, these spares actively participate in the switch's processing to broaden reliability and supplement capacity during short-term overload situations. The system's enhanced reliability and performance can translate into tangible subscriber satisfaction benefits.
- Auto provisioning of new processor elements, enhanced fault detection and isolation, simpler extraction of failed cards, and LED activity indicators are some of XA-Core's enhancements to operations, maintenance, and administration (OA&M). These enhancements can contribute to significant savings in craftsperson time spent on maintenance activities.
- Versatility-The new core's inherent flexibility opens new market opportunities for the service provider. XA-Core can serve as a platform to boost capacity for high-end offices hosting large line sizes or feature-rich services such as Advanced Intelligent Network and National ISDN-2.
- DMS SuperNode system compatibility- Existing components developed for the DMS SuperNode and DMS SuperNode SE systems-such as the Message Switch (MS), Enhanced Network (ENET), and Link Peripheral Processor (LPP) continue in service with XA-Core, thereby minimizing the cost of the transition to the new front end.
- Abundant processing capacity-With six times the capacity of any previous DMS processor, XA-Core can help make real time concerns a thing of the past as we enter the next century. In addition, dynamic call processing distribution and a 2-gigabyte addressable memory range expand call processing capacity and speed, and favorably enhance life cycle costs.

Table 4-34 — NA011/012 minimum configurations for CPU memory

SN	Baseline is either SN50 with Mixed Memory or SN60
SNSE	SN60
SN70EM	Media Point > 70K lines
	High Point > 45K lines
XA-Core	High Capacity Offices
Wireless	SN60 min.

Table 4-35 — NA012/013 minimum configurations for CPU memory

SN	Baseline is SN60
SNSE	SN60
SN70EM	Media Point > 70K lines
	High Point > 45K lines
XA-Core	High Capacity Offices
Wireless	SN60 min.

Non-Feature H/W Program XA-Core NTLX01CA Availability was NA012.

Figure 4-70 — DMS Core evolution
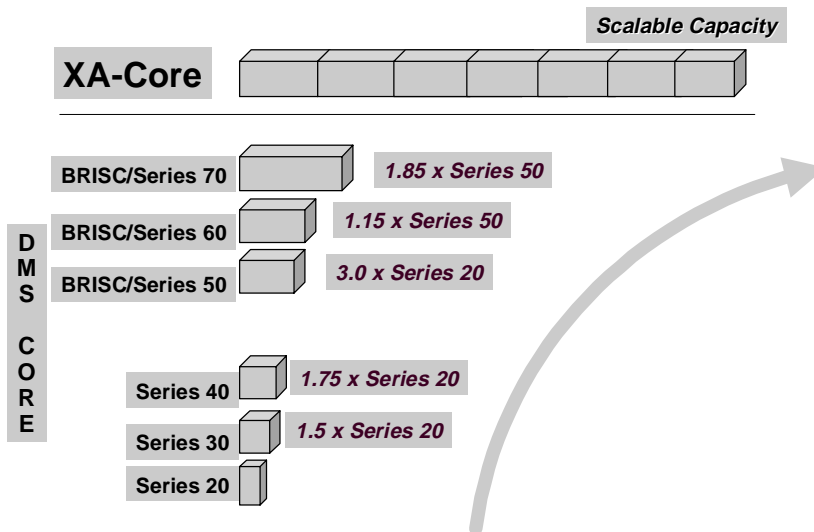
XA-Core features

- Scalable Capacity based on multi-processing
- Plug-in processors, memory, and I/O port cards
- Initially provides 2.3 times the capacity of SN70EM
    —3 active processors and 1 hot spare
    —768 MB of memory
- Initial use in large End Offices and Tandem switches
- Direct replacement for Computing Module
- Robust reliability through:
    —Fault detection and recovery
    —Built-in self-test and diagnostics
    —Auto identify, auto configure, auto test
- Future capability for 6 times capacity of SN70EM

Shared-Memory Parallel-Processing Machine

Independently Scalable Sub-Systems

- Processor Element (PE)
    — Power PC604EV
    — Duplicated per PE for fault detection
    — 256MB on-board memory for Program Store
    — Scaleable Real-time - in-service addition of PEs
    — Scaleable Reliability - 'n+m' reliability

- Shared Memory (SM)
    — Shared Data Store, Master Copy of Program Store
    — Duplex memory; independently mated 32MB blocks
    — Hot spare for reliability
    — 128MByte granularity; 1728MByte capacity

- Input/Output Processors
    — Common Host I/O Processors (IOP)
    — Individual personality 'Packlets' - 2 per IOP
        OC-3 / ATM MS Links
        RTIFs (RS-232)
        Provisionable mass storage devices: >= 4 GB Disks;   1.3 - 4 GB DAT
    — Fault Tolerant File System

Performance and reliability features

- Dynamic load balancing and fault recovery mechanisms
- Simplified upgrade process
- Enhanced data security (FTFS)
- Memory sparing level of "n+2" per side
- Simplified maintenance procedures: plug in PEs, hot insertion and removal of circuit packs, LED status indicators, improved fault detection and isolation

NA013 will support upgrades from SN60

XA-Core reference documents

- *XA-Core Reference Manual*, 297-8991-810
- *XA-Core Maintenance Manual*, 297-8991-510
- *DMS SuperNode and SuperNode SE XA-Core Maintenance Guide*, 297-8991-511
- *Digital Switching Systems DMS-100 Family Maintenance Managers Morning Report*, 297-1001-535
- *DMS Family Commands Reference Manual*, 297-1001-822
- *Switch Performance Monitoring System Application Guide*, 297-1001-330

SPM Overview and Maintenance

SPM overview

The DMS-Spectrum Peripheral Module (SPM) is functionally equivalent to a Digital Trunk Controller (DTC) for interswitch trunks. It provides Common Channel Signaling #7 (CCS7) and Per-Trunk Signaling (PTS) speech and data trunks on TR-782 compliant OC3 carriers. Internally, all trunks are treated as DS-0s or as sets of DS-0s.

The SPM is a set of information processing modules that provide telecommunications switches with direct access to optical carrier (OC) networks. The basic mechanical element of the SPM consists of a dual-shelf assembly that is mounted to a common backplane. A shelf assembly contains two identical shelves. Each shelf can contain up to 15 information-processing modules that plug into the backplane. The backplane provides the electrical inter-connection between the modules. The modules contain circuit packs that perform a variety of functions-from supplying electrical power to providing optical connections to a high-speed transport network. SPM modules also provide some call-processing and high-speed carrier capabilities.

The dual-shelf assembly of a basic SPM contains all the components required to represent an element or a node in the optical transport network. Therefore, the basic dual-shelf assembly is referred to as an SPM node. A standard telecommunication equipment frame accommodates two dual-shelf assemblies, which provides two SPM nodes.

The SPM in a telecom network

In a telecommunications (telecom) network, the SPM is positioned between a telecom switch and the optical carrier (OC) network. Telecom switches can be a DMS switch or a GSM wireless switch. The SPM node acts as an interface between a telecom switch and the OC transport network. The OC transport network uses the synchronous optical network (SONET) protocol to transport voice and data traffic to the other telecom switches on the network. The following figure shows the position of SPM nodes in a telecom network.

Using the SPM in a DMS network

The SPM provides a 1 + 1 redundant optical carrier 3 (OC3) trunking interface with integrated echo cancellation (ECAN). The following figure shows the position of SPMs in a DMS switching and transmission network.

Figure 4-71   —   SPMs in a DMS network
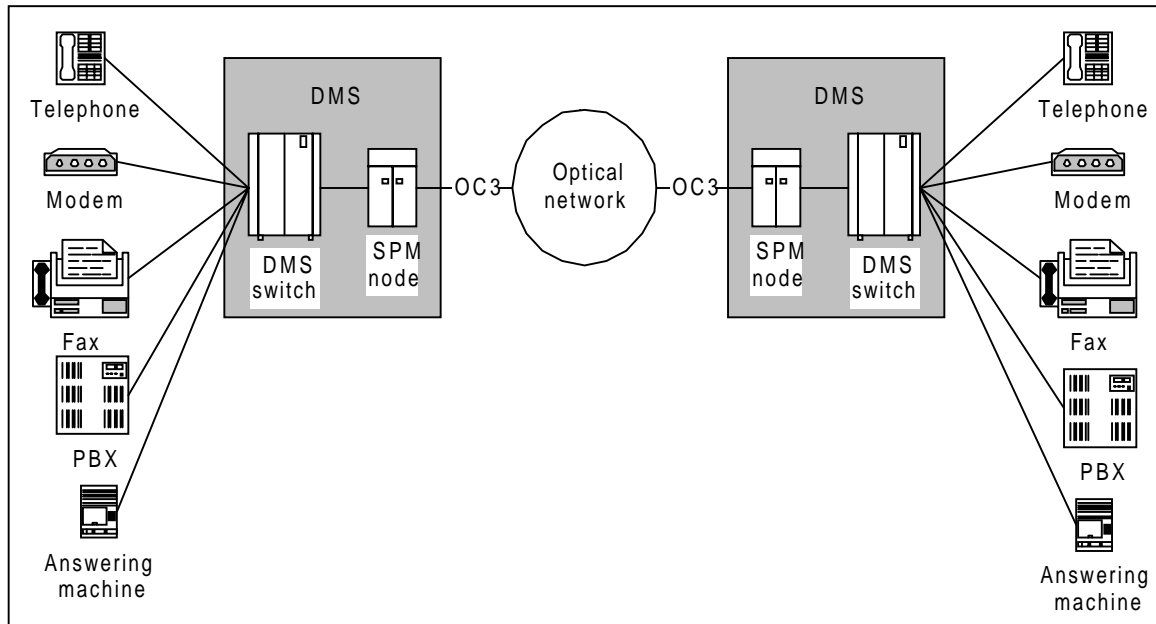
SPM nodes directly terminate an OC3 SONET carrier and feed the individual digital-signal-level-zero (DS-0) traffic from the carrier into the DMS switch.

The SPM system occupies a position in the DMS architecture that is similar to that of the digital trunk controller (DTC) peripheral. However, instead of terminating T1 trunks, an SPM node terminates a pair of 1 + 1 redundant OC3 optical-fiber connections. For example, if a DTC supports 20×24 T1 trunks, an SPM node can replace it and support 84×24 T1 trunks. This represents more than four times as many trunks as a single DTC.

The following figure illustrates both the position of the SPM node and the position of the DTC within the DMS switching architecture.

Figure 4-72 — Architectural Position of SPM node and DTC
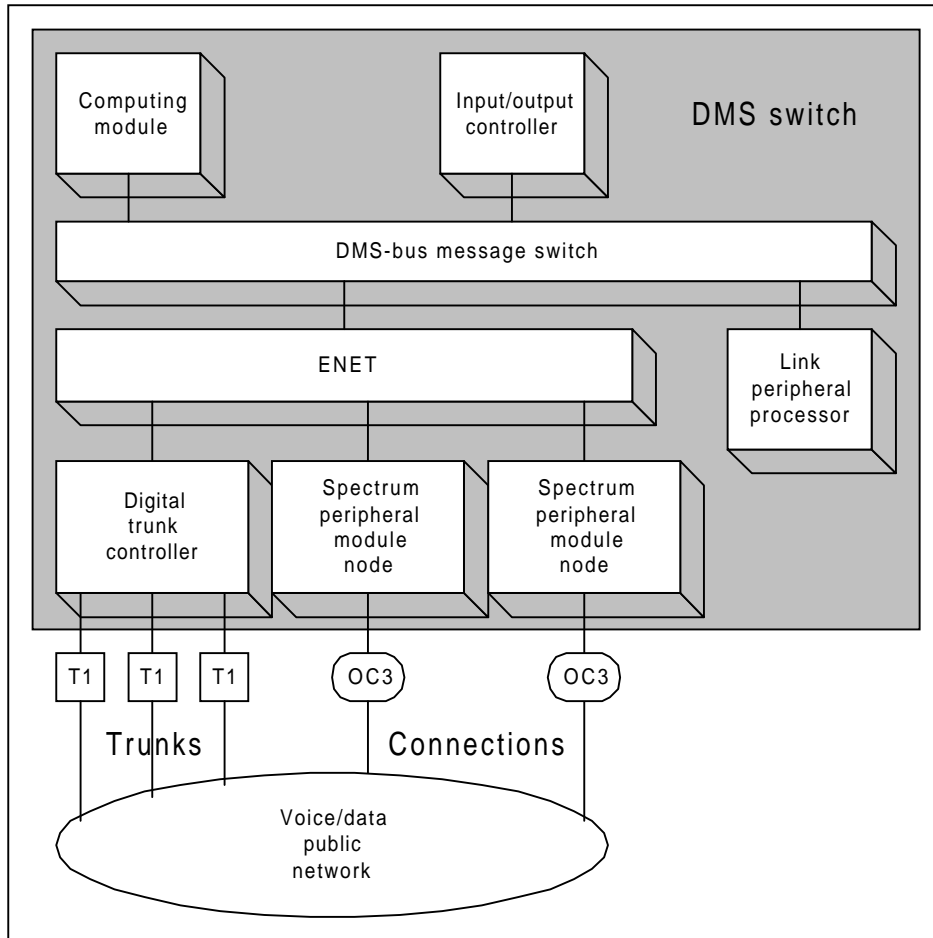
SPM interface to the DMS switch

The OC3 module in the SPM breaks down the incoming OC3 SONET time division multiplex (TDM) signals into their composite DS-0 timeslots. The OC3 module sends the signals to the 12K-port time switch in the SPM common equipment module (CEM). The CEM can route the signals to other digital signal processor (DSP) resource modules (RM) on the SPM shelf for additional processing. The CEM can also route the signals directly to the DMS enhanced network (ENET) for call processing. The signals pass through four DS-512 host links that are supported on the DMS switch by an ENET paddleboard.

The DS-512 links provide the ENET with 2048 channels of bandwidth, which accommodates a full OC3 payload (2016 DS-0 channels) plus the messaging between the SPM node and the DMS computing module (CM). These links provide full communication capability without bandwidth constraints. The following diagram shows the

optical links to the external network, the internal electrical links between the various SPM modules, and External network

Figure 4-73   —   Optical and electrical links
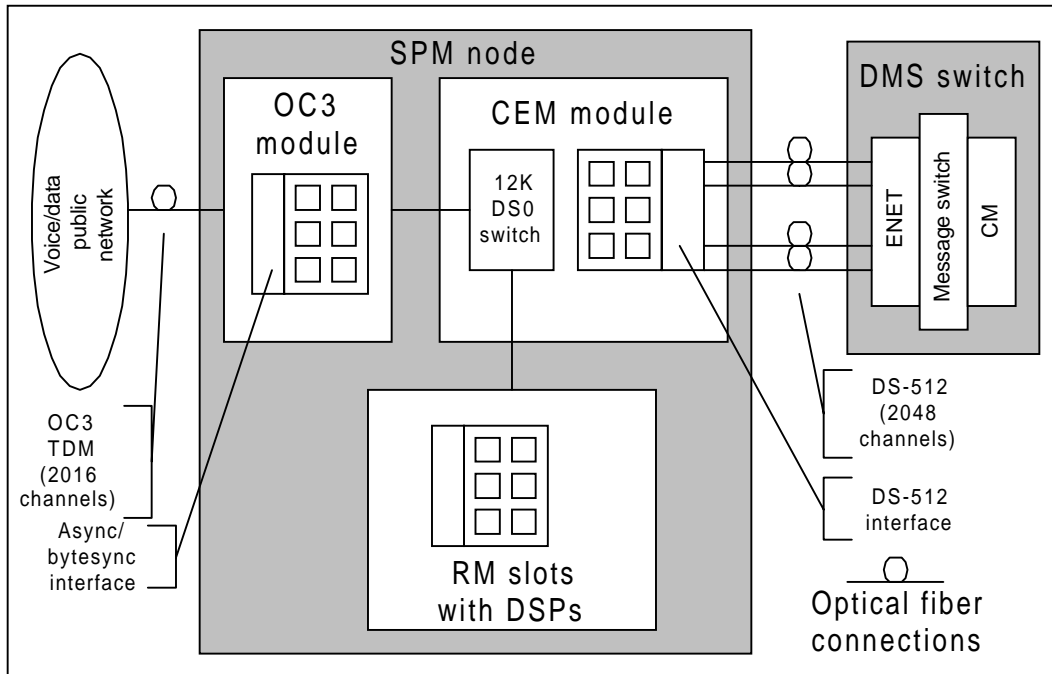
User interface

When SPMs are used with DMS switches, the DMS switch-based operations, administration, maintenance, and provisioning (OAM&P) software is used to control the SPM nodes through the MAP-terminal interface. Refer to the *DMS-Spectrum Peripheral Module Commands Reference Manual,* 297-1771-819 for detailed information about the SPM commands that are available at the MAP-terminal user interface.

OM reporting for ISUPUSAG

For SPM01 and SP10, operational measurement (OM) reporting for ISUPUSAG was done when the OM registers reached full capacity.

For SP11, OM reports containing the ISUPUSAG OM group data are sent at fifteen-minute intervals to the computing module. The OM reports are sent whether or not the OM registers are full. The availability of a scheduling mechanism for use within the SPM OM software matches the ISUP OM reporting provided by the digital trunk controller for SS7 (DTC7).

Visual alarm indicators

The DMS-Spectrum Peripheral Module (SPM) frames and modules have visual alarm indicators, which are connected to the DMS aisle alarm indicators.

MAP terminal

The MAP terminal displays the following alarm.

Figure 4-74   —   MAP display
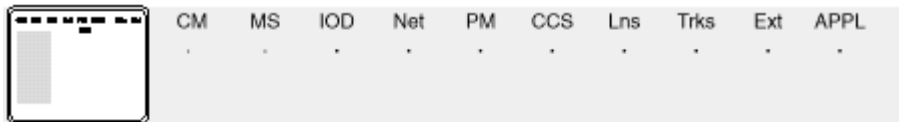
If an alarm is reportable and a higher level alarm does not mask it, the alarm indicator appears under the peripheral module (PM) category of the alarm banner on the MAP terminal.

Alarm indicators consist of two lines that include the following elements:

- **xxyyy**
- **zzz**

xx represents the number of the SPM unit with at least one alarm of the same severity

yyy represents the type of device, which is always SPM for SPM units

zzz represents one of the following severity codes

Table 4-36   —   DMS Alarm codes

Severity codes	Alarm level
C	critical alarm
M	major alarm
<blank>	minor alarm or no alarm

A higher level alarm masks all levels below it. For example, a critical (*C*) alarm masks both major (M) and minor ( ) alarms. If lower level alarms are present, they are reported in a log. When there are no alarms, a dot (·) appears in the device field (xxyyy).

List command

You can display a list of the alarms at all levels using the LISTALM command.

Logs

Each reportable alarm generates a log containing information about the alarm.

SPM alarm classifications

There are three different causes of SPM alarms, and these alarms are reported by various devices. These devices can be part of the SPM or part of the DMS alarm reporting system.

The following can cause SPM alarms:

- device failures
- network events
- threshold crossings

The following can report SPM alarms:

- an SPM network node
- individual SPM modules
- the DMS computing module (CM), which reports alarms for:
    — input/output devices (IOD)
    — common channel signaling (CCS)
    — trunks (TRKS)
    — carriers (CARR)

Device failures

Physical devices generate alarms when a detectable failure occurs. SYSBNA is an example of this type of alarm.

Network events

Various sources generate network-event alarms when monitored events occur on the network. AIS and LOS are examples of this type of alarm.

Threshold crossings

Alarms generate when monitored parameters or metered parameters exceed their datafilled settings. SPM devices or network events, or both, can cause these alarms. COTLOW and VCXO70 are examples of these types of alarms.

SPM network node

An SPM node consists of all the modules on shelves 0 and 1, which connect to the OC-3 network through the OC-3 modules in slot 9 and slot 10 on shelf 0.

SPM modules

The following SPM modules can generate alarms:

- common equipment module (CEM)
- OC-3 interface module (OC-3)

- ATM interface module (ATM)
- DLC interface module (DLC)
- digital signal processor (DSP)
- voice signal processor (VSP)

NOTE: Note: The VSP does not apply to all markets.

DMS computing module

SONET carriers can generate alarms at the following DMS computing module (CM) alarm reporting levels:

- trunks (Trks)
- input/output devices (IOD)
- common channel signaling (CSS)

Threshold-crossing alarms

The SPM CEM and the DMS CM can generate threshold-crossing alarms. Threshold-crossing alarms are one of the following types:

- steady-state faults
- performance parameters
- metered-performance parameters

You can enter high-threshold and low-threshold values for the various alarms in DMS data schema tables. Refer to the Data Schema Reference Manual or the data schema section of the Translation Guide, as appropriate. Alarms generate when the high-value threshold is crossed and they clear when the low-value threshold is crossed. See the alarm descriptions for the appropriate data schema table references.

Steady state faults

Steady state faults, or soaked defects, occur when a performance parameter crosses an upper threshold and remains above the lower threshold value for an extended period. AIS and RFI are examples of steady-state fault alarms.

Performance parameters

Performance parameters are counts of intermittent defects. Alarms generate when counts exceed threshold values. Performance parameters are collected over 15-minute periods and 1-day periods. Performance parameter counts are reset when collection periods end. CV and ES are examples of performance parameter alarms.

Metered performance parameters

Metered performance parameters are physical measurements. Alarms generate when a measured value exceeds its benchmark setting by the datafilled percentage. Bench-

mark settings can be reset. LBR and OPT are examples of metered performance parameter alarms.

Significance of alarm indicators

Alarm indicators are LEDs that appear at the top of each frame and at the top of the faceplate on each SPM module. All modules have a red and a green module-status indicator. Modules with external connections on the faceplate also have an additional amber signal-status indicator, which indicates the status of the external connections.

See the following tables for information about the significance of individual alarm indicators and alarm indicator combinations.

Table 4-37   —   Module

| Module-condition LED combinations | | |
Green	Red	Indication and action
Off	Off	Green LEDs are in sleep mode (module can also be not powered or not seated). When all LEDs are off, there are no critical faults and an indicator test is not underway. Use an indicator test to check LED function.
On	On	A power on self test (POST) or an LED indicator test is underway. During a POST, the LEDs are controlled by the initial boot loader (IBL) software. If both LEDs remain on for an extended period after a POST, the module is defective. For detailed instructions for replacement, see the appropriate Card Replacement Procedures.
On	Off	Normal operation—there are no critical faults and no action is required. Do not remove a module displaying this alarm-indicator combination.
Off	On	Critical fault—replace the module.

NOTE: To prolong LED life, program the green LEDs so it can enter the sleep mode. LED sleep-mode timing is controlled by the entry in field LEDTIMER in data schema table MNNODE. Sleep mode does not apply to red LEDs

Table 4-38   —   External

| External signal-status LEDs | |
Amber	Indication
Off	Normal operation—all external signal inputs to the module faceplate are valid.

External signal-status LEDs	
Amber	Indication
On	At least one external signal source entering the module faceplate is not carrying a valid signal.

NOTE: Sleep mode does not apply to amber LEDs.

NOTE: Note: Alarm indicators do not indicate maintenance states (such as manual busy, in service, or in service trouble) or activity states (active or inactive).

SPM alarms

The following tables list the alarms for the SPM and indicate the resource or control parameter generating the alarm.

Table 4-39 — Alarms appearing under the CCS banner

Source device or parameter										
Alarm Name	SPM Node	CEM	OC-3	DSP	VSP	ATM	DLC	DMS TRKS	CARR METER	CARR PERF
LBC								X	X	
OPT								X	X	
OPR								X	X	

Table 4-40 — Alarms appearing under the IOD banner

Source device or parameter										
Alarm Name	SPM Node	CEM	OC-3	DSP	VSP	ATM	DLC	DMS TRKS	CARR METER	CARR PERF
CSS										X
CV										X
CVFE										X
ES										X
ESFE										X
SEFS										X
SES										X
SESFE										X
UAS										X
UASFE										X

Table 4-41 — Alarms appearing under the PM banner

Source device or parameter										
Alarm Name	SPM Node	CEM	OC-3	DSP	VSP	ATM	DLC	DMS TRKS	CARR METER	CARR PERF
CLKOOS		X								
COTLOW	X									
DTMFLOW	X									
ECANLOW	X									
HLDOVR		X								
HLDOVR24		X								
MANB	X	X	X	X	X	X	X			
MANBNA	X	X	X	X	X	X	X			
MFLOW	X									
ISTB	X	X				X	X			
NOSPARE			X	X	X	X	X			
PROTFAIL			X	X	X	X	X			
SYSB	X	X	X	X	X	X	X			
SYSBNA	X	X	X	X	X	X	X			
TONESLOW	X									
VCXO70		X								
VCXO90		X								

Table 4-42 — Alarms appearing under the TRKS banner

Source device or parameter										
Alarm Name	SPM Node	CEM	OC-3	DSP	VSP	ATM	DLC	DMS TRKS	CARR METER	CARR PERF
AIS										
BERSD										
BERSF										
LOF										
LOP										
LOS										
RAI										
RFI										

NOTE: There are no SPM alarms appearing under the TRKS banner.

Software upgrade support

The telecommunications switch component of the SPM software (that is, the DMS switch) is upgraded using the standard DMS one night process (ONP). RM software loads are upgraded before the CEM load. CEM flash memories can be upgraded while in service, which minimizes the time spent in simplex mode. The new load can be moved from flash memory to random access memory by using a command at the DMS MAP terminal. For more information on how to upgrade the SPM, refer to *North American DMS-100 Spectrum Peripheral Module Release Document,* 297-1771-598.

The SPM is the first integrated direct optical interface to a switching system. It is a protected OC-3 interface that provides significant savings in floor space, cross-connects, power, and cabling. The SPM is an evolvable, new trunking peripheral supporting the high volume, high growth trunk types with both PTS and ISUP signaling.

- SPM supports the trunking growth of today's DMS-100/200
  - ISUP and PTS trunks for inter-office and tandem connection
  - IT, TI, TO, T2
  - IBNTI, IBNTO, IBNT2
  - ATC
  - Additional PTS trunks supported
  - PX, OC, ES, SC, CELL
  - Call processing services
  - Alerting, Treatments & announcements, digit collection
  - Basic service support
  - DISA, COT, Glare, Vacant Handling, Blocking, Call Back Queuing, Feature Group D, CAMA/SuperCAMA, DID
  - Access interactions
  - CLASS, Meridian Message Service, Centrex, AIN
- Full interworking with existing DTCs
  - SPM can be added to existing DTC offices to support growth needs
  - Trunk groups can be spread across DTCs and SPMs
- The SPM is a fully integrated DMS-100/200 peripheral.
- In general the same OAM&P interfaces, e.g. Table Editor, MAP, & Log System, are used for SPM as XPM.
- There are some differences because of the transmission nature of SPM OC-3. i.e. carrier maintenance and performance monitoring.
- Alarms provided for SPM node, CEM, and each type of RM.

- One new OM group (DSPRMAN), no changes to existing OM's. Existing OM's Reused OMs for OC3 carrier mtce replaced by Nodal performance monitoring Data.
- New Logs added, and two changes to existing Logs.

SPM Key Values

The first Integrated Optical Interface

- Footprint
    — 4032 Trunks in one frame
    — Integrated EC / Eliminates Muxs, X-Connects,
    — Up to 6.5X Reduction
    — Back-to-back /against wall deployment
- Cost of Ownership
    — 21X Cable Termination Reduction
    — Up to 11 times power savings
    — Reduced Sparing costs
    — Lower Engineering, Installation, Commissioning Costs
    — Lower Total Costs (incl Mux / XC / EC)
    — I/F enables in-house & 3rd party development
- Reliability
    — Hot Insertion / Extraction
    — Elimination of Points of Failure
    — Redundant 1+1 OC-3 Optical I/F
    — Lower Bit Rate Error Rates
    — No optical / electric conversion

SPM Applications

NA010

- Initial Market introduction
- OC-3 ISUP/PTSInterface for LEC
- Allows 112K Trunks on DMS (DTC and SPM mix)

NA011

- Support of Large System (56 SPMs)
- 112K Trunk capabilities on DMS

4-388 System Products

NA012

- NI-2 PRI on SPM

SPM Program Rollout

NA10/SP10

- Initial Market Introduction
- OC-3 ISUP/PTS interface for LEC (external routing)
- OSMINE/TIRKS Process Support
- CLEA Support

NA11/SP11

- Load File Comp/Decompression
- Test activity for Large System Support (up to 56 SPM's)
- ISDD OM's
- Log Transport (additional Logs)
- Query PM Fault
- PERFMON Clear All
- Scheduled OM's
- PANTHER Support (milestone loads)

NA12/SP12

- NI-2 PRI on SPM (new CP)
- Single Shelf ENET support
- Panther Support (all load types)

NA13/SP13

- Internal Routing
- Black box fraud prevention for PTS
- Reach through Surveillance
- SPM Patching
- OSS7 on IT trunks for TOPS
- NTNA ISP PRI on SPM

Related NTPs

Refer to the following documents for more information about SPM:

- *Spectrum Peripheral Module General Description*, 297-1771-130.

297-8991-500   Standard 04.02   March 2001

- *DMS-Spectrum Peripheral Module Feature Description Reference Manual*, 297-1771-330
- *Spectrum Peripheral Module Hardware Maintenance Reference Manual*, 297-1771-550
- *Spectrum Peripheral Module Maintenance Manual*, 297-1771-551
- *Spectrum Peripheral Module Commands Reference Manual*, 297-1771-819
- *Hardware Description Manual*, 297-8991-805
- SPM information is also included in the following NTPs:
  — Trouble Locating and Clearing Procedures
  — Alarm Clearing Procedures
  — Recovery Procedures
  — Routine Maintenance Procedures
  — Card Replacement Procedures
  — Operational Measurements
  — Data Schema
  — Logs

SPM capabilities

The SPM can be equipped with various types of modules to provide a variety of capabilities. Each module contains application specific integrated circuits (ASIC) and other components designed to provide specific capabilities.

SPMs provide:

- OC3 interfaces with SONET transport networks
- signal processing
- routine call processing in conjunction with telecom switches like the DMS switch
- replacements for, or adjuncts to, DMS digital trunk controllers (DTC) and ISDN digital trunk controllers (DTCI)
- call processing for ISUP and per trunk signaling (PTS)
- echo canceling (ECAN) with redundancy features
- an open module-interface that supports integrated modules from licensed third party developers, such as Tellabs and Coherent
- tone-generation and reception, and ISUP continuity-test (COT) testing

IOM Overview and Maintenance

IOM Functional description

The IOM user interface provides access to commands that allow operating company personnel to use IODs to enter machine controls, perform tests, and request information.

Maintenance and administrative IODs are in the integrated services module (ISM) shelf. The following sections describe the IOM and the associated IODs. The following sections also describe the ISM shelf, integrated services module (ISME) frame, and integrated services module (CISM) cabinet.

ISM shelf

The ISM is a single shelf unit that replaces the current trunk module (TM) shelf or the maintenance trunk module (MTM) shelf. The ISM shelf is on the cabinetized metallic ISM (CISM), the frame ISM (FISM), or cabinetized metallic test access (CMTA). The CISM, FISM and CMTA contain a maximum of four ISM shelves. The ISM shelf has the same functionality as current TM/MTM shelves. See *Hardware Description Manual*, 297-8xxx-805 for a complete description of the ISM shelf.

ISME frame

The ISME frame is a standard DMS frame that supports a maximum of four ISM shelves. The modular supervisory panel (MSP) provides power, and control for the frame hardware.

CISM cabinet

The CISM cabinet is a standard DMS cabinet that supports a maximum of four ISM shelves and a cooling unit shelf. The modular supervisory panel (MSP) provides power and control for the frame hardware.

IOM

The input/output module (IOM) is a direct replacement for the IOC shelf. The IOM provides all the functionality of the current IOC cards, with the exception of the NT6X91. The IOM with a digital audio tape (DAT) and a disk drive unit (DDU)

replace the IOC and magnetic tape drive (MTD). The IOM occupies three shelf slots. If a DAT is not required, the IOM controller cards provide 9-track MTD support.

The IOM supports all peripheral equipment that a completely provisioned IOC shelf supports.

The main IOM controller card (NTFX30) is in slots 3 or 4 of the integrated services module (ISM). This card has all the communication ports and

controller circuits for the storage media card. Together, the controller card and the storage media card provide all the communications and storage functions of a completely provisioned IOC shelf.

The storage media card (NTFX32AA) occupies slot 4 of the ISM shelf. The card has plug-in DAT (NTFX32CA) and DDU (NTFX32BA) units. The plug-in design gives maximum flexibility. The plug-in design does not require card replacement for upgrades and repairs. The NTFX31AA paddleboard mounted on the rear of the backplane supplies power to the IOM smart connectors. The backplane supplies power to the NTFX32AA card directly.

The main controller card provides the interface between the IOM and the IODs. The card has 20 DS-30 communication ports. Sixteen ports are general purpose input/output ports. The ports provide RS-232C, V.35, current loop or PERTEC interfaces with a smart connector at the end of the cable for the protocol conversion. Communication with the message switch (MS) requires two DS-30 ports. The remaining ports are not used.

Smart connectors have a 6-pin teledapt connector on the IOM side and a 25-pin connector on the user side. The PERTEC interface connects to the IOM through a 6-pin D-type connector on the IOM side. The interface also connects to the IOM through a 50-pin connector on the user side. The PERTEC conversion box is on the MTD in a vertical position. The cables from the box connect to the MTD or DPP.

The IOM controller card (NTFX34AA) has the option of setting the clock to internal or external. The option is only available when NTFX34AA is used as an MPC RS232 port. For other synchronous configurations, the smart connector expects clock from the modem or external devices.

In external clocking modes with NTFX34AA, NTFX35AA or NTFX35BA, the smart connector expects the external device to provide the receive clock and the transmit clock to be from the same source. The receive clock and the transmit lock should also be with the same frequency and locked in phase. The same frequency and locked in phase forces the user to set the same baud rate for both transmission and reception and disallows the use of modems that have limited clocking features with IOM. This is not in alignment with the IOC operation, and the solution is to replace the modem with another modem.

IOM subsystem components

The IOM controller card (NTFX30AA) and the associated paddleboard (NTFX31AA) are the main components of the IOM. The following sections describe the IOM cards.

IOM controller card (NTFX30)

The IOM controller card (NTFX30) contains hardware and firmware to support 16 general-purpose ports. The ports include the RS-232C, V.35, current loop and PERTEC. The hardware and firmware also support two DS-30 links to the message switch (MS) and two optional external SCSI devices on the storage media card. The NTFX30 controls the entire operation of the IOM.

IOM paddleboard (NTFX31)

The IOM paddleboard (NTFX31) contains the power feed circuits. The paddleboard contains a maximum of 16 smart connectors and circuits. The paddleboard implements a local loopback for diagnostic purposes. The paddleboard is at the rear of the backplane at the slot 3 position. The paddleboard has 20 connectors. Sixteen connectors supply power and the signal to the smart connector at the end of the cable. The four connectors that remain do not have power. Two of the connectors have connections to the MS and the last two are not used

IOM storage media card (NTFX32)

The IOM storage media card (NTFX32) is an optional unit for the IOM. The media card holds the 3.5 in. DDU (NTFX32BA) or DAT (NTFX32CA) units. With these units installed, the media card is functionally equivalent to the IOC DDU and/or nine-track MTD. You can use the media card in all applications that require a DDU and/or nine-track MTD.

Disk drive unit (DDU)

The IOM 3.5-in. DDU (NTFX32BA) has a capacity of 2-GByte. The DDU performs the same function as the current IOC SCSI DDU. The disk drive unit is on the IOM storage media card. The DDU is based on the industry standard small computer systems interface (SCSI).

Digital audio tape unit (DAT)

The DAT unit (NTFX32CA) has a capacity of 1.3-GBytes (not compressed). The DAT unit performs the same function as the IOC MTD. The DAT unit is on the IOM storage media card.

Bulkhead splitter unit (NTFX39)

The bulkhead splitter unit (NTFX39) is a one-to-nine cable splitter unit for the cabinetized ISM.

Fault conditions (IOC and IOM)

Fault conditions in the IOC or IOM are caused by product defects, or product failures during operation.

The IOM uses the same alarm indications as the IOC. The alarm clearing procedures for the IOM are different than the procedures for the IOC. The following sections explain the IOC and IOM level fault conditions.

Babbling device

The babbling device fault occurs when a device sends an excessive quantity of input/output (I/O) interrupt messages to the message switch (MS). This condition is referred to as babbling. The MS detects the babbling device when the quantity of I/O interrupt messages exceeds the threshold. When babbling starts, the babbling remains until maintenance actions correct it. The babbling device thresholds are set at low, medium, and critical. Removal of the IOD from service occurs for medium or critical levels. Refer to NTP 297-1001-590, *DMS-100 Family Input/Output Devices Maintenance Guide* section "IOD-related user interface commands" for additional information on babbling device thresholds.

CKEr

A circuit error (CKEr) fault occurs when one or more I/O or IOM devices disconnects at the IOC end of the link to the IOC or IOM.

CkOS

For IOC, the CkOS (circuit out-of-service) fault occurs when there is a problem with the terminal controller card (NT1X67). When the CkOS fault condition occurs there is no service to devices connected to the NT1X67 card.

For IOM, the CkOS fault occurs when a controller port is out-of-service. When a controller port is out-of-service, there is no service to devices connected to the NT1X67 card.

DDUOS

For IOC, the DDUOS (disk drive unit out-of-service) fault occurs when there is a problem in the disk drive controller card (NT1X55).

For IOM, the DDUOS fault occurs when one or more of the DDUs are out-of-service.

If the DDUOS fault occurs, you cannot record or download files to or from tape or the DDU.

IOCOS

For IOC, a problem in one of the IOC processor cards causes the IOCOS (input/output controller out-of-service) fault condition. The IOC processor cards are the I/O message processor card (NT1X62) or I/O terminator card (NT0X67).

For IOM, a problem in the IOM controller card (NTFX30) causes the IOCOS fault condition.

When the IOCOS fault condition occurs, all devices associated with the out-of-service IOC lose communication with the DMS-100 switch.

MPCOS

For IOC, the multiprotocol controller out-of-service (MPCOS) fault occurs when there is a problem in one or more multiprotocol controller cards (NT1X89). Remote terminals lose access to the DMS-100 switch for any affected cards.

For IOM, the MPCOS fault occurs when there is a problem with one or more multiprotocol ports. Remote terminals lose access to the DMS-100 switch for any affected ports.

MTDOS

For IOC, the MTDOS (magnetic tape drive out-of-service) fault condition occurs when there is a problem in the magnetic controller card (NT9X68).

If the Device Independent Recording Package (DIRP) utility uses the MTD to record billing data, loss of billing data occurs. If the DIRP utility does not use the MTD, you cannot download or record files to or from tape.

For IOM, the MTDOS or DATOS (digital audio tape out-of-service) fault condition occurs when there is a problem in one or more magnetic tape drives or digital audio tapes. If the DIRP utility uses the MTD or DAT to record billing data, loss of billing data occurs. If the DIRP utility does not use MTD or DAT, you cannot download or record files to or from tape.

Automatic maintenance

The system performs self-diagnostics. The system isolates and tests an IOD component that has faults. The system attempts to return the component that has faults to service, based on the results of the self-diagnostics.

Manual maintenance

When the system cannot clear an alarm, perform manual actions to clear the alarm. Perform manual maintenance on a periodic schedule according to local operating company policy.

WARNING Reformatting IOC/IOM-based disk drives can cause loss of billing, loss of service, or service degradation. For details regarding this procedure please refer to *Input/Output Devices Maintenance Guide*, 297-1001-590 (This manual contains the advanced maintenance procedures for DMS-100 input/output devices (IOD)).

Scheduling magnetic tape drive maintenance

Set up a routine maintenance schedule according to the information in the manuals supplied with the Hewlett Packard or Cooke magnetic tape drive. Perform the 1000 hour maintenance routine, described in the Hewlett Packard manual. Perform the routine every 3 months for the MTDs you used to record automatic message accounting (AMA) or call detail recording (CDR) data.

Scheduling digital audio tape (DAT) drives

Set up a routine maintenance schedule according to the number of digital data storage (DDS) cartridges used each day.

IOD-related logs

Logs are one of the primary resources used to monitor input/output controller (IOC) components in the input/output device (IOD) subsystem. Some logs help to isolate a problem to a single component. Other logs help to detect link problems. In addition to IOD logs, this document addresses the following logs that associate with the IOC and input/output module (IOM) subsystems:

- disk drive unit (DDU)
- multiprotocol converter (MPC)
- magnetic tape drive (MTD)

The tables in NTP 297-1001-590, *DMS-100 Family Input/Output Devices Maintenance Guide* describe IOD-related logs. Refer to the *Log Report Reference Manual* for details. For alarm and fault clearing procedures included in the tables, refer to the following IOD documents:

- Alarm and Performance Monitoring Procedures
- Trouble Locating and Clearing Procedures
- Routine Maintenance Procedures
- Card Replacement Procedures

IOD-related operational measurements

Operational measurements (OM) provide information on the performance of the DMS switch and the peripheral components of the DMS switch. The OM system controls collection, display, and generation of OM data for the operating company. The OM groups that associate with the input/output device (IOD) subsystem are IOC, IOSYS, and IOSYSERR.

The OM system does not create OM data. The OM system acquires OM data from DMS hardware and software sources. The system provides performance indicators for each part of the DMS switch. The OM group IOC monitors IOC and IOM perfor-

mance and maintenance. Each IOC provides an interface in one of the following areas:

- between an IOD and the message switch (MS) of a DMS SuperNode
- between an IOD and the central message controller (CMC) of an NT40 switch

OM group IOC

The OM group IOC supplies data to monitor IOD, IOC and IOM performance. Peg registers in this OM group count the following:

- IOC and IOM errors and faults
- device errors on peripheral-side (P-side) links
- system busy and manual busy links
- system busy and manual busy IOCs and IOMs

For a description of the registers in OM group IOC and the subsystems, please refer to NTP 297-1001-590, *DMS-100 Family Input/Output Devices Maintenance Guide*. For additional information on IOD related OMs, refer to the *Operational Measurements Reference Manual*. For additional information on logs, refer to the *Log Report Reference Manual*.

IOD level MAP display

The IOD MAP level provides access to IOD commands, IOD sublevels, and IOD status information. The IOD MAP display identifies IOD subsystems and indicates IOD subsystem states.

For IOM, the header IOC identifies 16 DS-30 ports for IO devices and two (optional) small computer systems interface (SCSI) devices. The devices use a maximum of 18 ports. The header STAT identifies the state of each port. To display the state of the devices that connect to the IOM, enter the LISTDEV command.

IOM level MAP display

If an IOM is provisioned, the IOC status display at the IOD level changes to an IOM status display. The display for IOM includes the state of the following:

- each port (numbered from 0 to 17) on each IOC device
- the type of each device on the IOM controller in the integrated services module (ISM) shelf

Refer to Figure 4-75 on page 4-397 for an example of an IOM level MAP display.

IOC and IOM maintenance states

One of the following activities can cause each IOC or IOM to have an assigned maintenance state:

- the system automatically assigns a maintenance state to each IOC or IOM
- you manually assign a maintenance state to each IOC or IOM from the MAP terminal

Each IOC or IOM state has a code that appears in the IOC or IOM status display. Table 4-43 describes IOC and IOM states, and mnemonic codes for each state.

Figure 4-75 — IOM level MAP display

```
  CM    MS    IOD    Net   PM    CCS   Lns    Trks    Ext    APPL
CM Flt  .   SMDR B   .   1RCC    .    .   *** CC 2 Maj   .
  M         *C*          *C*               *C*      M
IOC         IOD
 0 Quit     IOC  0 1 2 3
 2          STAT . . . .
 3
 4 ListDev_ DIRP: SMDR B  XFER: . SLM : . NOP : . NX25: .
 5          MLP :  .      DPPP: . DPPU: . SCAI: .
 6 Tst_
 7 Bsy_     IOC    PORT 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
 8 RTS_     (IOM) STAT . . . - . . - - - . - - - - - - - .  .
 9 Offl_     0    TYPE C C C   C M       M                    S  S
10 _IOC             O O O   O T       P                    C  C
11                  N N N   N D       C                       S  S
12
13
14 Trnsl
15
16 QIOM
17 Downld_
18 Port_
  ASIU
Time 12:58 >
```

Table 4-43 — IOC and IOM status codes

Code	Description
	The IOC or IOM is in service, and has no defects.
–	The IOC or IOM is unequipped.
C	All CM ports that connect to the IOC or IOM are out of service. The IOC or IOM is central-side (C-side) busy.
L	A minimum of one IOD link that connects to the IOC or IOM is out of service. These links include the following: terminals or consoles (CONS)— nCkOS magnetic tape drives (MTD) or digital audio units (DAT) — nMTDOS disk drive units (DDU)— nDDUOS
M	The complete IOC or IOM is manual busy.

Table 4-43 — IOC and IOM status codes

Code	Description
O	The complete IOC or IOM is offline.
S	The complete IOC or IOM is system busy.
N	Only base load runs on IOM.
Ld	Downloading or reprogramming is in progress.

Refer to NTP 297-1001-590, *DMS-100 Family Input/Output Devices Maintenance Guide* for a description of commands and MAP displays for the IOD, IOC, and IOM levels and their subsystems.

IOD-related card requirements

Description of card replacement procedures

Card replacement procedures can be stand-alone procedures or can be part of another maintenance procedure such as an alarm clearing procedure.

"IOD circuit card replacement" in the "IOD-related card requirements" section of *DMS-100 Family Input/Output Devices Maintenance Guide,* 297-1001-590 lists card replacement procedures for the input/output controller (IOC) shelf and the input/output module (IOM) in the integrated systems module (ISM) shelf.

Replacement procedures for DDU, MTD, and DAT

"DDU, MTD, and DAT replacement procedures" in the "IOD-related card requirements" section of *DMS-100 Family Input/Output Devices Maintenance Guide,* 297-1001-590 summarizes the replacement procedures for DDU, MTD, and DAT. The procedures are for the input/output devices (IODs) attached to the IOC or IOM cards listed in "IOD circuit card replacement" in the "IOD-related card requirements" section of *DMS-100 Family Input/Output Devices Maintenance Guide,* 297-1001-590.

Fault isolation and correction

This section describes fault isolation and correction procedures for input/output devices (IOD). The following devices are included in this section:

- an input/output controller (IOC)
- an input/output module controller (IOM) card
- a magnetic tape drive (MTD)
- a console or a terminal (CONS)
- a disk drive unit (DDU)
- a digital audio tape (DAT) drive

Fault isolation and correction procedures

IOD fault isolation and correction are performed at IOD MAP sublevels. These levels are IOC, IOM, Card, MTD and DAT, CONS, and DDU.

Each IOC has a separate MAP display. An IOC MAP display indicates the type of controller cards on an IOC shelf. The IOC MAP display also indicates the state of the equipped ports on each card. To display information for an IOC, include the number of an IOC in each command.

Each IOM has a separate MAP display. An IOM MAP display indicates the type of port on an IOM controller in an ISM shelf. The IOM MAP display also indicates the statue of the equipped ports on the controller.

To display information for an IOC, include the number of the IOC in each command.

An IOM MAP appears only if there is an IOM provisioned.

Fault isolation and correction procedures for IOD are categorized as follows:

- how to locate and clear faults
- fault isolation tests
- diagnostic tests
- product-specific test tools

Locating and clearing faults

Fault conditions for IOD are identified in the following:

- operational measurements (OM)
- log reports
- alarms
- data tables

Testing and isolating IOM cards

A test can fail after you perform standard problem solving procedures and after a system generates a card list. If a test fails, replace the IOM controller card that has faults.

Diagnostic tests

To identify faults, the system performs self-diagnostics. System actions on a IOD component that has faults include isolation and testing of the component. The actions can include an attempt to return the part to service. When system actions do not clear a fault, manual actions are required.

Detailed IOD fault-clearing procedures are included in the following publications:

- Alarm and Performance Monitoring Procedures
- Trouble Locating and Clearing Procedures

- Card Replacement Procedures.

Table 4-44 — Document key numbers

NTP type	Key number
Alarm and Performance Monitoring Procedures	543
Trouble Locating and Clearing Procedures	544
Card Replacement Procedures	547

Fault clearing

Refer to the NTP for information on IOD alarm clearing. Detailed trouble locating and clearing procedures for IODs are included in the Trouble Locating and Clearing Procedures section of that document.

IOM sparing guidelines

The following Table contains the Nortel Networks recommended sparing guidelines for IOM equipment hardware.

Table 4-45 — Recommended spares

Equipment	Quantity
NTFX30AA IOM Controller Card	1 spare
NTFX32BA DDU Plug- in Module	1 spare if provisioned
NTFX32CA DAT Plug- in Module	1 spare if provisioned
NTFX31AA Paddleboard	1 spare
NTFX32AA Storage Media Card	1 spare if provisioned
NTFX40HB SCSI Cable	1 spare if NTFX32 is provisioned
NTFX34AA RS-232 SC	1 spare per 20
NTFX35AA V.35 SC	1 spare per 20
NTFX36AA PERTEC SC	1 spare per 20
NTFX38AA Current Loop SC	1 spare per 20

IOM Documentation

Table 4-46 — Installation Procedures

Module-Method	Title
65-1651	IOM Upgrade
18-5352	IOM cabling for various ISM configurations
24-5638	Commissioning of the IOM
78-5639	IOC to IOM Migration
55-5631	IOC to IOM Replacement

Table 4-47 — IOM User Guides

NTP	Title
297-1001-590	Input/Output Devices Maintenance Guide
297-1001-129	Input/Output System Reference manual

IOM Training

The following table contains a list of courses available through Nortel Networks, at the time this document was written.

Table 4-48 — IOM courses

Course	Subject
1134	Introduction to ISME (Integrated Services Modules) (CBT)
	- IOM Functions and Features
	- IOM Hardware Components
	- IOM Menu level and Port level displays and commands
4004	DMS SuperNode Architecture
7309	DMS SuperNode System Provisioning
4352	Hardware Installation (Extensions)
4353	Hardware Installation (Initials/Extensions)

Please refer to the "Training" section in this document for information about how you may access current information on Nortel Networks Customer Information and Training Services courses.

Hardware elements

Table 4-49 — Key IOM Hardware Elements

PEC	Description
NTFX30AA	IOM Main Controller Card
NTFX31AA	IOM Paddleboard Assembly
NTFX32AA	IOM Storage Media Card
NTFX32BA	DDU Plug-in Unit
NTFX32CA	DAT Plug-in Unit
NTFX32DA	SMB Blank Plug-in Unit
NTFX34AA	IOM RS232 Smart Connector Assembly
NTFX35AA	IOM V.35 Smart Connector Assembly
NTFX35BA	512Kbps V.35 Smart Connector Assembly
NTFX36AA	IOM PERTEC Smart Connector Assembly
NTFX38AA	Current Loop Smart Connector Assembly
NTFX39AA	BH 1-9 Cable Splitter Assembly

Figure 4-76 — IOM smart connectors
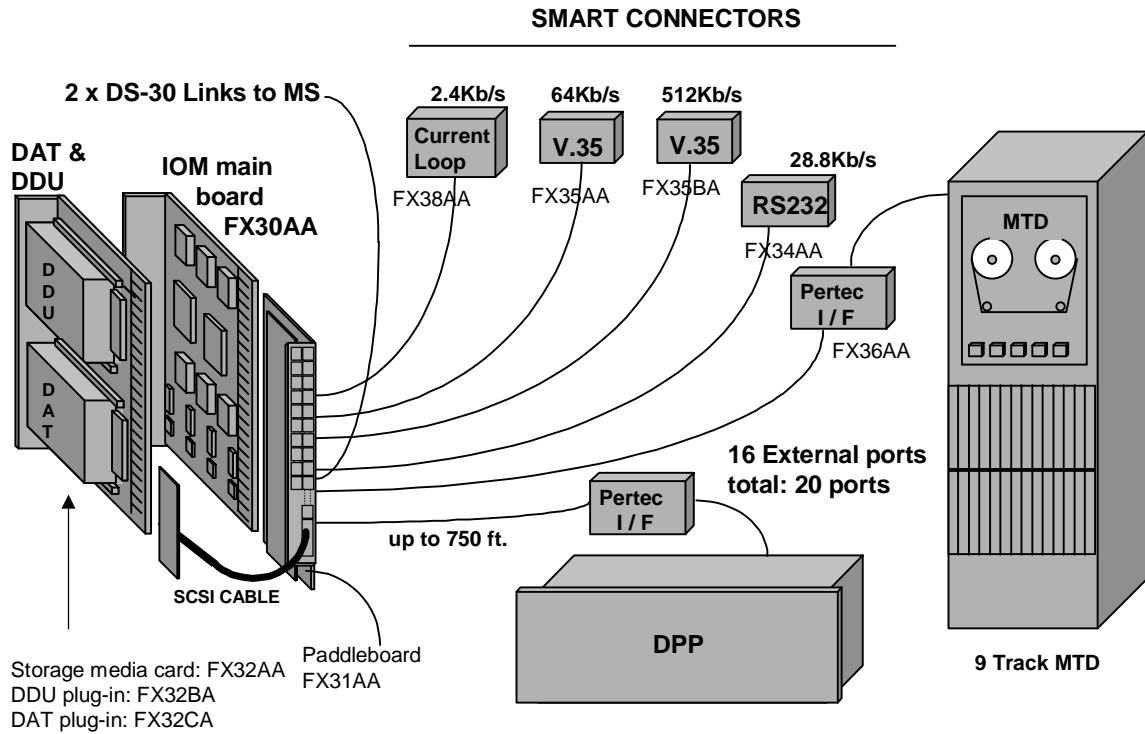
IOM key points

- The Input Output Module (IOM) was developed as a functionally equivalent of the IOC/IOE, while providing reduced customer cost of ownership.

- The IOM can replace a complete IOC, Disk and Mag. Tape Drive in initials. It can also be provisioned in extensions to coexist with in-place IOC's, Disk and Tape Drives.

- The IOM completes the evolution of Series I peripherals, (EDRAM, CTM, ISM, EDTU), which when deployed, can eliminate 1-3 frames from typical offices.

- In offices equipped with SDM, a minimum IOM configuration (1+1) can provide the remaining IO/OAM functionality

- Minimum IOC Requirement 22 packs

- Minimum IOM Requirement 4 packs+2 paddleboards

- IOM - Customer Benefits

  — Enhanced Communication Functionality

  — up to 16 ports from one card

  — 28.8 Kbps Asynch/64 Kbps Synch max./port

  — 512 Kb/sec synch. support (2 ports/IOM)

  — Full flexibility in port configurability, via smart connector

  — Increased disk capacity

  — 1 GB/drive, 10 GB/switch

  — Plug-in unit facilitates upgrades

  — Current, cost-effective tape drive technology (DAT)

  — Footprint reduction

  — 1 shelf => 1 card; 1 Frame => 2 cards, including tape drive

  — Power reduction

  — Support of current IO applications

  — Coexistence with current IOC (No hardware gating issues)

  — Reduced cable congestion

- IOM Provisioning Advantage

  — Up to 16 ports provisionable per circuit pack

  — Finer granularity in provisioning- 1 link vs. 2 links in 1X89 and 4 links in 1X67BD

  — Ports differentiated only by the Smart Connector

  — Adding a port as simple as adding a cable

  — DDU, DAT plug-in units allow easy on-site replacement

— Improved agility to handle Disk drive obsolescence

— Add higher capacity disk drives as they become available

— Dual DDUs possible in same circuit pack

- IOM Reliability Advantage

  — Controller / power supply failure can disable up to 36 IOC links vs 16 IOM links.

  — IOM survives power feed failure. It uses both A and B feeds.

  — IOM has better link sparing strategy. Designated spare port can be brought up via MAP replacing any failed link by switching to spare port.

  — IOM provides full isolation for all links - RS232, V.35, PERTEC etc., with higher noise immunity.

  — IOM provides higher link speeds. Reliability per transferred Mbyte is higher.

  — Disk drive and DAT can be replaced in the field, without impacting operations.

- IOM DAT Advantage over MTD

  — High MTBF (80,000 Power on hours vs. 20,000 for MTD)

  — Capable of higher data transfer rate (5 Mb/sec vs. 1.6 Kb/sec for MTD)

  — Low power consumption (10 watts vs. 250 watts for MTD)

  — Low weight (1 Kg (35.2 0z) vs 40 Kg (88 Lbs) for MTD)

  — Small footprint, PCB mountable (vs. 2 shelves for MTD)

  — Higher data storage (1.3 GB vs. 40 MB for MTD)

  — Greater range of operating temperatures (5-45º C = 41-113º F) vs. (16-32º C = 60.8-89.6º F for MTD)

  — Faster rewind speed

  — Reduced storage costs in Regional accounting offices

  — Reduced maintenance rates (US$2,000/yr vs. US$10,000/yr for MTD)

1-Meg Modem Overview and Maintenance

1-Meg Modem functional description

The 1-Meg Modem Service provides high-speed, data-over-voice communications over standard telephone lines to the home or small-office subscriber. The service provides the following functionality:

- high bandwidth with line transport rates up to 1280 kilobits per second (kbit/s) downstream and 320 kbit/s upstream
- simultaneous data and voice connection
- continuous data connection
- data traffic routed to data networks, which reduces congestion on the voice switch

The 1-Meg Modem Service uses a digital subscriber line (DSL) technology to provide the increased bandwidth with current office equipment and the subscriber loop.

Components

The 1-Meg Modem Service includes the following components:

- The 1-Meg Modem is customer premise equipment (CPE) that connects the telephone line, extension telephone, and computer. To the subscriber, the modem installs like a regular voice band modem, except the modem uses a 10BaseT Ethernet connection to the computer. Voice and data circuits are kept separate on the loop. This separation allows simultaneous voice and data traffic with no impact to other telephony features.
- The xDSL line card (xLC) replaces the subscriber's line card in an existing line concentrating module (LCM) drawer. The card provides full voice service in parallel with high-speed data communication with the 1-Meg Modem.

NOTE: The term xDSL refers to all the different DSL technologies., and xLC is an acronym for the xDSL Line Card.

- The data-enhanced bus interface card (DBIC) replaces the existing bus interface card (BIC) in the existing LCM drawer. The card is a concentrator for the voice and data connections within a single LCM drawer. The card also separates the voice and data traffic for routing to the correct networks.

- The xDSL Element Management System (xEMS) provides operations, administration, maintenance, and provisioning (OAM&P) functions from a Hewlett-Packard (HP) or Sun workstation. Based on HP OpenView, the xEMS is a graphical user interface (GUI) that uses icons and pull-down menus. Refer to *1-Meg Modem Service Network Implementation Guide*, 297-8063-200, for more information on xEMS.

- The transport network provides the connection to the service providers. Refer to *1-Meg Modem Service Network Implementation Guide*, 297-8063-200, for more information on transport networks.

The LCM line drawer contains the DBIC and xLCs. One LCM can hold up to 10 line drawers. Each line drawer can hold one DBIC and up to 31 xLCs. The line cards can be a mix of xLCs and plain old telephone service (POTS) line cards. Each 1-Meg Modem Service subscriber has an xLC. Each line drawer with xLCs must have a DBIC to provide data service. Each DBIC provides an Ethernet connection to the transport network for all subscribers in the LCM line drawer.

An LCM can have a maximum of ten Ethernet connections for all its 1-Meg Modem Service subscribers. The configuration of the transport network can require these Ethernet interfaces to connect to a mix of network components. The flexibility of the 1-Meg Modem Service allows you to change the interface to public and private wide area networks (WAN) to meet your requirements. Examples of WANs are Internet access providers (IAP), Internet service providers (ISP), and corporate networks.

Availability

The 1-Meg Modem Service is available on the following frame-based peripheral modules (PM) in DMS-100, DMS-500, and SL-100 offices:

- host LCMs
- remote LCMs
- Autovon LCM (ELCM)
- international LCM (ILCM)
- line concentration equipment (LCE)
- remote switching center (RSC) or remote cluster controller (RCC)
- remote switching center with SONET (RSC-S) or remote cluster controller 2 (RCC2)
- Star Remote Hub

NOTE: The 1-Meg Modem Service is also available for the S/DMS AccessNode office. Refer to the *AccessNode Express 1 Meg Modem Reference and Troubleshooting Guide*, P0887770, for information on the 1-Meg Modem Service in S/DMS AccessNode.

Hardware & Software Requirements

Hardware

- Phase 1 xDSL Line Card (XLC) NTEX17AA
- Data Enhanced BIC (DBIC) NTEX54AA
- 1-Meg Modem CPE NTEX35AA
- Cable Assembly Product Change Kit NTEX37AA
- Patch Panel Kit NTEX45AA

Software

- NA007 - HSTP 0002 DMS HOST H.S. DATA SERVICE SOFTWARE
- xEMS 0001 ELEMENT MANAGER SOFTWARE (MIBS)
- xDSL 0001 DBIC 1 MEG MODEM SOFTWARE

Compatibility

This describes compatibility between the 1-Meg Modem Service and other services.

Voice services

The 1-Meg Modem Service shares many components with the existing voice service. Some of these components are the following:

- LCE hardware, including power supplies and distribution
- the line drawer and the cards in the line drawer
- the subscriber's copper loop

Other data services

The 1-Meg Modem Service can function with the following data services in the same binder group:

- integrated services digital network (ISDN) basic rate interface (BRI)
- asymmetric digital subscriber line (ADSL)
- high bit rate digital subscriber line (HDSL) services

The 1-Meg Modem Service can function with T1 services in adjacent binder groups.

Ethernet

The Ethernet interfaces at the 1-Meg Modem and the DBIC meet standard *ANSI/IEEE Standard 802.3* with one exception. The 1-Meg Modem does not support the truncated binary exponential back off algorithm described in section 4.2.3.2.5 of the IEEE802.3 specification. This exception allows the best use of the bandwidth on the link. This exception also confirms a standard allocation between multiple users.

1-Meg Modem Service components

The following describes some of the components in the 1-Meg Modem Service.

xLC

The xDSL line card (xLC) provides full voice service and high speed data communication with a subscriber's 1-Meg Modem.

The xLC has the following features:

- located in a standard LCM line drawer with 1-Meg Modem Service capability
- provides standard voice service using the world line card (WLC)
- provides xDSL modem function over loops up to 18,000 feet on 26 American wire gauge (AWG) and 24,000 feet on 24 AWG
- rate-adaptable in both downstream (DS) and upstream (US) directions
- QAM modulation in both DS and US directions
- supports both narrowband and wideband DS spectra low and high transmission levels
- raw transport downstream data rates of 1280 kbit/s to 80 kbit/s
- raw transport upstream transport data rates of 320 kbit/s to 40 kbit/s
- provides an XLBUS interface to backplane
- -48 V power to data part of card
- self-identifying to DBIC on installation
- out-of-service data loopback capability for OAM
- low power design
- occupies a two-slot form factor

The xLC terminates the subscriber's line and transmits the call to the DBIC for multiplexing. The following figure illustrates the xLC in the 1-Meg Modem Service.

Figure 4-77   —   xDSL line card

xLC in 1-Meg Modem Service
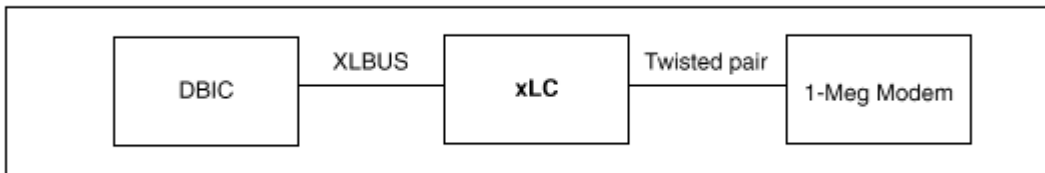
Types of xLCs

The 1-Meg Modem Service supports four types of xLCs. Each xLC supports different transmission rates, LCM drawer fill requirements, and PMs. Table 1-4 lists the xLCs that the 1-Meg Modem Service supports.

Table 4-50 — Types of xLCs

PEC	Maximum US/DS rates (kbit/s)	Maximum LCM drawer fill	PMs
NTEX17AA	960/120	16	All
NTEX17BA	1280/320	16	All
NTEX17CA	1280/320	31	All
NTEX17DA	1280/320	31	RLCM Star Remote Hub

NOTE: The section "Availability" in this chapter lists all the PMs that the 1-Meg Modem Service supports.

An LCM line drawer can contain a mix of POTS line cards and different types of xLCs. However, thermal constraints and power distribution determine the location and maximum number of each type of card. Refer to *1-Meg Modem Service Network Implementation Guide*, 297-8063-200 for more information.

Data-enhanced bus interface card

The DBIC replaces the existing BIC in each LCM drawer with an xLC. The DBIC separates the voice and data traffic. The card multiplexes the voice traffic to standard DS-30A interfaces to the existing circuit switched voice network. The card multiplexes the data traffic to one Ethernet connection to the transport network. The DBIC has the following features:

- half duplex, standard compliant Ethernet interface

- auto-sensing feature allows DBIC to connect at 10BaseT or 100BaseT

- maximum of 31 xLCs in a drawer

- connected to all line card slots through XLBUS

- backwards compatible with all POTS line cards compatible with the NT6X54AA

- different media access control (MAC) addresses for each xLC and DBIC

- demultiplex 64 voice channels from receive data (RD) links to XLBUS links

- multiplex 64 voice channels from XLBUS links to transmit data (TD) links

- +12.7v CODEC reference to all 64 line positions
- controls ring bus and automatic number identification (ANI)/COIN voltages using relays

Any LCM line drawer that contains xLCs must have a DBIC. The following figure illustrates the DBIC in the 1-Meg Modem Service.

Figure 4-78   —   DBIC in 1-Meg Modem Service
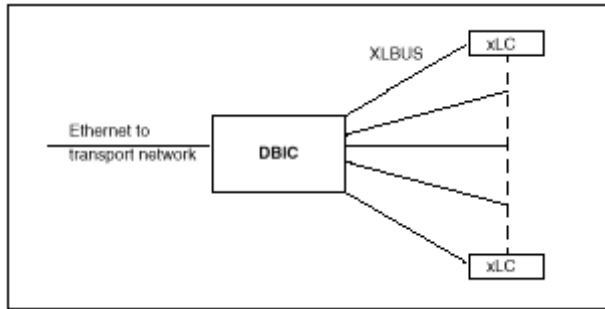
The 1-Meg Modem Service supports three types of DBICs. Each DBIC supports different transmission rates and Ethernet interfaces. The following table lists the DBICs supported by the 1-Meg Modem Service.

Table 4-51   —   Types of DBICs

PEC	Maximum US/DS rates (kbit/s)	Ethernet interface	PMs
NTEX54AA	960/120	10BaseT	All
NTEX54AB	1280/320	10BaseT	All
NTEX54BA	1280/320	10BaseT or 100BaseT	All
NTEX54CA	1280/320	10BaseT or 100BaseT	RLCM Star Remote Hub

xEMS

This describes the functionality of the xDSL Element Management System (xEMS).

NOTE: It describes xEMS functionality for a user with read-write access to xEMS. Users with read-only access to the xEMS will not see all the functionality described.

Introduction

The xEMS provides operations, administration, maintenance, and provisioning (OAM&P) functions for the data portion of the 1-Meg Modem Service. The MAP terminal provides OAM&P functions for the voice portion of the 1-Meg Modem Service.

The xEMS is a graphical user interface (GUI) based on HP OpenView that uses icons and pull-down menus. The xEMS runs on a Hewlett-Packard (HP) or Sun workstation.

Installation

The process to install 1-Meg Modem data service differs from the process to install voice services at the DMS. The 1-Meg Modem Service installation process involves the following tasks:

- A technician with experience in UNIX * and HP OpenView Network Node Manager * (NNM) sets up a Hewlett-Packard (HP) or Sun workstation as the xDSL Element Management System (xEMS) workstation.
- A technician with DMS experience installs or configures the DMS in the office to support 1-Meg Modem Service.
- A subscriber installs the 1-Meg Modem at the subscriber location.

Use the documents *1-Meg Modem Service xEMS Release Notes*, *1-Meg Modem Service DBIC Release Notes* and Installation Method (IM) *35-5543 xEMS Workstation for 1-Meg Modem* to install the 1-Meg Modem Service. Use these documents when you set up xEMS and the HP OpenView workstation. You can use the information in 297-8063-200, *1-Meg Modem Service Network Implementation Manual* to troubleshoot installation and operations problems. Operating company personnel with a working knowledge of UNIX and HP OpenView will set-up the HP OpenView workstation.

Testing

The 1-Meg Modem Service supports the following testing methods:

- in-service tests
- out-of-service (OOS) tests
- loopback tests

In service tests

The xEMS automatically performs an in-service test on a DBIC when one of the following actions occur:

- The xEMS discovers a DBIC.
- A DBIC is bootstrapped. A bootstrap is software on the DBIC that causes additional software to be loaded. A recovery condition, such as a reset, can cause a DBIC to be bootstrapped.
- A DBIC returns to service.

The test runs until the test fails or someone manually stops the test. If the test fails, xEMS changes the status of the drawer to Major or ISTb.

OOS tests

Use the Test selection from the pop-up menu of a selected object to perform an OOS test.

DBIC

You cannot perform an OOS test on a DBIC unless the DBIC is Restricted or ManB.

xLC

The Test selection for an xLC performs a loopback test that tests the data loop between the xLC and the 1-Meg Modem. A loopback test can help detect xLC hardware faults.

PING test

The PING utility in TCP/IP confirms that one PC can communicate with another PC. In xEMS, the PING test allows you to test communications between the HP Open-View workstation and a 1-Meg Modem Service component.

Perform the following steps to perform a PING test on an object:

- Select the object.

- Select **Fault:Ping** from the pull-down menu.

- The xEMS displays a window with the real-time results of the PING test. The PING test continues until you stop the test.

Loopback test

A loopback test allows you to test the connection between an xLC and another part of the 1-Meg Modem Service. Data received from the loop by the xLC is looped back to the originating object, such as a DBIC. To perform a loopback test on a selected xLC, use the Test selection from the pop-up menu.

Advanced loop debugging

Use the information in 297-8063-200, *1-Meg Modem Service Network Implementation Manual* to troubleshoot problems in the subscriber loop.

Troubleshooting

The 1-Meg Modem Service provides several functions to help in troubleshooting faults. Some of these functions follow:

- Events that track changes in status, maintenance, and provisioning

- symbol colors at the xEMS that reflect the status of an object

- graphs at the xEMS that allow you to monitor the real-time performance of a 1-Meg Modem Service object

Use the information in 297-8063-200, *1-Meg Modem Service Network Implementation Manual* to troubleshoot problems in the 1-Meg Modem Service.

Logs

Refer to 297-8063-200, *1-Meg Modem Service Network Implementation Manual* for information on log report PM181. Activities in the 1-Meg Modem Service can generate this log.

Refer to the *Log Reports Reference Manual* for your release for a complete description of PM181.

Translations and data schema

Refer to 297-8063-200, 1-Meg Modem Service Network Implementation Manual for information on:

- an introduction to 1-Meg Modem Service translations
- data schema information on table LCMDRINV
- data schema information on table LNINV

This information is also available in the Nortel Networks technical publication (NTP) *Translations Guide* or *Customer Data Schema Reference Manual* for your release.

Translations table flow

The HSTP0 DMS ADSL Capability translation tables are described in the following list:

- Table LCMDRINV
- Table LNINV

The following figure shows the HSTP0 DMS ADSL Capability translation process.

Figure 4-79   —   Translations process for HSTP0 DMS ADSL Capability
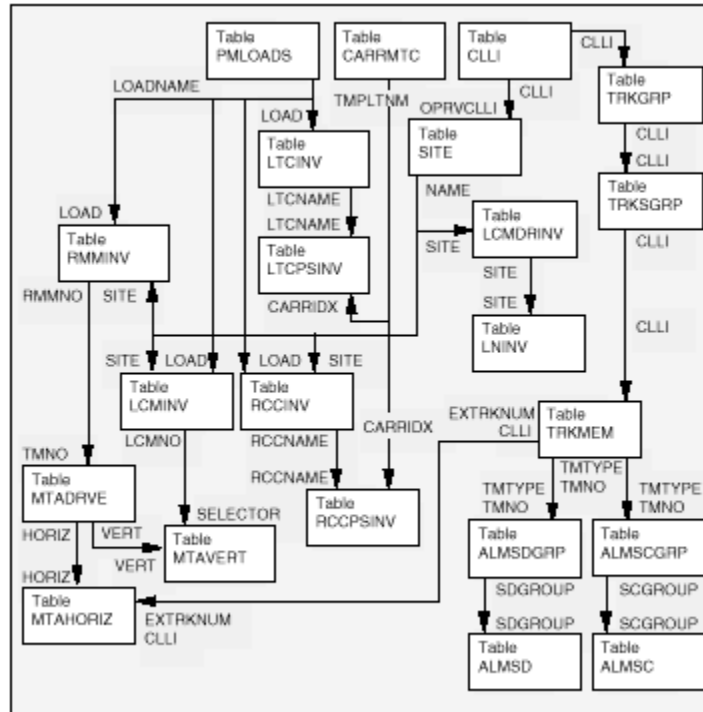
The following figure illustrates the table flow to datafill HSTP0 DMS ADSL Capability.

Figure 4-80   —   HSTP0 DMS ADSL Capability table flow
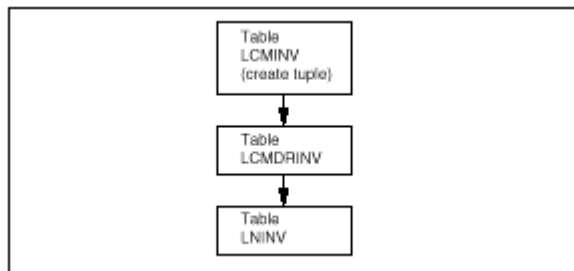
The datafill content for the tables in the previous flowchart follows:

- Table LCMINV lists data assignments for each bay with an LCM or a remote LCM (RLCM). Field SITE in table LCMINV matches the NAME tuple from table SITE. This field identifies the equipment for the switching unit and for all remote locations connected to the unit. Field LOAD in table LCMINV matches the LOADNAME tuple from table PMLOADS. This field stores the device location of each PM load file.

- Table LCMDRINV lists the LCMname, physical drawer numbers, product equipment code (PEC) of the drawers, drawer load name, and media access

control (MAC) address for each LCM and LCM variant in the host office. The line drawer applications use the information in this table to determine the functionality supported in each physical drawer. Table LCMDRINV only supports change operations and does not support manual additions or deletions. The switch automatically adds and deletes tuples to this table when a matching entry is made in table LCMINV.

- Table LNINV lists the site name with the line equipment number (LEN), and other data for each line card circuit in an office.

Limitations and restrictions

The following limitations and restrictions apply to HSTP0 DMS ADSL Capability:

- Each drawer entered in table LCMDRINV to support HSTP0 DMS ADSL Capability must have a DBIC.

- Each drawer with a DBIC must have an xLC to support HSTP0 DMS ADSL Capability. If the drawer does not have a DBIC, the xLC will only provide voice services.

- The 1-Meg Modem Service subscriber must have a 1-Meg Modem.

- When a tuple is added or deleted in table LCMINV, a corresponding tuple is automatically added or deleted in table LCMDRINV.

Datafill sequence and implications

You must datafill the following tables before table LNINV:

- LMINV
- LCMINV
- LCMDRINV
- LDTINV
- LNTDM
- ISGTDM
- You must datafill field LEN in the PM inventory tables (for example, RDT-INV) before you datafill table LNINV.

Network model

Refer to 297-8063-200, *1-Meg Modem Service Network Implementation Manual* for information on the network configuration and model for the 1-Meg Modem Service. The 1-Meg Modem Service uses the VLAN MAC network configuration and the PVC-Based High-Speed Data Connectivity model.

Network protocols

Figure 4-81 illustrates the network protocols in the data plane for PVC-Based High-Speed Data Connectivity.

Figure 4-81   —   Protocols in network
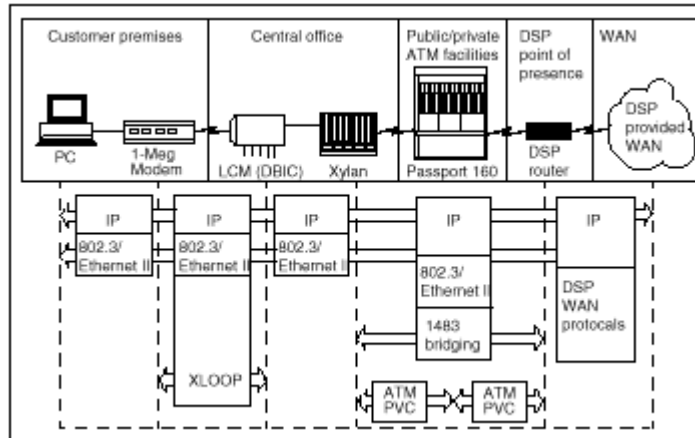
Figure 4-82 illustrates the VLAN configuration in PVC-Based High-Speed Data Connectivity.

Figure 4-82   —   VLAN configuration
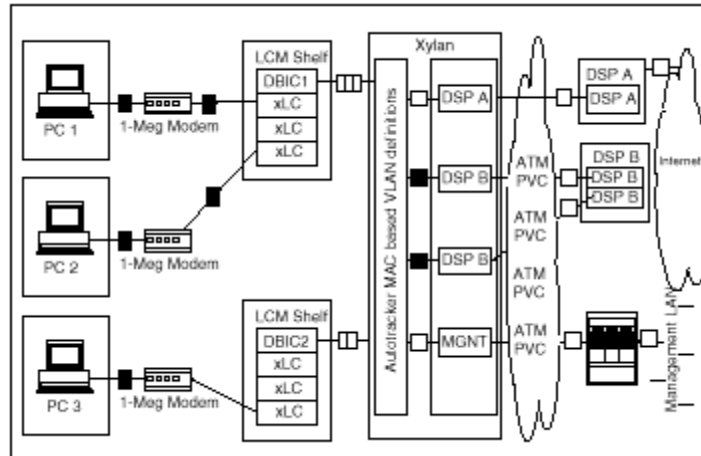
Star Remote System Overview and Maintenance

Star Remote System overview

The Star Remote System is Nortel Network's new line concentrating module (LCM) based remote product. The Star Remote System gives network providers a cost-effective way to provide service to their customers. The Star Remote System fills the need for a flexible remote that supports the following line installations for DMS-100 networks:

- under 200 lines
- 640 to 1100 lines

The Star Remote System accepts up to 16 DS-1 host links at full 1152 line configurations. The Star Remote System provides for traffic volumes of over 10 hundred-call seconds (CCS) and handles extended periods of Internet and work-at-home calling. Up to 1152 lines can connect to the Star Remote System. All services currently made available in Nortel Networks remote product line are also available from the Star Remote System. The Star Remote System includes the:

- Star Hub – The Star Hub is an improvement in technology and performance at a reduced cost. The Star Hub builds on the following Nortel Networks products:

  — Remote Line Concentrating Module (RLCM)

  — outside plant module (OPM)

  — outside plant access cabinet (OPAC)

- Star Module – The Star Module connects to the Star Hub through one or two DS-1 links. Up to 16 Star Modules, each supporting 64 lines, connect to the Star Hub. The Star Module exists in an outside or an inside cabinet configuration. The operating company can install the outside cabinet on a cement pad, wooden deck, or telephone pole. The operating company can install the inside cabinet on a wall.

Star Hub introduction

The Star Hub functions like an RLCM in that software, user interface, and functionality are the same. The Star Hub is a remote peripheral that connects to the SuperNode switch through a line trunk controller or line group controller with the

NTMX77AA unified processor (LTC+ or LGC+) or remote cluster controller 2 (RCC2).

The Star Hub:

- supports up to 1152 lines
- has one control shelf configured to support up to 18 local line drawers or up to 16 remote line drawers (RLD)
- provides for integrated services digital network (ISDN) lines when the ISDN line drawer for remotes (ILD-R) is installed where a standard line drawer is installed
- connects to the host office through 2 to 16 DS-1 links
- supports DMS-100 switch-based operations, administration, maintenance, and provisioning (OAM&P)
- supports the 1-Meg Modem service

The Star Hub is in a standard DMS-100 indoor frame, which is called a Star Remote Hub Equipment (SRHE) frame. The control shelf, frame supervisory panel (FSP), and up to three line drawer shelves (each containing up to six line drawers) are in the SRHE frame. The Star Hub uses existing line cards through a maximum of 18 line drawers, of which 16 can be Star Modules. The local line drawer in the Star Hub is a standard DMS-100 line drawer that supports up to 64 lines.

The Star Hub supports the following types of lines:

- plain old telephone service (POTS)
- custom local area signaling service (CLASS)
- coin
- Meridian Business Set (MBS), also known as proprietary phone (P-phone)
- x digital subscriber line (xDSL) line card (xLC) for 1-Meg Modem service

To support ISDN lines, up to six ILD-Rs can be installed.

Figure 4-83 — Star Remote System configuration

Figure: Star Remote System configuration. DMS SuperNode connects via DS30 or DS512 to LTC+, LGC+, or RCC2. This connects via 2 to 16 DS-1 to the Star Hub at the Remote site (below Host office). Up to five Star Remote Hubs can be connected to the host PM. Star Remote System. Up to 1152 subscriber lines. Star Hub contains ISDN line drawer and Local line drawer. Up to 18 local line drawers or up to 16 remote line drawers. ISDN lines, POTS/MBS lines. 1 or 2 DS-1s for each Module. Star Modules connect to POTS/MBS lines and ISDN lines. Up to 64 subscriber lines for each remote line drawer.

Star Hub hardware components

The following components make up the Star Hub:

- standard DMS-100 frame
- control shelf
- frame supervisory panel
- three line drawer shelves that contain up to 18 POTS line drawers. Six of the line drawers can be ILD-Rs, with a maximum of two ILD-Rs in each shelf.

Star Hub software

The Star Hub uses the software Functional Group BAS00012 "Remotes Generic" that provides:

- voice and data service – The Star Hub supports POTS, CLASS, coin, and Meridian Digital Centrex (MDC) voice and data from the DMS host office to remote subscribers.

- central operations, administration, and maintenance (OA&M) – The host DMS MAP (maintenance and administration position) terminal supports OA&M for the Star Hub.

- emergency stand-alone (ESA) – The Star Hub supports warm ESA entry and cold exit.

NOTE: The Star Hub supports non-ISDN calls while in ESA. When the Star Hub enters ESA, ISDN calls are released. Any attempts to originate an ISDN call after ESA entry are ignored.

- intraswitching – This feature enables a remote peripheral to switch calls internally, when both the calling and the called parties are served by the same peripheral. It also saves transmission links to the host. The Star Hub supports intraswitched calls.

- ISDN – The ILD-R using the NTBX27 line card, provides ISDN service for the Star Hub local drawers. Each drawer supports up to 28 ISDN basic rate interface (BRI) loops. There is a maximum of 168 ISDN lines if all six ILD-Rs are provisioned.

- ringing – The Star Hub supports coded, frequency selective, superimposed, distinctive, teen, and automatic number identification (ANI) and coin functions.

The Star Hub also uses the software Functional Group HSTP0002 "HSTP DMS ADSL Capability" for 1-Meg Modem service.

Star Module overview

The following components make up the Star Module:

- indoor or outside cabinet
- telephony subsystem (TSS) which contains
  — card cage with the control card, line maintenance card, power converter card, and ringing card
  — backplane
  — up to 64 line cards

Software defines and considers the Star Module a drawer in the Star Hub and not a stand-alone node. The Star Module mixes the functions of a line drawer and a line-concentrating device (LCD). The Star Module is a line drawer at a remote site in a cabinet adapted for its location with appropriate connections to power and to subscriber lines. The Star Hub can connect to up to 16 Star Modules.

The Star Module:

- supports up to 64 lines. The Star Module supports the same line types as the Star Hub, which was listed earlier

- is a remote line drawer (RLD) in a Star Remote Module Equipment (SRME) wall mounted cabinet or a Star Remote Module Outside (SRMO) cabinet

- supports up to 28 ISDN lines

- connects to the Star Hub using one or two DS-1 links

- uses DMS-100 switch-based OAM&P

Star Module

The Star Remote is line drawer in a cabinet located at a remote site. The Star Module connects to the the Star Hub through 1 or 2 DS-1 links. The maximum number of Star Remotes that can connect to one DMS-100 switch is 1,000. Up to 90 Star Modules (RLDs) can connect to a host PM such as RCC2, LTC+, or LGC+.

The Star Remote includes the following hardware components:

- telephony subsystem (TSS) includes all control, power, and maintenance cards and the backplane and plastic line card cage

- cabinet

  — Star Remote Module Equipment (SRME) cabinet that is installed on a wall

  — Star Remote Module Outside (SRMO) cabinet that is installed on a pole, concrete pad, or wood deck

- line termination unit (LTU), either copper or fiber, to terminate the DS-1 links from the Star Hub. The Star Hub requires an LTU to receive the DS-1 signals from the Star Module.

The following Figure 4-84 on page 4-422 shows the basic architecture of the Star Remote.

Figure 4-84 — Star Remote architecture
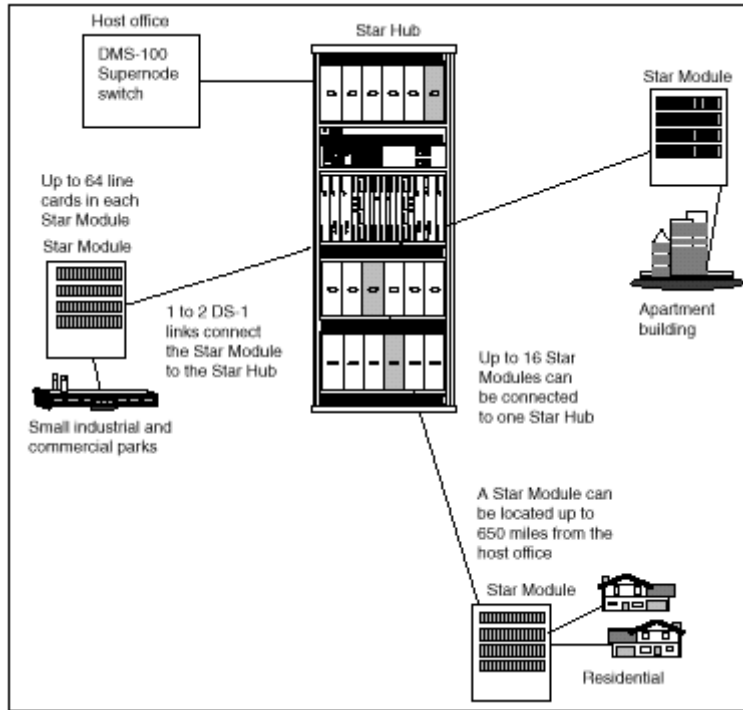
Star Remote System manual maintenance

This section introduces manual maintenance and troubleshooting methods which are useful for resolving problems with the Star Remote System or the subscriber lines connected to the Star Hub or Star Module.

In the discussions of manual maintenance in this section, the term line concentrating module (LCM) is used in a generic sense to refer to any peripheral module like the Star Hub. Therefore, when the term LCM is used in this context, the Star Hub is implied.

For STAR Remote System routine maintenance schedules, refer to Section 2 "Routine Maintenance" in this document.

Troubleshooting methods

Under normal circumstances, a faulty unit of the Star Hub is busied and tested. As a result of this testing, the maintenance and administration position (MAP) terminal may display a list of cards. The card at the top of the list often is the cause of the problem. Once the problem card is replaced, the originally faulty unit is tested again. If the unit passes this test, it is returned to service (RTS) and the troubleshooting procedure is complete. However, if normal troubleshooting procedures do not restore a unit to service, advanced troubleshooting procedures may be required. Experienced

operating company personnel may use MAP terminal responses from unsuccessful troubleshooting attempts to formulate a maintenance strategy.

The troubleshooting methods presented in this section are designed to assist in formulating a maintenance strategy. Basic troubleshooting methods include:

- monitoring performance indicators
- locating and clearing faults
- performing fault isolation tests
- monitoring results of diagnostic tests
- testing subscriber lines

Monitoring performance indicators

The first step in locating faults is to examine the performance indicators the system routinely generates. The existence of fault conditions is indicated by operational measurements (OM), log reports, and alarms.

Operational measurements

OMs are a data collecting system that tracks certain types of events and how often they occur. The OM data give an overall indication of performance and usage and are an excellent means for detecting both actual and potential system troubles. The OM thresholding feature should be used to monitor and report key STAR activity. These reports should be made routinely (daily or weekly) and should be the primary method of trouble detection. See *Extended Peripheral Module Operational Measurements Reference Manual*, 297-8321-814 for more information about the OMs that are specific to the Star Remote System.

Log reports

Logs, used primarily as an analysis tool, provide detailed information on call errors, diagnostic results, and system status. They are also good indicators of trouble conditions, especially when any of the following conditions exist:

- sudden increase in volume of logs
- message-not-printed reports
- large number of similar logs

Alarms

Audible and visual alarms indicate that something requires corrective action. Proper performance of routine system maintenance and use of OMs and logs should minimize the occurrence of alarms. Alarm severity and corresponding urgency for corrective action is indicated by the level of the alarm, and is expressed as minor, major, or critical. For alarm clearing procedures, see the "Star Remote System Alarm clearing procedures" chapter in NTP 297-8353-550, *DMS-100 Family Star Remote System Maintenance Manual*.

Alarms are generated because of:

- peripheral module (PM) failure (both units)
- unit failure (takeover)
- DS-1 link errors
- ringing generator failure
- circuit card failure
- dc/dc converter failure
- dc panel failure
- threshold of out-of-service (OOS) lines exceeded (software alarm)

Star Hub 1-Meg Modem Service

The Star Hub supports the 1-Meg Modem Service. The 1-Meg Modem Service provides high-speed, data-over-voice communications over standard telephone lines to the home or small-office subscriber. The service provides the following functionality:

- high bandwidth with line transport rates up to 1280 kilobits per second (kbit/s) downstream and 320 kbit/s upstream
- simultaneous data and voice connection
- continuous data connection
- data traffic routed to data networks, which reduces congestion on the voice switch

The 1-Meg Modem Service uses a digital subscriber line (DSL) technology to provide the increased bandwidth with current office equipment and the subscriber loop. In this document, the term xDSL refers to all the different DSL technologies.

Components

The 1-Meg Modem Service includes the following components:

- The 1-Meg Modem is customer premises equipment (CPE) that connects the telephone line, extension telephone, and computer. To the subscriber, the modem installs like a regular voice band modem, except the modem uses a 10BaseT Ethernet connection to the computer. Voice and data circuits are kept separate on the loop. This separation allows simultaneous voice and data traffic with no impact to other telephony features.

- The xDSL line card (xLC) replaces the subscriber's line card in an existing Star Hub drawer. The card provides full voice service in parallel with high speed data communication with the 1-Meg Modem.

- The data-enhanced bus interface card (DBIC) replaces the existing bus interface card (BIC) in the existing Star Hub line drawer. The card is as a concentrator for the voice and data connections within a single line drawer. The card also separates the voice and data traffic for routing to the correct networks.

- The xDSL Element Management System (xEMS) provides operations, administration, maintenance, and provisioning (OAM&P) functions from a Hewlett-Packard (HP) or Sun workstation. Based on HP OpenView, the xEMS is a graphical user interface (GUI) that uses icons and pull-down menus. Refer to *1-Meg Modem Service Network Implementation Manual*, 297-8063-200, for more information on xEMS.

- The transport network provides the connection to the service providers.

Refer to *1-Meg Modem Service Network Implementation Manual*, 297-8063-200, for more information on transport networks.

The following figure illustrates a network with the 1-Meg Modem Service.

Figure 4-85 — Telephone network with 1-Meg Modem Service
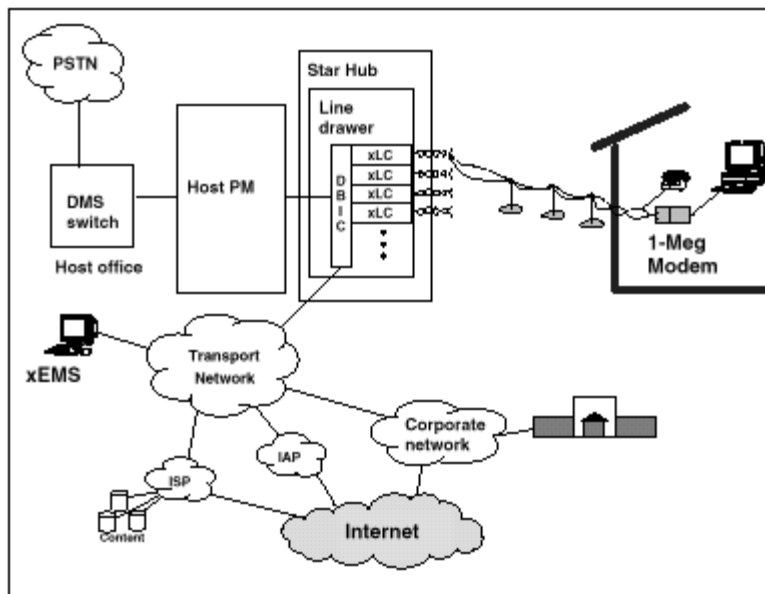
The Star Hub line drawer contains the DBIC and xLCs. The Star Hub can hold up to 18 line drawers. Each line drawer can hold one DBIC and up to 31 xLCs. The line cards can be a mix of xLCs and plain old telephone service (POTS) line cards. Each 1-Meg Modem Service subscriber has an xLC. Each line drawer with xLCs must have a DBIC to provide data service. Each DBIC provides an Ethernet connection to the transport network for all subscribers in the line drawer.

The Star Hub can have a maximum of 18 Ethernet connections for all its 1-Meg Modem Service subscribers. The configuration of the transport network can require these Ethernet interfaces to connect to a mix of network components. The flexibility of the 1-Meg Modem Service allows you to change the interface to public and private wide area networks (WAN) to meet your requirements. Examples of WANs are Internet access providers (IAP), Internet service providers (ISP), and corporate networks.

Compatibility

This section describes compatibility between the 1-Meg Modem Service and other services.

Voice services

The 1-Meg Modem Service shares many components with the existing voice service. Some of these components are the following:

- Star Hub hardware, including power supplies and distribution
- the line drawer and the cards in the line drawer
- the subscriber's copper loop

Other data services

The 1-Meg Modem Service can function with the following data services in the same binder group:

- integrated services digital network (ISDN) basic rate interface (BRI)
- asymmetric digital subscriber line (ADSL)
- high bit rate digital subscriber line (HDSL) services

The 1-Meg Modem Service can function with T1 services in adjacent binder groups.

XMS-based Peripheral Module Overview and Maintenance

Dual-shelf PM maintenance overview

XPM Maintenance Arbitrator

The XPM maintenance arbitrator (MtcArb) provides maintenance functionality, which triggers immediate analysis of anomalies that could result in service interruptions. This analysis involves determining which unit should have activity, based on the level of service each unit can provide. MtcArb functionality also notifies other maintenance systems and applications of important maintenance events. A load that contains MtcArb always provides the maintenance, with no ability to disable the function.

MtcArb provides maintenance functionality with mechanisms to:

- initiate immediate analysis of problems that could result in gaps in service
- provide periodic fault reporting with the log utility
- post XPMs based on the current alarm status displayed in the alarm banner, eliminating need to POST ALL and QUERYPM FLT each XPM
- determine which unit should be active, based on the level of service each XPM unit can provide
- notify other maintenance and applications of important maintenance events
- prompt the user to verify the correction of very important faults before attempting a manual return to service

The MtcArb maintenance functionality handles several major classes of DTC, LTC, and LGC faults associated with the NT6X41 speech bus formatter card, NT6X42 CSM card, and NT6X44 time switch cards.

If you attempt a manual SWACT, a pre–SWACT audit failure results in a MAP display. The MAP display identifies the internal resource of the XPM unit with the problem, and indicates the level of degradation.

After an autonomous SWACT, the system sets the newly inactive unit SysB for service level, which results in immediate RTS without diagnostics. The unit will return to service. After a SWACT for a very important problem, the system sets the newly inactive unit SysB for a MtcArb very important problem, which results in RTS by the audit with diagnostics. If the system detects a very important degradation during test-

ing, the unit will not return to service for diagnostic failure. If diagnostics do not detect the fault, then the unit will fail RTS. This failure occurs because the system recognizes the fault as a very important problem when the unit is active.

If MtcArb is present in the load, MtcArb makes the decision to perform a SWACT. While the CM maintains diagnostic history for XPMs, CM does not refuse SWACTs based on history. CM lets MtcArb make the decision.

Execution of the command QUERYPM FLT displays one of the three following service degradation levels:

- severe
- partial service levels
- minor or potential service levels

The command QUERYPM FLT also displays how MtcArb detected the faults and the conditions under which MtcArb detected the faults. The following list contains the fault types and the text for how MtcArb detected the fault:

- an inferred fault type: Fault inferred by maintenance
- a hard fault type: Fault detected by diagnostics
- an operational fault type: Operational fault

The command QUERYPM FLT also provides a list of potentially faulty cards.

NOTE: The PM181 log provides the same information displayed by the command QUE-RYPM FLT.

Basic audits

The following basic audits check two-shelf PM data to ensure hardware accuracy and agreement:

- XPM parity audit
- unsolicited report handler audit
- time switch connection audit
- IMC link audit
- data mismatch audit

NOTE: The time switch connection audit does not apply for the MSB6. This audit does not apply because Nortel does not supply the MSB6 with a time switch circuit card.

XPM parity audit

This audit runs as a low priority background task in the MP and SP cards. When the audit runs, the audit tests reading memory locations of the SP and MP memory cards. If the audit finds an area that has faults, the audit will reread the location. If the reread

has faults, the audit tries to write a test pattern to the memory location that has faults. The CC acts on this audit so that the memory fault can be corrected quickly.

Unsolicited report handler audit

This audit causes a software error (PM180) message when a two-shelf PM receives an unsolicited message that is not defined.

Time switch connection audit

This audit checks and corrects the time switch connection after every warm SWACT. The network requires this operation because message transfer between the active and inactive PM units occurs at a lower priority than other tasks. The message transfer contains call connection information with other data. As a result, the newly active and formerly active PM units can contain different information after a SWACT.

IMC link audit

The system audits both IMC links in a two-shelf PM to monitor the sanity of messages between the units. One IMC link appears between the NT6X69 message protocol cards and one appears between the processor cards. The system places the node (both units of the PM) in the ISTb state. This process occurs if the IMC audit fails and the system detects the fault at the node level. The system places the fault unit in the ISTb state if the system detects the fault at the unit level.

The following events occur when the system detects an IMC link failure:

- the system reports the fault to the CC
- the link closes and PM status changes to ISTb
- the PM processors no longer use link
- the system prevents warm SWACTs

Refer to "Handling an IMC link fault" in 297-1001-592, *DMS-100 Family Peripheral Modules Maintenance Guide* for additional information. Refer to "Dual–shelf PM trouble isolation and correction" for corrective action. When the system fixes the fault, the system audit reopens the link.

Data mismatch audit

An audit continuously checks for a data mismatch between the CC and the units of the XPM for PMs. The types of PMs that the audit checks for are LTC, LGC, and DTC. The audit compares the static data and the execs with the CC while the XPM is in-service. The CC determines if a unit requires reloading based on the data checksum of the audit. On a following RTS, the CC does not load the XPM (opposed to other XPMs). This condition occurs if the audit verifies that the static data and the execs match. The following occurs if the audit finds a mismatch:

- In the active unit, the system causes a SWACT to make the unit SysB. The system then executes the RTS command, which reloads the static data and the execs.

- In the inactive unit, the system makes the unit SysB and executes the RTS command, which reloads the static data and the execs.

Pre-SWACT and post-SWACT audits

The SWACT audits provide a mechanism in the XPM that increases SWACT reliability. The prevention of a SWACT to a mate unit that cannot maintain activity increases SWACT reliability. The system attempts a SWACT back to the originally active unit. This process occurs if a SWACT occurs and the newly active unit does not establish two-way communication with the CC. The new mechanism that provides additional SWACT reliability is based on the following audits:

- pre-SWACT

    — pre-drop

    — pre-gain

- post-SWACT

    — post-gain

    — post-drop

Each of the audits listed above is present in each unit. Every audit performs a different action in the states of a SWACT. For example, a SWACT drops the activity of one unit and gains the activity of the mate unit of a peripheral.

The following sections describe audits that control a SWACT in the XPM in more detail.

NOTE: The system can execute a pre-SWACT and post-SWACT audit on the following PMs: LGC, LTC, and DTC. This audit occurs because feature AF5007 applies to the LGC, LTC, and DTC peripheral modules. The audits cannot run on the derivatives of the three PMs described in this section.

Pre-drop audit

The pre-drop audit accepts a request to drop activity. This audit also determines if the mate unit is in a acceptable condition to accept activity. This audit only runs in the active XPM unit.

One of two possible sources can initiate a SWACT of the peripheral. The following are the two possible sources:

- the CC, in the form of a request to the active unit to drop activity
- the active XPM unit, that causes a not controlled SWACT

The pre-drop audit evaluates the following information to determine if the audit can drop activity:

- source of the request (CC or XPM)

- type of drop request
- known status and history of the currently active unit
- known status and history of the inactive mate unit

The SWACT controller queries the XPM for a CC-initiated SWACT. The pre-drop audit in the XPM responds to this query. The audit informs the CC if the active unit can comply with the request to drop.

Pre-gain audit

The pre-gain audit monitors the XPM status data in the inactive unit. The audit sends this information to the pre-drop audit in the active unit. The pre-drop audit uses this information to determine if the active unit can drop activity. The audit examines the XPM status data. The XPM status data includes the following:

- Facility audits that initiated the result of the last run for each diagnostic in the facility audit for a given peripheral. The system records the facility audits in the XPM.
- Status information that includes if the inactive unit:
  - is in service and ready
  - has CC links OK
  - does not have corrupt static data
  - is in sync
  - is not jammed as the inactive unit

NOTE: The inactive unit cannot reach all diagnostic paths. As a result, the performance of a manual SWACT with the FORCE option can be required. This procedure clears a failure from the pre-gain audit record.

The pre-gain audit continues to monitor and report unit status and condition information while the unit is inactive. The pre-drop audit determines if the active unit can drop activity. The audit uses the information provided by the pre-gain audit to determine if the active unit can drop activity. After the audit performs this procedure, a warm SWACT occurs. The post-gain audit in the newly active unit also starts to run.

Post-gain audit

The post-gain audit runs in the newly active unit. The single purpose of the post-gain audit is to verify that the unit establishes two-way communication with the CC. If the audit establishes communication, the newly active unit maintains activity. If the communication check fails, the unit forces a drop of activity. The drop of activity initiates a SWACT back to the originally active unit. In this event, the pre-drop audit allows the SWACT to proceed and does not refuse the SWACT. If the SWACT back fails, the system busies the XPM node and returns the node to service.

Post-drop audit

The post-drop audit runs in the newly inactive unit. The newly inactive unit remains in service for a limited time without initializing. The post-drop audit cleans up the call processing data structures of unstable calls and non-synced stable calls. The audit determines that the system does not require a SWACT back or a SWACT back is complete. After the audit performs this procedure, the XPM informs the CC. The system busies the inactive unit and returns the unit to service.

NT6X69 cards: tests and audits

The NT6X69 message protocol card performs self-tests when you enter the TST command. The protocol card also performs self-tests when the PM unit is inactive and OOS. The protocol card is a part of the PM unit. The NT6X69 message protocol card performs the following tests:

- the destructive test that replaces the contents of the CM
- the nondestructive test that does not test the CM

Destructive test

The destructive test fails when one of the stages of the test fails. The destructive test performs the following tests in sequence:

- resets the message protocol card
- checks the message buffer
- checks the speech bus and CM and the message buffer access from the P-side
- checks the time slice of messaging
- tests the speech bus interface (incoming and outgoing). To perform this test, the destructive test allows the system to transmit and copy the PCM into the buffers
- tests the ROM
- resets the message protocol card

If any stage of a test fails, you must replace the NT6X69 message protocol card. Refer to Card Replacement Procedures for additional information.

Nondestructive test

The NT6X69 message protocol cards run nondestructive tests when the protocol cards cannot run destructive tests. The tests include the following:

- P-side tests
  - use a dedicated channel of the time switch card to run a loop-around test on the P-side links. The links must be DS-30A or DS-1. The link cannot be a PCM30 because it does not have dedicated channels in use, and cannot be identified.
  - allow the CM for the dedicated channel and transmitting PCM samples

— check the received PCM samples. If the sample fails, the system lists the suspected card or cards and generates a log.

- C-side tests
    - use a C-side maintenance channel and CSM for a loop-around test
    - allow the CM for the channel and transmitting CSM
    - check the received CSM samples. If the sample fails, the system lists the suspected card or cards and generates a log.
- speech bus interface
    - sends PCM samples through the CM to copy into the receiving buffers
    - the outgoing speech bus transfers the PCM
    - the incoming speech bus transfers the PCM
- ROM
    - The message protocol card tests the ROM.

Interrupt by audit

The system automatically runs the audit and does not require manual interruption. The system does not require maintenance action because of the audit.

The NT6X69 card can receive messages from the network interface (C-side) or speech bus interface (P-side). The system includes messages between modules in the speech bus interface. If the interrupt line to the signaling processor (SP) of the XPM disconnects, the SP cannot receive any messages. The SP can continue to send messages. This condition means the CC cannot signal the XPM to drop activity. To prevent this potential stalemate, an audit of the NT6X69 card checks if the interrupt occurred. If the interrupt did not occur, the audit checks the incoming queues. The audit checks the queues to make sure the SP did not place messages in the queues. The audit generates a software error report (SWERR) and allows message processing to occur so that the SP receives messages. (The QUERYPM command displays the total quantity of SWERRs for a unit for a given time period.) This process occurs if messages that require processing exist but the interrupt is not raised. If the audit detects this condition two consecutive times, the audit sends a request for the XPM to drop activity. The audit also runs when the XPM is ManB. The audit also checks if the message interrupt is permanently disabled. If the message interrupt is disabled, the incoming message handler can check for messages continuously. The incoming message handler can also use the real time of the SP. To prevent this condition, the audit also checks if the interrupt is disabled and messages that require processing do not exist. If this condition occurs, the audit generates SWERRs and disables message processing. If the audit detects this condition two consecutive times, the audit then sends a request for the XPM to drop activity.

Lost message counts

The XPM cannot send a message if not enough message buffers exist. If this condition occurs, the XPM places the message in an interperipheral connection (IPC) buffer and in a holding queue. The XPM loses the message if the PM cannot obtain an IPC buffer or the holding queue is full. The XPM can also lose received messages if IPC buffers are not available.

The system increments two counts at the data link level:

- one for lost received messages
- one for lost transmitted messages

The counts appear at the data link level of the XPM monitor. The counts store information about lost messages that the system did not save. The counts also indicate when messaging overloads.

NOTE: The NT6X69 card test does not apply for the MSB6 because Nortel Networks does not supply the MSB6 with an NT6X69 card.

REx tests

The system performs routine exercise (REx) testing to maintain the XPM service. The system performs the following actions in a REx test:

- system busies the inactive unit
- returns to service the inactive unit that includes
  — out-of-service tests
  — downloading of static data and execs
  — a return to service
- delays to allow the unit to achieve superframe and data synchronization
- performs a warm SWACT
- system busies the new inactive unit
- runs in-service diagnostics on the active unit
- returns to service the newly inactive unit
- delays to allow the unit to achieve superframe and data synchronization

After the successful completion of the REx test, the system makes the inactive unit of the XPM the active unit. The test ends if a fault occurs on an XPM during REx testing. The system then generates a log to indicate the failure. The state of the XPM at the time of the fault remains the same. The REx testing occurs automatically by default. Manual or system maintenance actions can override testing.

Automatic REx testing

The REx test starts at the same time daily (START time) and tests the XPMs of the office one at a time. The tests occur until the test reaches the STOP time. If the test for the last XPM starts before the STOP time, the test continues to complete. If the system suspends the testing before the STOP time, the system continues the tests at the START time of the following day. When the system suspends testing before the STOP time, the XPMs are not tested between the START and STOP times. The operating company can set the start and stop times in data table OFCVAR with parameter NODEREXCONTROL.

The system REx (SREx) controller coordinates the automatic REx tests. The SREx is a dedicated software facility resident in the computing module (CM). The SREx controller allows compatible REx tests to run at the same time. This condition makes sure that the system can REx test all XPMs in the office within the designated test cycle. The designated test cycle is normally one week. The SREx controller also makes sure that incompatible REx tests are not run at the same time. For example, the system cannot test host and subtending XPMs at the same time. In addition, the SREx controller makes sure that REx tests are not run at the same time with incompatible activities. Incompatible activities include AUTODUMP and AUTOPATCH.

The table REXSCHED controls scheduling for automatic REx tests. In addition to basic scheduling parameters, this table also allows the naming of parallel XPM testing as automatic. As a result, the system automatically computes and adjusts the number of host XPM REx tests that can run together.

Manual REx testing

The command TST REX NOW can run REx tests manually or interrupt the tests after posting the XPM. The display for the command QUERYPM includes the status of the tests. The display also includes the time and date that the system last tested the XPM.

Different procedures exist to run REx tests on XPMs. The use of different procedures depends on the XPM having a REx controller. The following are summaries of the procedures.

XPMs without REx controller

The following summarizes the procedure to run a REx test on an XPM without a REx controller.

1. Busy the inactive unit.

2. RTS the inactive unit (includes out-of-service diagnostics).

3. Wait for the super frame and data sync.

4. Perform a warm SWACT.

5. BSY the newly inactive unit.

6. Run InSv diagnostics on the newly active unit.

7. RTS the newly inactive unit (includes OOS diagnostics).

8. Wait for the super frame and data sync.

XPMs with REx controller

The following summarizes the procedure to run a REx test on an XPM with a REx controller.

1. Test the inactive unit (includes in-service tests only).

2. SysB the inactive unit.

3. RTS the inactive unit (includes out-of-service tests only).

4. Wait for the superframe and data sync.

5. Perform a pre-SWACT audit.

6. Perform a warm SWACT.

7. SysB the newly inactive unit.

8. RTS the inactive unit.

9. Wait for the superframe and data sync.

10. Run in-service diagnostics (TST) on the newly active unit.

11. Run in-service diagnostics (TST) on the inactive unit.

The REx tests for XPMs with the REx controller apply to PMs that support feature AF5008. The tests also apply to PMs that support XPM REX Control and Trouble Notification Improvements. In this guide, the PMs that support the above features include the LTC, LGC, DTC, PDTC, and the DTCO.

A REx test for a given XPM only occurs for the following conditions:

• The REXSCHED table must turn on REX for an XPM.

• The system sets the value for the NODEREXCONTROL parameter in table OFCVAR to on.

• The system clock is within the start and stop times set in table OFCVAR.

• The XPM is the next one the system selects.

• You did not enter the TST REX OFF command for the XPM.

• The XPM node status does not show the following ISTb conditions:

— inact OOS

— overload

The MAP level commands QUERYPM and TST REX QUERY display the results of the last REx test. The MAP level command QUERYPM FLT gives the reason for the status of the XPM unit. When an XPM unit fails a REx test, the system places the unit as in-service trouble with a reason REX Failed. A successful REx test or a manual return to service can clear the in-service trouble status.

The REx test generates a log at the start time daily and when the system turns off REx testing. The REx test generates logs for each XPM during the testing. The REx test

generates Log PM181 if manual interruption affects automatic testing. The log also mentions when the REx test does not test an XPM because of the interruption.

Logs generated by the REx testing have the identifier IOAU112. Logs indicate one of the following conditions:

- The REx testing does not run.

- The testing timed out while the test waited for a REx test reply.

- Table OFCVAR changes the REx testing by setting the start, stop, on, and off parameters.

Operational measurements, counts, and alarms that the system normally generates for some system actions are suppressed. For example, activity of the REx test can accidentally activate counts.

The period of the REx tests, vary according to the type of XPM. According to the duration of a test, the quantity of XPMs tested between the start and stop times is measured. The period helps to estimate the time it takes to test all of the XPMs in the office. Table 4-52, "Duration of REx tests" notes the measured period for the XPM types.

Table 4-52 — Duration of REx tests

PM	Duration
ADTC	less than 15 min (estimate)
DTC	10 min (according to lab tests)
IDTC	12 min (according to lab tests)
LGC	12 min (according to lab tests)
ILTC	12 min (according to lab tests)
LTC	10 min (according to lab tests)
MSB6	less than 12 min (estimate)
MSB7	10 min (according to lab tests)
PDTC	less than 15 min (estimate)

Interface to the pre-SWACT and post-SWACT audits

The REx state machine (or controller) permits the SWACT controller to refuse to attempt a SWACT. The REx controller performs the following:

- calls the SWACT controller during the pre-SWACT step before the SWACT controller initiates the SWACT request. The SWACT controller determines if a SWACT can be attempted based on the diagnostic history of the unit. The diagnostic history of the unit is maintained in the diagnostic history database. The diagnostic history database is the result of the last SWACT attempt to the inactive unit. The database is also the result of the data returned by the XPM in the

pre-SWACT query message. This condition means an XPM can fail the pre-SWACT step of REx. In addition, the XPM cannot show any failures in the DiagHist level of the MAP display. This condition occurs if the reason for the pre-SWACT failure does not include diagnostic failures.

- accounts for SWACT denial and failure reasons
- terminates a REx test if a SWACT is denied
- terminates a REx test if a SWACT occurs. The active unit of the XPM does not change from the time the REx test started. If the test supports the feature AF5007, REx terminates without recovery actions. This termination occurs because the SWACT code submits a BSY/RTS of the inactive unit.
- displays the failure reason for a SWACT denial or failure performed during a manual REx at the MAP terminal as REx failed. The command string TST REX QUERY gives the reason for the failure for the posted XPM. In addition, the REx generates a PM600 log report detailing the reason of the REx failure.

Digital phase lock loop clock failure

The system identifies when a loss of sync causes a system busy following a digital phase lock loop (DPLL) clock failure. The enhanced field failure information feature allows the system to perform this procedure. To address the problem, the CC acknowledges the reception of the sync lost message. If the PM does not receive the acknowledgment, the PM goes SysB. As a result, the next time the PM returns to InSv the PM generates a sync_was_lost log. This feature logs all large out-of-phase readings to provide information on the time the DPLL clock had problems.

Automatic XPM reload

When an XPM requires a reload, the system can reload the XPM automatically without manual intervention. An automatic reload requires datafill in tables PMLOADS and LTCINV. Automatic loading (auto loading) only occurs when the system stores the loads on a storage device like a system load module (SLM) tape or a disk. Auto loading occurs when the XPM is system busy and the system failed to return the XPM to service twice. When the system attempts auto loading, the status display of the XPM shows the name LOAD. The following is an example:

```
LGC 0 ISTb Links_OOS: CSide 0 PSide 0

Unit 0: Act InSv

Unit 1: Inact SysB LOAD
```

If the resources required for loading are not available when the attempt occurs, an audit attempts the auto-loading again. If the XPM fails the ROM test of the auto-loading, the attempt occurs one more time. After two consecutive failures to load the XPM, the system aborts the load and cancels the audit. The failed attempts include a 10-minute time-out for the InSv that remains. The status of the XPM remains SysB.

You must datafill Table PMLOADS before you datafill table LTCINV. To remove a load name from table PMLOADS, you must first remove the load name from table

LTCINV. Table PMLOADS lists the names and the locations of the loads for the XPMs. Data is automatically datafilled in table PMLOADS during the dump and restore and first datafill. This process occurs when you datafill table LTCINV. If you already datafilled table LTCINV, the dump and restore of the office copies the data of the office.

You must add a device name to the table. The device name in table LTCINV identifies the device that stores the load files. When an audit attempts an auto load, a minor alarm can occur. The alarm occurs if the system does not store any of the load names in table PMLOADS on a storage device. The system displays the alarm as PMLOAD. The PMLOAD appears under the header PM of the continuous status display of the MTC level. This condition assumes that a more important alarm does not occur at the same time.

Increase to manual maintenance

When automatic maintenance fails to correct a fault in the DMS switch, the DMS switch provides trouble indicators. The trouble indicators reveal that a fault condition continues to exist. Alarms are examples of trouble indicators. Some OMs and logs also indicate a fault condition and a failure of automatic maintenance. The DMS switch requires manual intervention by maintenance personnel terminal to clear the fault.

XPM memory parity faults

The CC handles parity faults when possible so that the network can perform an RTS quickly. The following are three types of parity faults:

- hard (requires intervention by operating company personnel)
- soft (the CC can clear this type of fault)
- not continuous (the CC can clear this type of fault)

A PM181 log informs operating company personnel about the type of parity fault. Other logs, like PM128 and PM106, inform operating company personnel the action (if any) the CC performs. The logs also inform the operating company personnel if the CC cleared the fault. You can also use the QUERYPM FLT command to become informed about the type of parity fault.

IP Services on XPM feature description (IP XPM)

This feature provides IP services on XPMs of the SX05 platform. A standard IP operational framework is provided to support IP applications. For XPM12, two IP applications are supported: TOPS IP and peer-to-peer messaging.

- A remote socket interface is provided on XPM and CM so that TOPS CM applications can interact with IP networks using XPMs as proxies. For details on the related CM work items, please see activity ''59007541 TOPS IP Data Communication''.

- XPM peer-to-peer messages are automatically routed via IP messaging when IP services are available. This avoids having to bounce messages off CM, thus saving CM real-time.

The following are some highlights of the functionalities provided by this feature:

- The standard TCP/IP protocols are provided for XPM applications at task level. A TCP/IP protocol stack was purchased from a third-party vendor (EBS) and integrated into XPM software loads. The introduced IP messaging conforms to industry standards and is more efficient and flexible than our proprietary messaging protocols.

- XPMs can be bootstrapped using standard BOOTP (BOOTstrap Protocol) or DHCP (Dynamic Host Configuration Protocol) approaches. This allows easier management of bootstrapping for the XPMs. A CM datafill approach is also supported.

- An XPM node is addressed by the same IP always, even when the XPM SWACTs. The two units of an XPM node are both equipped with an Ethernet interface and both units are assigned with two different IP addresses: an even address I for the active unit and I+1 for the inactive unit, e.g. 47.108.0.114 and 47.108.0.115. The even address I is always bound to the current active unit. Both units are addressable on the IP network.

- XPMs can also be addressed using domain host names if DNS server(s) are provided on the IP intranet.

- IP packets can be routed to other networks if a gateway (router) is provided.

- Additional reliabilities are provided when default gateways are provided. XPM will dynamically re-select default gateway on failure and SWACTs if necessary.

- A remote socket interface (RSI) is provided on XPM (and CM) so that CM applications can issue IP-related calls on XPMs and thus get access to the IP networks.

- UDP sockets created by CM applications will be automatically re-constructed by XPM RSI when XPM SWACTs. TCP connections will be lost when XPM SWACTs. Errors will be returned if these TCP sockets are accessed. Applications have to re-establish the connections if they wish to.

- XPM-to-XPM (peer-to-peer) messages are routed using IP. Presently peer-to-peer messages are bounced off CM. By sending the peer-to-peer messages through the IP channel directly, CM real-time can be saved.

- Many new PMDEBUG levels for IP/RSI/peer-to-peer debugging facilities are added.

Figure 4-86 illustrates an IP network of XPM peripherals. Each XPM peripheral has two Ethernet links to the IP network, one from each unit. Both units are addressable on the IP network.

Figure 4-86 — IP Messaging System Topology
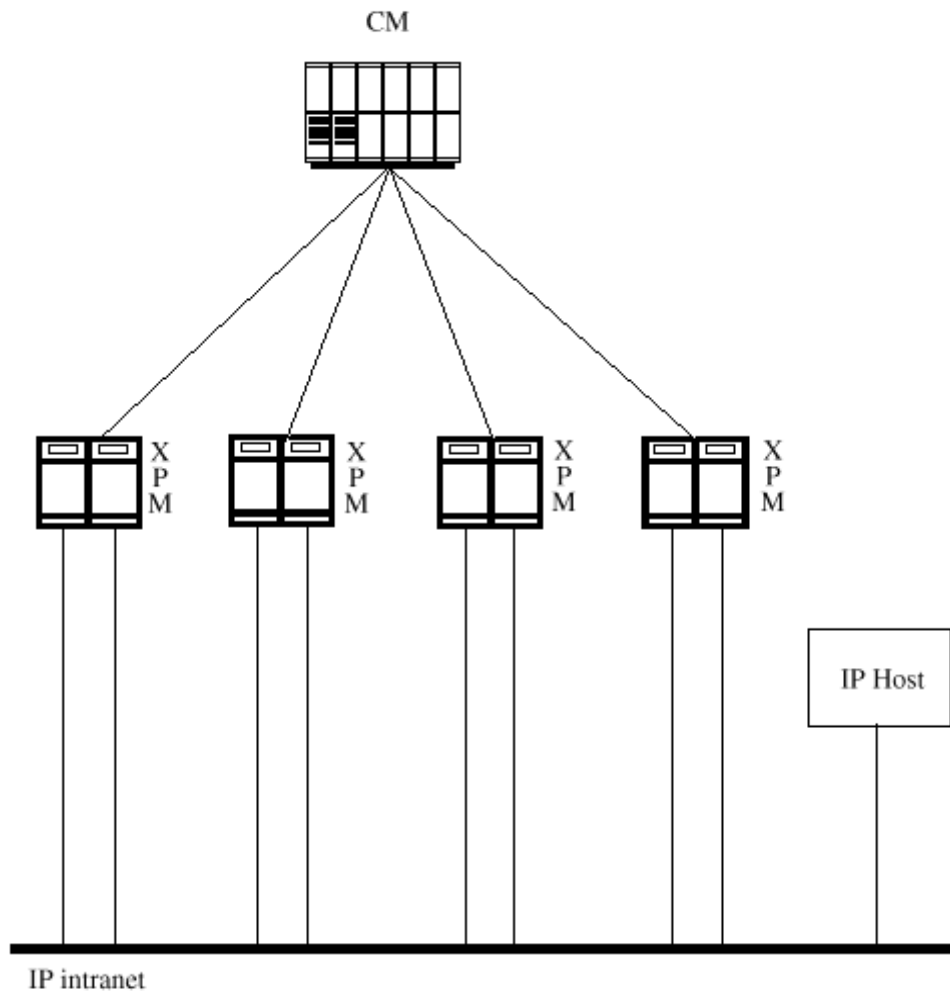
UEN Overview and Maintenance

UEN (UE9000)

The UEN/UE9000 is a type of LCM variance peripheral for the DMS–100F. This document is limited to the DMS-100F peripheral application only, and does <u>not</u> include Universal Edge 9000 information for the Access Node .

NOTE: The terms UEN and UE9000 are used interchangably throughout Nortel Networks documentation to identify the Universal Edge 9000 product.

UEN description

The UEN is a type of peripheral module for the DMS-100 introduced in the NA0012 release. The UEN is a Line Concentration Device (LCD) and is designed to provide high density Plain Ordinary Telephone Service (POTS) and Asymmetric Digital Subscriber Loop (ADSL) service (3rd generation copper).

The UEN is designed to look and behave like a Line Concentrating Module (LCM) from a maintenance and call processing point of view, and is connected to the DMS network through a XPM (LGC/LTC/RCC2). However, unlike LCM, which uses multiple single-circuit Line Cards (LCs) in a Line Drawer to provide service to multiple subscribers, the UEN uses Multi-Circuit Line Cards (MCLC) to provide the service.

A typical UEN shelf could contain two TDM Interface Cards, two ATM Interface Cards, sixteen Line Cards, a Power I/O card and a Metallic Test Access Card (MTAC).

NOTE: The UEN has a physical TDM DS30A interface (up to 6 DS30A links) and can subtend the XPM products LGC, LTC, and RCC2. The TDM card has DIP switches to adjust the cable length from the standard DS30A length of 50 feet up to 250 feet.

Figure 4-87 on page 4-443 shows a typical DMS-100 switch configuration with a UEN.

Figure 4-87 — Typical DMS-100 switch configuration
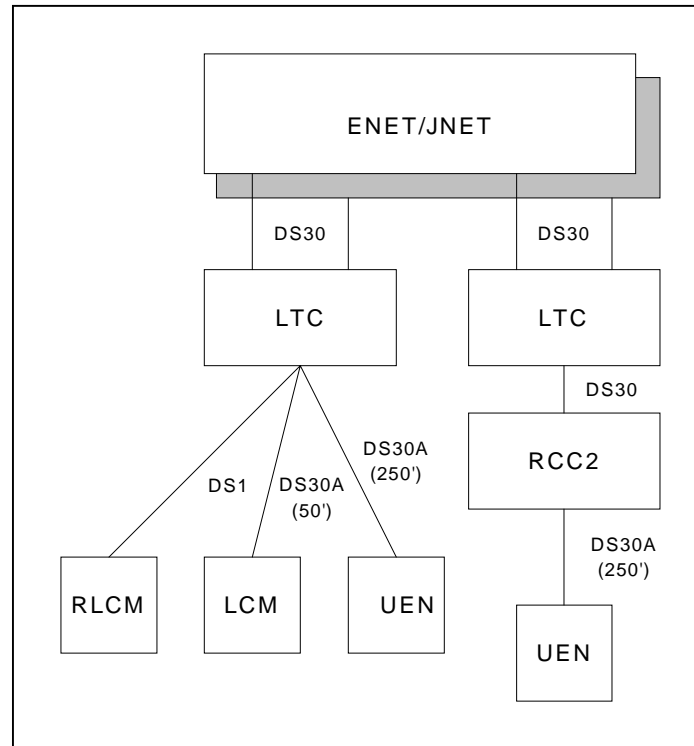
The UE9000 is a type of LCM variance peripheral for the DMS–100. The UE9000 MCLC cannot be used in any other LCM variance.

The UE9000 uses multi–circuit line cards (MCLC). Each line circuit must be treated as a world line card. The UE9000 provides voice and data service as:

• plain ordinary telephone service (POTS)

• asymmetric digital subscriber loop service (ADSL)

32 circuits POTS card

This feature introduced the 32 circuit Plain Old Telephone Service (POTS) line card for the Universal Edge 9000 (UE9000, UEN). Since the UEN has 16 LC slots, a sin-gle UEN can provide 512 (32X16) POTS lines.

NOTE: The UEN can also support a combination of both the 32 POTS line card and the ADSL (4x4) cards. Previously, the UEN only supported the ADSL (4x4) card.

ADSL (4x4) card

The ADSL DMT combination line card can terminate a maximum of four two-wire loops. Each loop carries a data service component and a voice service component. The voice and data are separated at the line card by a passive splitter circuit. The sep-

arated voice and data is terminated by either a Codec or a Modem interface circuit on the line card.

Hardware requirements

Below is the UEN line card data summary.

Table 4-53 —

Platform	Service	No of Voice Circuits per card	No of Data Circuits per card	PEC Code
UEN	ADSL	4	4	NTNP44AA
UEN	POTS	32	0	NTNP50AA

Changed logs

Limitations and restrictions, interactions, and new or changed logs summary

Table 4-54 —

Limitations and restrictions	Interactions	Logs
None	None	No new logs, two changed logs

PM179 Format 10

```
PM179 mmmdd hh:mm:ss ssdd TBL PM HW EXCEPTION REPORT
     pmid acttxt        Unit n
     <HWEX_String> Processor ID:
     Status Register: Time:
     Program Counter: Stack Pointer:
     Data: hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh
           hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh
```

PM180 Format 5

```
PM180 mmmdd hh:mm:ss ssdd TBL PM EXCEPTION REPORT
     pmid        UNIT n
     Software Exception:
     Processor ID:            Task ID:
     Time:
     Data:
```

Table 4-55 — Changed logs

Associated logs	Explanation	Format	Action
PM179	The Peripheral Module (PM) subsystem generates PM179. The subsystem generates PM179 when a hardware condition affects the normal operation of the DMS switch or the peripherals of the DMS switch. The PM subsystem generates PM179 to provide information on a PM hardware (HW) exception report.	For Format 10, the log contains processor information about the remote line concentrating module with extended distance capability (RLCM-EDC) and the universal edge 9000 (UE9000). The field values depend on the task and the type of trap.	For Format 10, save all reports generated during the 6 hours before the system generated the PM179 report. Contact the next level of support.
PM180	The peripheral module (PM) subsystem generates log report PM180. This report appears when the system encounters a software exception. A software exception occurs when software is not used correctly. Operating company personnel use log report PM180 to identify and correct software errors. A software exception that relates to hardware can also generate log report PM180. The PM subsystem generates this report when a software condition occurs. This software condition affects normal operation of the DMS or the peripherals of the DMS.	Format 5 identifies software exceptions in the remote line concentrating module with extended distance capability (RLCM-EDC) and the universal edge 9000 (UE9000).	For format 5, save all reports generated during the 6 hours before the subsystem generated log report PM180. Contact the next level of support.

Data schema

UEN new/modified tables

Table 4-56 — New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
LNINV	Changed	Unchanged
LCMDRINV	Changed	Unchanged

NOTE: Table LCMINV must be datafilled before table LCMDRINV. Table LCMDRINV must be datafilled before table LNINV.

Other changes caused by UEN

Table 4-57 — Other changes

Category	Change
Office parameters (OP) New/modified office parameters	No new or modified office parameters.
Service orders (SO)	No new or modified Service orders.
Alarms (AL) New/modified directories	No new or modified alarms.
Command interface (CI) New/modified commands	No new or modified CIs.
Operational measurements (OM) New/modified OM groups	No new or modified OMs.
AMA/Billing information (AM) New/changed AMA/billing information	No changes made to AMA.
Software optionality control (SOC)	This feature does not utilize SOC.

For more information refer to section "Data schema tables" table LNINV in NTP 297-8001-351, *DMS-100 Family NA100 Customer Data Schema Reference Manual*

NTNP44AA Product description

The NTNP44AA Combo 4+4 ADSL-DMT line card:

- is a voice and data interface to the subscriber loop for the Universal Edge 9000 (UE9000)

- terminates four subscriber loop pairs for analog voice telephone service and standard compliant ADSL-DMT ATM data services

The NTNP44AA can reside in any of slots 0-7 and 8-15 in the UE9000 shelf.

The NTNP44AA terminates four fully compliant ADSL DMT subscriber loops. Each loop interface has a splitter circuit to either separate or join the lifeline voice service with the value-added ATM data cell traffic for the subscriber. The voice traffic routes to the TDM common equipment cards through the Memphis ASIC. The data traffic routes to the ATM common equipment card.

The NTNP44AA includes the following functions:

- ATM ADSL and control

The ATMADSL subsystem transports cells between the ATMswitch card and all the ADSL modems on the card through a backplane serial link and an ATM cell multiplexer chip. The ATM serial link to the backplane is redundant.

- TDM voice

The POTS voice circuits support four circuits

- power supplies

The line card is powered from -48V signal battery. Two 48V point-of-use power supplies (PUPS) provide the following voltages for the card:

— single +5V 5W output

— triple +12V, -12V, and +3.3V 20W output

NTNP50AA Product description

The NTNP50AA POTS 32 Multi-circuit Line Card (POTS32) is a line card module used in the Universal Edge 9000 (UE9000).

The NTNP50AA POTS 32 line card resides in any of slots 0-7 and 8-15 in the UE9000 shelf.

The NTNP50AA POTS Multi circuit line card (POTS 32):

- uses the single in line package version of the World Line Card
- serves 32 subscriber loops
- has an onboard point-of-use power supply (PUPS) that generates dc voltages required to power the electronics from a -48V power distribution on the backplane
- has an onboard ringing generator pre-set to ring at 20 Hz superimposed on -48V dc
- is compatible with terminal sets with input and balance impedance according to North American standards
- is protected from electronic overvoltage in hostile electrical environments
- includes software selectable loop feed current limit characteristics with software selectable automatic loss equalization for short loops
- has two test-in / test-out busses, test bus 1 and test bus 2, and each subscriber interface circuit can access either bus
- has a hold clip circuit that allows the UE9000 shelf to place all loop interface circuits into protection. This allows the circuits to be removed from any external voltages.
- has an interface to the backplane through the Memphis line card interface application-specific integrated circuit (ASIC)
- has a Grace LAN (GLAN) bus, which is a three-wire serial interface (clock, downstream data, and upstream data) which provides control oriented information

NTNP50AA includes the following functions:

- supervision

The supervision block includes loop detection, ringing supervision, a loop current limiting function, and dial pulse detection.

- transmission

The transmission block includes loop termination, voice path, hybrid balance, equalization loss pads, and analog-to-digital and digital-to-analog conversion of the voice frequency signal.

- overvoltage protection

The overvoltage protection block increases the survivability of the card in hostile electrical environments.

- B11 overcurrent protection

The B11 overcurrent protection block protects against ground faults on the ring lead and against short circuits between the tip and ring leads by sensing the condition and limiting the current that can flow in the ring to a value that will not cause the line card any damage.

- relays

The relays block includes the following relays.

— The test-in relay in each line interface circuit allows access to the tip and ring for circuit testing purposes.

— The test-out relay in each line interface circuit allows bridging access to the tip and ring for loop testing purposes.

— The cutover / protection relay is used to isolate a subscriber loop interface circuit from the loop and is used for a variety of purposes such as line circuit protection from hazardous potentials, diagnostics, and office installation.

— The ringing relay connects the ringing generator output to the line circuit tip and ring in conjunction with office talk battery to ring the telephone connected to a subscriber loop interface circuit.

- WLC single in-line package (SIP) modules

The WLC SIP module block includes a loop interface circuit and a 5V regulator. There is one module for each subscriber for a total of 32 modules on each NTNP50AA card.

- point-of-use power supply (PUPS)

The PUPS block supplies +3.3V, +5V, +10V, and +15V outputs to the card from a -48V input to reduce the number of backplane pins and simplify backplane cabling.

- ringing generator

The ringing generator block provides ringing voltage to the line circuits. Having a ringing generator on each line card reduces the number of backplane pins and simplifies backplane cabling.

- talk battery and signal battery current limiting

The talk battery and signal battery current limiting block performs the following:

— Talk battery current is limited to approximately 1.6A. This circuit operates in the presence of a lightning strike to ensure that excess energy is shunted to ground, not to talk battery.

— Signal battery current is limited by a soft-start circuit. This circuit limits the current inrush during hot-swap.

— Lightning protection technology designed to meet first level lightning surge requirements up to 2 kV and all second level lightning surge requirements. In addition, each line circuit has a unidirectional clamping device to protect each circuit from arcing across test bus relays.

For more information refer toNTP 297-8991-805, *DMS-100 Family Hardware Description Manual*

THIS PAGE INTENTIONALLY LEFT BLANK

Performance – General

The primary goal of monitoring switch performance is to identify switch problems, analyze the cause, and initiate action to resolve any problems—*before* customers are affected. The method for monitoring switch performance involves the use of the software tools available within the switch as well as various operating company support system databases. This section of the MOM will provide an overview of some of the tools available within the DMS-100F switch and references to the NTPs that support those tools.

Log reports and operational measurements (OMs) are the basic tools in the DMS-100F switch for monitoring customer service and switch performance. To analyze the huge amounts of logs and OMs data would be very difficult even for an experienced analyst. To provide a more efficient and effective method of monitoring switch performance, specialized tools have been developed through various feature packages that may be installed on the DMS-100F switch. The tools to be described within this section are the:

- Switch Performance Monitoring System (SPMS).
- Real time performance indicators.
- Service Analysis System.
- DMS Monitoring System (DMSMON).
- Maintenance Managers Morning Report.

Service problem analysis

Monitoring switch performance requires an analyst with a diversified knowledge of the switch and the telephone network. The function of the analyst can vary depending upon their company operations and the analyst's working knowledge of the telephone network. For analyst support, see NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*. This NTP defines the analyst's role and provides an overview of information in the following areas:

- Tools for monitoring service indicators
    - Working with the MAP
    - Switch Performance Monitoring System (SPMS)
    - Real-time performance indicators

— XPM real-time and performance indicators

— CPStatus tool

— Service analysis

— DMS Monitoring System (DMSMON)

- Features that affect service

  — Network management controls

  — Other network controls

  — Emergency stand-alone (ESA)

- Analyzing service data

  — Software parameters

  — Service indicators

  — Troubleshooting with OMs

- Special reports

  — OM thresholding

  — OMRS special reports

  — Killer trunk feature

The following are other supporting NTPs for analysis of various types of problems:

- NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System (See the following subsection on SPMS)*

- NTP 297-YYYY-543, *DMS-100F Alarm and Performance Monitoring Procedures*

- NTP 297-YYYY-547, *DMS-100F Card Replacement Procedures*

DMS-100F equipment performance

For anyone needing equipment performance specification requirements concerning the environment, electromagnetic interference, audio noise emissions, and power, you should reference PLN-5001-001, *DMS-100F DMS SuperNode Technical Specification* document.

Switch Performance Monitoring System

SPMS purpose

The Switch Performance Monitoring System (SPMS) monitors all areas of switch operation and provides reports on the performance of the switch. The reports consist of detailed as well as summary data and are based upon a range of index values computed from OMs. The index values are computed and can be output on a daily basis or customer defined on a monthly basis. SPMS results on the daily basis are used to identify and correct trouble spots in the switch. Customers can use the monthly reports for evaluation of the quality of switch performance, or for an overall office performance index plan.

SPMS reports identify trouble spots with two asterisks (**), and less serious problems with one asterisk (*). Historical SPMS data could be stored or maintained to help identify intermittent problems or records of maintenance activity that is affecting service. SPMS is primarily a proactive maintenance tool that should be used on a daily basis to identify and correct maintenance and provisioning problems undetected by other means.

Once an SPMS index plan is in place, an operating company would be able to evaluate switch operation over frequent intervals or over an extended period of time. SPMS indices from a number of DMS-100F switches may be combined to derive section, district, or corporate results. This is a manual operation, and the individual indices must be weighted using call attempts before striking the composite index.

SPMS provides a medium-term review that includes details as well as summary level index values. Approximately 300 standardized performance indices are produced by SPMS that cover all areas of the switch, including CCS7 and ENET. Indices are standardized as follows:

- 100 indicates excellent performance.
- 95 indicates average performance as observed over a large number of switches of various types and various performance levels. A well run switch generally exceeds a 95 index; however, most companies look for an index over 98.
- 90 or below indicates a situation requiring immediate action.

NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System Application Guide*, describes the SPMS system in detail. For an explanation of how the index is calculated, see "How SPMS index values are calculated" within this NTP.

SPMS automatic report setup

SPMS reports can be automatically generated at a time you specify when SPMS software package NTX738 is present. The customer need only set the day of the month for the start of the report month in the table OFCENG. Then the customer must add the SPMS report to the list of automatically generated reports in table OMREPORT. The reports assigned to table OMREPORT are called OMRS reports.

Assign SPMSREP in table OMREPORT

To add the SPMS report to the list of automatically generated reports, enter the following CI level command:

>Table OMREPORT

The system responds with

Table: OMREPORT

Once you have entered Table OMREPORT, select a spare report to be assigned the name SPMSREP.

Enter the <LIST ALL> command. You should see a list of all the reports. Any report with ***SPARE*** in the DATA field is available for use.

Once you have determined which report to use, position on the tuple associated with that report and change the following information:

>POS XX	(Position on a spare report number (XX tuple or report number).)
>CHA	(Change the existing tuple.)
ACTIVE: N	**(** Status of report.)
>Y	
REP: AUTO	(Type of report.)
>DEVDAY	
WHEN:	(Time of report.)
>8 C30	(Enter time of your choice.)
CLASS: HOLDING	
>(cr)	(Return or Enter.)
NAME:*SPARE*	(Name of report.)
>SPMSREP	

TUPLE TO BE CHANGED

SCHEDNO	ACTIVE	DATA	WHEN	CLASS
23	Y		DEVDAY 8 C30	HOLDING

```
 SPMSREP
```

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>Y

TUPLE CHANGED

Once you have completed the procedure above, you will have created the OMRS report necessary to schedule the SPMS automatic report. In order for the report to print, you must assign the OMRS report to a log class in table LOGCLASS and ensure that a printer has been assigned as described later.

NOTE: There are 24 provisionable reports in table OMREPORT. Only twenty-three of the twenty-four entries can be assigned by the operating company, the remaining entry is designated report name *spare*.

Assign OMRS report to table LOGCLASS

Now that you have established the OMRS report and indicated the time for the report to print, you must assign the OMRS report to a log class in table LOGCLASS.

>Table LOGCLASS:

>ADD   (Add Report)

REPNAME:

>OMRS 23   (Enter OMRS report for SPMS)

CLASS:

>15   (Log Class assignment to report)

THRESHOLD:

>0

SUPPRESS:

>N

TUNITS:

>-1

SYSLOG:

>N

TUPLE TO BE ADDED:

OMRS 231   15   0   N   -1 N

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>Y

TUPLE CHANGED

Explanation of table LOGCLASS fields

TUNITS

TUNITS indicates the time units. Enter the time in minutes when the register counts associated with a threshold report is to be reset to zero. A maximum of 100 unique TUNITS is allowed. Zero (0) or a negative value means print all reports. Enter 0 or a negative value when no reset is required. The range of values is from -32767 to 32767.

THRESHOLD

THRESHOLD specifies which messages are to be printed out. Where threshold is zero (0), all messages are to be printed out. Where threshold is 1 – 255, office parameter THRESHOLD_IS_SAMPLING in Table OFCVAR controls the action for log thresholding.

SUPPRESS

SUPPRESS allows you either to suppress or not to suppress the log output. Enter Y (yes), where no report or log is to be output. Enter N (no), where report log is to be output. When threshold is set from 1 - 255, the office parameter BUFFER_THRESHOLD_REPORTS in Table OFCVAR controls the disposal of reports that have not been output due to log thresholding.

SYSLOG

Enter "Y" where log is a syslog, otherwise, enter "N". All syslogs are placed in Table LOGCLASS with the field SYSLOG = Y from the EXT files at loadbuild time.

Defining a printer

Once a log class has been assigned to the OMRS report, the log will have to be routed to a device that is available at the time specified to print the report. To use an existing printing device or to add a new device, follow the procedures in NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System Application Guide*, as described in "Start-up procedures" under "Defining a printer." Be careful when defining the PRIORITY and GUAR fields for table LOGCLASS. If necessary, see NTP 297-YYYY-350, *DMS-100F Translation Guides* for a description of those fields.

SPMS commands

The commands used in SPMS are as follows:

- SET (sets the parameters for the DISPLAY command)
- SETREP (sets the parameters for the SPMSREP automated log report)
- DISPLAY (displays the index values over the last N days or a date)
- DESCRIBE (used to describe the indexes you have selected)
- EXCEPTION (displays the critical index values over the last N days)

- QUIT (used to exit the system)

For a description of the SPMS commands and input examples and sample reports, see NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System Application Guide*.

Index hierarchy

SPMS has a capacity for 10 levels (TREETOPS) of indices, but only seven are used at this time (excluding the actual OM data—see Table 5-1 on page 5-14).

Level 0 TREETOP OFCPERF

The uppermost treetop level "0" is entitled OFCPERF (Office Performance) and is the overall performance index for the switch. OFCPERF is derived from the three subindices at level one, which are the three basic functional divisions for maintenance and administration:

- SERVICE
- MTCE PERF (Maintenance Performance)
- PROVRES (Provisioned Resources)

Table 5-1through Table 5-3 lists all the various indices and treetop levels by the three functional divisions: SERVICE, MTCEPERF, and PROVRES. Also recorded are the operational measurements used to derive the basic indices.

Level 1 TREETOP SERVICE

Service, first of three subindices that make up the overall performance OFCPERF index. The SERVICE index measures switch performance from the caller's viewpoint. In other words, the impact of problems that were noticeable to the customer (e.g., problems in transmitting the proper digits that were dialed, noticeable delays in receiving dial tone, call cutoffs, and all-trunks-busy conditions) are registered and evaluated in this SPMS index. It, in turn, is comprised of other indices in the service tree that graphically pinpoint the area of the switch experiencing the problems, and also identifies the problems that are maintenance or provisioning related.

Level 1 TREETOP MTCEPERF

MTCEPERF (Maintenance Performance), the second ingredient of the overall office performance OFCPERF index covers how well the switch performed from a component viewpoint. In other words, many of the switch's components (e.g., CCCs, IOCs, NMs, and PMs) are duplicated for backup purposes, so their failures and unavailability won't be noticeable to the callers. When component failure occurs, but is not noticed by the customer, it is reflected in this SPMS index MTCEPERF, but not in the first general index SERVICE. Thus, MTCEPERF reflects any problems in switch components, regardless of whether or not they were apparent to the callers. This index is comprised of other indices in the MTCEPERF TREE that pinpoint the specific component area of the switch experiencing the problems.

Level 1 TREETOP PROVRES

PROVRES (Provisioning Resources), the last broad ingredient of the overall office performance OFCPERF index covers the sufficiency of traffic engineering components of the switch to handle calls.

These traffic engineering components includes: call processing resources, conference circuits, receivers, junctors, speech links, announcements, and tones. Most of the time, the caller is unaware of any shortages in these components, since the switch attempts to compensate for any shortages in these components by automatically queuing for the next available component, or by automatically retrying the attempt. These shortages are counted in the PROVRES index and not SERVICE. The PROVRES index is comprised of other lower indices in the PROVRES TREE that pinpoint the specific component area of the switch experiencing the problem.

The indices are calculated once every 24 hours, day-by-day, and over the report month (to date) from switch generated Operational Measurements (OMs). For further details on the indices as related to the NT40 and the SuperNode switches, see NTP 297-1001-330, *DMS-100F Switch Performance Monitoring System Application Guide*, under the section "The indexing hierarchy."

SPMS plan application

Daily report

SPMS performance indicators are used both by switchroom management, as well as technicians, for their respective job responsibilities. Management, for example, can use SPMS to easily evaluate the overall quality of switch performance. It also helps them to determine what factors (i.e., maintenance factors versus provisioning factors) affected the switch performance each day. Technicians can use SPMS, since it easily identifies many problem areas that are not as apparent when using other troubleshooting tools.

A hard copy of the SPMS results should be requested daily, showing last month's results, current month results to date, and the previous day's results. See Exhibit A on page 5-36 at the end of this subsection for an example of an SPMS report.

SPMS should be used daily to detect and correct maintenance and provisioning problems not identified by the normal real time surveillance and trouble detection techniques described in the *Preventive Maintenance* tab of this manual. Attention should be given first to items highlighted with a double asterisk, next to items highlighted by a single asterisk, and finally to items not meeting operating company objectives.

Supplement OM data

OM data is required at times to supplement the SPMS index information, especially when sectionalizing obscure and constant trouble conditions. The OM groups and registers associated with the SPMS plan are listed in the *Preventive Maintenance* section within the OM subsection category. These are recommended daily and monthly

outputs respectively, and should be used to complement the SPMS troubleshooting procedure when required.

Table 5-2 through Table 5-3 (starting on Page 5-15) identify subindices, OM groups, and registers that can lead to trouble identification. See NTP 297-YYYY-814, *DMS-100F Operational Measurements* for an OM to log association table.

For aggregation of index results over a number of switches, the use of a weighted average of individual switch results is suggested. Suitable weights are provided by the total call attempt volumes reported by SPMS. These ensure that the offices processing the largest call volumes get the largest weights. This process is a manual operation.

SPMS for ENET

This section introduces SPMS indices for the Enhanced Network (ENET). When ENET is the active network, the indices replace all JNET (also called Network Module) indices. There are two major indices, ENETPERF and ENETLKPF. ENETPERF, for ENET system performance, gives a measure of how well the ENET system is performing. ENETLKPF, for ENET link performance, represents the performance of the links within the ENET. Each of these indices has several child indices that provides a detailed description of the performance of the ENET.

In offices equipped with ENET, the network module branches NMCPERF and NMLNKPF are replaced with ENETPERF and ENETLKPF, respectively. ENETPERF summarizes OM fields in the ENETSYS group. This group involves the major components of control in the ENET (i.e., the system cards), and so ENETPERF is part of the CONTROL branch in the SPMS tree. ENETLKPF summarizes OM fields in the ENETMAT and ENETPLNK groups. These groups involve network switching and P-side links and hence ENETLKPF is part of the LINKPERF branch in the SPMS tree.

See Tables 5-10 through 5-15 for ENET performance and link indices.

OMs for ENET

There are four OM groups in ENET containing a total of 49 fields. They measure faults of varying severity in each of the network's components. The fields are organized into the following groups:

- ENETSYS contains all the OM fields defined for the ENET system cards. There are 16 fields in this group.

- ENETMAT contains all the OM fields defined for the ENET matrix cards. There are 21 fields in this group.

- ENETPLNK contains all the OM fields defined for the ENET P-side links. There are 11 fields in this group.

- ENETOCC contains the CPU occupancies for each ENET shelf processor. There is one multi-tuple field per ENET shelf in this group.

For further information on the ENET OM groups and their associated registers and logs, see the "ENET Overview and Maintenance" subsection within the *System Products* tab of this manual.

Existing SPMS indices affected by ENET

The addition of the ENET indices above causes the interpretation of two existing indices to change. NETBLK and INTEGFL are basic indices and monitor service from the customer's point of view.

The changed interpretations for both indices are presented below. Table 5-3 shows where these indices exist in the SPMS hierarchy. Only the *diagnostic* sections have been altered.

NETBLK

Index Type: Basic

Description: Index of the proportion of calls failing because they cannot be connected through the core network.

Diagnostics: Confirm the incidence of network blocking with PROVRES index NETCHOVF. Check whether it has a maintenance related cause by examining MTCEPERF indices contributing to the NMLNKPF or ENETLKPF aggregate indices. If so, review network integrity performance by (a) using the NETINTEG analysis tool at the NET level of the MAP if JNET is the active network, or (b) entering INTEG at the ENET level of the MAP as well as checking OM ENCALDND if ENET is the active network. Further information may be provided by the periodic NETM110-111 summary count 3 logs, by analysis of NET130-132, NET136, ENCPl00, 102, and ENCP136 logs, and by analysis of TRK138 and LINE138 logs if they have been enabled for NBLH treatment. If blocking is persistent and does not seem to relate to maintenance problems, check network traffic usage in OM group TS against traffic provisioning recommendations.

INTEGFL

Index Type: Basic

Description: Index of the proportion of calls in a ringing or talking state that are cut off due to a loss of cross-switch path integrity detected and reported by a PM.

Diagnostics: The same network hits and faults that influence INTEGFL may cause worsened values of index NETBLK, worsened values of indices NMSPCHER and NMSPCHFL if JNET is the active network, and worsened values of ENLKERR and ENLKFLT if ENET is the active network. See the maintenance related diagnostics given for index NETBLK.

Performance monitoring for SS7

The SS7 components that are being monitored by the SPMS feature are divided into four functional areas as follows:

- Message Transfer Part (MTP) levels 1, 2, & 3
- Signaling Connection Control Part (SCCP) messaging performance
- ISDN User Part for Trunks (ISUP Trunks)
- Peripheral Module Performance

Overall, the MTP functions as a transport system providing reliable signaling message transfer in correct sequence, without loss or duplication, between adjacent nodes of the SS7 network. The key SPMS indicators for MTP performance are:

- C7LNKPF
- C7RTPERF

The SCCP provides additional functions to the MTP and serves connectionless as well as connection oriented network services. The main function of the SCCP includes the transfer of signaling messages with or without the use of logical signaling connection. It also includes performing global title translations. The key SPMS index for SCCP performance is:

- C7MSUPF

ISUP trunking uses SS7 signaling to provide enhanced call processing. The existing SPMS index TRKPERF has been enhanced to include information for ISUP trunks. The key SPMS indicator for ISUP trunking is:

- C7TRKCFL

An aggregate index called SOSPMPF (SOS based Peripheral Module Performance) is created. It provides a summary of the performance of the SOS related peripheral types. These include the LIU7 and LIM and are referred to as the Link Peripheral Processor (LPP).

NOTE: MSB7 and ST peripheral equipment are monitored under PM and PM1, respectively.

Investigating fault conditions identified by the SS7 SPMS indicators may require a more in-depth analysis of related OMs to identify the trouble. The SS7 performance indicators have been integrated into existing SPMS treetop layouts. Table 5-1 through (starting on Page 5-14) record this relationship.

Link Performance (C7LNKPF)

The link performance index C7LNKPF is an aggregate of C7LINK and C7LSOUT (see Table 5-5). The basic indices, along with their component makeup, are listed below:

- C7LNKSFL counts link failures due to:
    - abnormal FIB (Forward Indicator Bit)
    - abnormal BSN (Backward Sequence Number)
    - excessive delay in ST acknowledgment

> — excessive delay due to congestion
>
> — inability to allocate ST
>
> — inability to allocate SL
>
> — failure to complete network connection
>
> — SL test failure

- C7LNKOUT pegs usage when link(s) are unavailable (SYSBSY or MANBSY).
- C7LSOUT pegs usage when linksets are unavailable (SYSBSY or MANBSY).

Route Performance (C7RTPERF)

The route performance index C7RTPERF is an aggregate of C7ROUTE and
C7RTSET —see Table 5-6. The basic indices along with their component makeup are
listed below:

- C7RTDEGR part of the C7ROUTE aggregate counts transfer prohibited inci-
  dents that are Message Units (MU) destined for this route, but the network can-
  not accept transmission (delivery).
- C7RTOUT part of the C7ROUTE aggregate, pegs usage when routes are
  unavailable (SYSBSY or MANBSY).

NOTE: A route failure is an **ISOLATION** of switching entities from the network.

- C7RTSTCO part of the C7RTSET aggregate, counts routeset congestion. Mes-
  saging is limited since the messages are routed in order of priority.
- C7RTSTOU part of C7RTSET aggregate, pegs usage when routesets are
  unavailable.

NOTE: A routeset failure is an **ISOLATION** of switching entities from the network.

Messaging Performance (C7MSUPF)

The messaging performance index C7MSUPF is an aggregate of C7MSUFL and
C7SCCPMP, which measures lost or fail-to-route message signaling units, respec-
tively (see Table 5-2). The basic SCCP performance indices, along with their compo-
nent's makeup are listed below:

- C7MSUFL counts the number of MSUs lost and discarded by the MTP.
- C7SCCPMP counts the number of MSUs received by the SCCP Routing Con-
  trol (SCRC) that could not be routed.

Gateway screening (C7GTWERR)

The gateway screening performance index C7GTWERR is a basic index that applies
to STP locations.

- C7GTWERR counts the number of MSUs that caused an error in a screening function (MSUs that should have been blocked).

Table 5-3 associates the source data, OM groups, and registers with the basic indices used to derive the SS7 SPMS performance information.

ISUP connection failures (C7TRKCFL)

The ISUP connection failure index (C7TRKCFL) is a basic index that monitors the ISUP end-to-end connectivity. C7TRKCFL counts failures due to: switching equipment congestion, circuit unavailability, incomplete address, temporary failures, and continuity check request test failures.

Table 5-1   —   SPMS Index Levels (TREETOPS)

LEVEL 0	LEVEL 1	LEVEL 2	Continued With
	SERVICE	MTCESERV	Table 5-2
		PROSERV	Table 5-3
	MTCEPERF	CONTROL	Table 5-4
		LINKPERF	Table 5-5
OFCPERF		TERMINALS	Table 5-6
		BILLPERF	Table 5-7
	PROVRES	CPRES	Table 5-7
		FREQRES	Table 5-7
		EXTBLOCKS	Table 5-8
		SERVCTRES	Table 5-9
		CHANRES	Table 5-9

Table 5-2 — SPMS Index Levels (TREETOPS) MTCESERV Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP - REGISTER
MTCESERV	MTCACCS	CCRESET			CP-INITDENY
		ORGLNOUT			SYSPERF-LINPMBU
					SYSPERF-LINCCTBU
					OFZ-NORG **(NOTE 1)**
		ORGPMPLK			LMD-ORIGBLK **(NOTE 2)**
	INSIGFL	TINSIGFL			SYSPERF-TKBADDG
					OFZ2-PSGM
					OFZ2-PDLM
		LINSIGFL			SYSPERF-LINBADDG
	MISCFL				CP-CPTRAP
					CP-CPSUIC
					CP-NINTC
	MTCCMPL	SPCHBLK	NETBLK		TRMTRS-TRSNBLH
			TRMPMBLK		TRMTRS-TRSNBLN
					PMOVLD-PTRMDENY **(NOTE 2)**
		LINOUTFL	TLINOUT		SYSPERF-TRMLNFL
			RNGFL		LMD-PERCLFL **(NOTE 2)**
		OUTSIGFL			OFZ-OUTROSF
	CUTOFFS	CTLCTO	CCCTO		CP-CINITC
			PMCTO		PMTYP-PMTMBTCO
					PMTYP-PMTSBTCO **(NOTE 2)**
		INTEGFL			SYSPERF-CINTEGFL
	C7MSUPF	C7MSUFL			C7LINK2-C7MSUDSC
					C7LINK2-C7MSUDC1
					C7LINK2-C7MSUDC2
					C7LINK2-C7MSUDC3
		C7SCCPMP			C7SCCP- C7RTFALL

Table 5-3 — SPMS Index Levels (TREETOPS) PROVSERV Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
PROVSERV	PROVACCS	DTSR			DTSR-DTSTESTC
					DTSR-DTSDLYPC
		PMDNY			PMOVLD-PORGDENY **(NOTE 2)**
		MISCDNY			OFZ-ORIGLKT
					OFZ-INLKT
					CP-ORIGDENY
					CP-CCBOVFL
					CP CPLLOVFL
					(LMD-ORIGBLK) **(NOTES 2 & 3)**
	MISCBLK				TRMTRS-TRSNOSR
					TRMTRS-TRSNOSC
					TRMTRS-TRSSORD
					TRMTRS-TRSCQOV
					TRMTRS-TRSEMER3
					TRMTRS-TRSEMER4
					TRMTRS-TRSEMER5
					TRMTR-TRSEMER6
					TRMTCM-TCMATBS
	TRKPROV	NWMBLK			TRMTRS-TRSEMER1
					TRMTRS-TRSEMER2
					TRMTRS-TRSNCRT
					TRMTRS-TRSTOVD
		FINALBSY			TRMTRS-TRSGNCT
					TRMTRS-TRSNECG
	INTFEATR **(International)**	ICONFOVF			ICONF-TWCUSGE
					ICONF-SWUSGE
					ICONF-TWCOVRFL
					ICONF-SWCOVFL
		ICWTOVFL			ICWT-CWTUSGE
					ICWT-CWTOVFL
		IFDLOVFL			IFDL-HTLUSGE
					IFDL-WLNUSGE
					IFDL-HTLOVFL
					IFDL-WLNOVFL
		IWUCOVFL			IWUC-WUCUSGE
					IWUC-WUCOVFL
					IWUC-WUCNRSC
	C7GTWERR				C7GTWSCR-MSUSCRER

Table 5-4 — SPMS Index Levels (TREETOPs) CONTROL Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
CONTROL	CCPERF (NT40)	CCERRINT			CPU-MATCHINT
		CCFLT			CPU-CPUFLT
					CPU-MSYLOSSU
		CCNOSYNC			
					CPU-SSYLOSSU
	CMCPERF (NT40)	CMCERR			CMC-CMCERR
		CMCFLT			CMC-CMCFLT
					CMC-CMCSBU
		CMCUOUT			
					CMC-CMCMBU
					CM-CMTRMISM
	CMPERF (SuperNode)	CMCERRINT			
					CM-CMDPSYNC
					CM-CMCPUFLT
					CM-CMMEMFLT
					CM-SSCFLT
		CMFLT			CM-CMMCSBSY
					CM-CMRCPUFL
					CM-CMRMEMFL
					CM-CMRSSCFL
					CM-CMRMCFL
					CM-CMMSMPXU
		CMNOSYNC			
					CM-CMSSMPXU
	MSPERF (SuperNode)	MSERR			MS-MSERR
		MSFLT			MS-MSFLT
					MS-MSSBU
		MSUOUT			
					MS-MSMBU
	MSCDPERF (SuperNode)	MSCDERR			MS-MSCDERR
		MSCDFLT			MS-MSCDFLT
					MS-MSCDSBU
		MSCDUOUT			
					MS-MSCDMBU
	IOCPERF	IOCERR			IOC-IOCERR
		IOCFLT			IOC-IOCFLT
					IOC-IOCSBU
		IOCUOUT			
					IOC-IOCMBU
	EIOCPERF	EIOCERR			EIOC-EIOCERR
		EIOCFLT			EIOC-EIOCFLT EIOCMBU
		EIOCUOUT			EIOC EIOCSBU

Continued on next page

Table 5-4 — SPMS Index Levels (TREETOPs) CONTROL Subindices (continued)

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
CONTROL (Continued)	ENETPERF				
		ENETERR			ENETSYS-ENERR
		ENETFLT			ENETSYS-ENFLT
		ENETSOUT			ENETSYS-ENSBU
		ENETMOUT			ENETSYS-ENMBU
	NMCPERF	NMCERR			NMC-NMCERR
		NMCFLT			NMC-NMCFLT
		NMCUOUT			NMC-NMSBU
					NMC-NMMBU
	PMPERF	PMTOTPF	PMTOTERR		PMTYP-PMTERR **(NOTE 2)**
			PMTOTFLT		PMTYP-PMTFLT **(NOTE 2)**
			PMTOUSOU		PMTYP-PMTUSBU
			PMTOUMOU		PMTYP-PMTUMBU **(NOTE 2)**
		XXXPERF **(NOTE 4) (NOTE 8)**	XXXERR		PMTYP-PMTERR **(NOTE 4)**
			XXXFLT		PMTYP-PMTFLT **(NOTE 4)**
			XXXUOUT		PMTYP-PMTUSBU
					PMTYP-PMTUMBU **(NOTE 4)**
	SWINTEG	PMSWINTG	PMSWERR		LOGS-PMSERCT
			PMTRAP		LOGS-PMTRAPCT
		CCSWINTG	CCSWERR		LOGS-SWERRCT
			TRAPS	NONCPTRP	CPU-TRAPINT CM-CMTRAP (CP-CPTRAP) **(NOTE 3)**
				CPTRAPS	CP-CPTRAP
		CPSUICDS			CP-CPSUIC
		CCINIT	CCWINIT		CPU-SYSWINIT
					CM-CMSWINIT
					CM-CMMWINIT
			CCCINIT		CPU-SYSCINIT
					CM-CMSCINIT
					CM-CMSWINIT

Table 5-5 — SPMS Index Levels (TREETOPs) LINKPERF Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
LINKPERF	CMCLNKPF (NT40)	CMCLNKER			CMC-CMCLERR (NOTE 2)
		CMCLNKUO			CMC-CMCLKSBU
					CMC-CMCLKMBU (NOTE 2)
	MSLNKPF (SuperNode)	MSLNKERR			MS-MSLKERR
		MSLNKFLT			MS-MSPTFLT
		MSLNKUO			MS-MSLKSBU
					MS-MSLKMBU
	IOCLNKPF	IOCLNKER			IOC-IOCLKERR
		IOCLNKUO			IOC-IOCLKSBU
					IOC-IOCLKMBU
	ENETLKPF	ENETLKERR	ENETMAT		ENCDFLT
					ENPBFLT
			ENETPLNK		ENLKFLT
		ENETLKFLT	ENETMAT		ENCDFLT
					ENPBFLT
			ENETPLNK		ENLKFLT
		ENLKSOUT	ENETMAT		ENSBPBU
					ENSBCDU
			ENETPLNK		ENSBLKU
		ENLKMOUT	ENETMAT		ENMBCDU
					ENMBPBU
			ENETPLNK		ENMBLKU
		ENLKINAC	ENETSYS		ENPARU
			ENETMAT		ENCDPARU
					ENPBPARU
			ENETPLNK		ENLKPARU
		ENKISOL	ENETMAT		ENPBISOU
					ENCDISOU
			ENETSYS		ENISOU
			ENETPLNK		ENELKISOU

Continued on next page

Table 5-5 — SPMS Index Levels (TREETOPs) LINKPERF Subindices (continued)

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
LINKPERF (Continued)	NMLNKPF	NMMSGLPF	NMMSGLER		NMC-NMMSGER
			NMMSGLFL		NMC-NMMSGFL
		NMMSPCHPF	NMSPCHER		NMC-NMSPCHER
			NMSPCHFL		NMC-NMSPCHFL
	NMPTOUT				NMC-NMPTSBU
					NMC-NMPTMBU
	NMJCTOUT				NMC-NMJRSBU
					NMC-NMJRMBU
	PMLNKPF	PMLNKERR			DS1CARR-DS1BPV
					DS1CARR-DS1LOF
					DS1CARR-DS1SLP
		PMLNKFLT			DS1CARR-DS1LCGA
					DS1CARR-DS1RCGA
		PMLNKUO			DS1CARR-DS1SBU
					DS1CARR-DS1MBU
	C7LNKPF	C7LINK	C7LNKSFL		C7LINK1-C7LKFAIL
			C7LNKOUT		C7LINK1-C7STALFL
					C7LINK1-C7TLALFL
					C7LINK1-C7NETCON
					C7LINK1-C7SLTFL
					C7LINK1-C7LKUNAU
					C7LINK1-C7LKUNAU
		C7LSOUT			C7LKSET-C7LSUNAU

Table 5-6 — SPMS Index Levels (TREETOPs) TERMINALS Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
TERMINALS	IODEV	MTUPERF	MTUERR		MTU-MTUERR
			MTUFLT		MTU-MTUFLT
			MTUOUT		MTU-MTUSBU
					MTU-MTUMBU
		DDUPERF	DDUERR		DDU-DDUERROR
			DDUFLT		DDU-DDUFAULT
			DDUOUT		DDU-DDUSBUSY
					DDU-DDUMBUSY
		CONSOLPF	CSLERR		CSL-CSLERR
			CSLOUT		CSL-CSLSBU
					CSL-CSLMBU
	SRVCCTPF	CONFPERF	CNF3PERF		CF3P-CNFSBU
					CF3P-CNFMBU
			CNF6PERF		CF6P-CF6SBU
					CF6P-CF6MBU
		ANNSTNPF			ANN-ANNSBU
					ANN-ANNMBU
					STN-STNSBU
					STN-STNMBU
		ESUFFERF			ESUP-DESSBU
					ESUP-DESMBU
		RCVRPERF			RCVR-RCVSBU
					RCVR-RCVMBU
		SPECSVPF			SVCT-SVCSBU
					SVCT-SVCMBU

Continued on next page

Table 5-6 — SPMS Index Levels (TREETOPs) TERMINALS Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
TERMINALS (Continued)	CARRPERF	CARRERR			DS1CARR-DS1BVP
					DS1CARR-DS1LOF
					DS1CARR-DS1SLP
					DS1CARR-DS1LCGA
		CARRFLT			DS1CARR-DS1RCGA
					DS1CARR-DS1SBU
		CARROUT			DS1CARR-DS1MBU
	C7RTPERF	C7ROUTE	C7RTDEGR		C7ROUTE-C7TFP
					C7ROUTE-C7FRCRER
			C7RTOUT		C7ROUTE-C7RTUNAU
		C7RTSET	C7RTSTCO		C7RTESET-C7RSCNGU
			C7RTSTOU		C7RTESET-C7RSUNAU

Continued on next page

Table 5-6   —   SPMS Index Levels (TREETOPs) TERMINALS Subindices

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
TERMINALS (Continued)	OPPOSPF	TOPSPERF	TPOSFLT		TOPSMTCE-POSDF
					TOPSMTCE-POSTRKDF
					TOPSMTCE-POSDMDF
			TPOSOUT		TOPSUSE-POSMTCE
			VIRTCFL		TOPSVC-VCFL
		CPOSPERF			ONI-ONISBU
					ONI-ONIMBU
		AOSSPERF	AOSSPFLT		AOSS-AOSSDF
			AOSSPOUT		AOSS-AOSSOD
		ATTCONPF	ATTCNERR		ACSYSTR-ACDMFL
					ACSYSTR-ACCF3PFL
					ACSYSTR-ACERR
			ATTCNFLT		ACSYSTR-ACFLT
	LINEPERF	LINEFLT			PMTYP-PMTCCTOP **(NOTE 2)**
		LINEOUT			SYSPERF-LINCCTBU
	SLMPERF	SLMFAULT			SLM-SLMFLT
		SLMSOUT			SLM-SLMSBSU
		SLMMOUT			SLM-SLMMBSU
	TRKPERF	TRKFLT			PMTYP-PMTCCTOP (NOTE 2)
		INTRKOUT			TRK-SBU
					TRK-MBU **(NOTE 5)**
		OGTRKOUT			TRK-SBU
					TRK-MBU **(NOTE 6**)
		C7TRKCFL			ISUPCONN-ISCONUCE
					ISUPCONN-ISCONUCC
					ISUPCONN-ISCONUCA
					ISUPCONN-ISCONUCF
					ISUPCONN-ISCONCOT

Table 5-7 — SPMS Index Levels (TREETOPs) BILLPERF, CPRES, and FREQRES Subindices and OMs

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
BILLPERF	METERERR				MTRPERF-DTCALLP
					MTRPERF-DTXPM
					MTRPERF-DTFEAT
					MTRPERF-TIMESTO
					MTRPERF-DURERR
					MTRPERF-COUNTERR
					MTRPERF-MTRBKERR
					MTRPERF-MTRAUDER
					MTRPERF-RECYCFND
					MTRPERF-RECYCCLR
					MTRPERF-THQOVFL
					MTRPERF-THQERR
	AMABEVFL				AMA-AMAFREE
					AMA-AMAROUTE
CPRES	CCOCCUP				CP2-CPWORKU
	CCBOVFL				CP-CCBOVFL
	CPMAXBSY				CP-WAITDENY
	CPLOVFL				CP-CPLOOVFL
					CP-CPLPOVFL
	OUTBOVFL				CP-OUTBOVFL
	MULTBOVF				CP-MULTOVFL
	WAKEOVFL				CP-WAKEOVFL
	ECCBOVFL				CP2-ECCBOVFL
FTRQRES	FQAGOVFL				FTRQ-FTRQOVFL*
	FQOWOVFL				FTRQ-FTRQOVFL*
	FQ2WOVFL				FTRQ-FTRQOVFL*
	FQ4WOVFL				FTRQ-FTRQOVFL*
	FQ8WOVFL				FTRQ-FTRQOVFL*
	FQ16WOVFL				FTRQ-FTRQOVFL*

*REFERENCE Table 5-13

Table 5-8 — SPMS Levels (TREETOPs) EXTBLKS Subindices & OMs

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
EXTBLKS	FTREXT	PERMXOVF			EXT-EXTOVFL*
		CCISIXOV			EXT-EXTOVFL*
		TWCXOVFL			EXT-EXTOVFL*
		MTXHOVFL			EXT-EXTOVFL*
		CFWXOVFL			EXT-EXTOVFL*
		CSDDPXOV			EXT-EXTOVFL*
		ROTLPXOV			EXT-EXTOVFL*
		CWTXOVFL			EXT-EXTOVFL*
		IBNCQXOV			EXT-EXTOVFL*
		ALTADXOV			EXT-EXTOVFL*
		CFOXOVFL			EXT-EXTOVFL*
		FTRCTLXO			EXT-EXTOVFL*
		FTRDATXO			EXT-EXTOVFL*
		SDPATCXO			EXT-EXTOVFL*
		LTDXOVFL			EXT-EXTOVFL*
		KSHUNTXO			EXT-EXTOVFL*
		NSCXOVFL			EXT-EXTOVFL*
		DCRXOVFL			EXT-EXTOVFL*
		REGNSEMO			EXT-EXTOVFL*
		IBNIXOVF			EXT-EXTOVFL*
		LCOXOVFL			EXT-EXTOVFL*
		NCSXOVFL			EXT-EXTOVFL*
		ACCRSXOV			EXT-EXTOVFL*
		CDIVXOVF			EXT-EXTOVFL*
		E800TCXO			EXT-EXTOVFL*
		ISUPMSXO			EXT-EXTOVFL*
		SP250XOV			EXT-EXTOVFL*
		DMS250XO			EXT-EXTOVFL*
		RDBXFMTO			EXT-EXTOVFL*
		FTRXLAXO			EXT-EXTOVFL*
		PCFDXOVF			EXT-EXTOVFL*
		ACCSTXOV			EXT-EXTOVFL*
		HISCNTXO			EXT-EXTOVFL*
		HISDXOVF			EXT-EXTOVFL*
		PVNXOVFL			EXT-EXTOVFL*
		DPNSSXOV			EXT-EXTOVFL*
		AUXXOVFL			EXT-EXTOVFL*
		TCAPSXOV			EXT-EXTOVFL*
		TCAPLXOV			EXT-EXTOVFL*
		TCAPXLXO			EXT-EXTOVFL*
		PVNTCAXO			EXT-EXTOVFL*
		ICTFRMXO			EXT-EXTOVFL*
		TCAPMXOV			EXT-EXTOVFL*
		PVNTRMXO			EXT-EXTOVFL*
		DMS250BO			EXT-EXTOVFL*
		TPBXXOVF			EXT-EXTOVFL*
		SCSXOVFL			EXT-EXTOVFL*

Continued on next page

Table 5-8 — SPMS Levels (TREETOPs) EXTBLKS Subindices & OMs

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
EXTBLKS	BILLEXT	AOSSRUOV			EXT-EXTOVFL*
		NTRUOVFL			EXT-EXTOVFL*
		TOPSRUOV			EXT-EXTOVFL*
		CATPSRUO			EXT-EXTOVFL*
		SMDRRUOV			EXT-EXTOVFL*
		ASORUOVF			EXT-EXTOVFL*
		AVCDRRUO			EXT-EXTOVFL*
		MCDRRUOV			EXT-EXTOVFL*
		BCROVFL			EXT-EXTOVFL*
		BCLMRUO			EXT-EXTOVFL*
		NSGUOVF			EXT-EXTOVFL*
		CDRRUOV			EXT-EXTOVFL*
		OESRUOV			EXT-EXTOVFL*
		AVDSAROV			EXT-EXTOVFL*
		INTLROVF			EXT-EXTOVFL*
		OCCROVFL			EXT-EXTOVFL*
		ICAMAROV			EXT-EXTOVFL*
		SORUOVFL			EXT-EXTOVFL*
		ITOPSROV			EXT-EXTOVFL*
		DMS250EX			EXT-EXTOVFL*
		CDRMTXOV			EXT-EXTOVFL*
		RU250XOV			EXT-EXTOVFL*
		INTLCCMO			EXT-EXTOVFL*

*Reference Table 5-13

Table 5-9 — SPMS Levels (TREETOPs) SRVCTRES and CHANRES Subindices and OMs

LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	LEVEL 6	OM GROUP REGISTER
SRVCTRES		ANNOVFL			ANN-ANNOVFL
		STNOVFL			STN-STNOVFL
		UTROVFL			UTR-UTRQOVFL
		ESUPOVL			ESUP-DESOVFL
		SPSVOVFL			SVCT-SVCQOVFL
		CONFRES	CONF3OVF		CF3P-CNFQOVFL
			CONF6OVF		CF6P-CF6QOVFL
		RCVRES	RCVRMFOV		RCVR-RCUQOVFL
			RCVRDGOV		RCVR-RCVQOVFL
			RCVRATDO		RCVR-RCVQOVFL
			RCVRCNOV		RCVR-RCVQOVFL
			RCVRMCSO		RCVR-RCVQOVFL
			MF3OOOVF		RCVR-RCVQOVFL
			DGTOOOV		RCVR-RCVQOVFL
CHANRES		NETCHOVF			OFZ-OUTMFL
					OFZ-TRMMFL
					AVOFZ-ALTRMMFL **(NOTE 3)**
		LPMCHAN			OFZ-TRMBLK
					LMD-ORIGBLK **(NOTE 2)**

Notes for Tables 5-2 through 5-9

1. ORIGLNOUT is a derived estimate of lost originating calls.

2. Totalized for all the units in the office.

3. OM in brackets is subtracted.

Continued on next page

4. XXX may be any peripheral module type in the office totalized for all of the same type (dual processor). In addition, XXX may be XPM, which provides a summary of all dual-processor peripheral modules in the office, totalized only for dual-processor peripheral modules.

5. Totalized for all incoming and 2-way trunk groups in the office.

6. Totalized for all outgoing trunk groups in the office.

7. SOS based Peripheral Module Performance has been added to the maintenance performance branch of SPMS. SOS based Peripheral Performance is located under PMTOTPF. For an explanation of CCS7-related indices, see the "SS7 Overview and Maintenance" subsection within the *Preventive Maintenance* tab of this manual.

Figure 5-1 — ENET part of the SPMS Tree
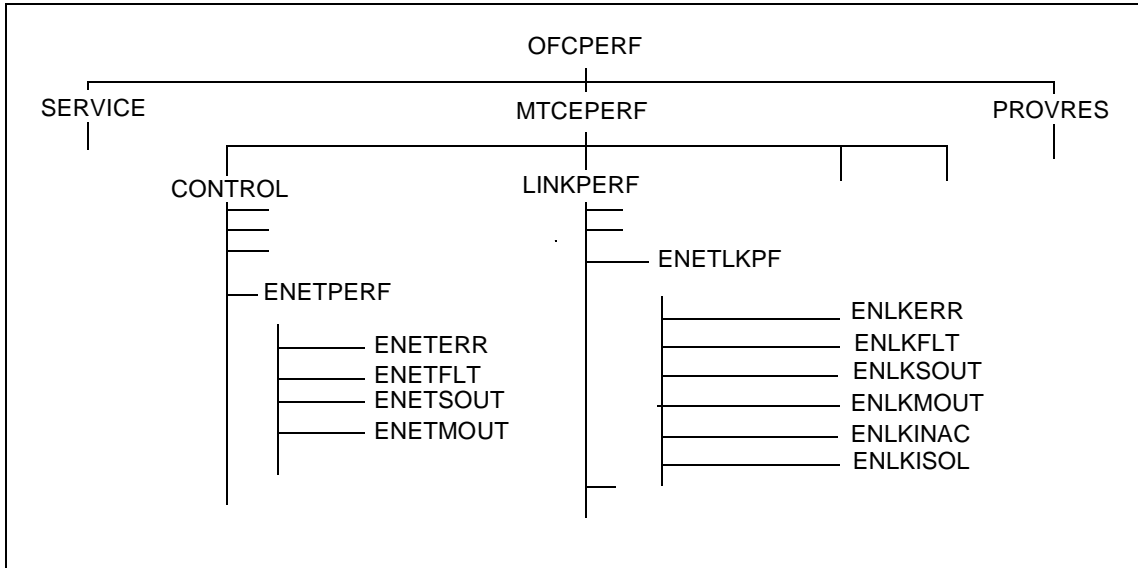
Table 5-10 — ENET System Performance—Part of SPMS

This section uses most of the fields from the first three groups above. This chart provides a description of the indices in Table 5-10.			
Index	**Name**	**Index type**	**Description**
ENETPERF	ENET system performance	Aggregate	Summary of the performance of the ENET system cards.
ENETERR	ENET System Errors	Basic	Monitors the number of errors detected in the ENET system cards.
ENETFLT	ENET System Faults	Basic	Monitors the number of errors detected in the ENET system cards.
ENETSOUT	ENET - System Busy Shelves	Basic	Monitors system busy ENET shelves.
ENETMOUNT	ENET - Manual Busy Shelves	Basic	Monitors manual busy ENET shelves.

Figure 5-2 — ENET system performance part of SPMS
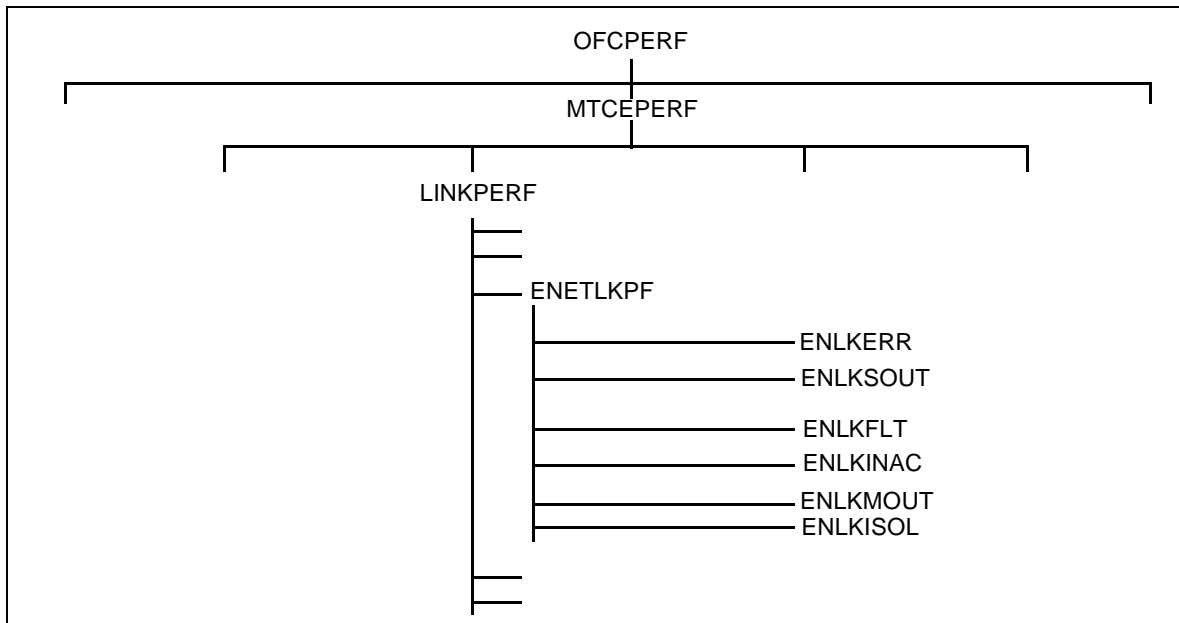
Table 5-11 — ENET Link Performance Indices

The term "link" is intended to include the ENET switching network as well as the P-side links. A description of the indices in Table 5-3 on the previous page.			
Index	**Name**	**Index type**	**Description**
ENLKPERF	ENET Link Performance	Aggregate	Summary of the performance of the ENET matrix cards and P-side links. Child indices: ENLKERR, ENLKFLT, ENLKSOUT, ENLKMOUT, ENLKNOAC, and ENLKISOL.
ENLKINAC	ENET - Inaccessible Paths	Basic	Monitors the number of inaccessible paths between P-side links due to out-of-service components in the ENET.
ENLKISOL	ENET - Isolated Peripherals	Basic	Monitors the number of isolated PMs due to out-of-service components in the ENET.
ENLKERR	ENET Link Errors	Basic	Monitors the number of errors occurring in the link components of the ENET. This includes the P-side links as well as the matrix card components (i.e.: crosspoint cards and paddle boards
ENLKFLT	ENET Link Faults	Basic	Monitors the number of hard faults occurring in the link components of the ENET.
ENLKSOUT	ENET - System Busy Link Components	Basic	Monitors system busy link components in the ENET.
ENLKMOUT	ENET - Manual Busy Link Components	Basic	Monitors manual busy link components in the ENET.

Figure 5-3 — ENET link performance part of SPMS

```
                              OFCPERF
                    |_____|_____|
        SERVICE
          |
          MTCESERV
          |___
          |___
          |___
          |    MTCCMPL
          |____|___
          |        |___ SPCHBLK
          |        |         |_____ NETBLK
          |        |         |_____|
          |        |___
          |
          |___ CUTOFFS
          |        |_____ INTEGFL
          |_____|___
```
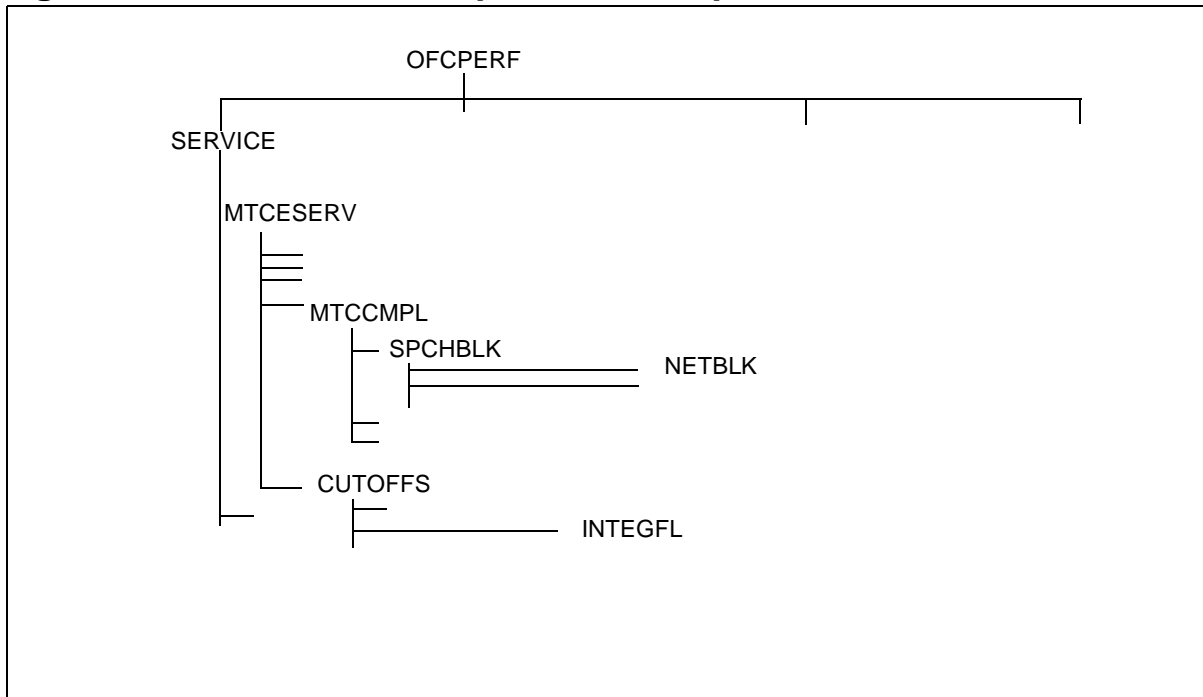
Figure 5-4 — Existing SPMS indices affected by ENET

```
                              OFCPERF
          |_____|_____|
                              MTCEPERF
              |_____|_____|_____|
        CONTROL
          |___
          |___
          |___
          |___ ENETPERF ___
          |        |_____ ENETERR
          |        |_____ ENETFLT
          |        |_____ ENETSOUT
          |        |_____ ENETMOUT
          |___
          |___
```
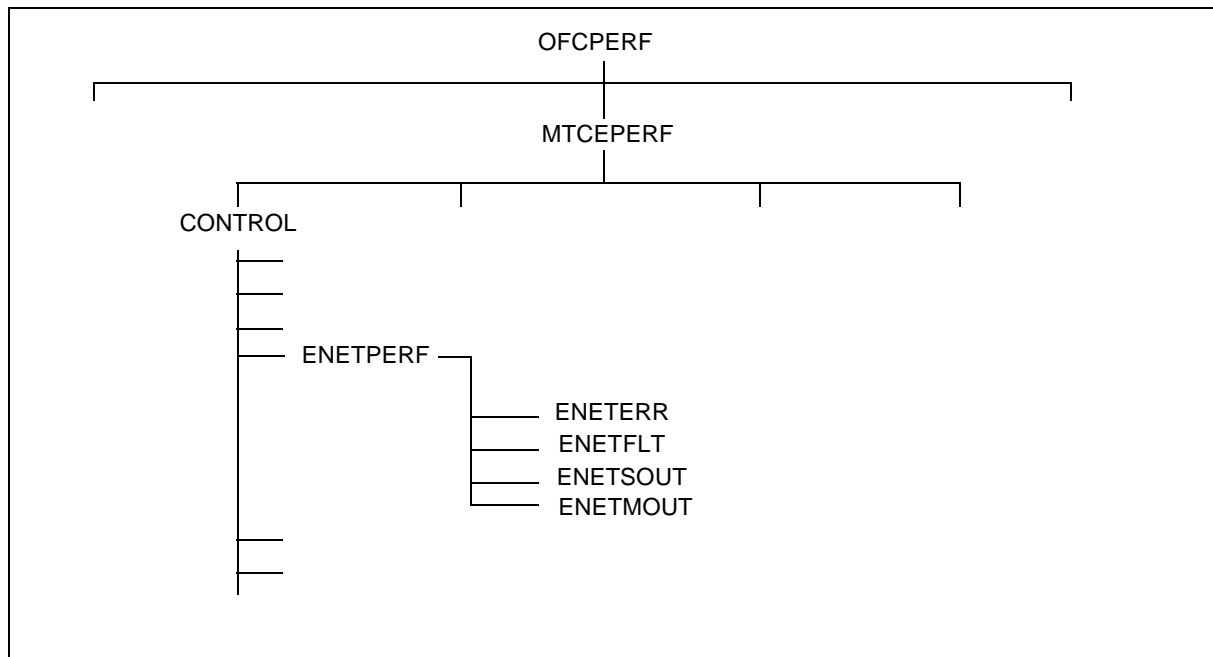
Table 5-12 — Association of OM group & register with SPMS basic index

SPMS Operational Measurements			
Basic Index	**Group**	**Register**	**Explanation**
C7LNKSFL	C7LINK1	C7LKFAIL	link SYNC features
C7LNKSFL	C7LINK1	C7STALFL	signaling terminal cannot be found
C7LNKSFL	C7LINK1	C7TLALFL	transmission link cannot be found
C7LNKSFL	C7LINK1	C7NETCOM	TL fails to connect with network
C7LNKSFL	C7LINK1	C7SLTFL	signaling link test failure
C7LNKOUT	C7LINK1	C7LKUNAU	link not available for service
C7LSOUT	C7LKSET	C7LKUNAU	linkset(s) out-of-service
C7RTDEGR	C7ROUTE	C7TFP	transfer prohibited
C7RTDEGR	C7ROUTE	C7FRCRER	forced routing procedures
C7RTOUT	C7ROUTE	C7RTUNAU	route unavailable (isolation)
C7RTSTCO	C7RTESET	C7RSCNGU	routeset congestion
C7RTSTOU	C7RTESET	C7RSUNAU	routeset unavailable (isolation)
C7MSULF	C7LINK2	C7MSUDSC	MSUs discarded—ST congestion
C7MSULF	C7LINK2	C7MSUDC-1	MSUs discarded—congestion level 1
C7MSULF	C7LINK2	C7MSUDC-2	MSUs discarded—congestion level 2
C7MSULF	C7LINK2	C7MSUDC-3	MSUs discarded—congestion level 3
C7SCCPMP	C7SCCP	C7RTFALL	MSUs received at SCCP but can't route
C7GTWERR	C7GTWSCR	MSUSCRER	MSUs causing screening errors at STP
C7TRKCFL	ISUPCONN	ISCONUCE	switch equipment overload far-end office
C7TRKCFL	ISUPCONN	ISCONUCC	no idle circuit in far-end office
C7TRKCFL	ISUPCONN	ISCONUCA	unsuccessful attempts - #invalid
C7TRKCFL	ISUPCONN	ISCONUCF	temporary fault far-end office
C7TRKCFL	ISUPCONN	ISCONCOT	first continuity check failure
SOSPMERR	PMTYP	PMTERR	hardware/software errors
SOSPMFLT	PMTYP	PMTFLT	failure rate
SOSPMMOU	PMTYP	PMTUMBU	manual outages
SOSPMSOU	PMTYP	PMTUSBU	system outage
SOSPMERR	PM1	PM1ERR	hardware/software errors
SOSPMFLT	PM1	PM1FLT	failure rate
SOSPMMOU	PM1	PM1SBU	manual outages
SOSPMSOU	PM1	PM1SBU	system outage

Table 5-13 — SPMS basic index OM group field to Office Parameter cross reference table

SPMS INDEX	OM FIELD	OFFICE PARAMETER
FREQRES, FTRQ OM GROUP		
FQAGOVFL	FTRQAGENTS	FTRQAGENTS
FQ0WOVFL	FTRQ0WAREAS	FTRQ0WAREAS
FQ2WOVFL	FTRQ2WAREAS	FTRQ2WAREAS
FQ4WOVFL	FTRQ4WAREAS	FTRQ4WAREAS
FQ8WOVFL	FTRQ8WAREAS	FTRQ8WAREAS
FQ16WOVFL	FTRQ16WAREAS	FTRQ16WAREAS
FTREXT, EXT OM GROUP		
PERMXOVF	PERM	NUMPERMEXT
CCISIXOV	CCIS_INWATS_BLOCKS	#_OF_CCIS_INWATS_BLOCKS
TWCXOVFL	TWC_EXTENSION_BLOCK	NO_OF_TWC_EXT_BLKS
MTXHOVFL	MTX_HANDOFF_BLOCK	HANDOFF_BLOCK_COUNT
CFWXOVFL	CFW_EXTENSION	CFW_EXT_BLOCKS
CSDDPXOV	CSDDSPERM	NUMCSDDSPERMEXT
ROTLPXOV	ROLT_PRIMING_BLOCK	ONE PER TEST PORT
CWTXOVFL	CUSTOM_CALLING_DATA	NO_OF_SC_EXT_BLKS
IBNCQXOV	IBNCQEXT	NUMIBNCQEXTBLK
ALTADXOV	ALTADDR_EXTENSION	FIXED AT 64
CFDXOVFL	CFD_EXTENSION	CFD_EXT_BLOCKS
FTRCTLXO	FEATURE_CONTROL_DATA	NO_OF_FTR_CONTROL_BLKS
FTRDATXO	FEATURE_DATA	NO_OF_FTR_DATA_BLKS
SDPATCXO	SDPATC_EXTENSION	NUMSDPATCEXTBLK
LTDXOVFL	LTD_EXT_DATA	FIXED AT 20
KSHUNTXO	KEY_SHORT_HUNT_EXT	KSHUNT_EXT_BLOCKS
NSCXOVFL	NSC_EXT_BLOCK	#_OFNSC_EXT_BLK
DCRXOVFL	DCR_EXT_FC	NO_DCR_EXT_BLKS
REGNSEMO	REGNSEMA	NUM_REGNSEMA_EXT_BLOCKS
Continued on next page		

Table 5-13 — SPMS basic index OM group field to Office Parameter cross reference table (continued)

SPMS INDEX	OM FIELD	OFFICE PARAMETER
REGNSEMO	REGNSEMA	NUM_REGNSEMA_EXT_BLOCKS
IBNIXOVF	IBN_INTL_XLA_EXT_BLOCK	NUM_IBN_IXLA_EXT_BLOCKS
LCOXOVFL	LCO_EXTENSION_BLOCK	NO_LOCAL_COIN_EXT_BLKS
NCSXOVFL	NCS_EXTENSION_BLK	NUMBER_NCS_EXTENSION_BLOCKS
ACCRSXOV	AUTOVON_CRS_BLOCK	FIXED AT 50
CDIVXOVF	CDIV_EXTENSION	CDIV_EXT_BLOCKS
E800TCXO	E800_TCAP_EXT_BLK	NO_OF_TRANSACTION_IDS
ISUPMSXO	ISUP_EXTENSION_BLOCK	NUM_ISUP_EXT_BLKS
SP250XOV	SCRPAD_EXTEN_BLK	NUMBER_ECCB_SCRATCHPAD_AREAS
DMS250XO	MCCS_EXTEN_BLK	NUMECCBS
RDBXFMTO	RDB_EXT_FMT	NUM_RDB_EXTS
FTRXLAXO	FEATURE_XLA_DATA	NO_OF_FTR_XLA_BLKS
PCFDXOVF	POTS_CFZ_EXTENSION	CFZ_EXT_BLOCKS
ACCSTXOV	ACCS_TCAP_EXT_BLK	ACCS_MAX_QUERIES
HISCNTXO	HISTORY_CONTROL_DATA	NO_OF_HIS_CONTROL_BLKS
HISDXOVF	HISTORY_DATA	NO_OF_HIS_DATA_BLKS
PVNXOVFL	PVN_EXT_BLK	NO_OF_PVN_EXT_BLK
DPNSSXOV	DPNSS_EXTENSION_BLOCK	NUMBER_OF_DPNSS_EXT_BLOCKS
AUXXOVFL	AUX_EXTENSION_BLK	NUMBER_AUX_EXTENSION_BLOCKS
TCAPSXOV	TC_AP_SMALL_EXT_BLK	NO_OF_SMALL_EXT_BLKS
TCAPLXOV	TC_AP_LARGE_EXT_BLK	NO_OF_LARGE_EXT_BLKS
TCAPXLXO	TC_AP_XLARGE_EXT_BLK	NO_OF_XLARGE_EXT_BLKS
PVNTCAXO	PVN_TCAP_EXT_BLK	NO_OF_PVN_EXTBLK
ICTFRMXO	ICT_EXT_BLOCK	NUM_ICT_EXT_BLKS
TCAPMXOV	TC_AP_MEDIUM_EXT_BLK	NO_OF_MEDIUM_EXT_BLKS
PVNTRMXO	PVN_TERM_EXT_BLK	NO_OF_PVN_TERM_EXTBLK
DMS250BO	DMS250_BBF_EXT_BLK	NO_OF_DMS250_BBF_EXT_BLK
TPBXXOVF	TPBX_EXTENSION	NUM_TPBX_EXT_BLKS
SCSXOVFL	SCS_EXTENSION	NUM_OF_SCS_EXTBLKS
Continued on next page		

Table 5-13 — SPMS basic index OM group field to Office Parameter cross reference table (continued)

SPMS INDEX	OM FIELD	OFFICE PARAMETER
BILLEXT, OM GROUP EXT		
AOSSRUOV	AOSS_RU	AOSS_NUM_RECORDING_UNITS
NTRUOVFL	NT_RECORDING_UNIT	#_OF_NT_RECORDING_UNITS
TOPSRUOV	TOPSRO	TOPS_NUM_RU
CATRSUO	CAMATOPS_RU	TOPS_NUM_CAMA_RU
SMDRRUOV	SMDR_RECORDING_UNIT	NO_OF_SMDR_REC_UNITS
ASORUUOVF	ASO_RECORDING_UNIT	FIXED AT 128
AVCDRRUO	AVCDRU	AVCDR_RU_COUNT
MCDRRUOV	MCDR_RECORDING_UNIT	NO_OF_MCDR_REC_UNITS
BCRUOVFL	BC_RECORDING_UNIT	#_OF_BC_AMA_UNITS
BCLAMRUO	BC_LAMA_REC_UNIT	#_OF_BC_LAMA_REC_UNITS
NSGRUOVF	NSG_RECORDING_UNIT	NO_OF_REC_UNITS
CDR3RUOV	CDR300_RECORDING_UNIT	NUMBER_OF_CDR_UNITS
OESDRUOV	OESD_RECORD_UNIT	RESERVED FOR OESD OFFICES
AVDSAROV	ASARU	DSA_RU_CNT
INTLROVF	INTL_RECORDING_UNIT	NUM_INTL_RECORDING_UNITS
OCCROVF	OOCRU	OCC_NUM_RU
ICAMAROV	ICAMA_RECORDING_UNIT	NUM_ICAMA_RECORDING_UNITS
SORUOVFL	SO_RECORD_UNIT	KSAMA_NO_OFRU_FOR_SO
ITOPSROV	ITOPSRU	TOPS_NUM_RU
DMS250EX	EOPS_RECORDING_UNIT	NUM_OF_EOPS_REC_UNITS
CDRMTXOV	MTX_RECORDING_UNIT	MTX_CDR_RU_COUNT
RU250XOV	RU250_RECORDING_UNIT	NO_OF_DMS250_REC_UNITS
INTLCCMO	INTL_CCMTR_EXT_BLOCK	NUM_CCMTR_EXT_BLOCKS

Exhibit A   SPMS Sample Display

```
                      L ! 990215   99 JAN   99 FEB
                        !           TO DATE
TOTATT (K)              !     766    38853    45321
                        !
                      --!----------------------------
OFCPERF                A !  99.7     98.9     99.3
..SERVICE              A !  99.8     99.1     99.3
....MTCESERV           A !  99.8     98.9     99.2
......MTCACCS          A ! 100.0     98.8     99.4
........CCRESET        B ! 100.0    100.0    100.0
........ORGLNOUT       B !  99.9     99.3     99.4
........ORGPMBLK       B ! 100.0     96.1     98.2
......INSIGFL          A !  97.8     98.8     99.2
........TINSIGFL       B ! 100.0     99.8    100.0
........LINSIGFL       B !  94.6     97.3     97.9
......MISCFL           B ! 100.0     99.4     98.3
......MTCCMPL          A ! 100.0     97.6     98.7
........SPCHBLK        A ! 100.0     97.9     99.1
..........NETBLK       B ! 100.0     99.3    100.0
..........TRMPMBLK     B ! 100.0     97.0     98.5
........LINOUTFL       A !  99.9     99.5     99.6
..........TLINOUT      B ! 100.0     99.9    100.0
..........RNGFL        B !  99.7     99.0     99.2
........OUTSIGFL       B ! 100.0     95.0     97.3
......CUTOFFS          A !  99.9     99.4     99.4
........CTLCTO         A ! 100.0     99.8     99.8
..........CCCTO        B ! 100.0    100.0    100.0
..........PMCTO        B ! 100.0     99.6     99.6
........INTEGFL        B !  99.8     98.9     98.9
......C7MSUPF          A ! 100.0    100.0    100.0
........C7MSUFL        B ! 100.0    100.0    100.0
........C7SCCPMP       B ! 100.0    100.0    100.0
....PROVSERV           A !  99.7     99.4     99.4
......PROVACCS         A !  99.7     99.6     99.6
........DTSR           B !  99.4     98.8     99.3
........PMDNY          B ! 100.0    100.0    100.0
........MISCDNY        B !  99.7     99.6     99.5
......MISCBLK          B ! 100.0    100.0    100.0
......TRKPROV          A !  99.1     98.0     98.2
........NWMBLK         B !  96.4     94.9     93.9
........FINALBSY       B !  99.8     98.8     99.3
......C7GTWERR         B ! 100.0    100.0    100.0
```

Continued on next page

Exhibit A   SPMS Sample Display (continued)

```
..MTCEPERF              A !  99.4     98.7      99.0
....CONTROL             A !  99.7     98.9      99.2
......CMPERF            A ! 100.0     98.0      98.6
........CMERRINT        B ! 100.0    100.0     100.0
........CMFLT           B ! 100.0    100.0     100.0
........CMNOSYNC        B ! 100.0     94.9      96.4
......MSPERF            A ! 100.0    100.0      98.8
........MSERR           B ! 100.0    100.0      97.5
........MSFLT           B ! 100.0    100.0     100.0
........MSUSOUT         B ! 100.0    100.0     100.0
........MSUMOUT         B ! 100.0    100.0      94.6
......MSCDPERF          A ! 100.0     99.3      99.8
........MSCDERR         B ! 100.0    100.0     100.0
........MSCDFLT         B ! 100.0    100.0     100.0
........MSCDSOUT        B ! 100.0    100.0     100.0
........MSCDMOUT        B ! 100.0     94.6      98.3
......IOCPERF           A ! 100.0    100.0     100.0
........IOCERR          B ! 100.0    100.0     100.0
........IOCFLT          B ! 100.0    100.0     100.0
........IOCUSOUT        B ! 100.0    100.0     100.0
........IOCUMOUT        B ! 100.0    100.0     100.0
......ENETPERF          A !  97.7     98.7      99.6
........ENETERR         B ! 100.0    100.0     100.0
........ENETFLT         B ! 100.0    100.0     100.0
........ENETSOUT        B !  93.7     99.0      98.9
........ENETMOUT        B ! 100.0     94.8     100.0
......PMPERF            A !  99.7     98.5      99.6
........PMTOTPF         A !  99.7     98.5      99.6
..........PMTOTERR      B !  98.5     99.6      99.7
..........PMTOTFLT      B ! 100.0     98.2      99.6
..........PMTOUSOU      B ! 100.0     98.1      99.2
..........PMTOUMOU      B ! 100.0     98.6     100.0
........XPMPERF         A !  99.1     99.0      99.8
..........XPMERR        B !  95.7     99.1      99.2
..........XPMFLT        B ! 100.0     98.9      99.8
..........XPMUSOUT      B ! 100.0     99.7     100.0
..........XPMUMOUT      B ! 100.0     97.5     100.0
........LMPERF          A ! 100.0     96.2      95.3
..........LMERR         B ! 100.0     97.9      98.4
..........LMFLT         B ! 100.0     92.9      92.8
..........LMUSOUT       B ! 100.0     98.0      96.8
..........LMUMOUT       B ! 100.0    100.0      94.9
........LCMPERF         A ! 100.0     97.0      99.0
..........LCMERR        B ! 100.0    100.0     100.0
..........LCMFLT        B ! 100.0     96.2      99.5
..........LCMUSOUT      B ! 100.0     94.9      97.2
..........LCMUMOUT      B ! 100.0     99.0     100.0
```
Continued on next page

Exhibit A   SPMS Sample Display (continued)

```
........TMPERF          A ! 100.0    96.7    98.2
..........TMERR         B ! 100.0   100.0    99.7
..........TMFLT         B ! 100.0    94.9    96.8
..........TMUSOUT       B ! 100.0    95.5    98.4
..........TMUMOUT       B ! 100.0   100.0    99.8
........NDPERF          A ! 100.0   100.0    99.8
..........NDTOERR       B ! 100.0   100.0    99.2
..........NDTOFLT       B ! 100.0   100.0   100.0
..........NDTOOUT       B ! 100.0   100.0   100.0
........SOSPMPF         A ! 100.0    99.9   100.0
..........SOSPMERR      B ! 100.0   100.0   100.0
..........SOSPMFLT      B ! 100.0   100.0   100.0
..........SOSPMSOU      B ! 100.0   100.0   100.0
..........SOSPMMOU      B ! 100.0    99.6   100.0
......SWINTEG           A !  99.9    99.6    99.2
........PMSWINTG        A ! 100.0   100.0   100.0
..........PMSWERR       B ! 100.0   100.0   100.0
..........PMTRAP        B ! 100.0   100.0   100.0
........CCSWINTG        A !  99.6    99.5    98.2
..........CCSWERR       B !  98.3    99.2    99.2
..........TRAPS         A ! 100.0    99.6    97.8
............NONCPTRP     B ! 100.0    99.8   100.0
............CPTRAPS      B ! 100.0    99.3    95.0
........CPSUICDS        B ! 100.0    99.2    98.6
........CCINIT          A ! 100.0   100.0   100.0
..........CCWINIT       B ! 100.0   100.0   100.0
..........CCCINIT       B ! 100.0   100.0   100.0
....LINKPERF            A !  98.9    98.5    99.0
......MSLNKPF           A !  99.0   100.0    99.3
........MSLNKERR        B !  94.9    99.9    99.7
........MSLNKFLT        B ! 100.0   100.0    98.7
........MSLNKSUO        B ! 100.0   100.0    99.6
........MSLNKMUO        B ! 100.0   100.0   100.0
......IOCLNKPF          A ! 100.0   100.0   100.0
........IOCLNKER        B ! 100.0   100.0   100.0
........IOCLKSUO        B ! 100.0   100.0   100.0
........IOCLKMUO        B ! 100.0   100.0   100.0
......ENETLKPF          A !  98.6    98.1    99.2
........ENLKERR         B !  99.9    99.6    99.8
........ENLKFLT         B ! 100.0    99.6    99.6
........ENLKSOUT        B !  93.2    98.8    98.9
........ENLKMOUT        B ! 100.0    97.5   100.0
........ENLKINAC        B ! 100.0    98.9   100.0
........ENLKISOL        B ! 100.0    96.3    98.4
```

Continued on next page

Exhibit A SPMS Sample Display (continued)

```
......PMLNKPF           A !  98.0    96.2    97.7
........PMLNKERR        B !  93.2    94.3    99.2
........PMLNKFLT        B ! 100.0    94.9    95.0
........PMLKSUOU        B ! 100.0    99.2    98.8
........PMLKMUOU        B ! 100.0    98.8    99.8
......C7LNKPF           A ! 100.0   100.0    99.3
........C7LSOUT         B ! 100.0   100.0    99.0
........C7LINK          A ! 100.0   100.0    99.8
..........C7LNKSFL      B ! 100.0   100.0    99.9
..........C7LNKOUT      B ! 100.0   100.0    99.7
....TERMNALS           A !  99.1    98.3    98.4
......IODEV            A ! 100.0   100.0   100.0
........MTUPERF         A ! 100.0   100.0   100.0
..........MTUERR        B ! 100.0   100.0   100.0
..........MTUFLT        B ! 100.0   100.0   100.0
..........MTUSOUT       B ! 100.0   100.0   100.0
..........MTUMOUT       B ! 100.0   100.0   100.0
........DDUPERF         A ! 100.0   100.0   100.0
..........DDUERR        B ! 100.0   100.0   100.0
..........DDUFLT        B ! 100.0   100.0   100.0
..........DDUSOUT       B ! 100.0   100.0   100.0
..........DDUMOUT       B ! 100.0   100.0   100.0
........CONSOLPF        A ! 100.0    99.7    99.5
..........CSLERR        B ! 100.0    99.2    98.4
..........CSLSOUT       B ! 100.0    99.8    99.6
..........CSLMOUT       B ! 100.0   100.0   100.0
......SRVCCTPF          A !  99.9    99.0    98.5
........ANNSTNPF        B ! 100.0   100.0    99.8
........CONFPERF        A !  99.5    96.1    96.3
..........CNF3PERF      B ! 100.0    96.0    96.0
..........CNF6PERF      B !  99.0    96.1    96.5
........RCVRPERF        B ! 100.0   100.0    98.2
........SPECSVPF        B ! 100.0   100.0   100.0
......OPPOSPF           A !  99.8    94.6    97.4
........ATTCONPF        A !  99.8    94.6    97.4
..........ATTCNERR      B !  98.9    95.0   100.0
..........ATTCNFLT      B ! 100.0    94.5    96.8
......SLMPERF           A ! 100.0   100.0   100.0
........SLMFAULT        B ! 100.0   100.0   100.0
........SLMSOUT         B ! 100.0   100.0   100.0
........SLMMOUT         B ! 100.0   100.0   100.0
......LINEPERF          A !  98.9    98.7    98.9
........LINEFLT         B !  99.4    99.6    99.9
........LINEOUT         B !  98.4    97.7    97.9
```

Continued on next page

Exhibit A   SPMS Sample Display (continued)

```
......TRKPERF           A !  97.3     98.5     98.3
........TRKFLT          B ! 100.0    100.0    100.0
........INTRKSOU        B !  94.9    100.0     98.5
........INTRKMOU        B !  98.9     99.4    100.0
........OGTRKSOU        B !  97.9     98.1     99.6
........OGTRKMOU        B !  99.7     99.8    100.0
........C7TRKCFL        B !  94.5     94.2     92.6
......CARRPERF          A !  97.7     96.8     96.5
........CARRERR         B ! 100.0     99.4     94.8
........CARRFLT         B !  94.3     94.8     95.3
........CARRSOUT        B !  98.8     94.9     98.8
........CARRMOUT        B ! 100.0     99.5     99.7
......C7RTPERF          A ! 100.0     99.9     98.9
........C7ROUTE         A ! 100.0     99.8     98.0
..........C7RTDEGR      B ! 100.0     99.5     97.6
..........C7RTOUT       B ! 100.0    100.0     98.3
........C7RTSET         A ! 100.0    100.0     99.8
..........C7RTSTCO      B ! 100.0    100.0    100.0
..........C7RTSTOU      B ! 100.0    100.0     99.5
....BILLPERF            A ! 100.0    100.0    100.0
......AMADEVFL          B ! 100.0    100.0    100.0
..PROVRES               A !  99.6     98.6     99.5
....CPRES               A ! 100.0    100.0    100.0
......CCBOVFL           B ! 100.0    100.0    100.0
......CPLOVFL           B ! 100.0    100.0    100.0
......MULTBOVF          B ! 100.0    100.0    100.0
......WAKEOVFL          B ! 100.0    100.0    100.0
......CPMAXBSY          B ! 100.0    100.0    100.0
......CCOCCUP           B ! 100.0    100.0    100.0
....FTRQRES             A ! 100.0    100.0    100.0
......FQAGOVFL          B ! 100.0    100.0    100.0
......FQ2WOVFL          B ! 100.0    100.0    100.0
......FQ4WOVFL          B ! 100.0    100.0    100.0
......FQ8WOVFL          B ! 100.0    100.0    100.0
......FQ16WOVF          B ! 100.0    100.0    100.0
....EXTBLKS             A ! 100.0    100.0    100.0
......FTREXT            A ! 100.0    100.0    100.0
........PERMXOVF        B ! 100.0    100.0    100.0
........CFWXOVFL        B ! 100.0    100.0    100.0
........CWTXOVFL        B ! 100.0    100.0    100.0
........IBNCQXOV        B !    NA    100.0    100.0
........CFDXOVFL        B ! 100.0    100.0    100.0
........FTRCTLXO        B ! 100.0    100.0    100.0
........LTDXOVFL        B ! 100.0    100.0    100.0
```

Continued on next page

Exhibit A   SPMS Sample Display (continued)

```
........KSHUNTXO          B !  100.0      100.0      100.0
........FTRXLAXO          B !  100.0      100.0      100.0
........PCFDXOVF          B !  100.0      100.0      100.0
........HISCNTXO          B !  100.0      100.0      100.0
........TCAPSXOV          B !    NA       100.0      100.0
........TCAPXLXO          B !  100.0      100.0      100.0
....SRVCTRES              A !   98.2       98.0       98.4
......ANNOVFL             B !  100.0       99.4       99.9
......STNOVFL             B !   89.7   *   91.1       90.8
......UTROVFL             B !  100.0      100.0      100.0
......CONFRES             A !  100.0      100.0      100.0
........CONF3OVF          B !  100.0      100.0      100.0
........CONF6OVF          B !  100.0      100.0      100.0
......RCVRES              A !  100.0       98.9      100.0
........RCVRMFOV          B !  100.0      100.0      100.0
........RCVRDGOV          B !  100.0       97.8      100.0
....CHANRES               A !  100.0       95.3       99.2
......NETCHOVF            B !  100.0       94.8      100.0
......LPMCHAN             B !  100.0       96.0       98.3



                              end
```

Real Time Performance Indicators

This subsection briefly describes CPU real time capacity, tools available to monitor CPU as well as XPM real time performance, and Dial Tone Speed Recording (DTSR). For details beyond what is described within this subsection, reference NTP 297-1001-304, *DMS-100F Capacity Administration Manual* and NTP 297-1001-305, *DMS-100F Memory Administration Guide*.

The following topics are described within the NTP 297-1001-304, *DMS-100F Capacity Administration Manual*:

- Understanding capacity administration
- Administering CPU real time capacity
- Administering line peripheral capacity
- Administering service circuit capacity
- Administering trunk peripheral capacity
- Operational measurements used to evaluate capacity
- Capacity tracking work sheets

What is CPU real time capacity?

The actual time that the Central Processing Unit (CPU for the DMS-Core or SuperNode) perform their functions is called *real time*. The real time is divided into two main categories: call processing time and noncall processing time (see the following figure for a break down of the time). The categories include work time for the acceptance of call origination and call progression to completion or treatment. The CPU is usually performing a combination of call processing and noncall processing activities. When no call requests are being received, the CPU remains active for 100 percent of the period by using the entire time on noncall activities. For this subsection, "CPU" applies to the SuperNode switch.

The noncall processing category can be divided into subcategories of work that can be deferred, and work that cannot be deferred. Work that can be deferred is postponed (if there are sufficient requests for call processing) until there is leftover call processing time in which to perform the work. Work that cannot be deferred is activity that the CPU must perform during each cycle of the system clock, referred to as overhead. The percentage of real time used for overhead depends on the type and number of fea-

tures loaded, and the requirements for maintenance input/output devices. Theoretically, up to 31 percent of real time can be used by overhead if the switch is equipped for all features. In practice, switches do not contain all features available; therefore, the real time used for overhead is somewhere between the minimum and maximum values. Each switch configuration should be evaluated on its design and load to determine its overhead requirements.

Call processing occupancy

The switch architecture provides distributed processing over three switching stages controlled by the CPU. The capacity of the CPU is defined in terms of overhead and call processing occupancies. The overhead occupancy includes nondeferrable priority processes, such as task assignment, scheduling, and system integrity; and deferrable functions such as operations, administration, and maintenance (OA&M), and auditing routines. The call processing occupancy includes the originating call processes and the incoming system call processes and related tasks such as call request interrupt.

The maximum amount of real time available for call processing in a SuperNode central call processing unit (CPU) that has a minimum of 14% overhead is 86% (100% - 14%). Refer to the following figure for an illustration of real time availability.

Figure 5-5   Real time call processing availability
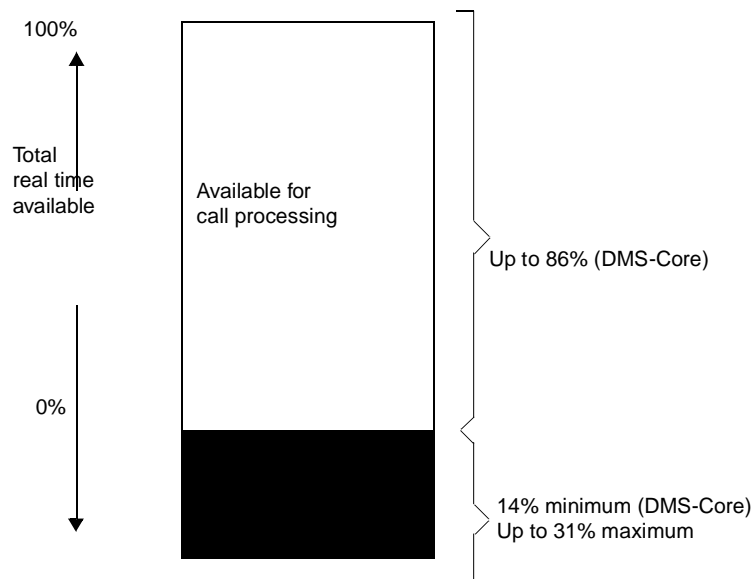
Real Time capacity tools

Automated tools

Several automated tools are available to the administrator that will aid in the monitoring of capacity. Nortel Networks developed these tools to assist in the initial provisioning of an office and for use in the ongoing surveillance of a working switch.

REAL::TIME

REAL::TIME is a PC program designed to provide an estimate of the DMS-100 Family CPU real time requirements. The DMS-100 switch provides distributed processing over many switching entities. The call attempt capacity of each of these switching entities must be predicted to establish operating guidelines. These guidelines are used to determine the loading levels for specific applications, including residential services. The real time can be predicted by using the anticipated call mix and timing per call. Using traffic criteria along with detailed office provisioning data, REAL::TIME generates an estimated occupancy for the central processor. REAL::TIME can be used in the following office configurations:

- DMS-100 plain old telephone service (POTS), MDC (including MADN), or both in an equal access end office (EAEO)
- DMS-200 in an access tandem operation
- DMS-100/200 in a combination of the above
- TOPS applications
- Signaling System #7 trunking applications
- Enhanced 800 Service
- Integrated Services Digital Network applications

For more information on this tool, see the *REAL::TIME User's Guide.*

REAL::QUICK

REAL::QUICK is an abbreviated form of REAL::TIME. Some assumptions and considerations are applicable to each processor. If there is a significant variance from these assumptions and considerations, a more detailed study should be performed using PRTCALC or REAL::TIME.

PRTCALC

PRTCALC is a PC program designed to provide an estimate of DMS-100 Family peripheral real time requirements and can be used to calculate the real time call attempt capacity for peripheral modules. PRTCALC is composed of three sections:

- an input section used to organize the controller call data and feature requirements.

- a work sheet section that contains the PRTCALC call mix calculations. The call types derived from the input data are combined with the pre-call timings to determine the real time requirements.
- an output section that is a summary of both the input and the work sheet calculations.

Input for PRTCALC comes either from projected/forecasted data based on current operational measurement trends, or from inputs to the NT-ACCESS tool.

ACTIVITY tool

The *ACTIVITY* tool is part of the Real Time Performance Indicators feature package (NTX291AA) and provides information on:

- the amount of traffic being handled
- CPU occupancy for various types of system activities
- grade of service
- overload protection
- dial tone speed

ACTIVITY is a subsystem off the MTC level of the MAP and provides an on-screen display that gives minute-by-minute indications on the five areas listed above. Besides display indications, logs are generated for ACTIVITY measurements. The ACT100 log provides a summary for data collected over a 15 minute period. The ACT101 log is generated to inform the user if ACTIVITY has to be shut down due to a transient mismatch in the switch.

NOTE: The ACTIVITY tool, when running, uses up to "three percent" of call processing for the SuperNode. A more accurate evaluation of real time can be made with the ACTIVITY tool turned off. Reference NTP 297-1001-304, *DMS-100F Capacity Administration Guide*, for a data evaluation procedure using OMs, an Average Work Time (AWT) formula, and the CPStatus tool.

For details on the operation of the ACTIVITY tool and its commands, see NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide.*

CPStatus tool

For a more accurate measurement of CPU capacity than the ACTIVITY tool can provide, use the CPStatus tool. This tool indicates switch performance according to the switch's capacity threshold, or engineering level. This is done by measuring all CPU occupancies and calculating the remaining CPU time available for call processing.

CPStatus can be accessed at any level of the MAP by entering command CPSTAT, or entering CPSTATUS at the MTC level of the MAP. CPStatus is also part of the Network Management (NWM) level of the MAP.

The BNR Reduced Instruction Set Computing (BRISC) for SuperNode provides a real time performance gain of 2.5 times over the NT9X13BC CPU. The BRISC processor usage is reported through the CI level CPSTAT command and the MAP level CPSTATUS level command.

For details on the operation of the CPStatus tool, see NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*, and NTP 297-1001-453, *DMS-100F Network Management System Reference Manual.*

XPM real time and performance tool

When XPMs go into an active overload, the following indicators notify personnel of the event:

- operational measurements
- log messages
- PM Activity tool (PERFORM)
- service indications with SPMS
- dial tone delays
- matching loss
- customer reports

PERFORM tool

PERFORM is available in feature packages NTX827, or NTX750 for ISDN. The PERFORM tool can be accessed off the PM level of the MAP by posting a PM and entering the PERFORM command. PERFORM displays information about processors (Master and Signalling processors) of the posted PM, and dial tone and post dialing delays.

Posted PMs include LGC, LTC, DTC, DTCI, or RCC, including node type LGC or LTC equipped with ISDN Signalling Preprocessor (ISP) and DCH cards for ISDN BRI services. Displayed results for PRI call types are displayed when monitoring LTC or DTCI peripherals. In BCS35, the ISP sublevel was added to the DTCI and LTC XPMs. A PRFM207 log can be started from the ISP sublevel to provide activity data for the selected XPM.

From the PERFORM level, access is provided to:

- PMACT, which provides XPM activity information
- DELAYS, which provides information about delays

The MAP display for PERFORM is similar to the activity display and uses the same commands. Reference NTP 297-1001-592, *DMS-100F Peripheral Modules Maintenance Guide* for a description of the PERFORM commands. Also, see NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*, for further information on the PERFORM level tool.

Dial Tone Speed Recording (DTSR)

Dial Tone Speed Recording (DTSR) measures the ability of a switch to return dial tone within three seconds after a subscriber goes off hook. A delay in receiving dial tone less than three seconds is generally acceptable by most operating companies. Over three seconds is unacceptable. Grade of service indicates the maximum permissible percentage of calls with a dial tone delay of more than three seconds. During the Average Busy Season Busy Hour (ABSBH), the limit is 1.5 percent, but during the High Day Busy Hour (HDBH), the limit rises to 20 percent of calls.

DTSR measurements

Series I PM DTSR measurements for PMs such as LMs and RLMs are made using test calls generated by the Central Control (CC). Series II PM DTSR measurements for LCMs and RLCMs are made using real calls. Dial tone speed measurements are recorded within the DTSR OM group for the whole office, in the DTSRPM OM group for individual PMs, and in the SITE OM group for remote PMs. With the use of the OM Threshold feature, the DTSR OM registers could be set to trigger real time alerts to slow dial tone problems.

Before BCS35, if a call has not received dial tone after three seconds and the caller goes on-hook, the DTSR OM register would not be incremented. In BCS35 the DTSR measurement is enhanced to include calls that are abandoned after three seconds and before receiving dial tone.

For analysis of dial tone speed problems or related receiver attachment delay recorder (RADR) problems, see NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*, and the "Troubleshooting with OMs" section. Also see the "ACTIVITY tool" previously mentioned within this subsection.

References

For further information on capacity, memory, loading, DTSR, and related subject matter, it is suggested that NTP 297-1001-304, *DMS-100F Capacity Administration Guide,* NTP 297-1001-305, *DMS-100F Memory Administration Manual*, and NTP 297-1001-306, *DMS-100F Loading Administration Guide* be referenced.

Service Analysis System

Overview

Service Analysis (SA) feature is an observation system that can be used to evaluate and analyze the quality of real time customer service provided by the operating company. Service is measured on call classifications, such as Direct Distant Dialing (DDD) or International DDD. Calls are selected on a random basis within a given call classification to obtain data that can be analyzed and evaluated.

Observations are performed by a service analyst by monitoring calls and noting the events in a call as they occur. A dial-back feature provides the capability to monitor calls from a remote location.

The events fall into the following two categories:

- analyst detected events, subjective information pertaining to a call as contributed by the analyst
- machine detected events, nonsubjective information pertaining to a call as contributed by the system

Analyst detected events

Analyst detected events are *subjective observations* about the quality of the call, such as noise and signal distortion. The system provides a listen-only monitor link which the analyst uses to listen for call events. The analyst observations are noted manually by entering commands on the appropriate menu of the MAP.

Machine detected events

Machine detected events consist of *nonsubjective data* such as connect time, transmission voice level, and signalling accuracy. Events are noted automatically by the system and immediately displayed on the screen.

SA operation

If equipped with the SA feature package, the Service Analysis system can be accessed from CI level of the MAP by entering MAPCI;SASELECT. Once logged in, the following series of MAP menus are available:

- SASelect (for selecting the call classification)

- LineSel (for entering the attributes of lines to be analyzed)
- SA (for displaying or printing selected call events)
- SAedit (for checking, editing, or printing noted call events)
- GWsel (for selecting gateway trunks for service)
- GWSA (for defining the attributes of gateway trunks to be service analyzed)
- Quota (for modifying any of the quotas for call types presented with gateway trunks)
- AOSSelect (for invoking service analysis of Auxiliary Operator Service System (AOSS), Traffic Operator Position System (TOPS), and Intertoll (IT) type incoming groups that route to an AOSS position for directory assistance)

SA printouts

A log message printout can be obtained at the SA or SAedit MAP levels by entering the PRINT command. This generates an SA201 through SA205 log based upon the service analyst position one through five. Within the log is a 58 character comment field that is provided by the analyst as needed.

SA references

NTP 297-1001-471, *DMS-100F Service Analysis*, that provides the details that support the Service Analysis feature has been canceled.

DMSMON

Overview

The DMS Monitoring (DMSMON) System was initially developed to compare the performance of a new software release with a previous version in the office. However, since its release, DMSMON has proven to be a useful analysis tool in determining office performance and highlighting potential problem areas in the switch. The feature displays information about patches, restarts, memory usage, switch downtime, high watermark values, and counts of logs, traps, software errors, and mismatches. If needed, reports on the configuration of PMs, the types and numbers of memory cards, and counts of hardware and other fixed items can be obtained. From this information, a DMSMON analyst could determine areas of concern before they become serious problems.

DMSMON operation

DMSMON can be accessed at the MAPCI level by entering the DMSMON command. Once accessed, all of the DMSMON commands are available for use.

Following is a list of DMSMON commands and a brief description of each one:

Table 5-14 — DMSMON commands

COMMAND	DESCRIPTION
DUMPALL	Dump the following information: • counts of major OMs • log counts • number of restarts and associated downtime • traps, software errors, and associated downtime • configuration of PMs • equipment counts • memory use • PM loads on the switch • new patches • high water CP occupancy • high-water mark for office parameters • digit block counts
OMS	counts major OMs
LOGCOUNT	counts log occurrences
RESTARTINFO	reports number of restarts and associated downtime
LOGBUFFER	dumps the Traps, SWERRs, and MM buffers

Table 5-14 — DMSMON commands (continued)

COMMAND	DESCRIPTION
PMCONFIG	displays the office PM configuration
EQPCOUNTS	displays the office equipment counts
MEMORY	displays the memory use
PMLOADS	displays the PM loads currently available
ASSESS	displays normalized peg counts
HIGHPARMS	displays the high-water marks for office parameters
COUNT	executes the count procedures
NEWPATCH	lists the new patches applied to the switch
HIGHCPOCC	displays non-BRISC high water CP occupancy
HIGHCAP	displays BRISC high water CP occupancy
HIGHLOGS	displays the 20 logs most frequently issued
OPR	creates an office performance report
DBLOCKS	displays digit block counts
RESET	can be entered with any of the following parameters:
RESET ALL	resets: OMs, log counts, and restarts to 0, and sets the new patch date to the current date
RESET OMS	resets the OMs to 0
RESET LOGCOUNT	resets the log counts to 0
RESET RESTARTINFO	resets the number of restarts to 0
RESET NEWPATCH	sets the new patch date to the current date
Note: Enter reset commands in the form: RESET [parameter] (for example: RESET OMS).	

CAUTION:
POSSIBLE LOSS OF DATA
When the RESET command is used, all accumulated data in the specified DMSMON registers is permanently deleted.

DMSMON can be reviewed daily, weekly, or monthly. The manual comparison of printed data can be performed at any interval the operating company chooses. The data can be left to accumulate or be reset after the manual review.

DMSMON references

The best source of information for DMSMON can be found in NTP 297-1001-318, *DMS-100F Service Problem Analysis Administration Guide*. For details on the DMSMON commands, see NTP 297-1001-822, *DMS-100F Commands Reference Manual*.

Maintenance Managers Morning Report

Overview

The Maintenance Managers Morning Report feature is also referred to as the AM Report (AMREP) or "Good Morning Report." Sometimes this software feature has been confused with the "SWSTATUS" store file program that was developed as a "Good Morning Report."

This feature provides a 24 hour automated summary log report of performance, administrative, and maintenance information for the DMS switch. The log report can be generated automatically at a scheduled time, or it can be generated on request from the MAP. NTP 297-1001-535, *DMS-100F Maintenance Managers Morning Report* provides the support for this feature.

The "Maintenance Managers Morning Report" is generated as an OMRS log and contains the following types of information:

- SPMS indicators (if feature is present)
- Call processing performance
- CPU occupancy (high-water mark)
- PM SWACT and Takeover information
- Network Integ fail counts
- Trap and SWERR counts
- Focus Maintenance and OM log count (if features are present)
- ALT results
- ATT results
- Outage information
- CM image dump results
- PRSU summary information (XPM Post Release Software Updates)
- XPM REX test information
- TABAUDIT information
- Outage information

Setup

The following is a guide for implementing AMREP. The first step is to verify that the feature has been turned on in table OFCOPT. To accomplish this, enter table OFCOPT and position on tuple AMREP_ACTIVE, if set to "N", then change to "Y". This is a write restricted tuple. If you are unable to change the tuple, contact your next level of support or your local regional office for assistance.

The report is available on demand, or it can be scheduled. In either case, the tuple must be datafilled in table OMREPORT. If this tuple is not datafilled, then no report is generated by the system.

To schedule the report, enter table OMREPORT, list all, review the output, and locate a spare or unused tuple. After locating a tuple that can be used, position on that tuple and enter:

>POS X

>CHANGE

ACTIVE

>Y

REP:

>DEVDAY

WHEN:

>7 COO   (suggested printing time for 7 a.m.)

CLASS:

>HOLDING

NAME:

>AMREPORT

TUPLE TO BE CHANGE

>Y

The Maintenance Managers Morning Report is generated as an OMRS log report; therefore, the routing capability of the report is similar to that of any other log in the system. The report can be routed to a printer(s) or appropriate device as datafilled in table LOGDEV.

To generate the report manually, the previous procedures for the table OMREPORT must be performed. The manual generation of the report requires that the user know the tuple number assigned to the report. Once this has been determined, the user can manually generate the report by entering OMREPORT from CI and requesting that specific report number (enter REQUEST X (X = tuple number of AMREPORT)). The report is then sent to LOGUTIL. The user then must enter LOGUTIL and enter OPEN OMRS to review the report.

Recommendations

The report should never be scheduled for automatic generation between 11:45 p.m. and 00:15 a.m., this time is used for gathering of report data and generation is not allowed. It is recommended that the report be printed during light traffic. It is also recommended that the report be printed in the morning for review by the user at the start of the day.

Commands

The AMREPCI command can be accessed from any MAP level and provides the following commands:

SETCPUTHRESH   is used to set the peak CPU occupancy threshold. The default value is 60%, but the operating company may set it to any level desired.

QUERYCPUTHRESH   is used to query or display the current setting of the CPU occupancy threshold.

AMREPED   is used to tailor or edit the report items.

\<ADD\> \<item name\>   is used to add an item to the report

\<DEL\> \<item name\>   is used to delete an item from the report

\<LIST\>   is used to list the current items in the report. Items in the report that can be added, deleted, or listed to the report are listed below:

* SPMS	* CPPERF	*CPU	* NETINTEG
* SWERTRAP	* LOGS	* CCTST (NT40)	* ALT
* ATT	* IMAGE	* PATCH	* OUTAGE
* XPMREX	* TABAUDIT	* SWACT	

QUIT is used to leave the AMREPCI level.

AMREP output description

SPMS Indicators

The SPMS (Switch Performance Monitoring System) indicator section displays indices for the first two levels of the SPMS hierarchy. The first level being the OFCPERF, the second level being the SERVICE, MTCPERF, and PROVRES branches of the SPMS hierarchy.

SPMS is a problem trend indicator. When a certain index score is low (below 95) for more than one day, it points to an area (DMS component) requiring further investigation. Please review the previous subsection on SPMS for further information.

CPPERF Indicator

This section provides users with the call processing performance (CPPERF) rating of the DMS's call processing for the last 24 hours. The displayed information includes:

- total call attempts
- total lost calls
- completion percentage

The total call attempts is the sum of originating attempts and incoming attempts. This sum reflects the traffic volumes for the last 24 hours. The total lost calls is the sum of lost calls due to network integrity failures, lost call due to cold and warm restarts, and lost calls due to PM's being out-of-service. The completion percentage is computed by the following formula:

Completion % = (total lost calls * 100) / total call attempts

The use of this indicator requires that a bogey be established for the **Completion % Component**. Review the report daily. If the completion percentage begins to deteriorate further, an investigation is required.

CPU Indicator

The **CPU Occupancy Indicator** provides the high-water mark for CPU usage for the report period. The indicator also provides the current setting for the high-water mark and peg counts for the number of times the CPU threshold was exceeded.

The threshold value is automatically set to 60% by the DMS. This default value may be queried with the SETCPUTHRESH command. A new CPU usage figure is computed by the DMS every minute; therefore, the peg count may be very large if the threshold value is set too low.

The use of this indicator requires that a bogey be established for the high-water mark or the number of times the threshold may be exceeded in a 24-hour period. If the high-water mark or the threshold count is exceeded more than usual, analysis of the abnormality is required.

SWACT Indicator

The **PM SWACT Indicator** provides a list of PMs, by type, that have been SWACTed. The items contained in the indicator include PM type, a count of manual and system initiated cold SWACTs, and a count of manual and system initiated warm SWACTs.

PM SWACTs can be initiated by the CC or through commands at the MAP. During warm SWACTs, only calls that are in the talking state survive the SWACT. Calls that have not reached the talking state are dropped. During a cold SWACT, all calls are dropped.

The **PM SWACT Indicator** is used to report troubled peripherals. If the report shows a count of *system* initiated SWACTs, corrective maintenance active is required.

NETINTEG Indicator

The **Network Integ Fail Count Indicator** provides a peg count of network integrity failures and total calls. The number of network integrity failure reports is equal to the number of integrity failures received from all the peripheral module controllers with in the switch.

The use of this indicator requires that bogeys be set to track the performance of the network. The bogeys used must be based on total calls versus network integrity failures for the reporting period.

TRAP/SWERR Indicator

The **Trap/Swerr Count Indicator** provides a count of the number of CC *swerrs* and *traps* that have occurred during the reporting period. This information allows the operating company to evaluate the performance of the switch and to implement early preventive maintenance.

The tracking of this indicator requires the establishment of a bogey(s) for the trap and swerr count. Once the bogey(s) have been exceeded, or continue on an upward trend, then further analysis is required.

LOGS

The Focus Maintenance and OM Threshold Log Count indicator provides a count of *focus maintenance* and *OM thresholding* logs that were printed during the report period.

The tracking of this indicator requires the establishment of bogeys for the focus maintenance and OM thresholding log count. Once the bogeys have been exceeded, or continue on an upward trend, then further analysis is required.

CCTST Indicator (NT40)

This indicator is applicable to the NT40 Processor only. The CC Scheduled Test Results Indicator provides test results and completion time for the following CC tests: REX Test, Image Test, and Data Store Retention Test.

This indicator provides maintenance personnel with the results of CC scheduled tests. If one or more of the tests indicates a failure, then corrective maintenance action is required.

ALT Indicator

The **ALT Indicator** is only applicable to offices equipped with the Automatic Line Test (ALT) feature. The **ALT Indicator** provides counts on the number of lines tested, passed, failed and skipped by the ALT feature for the past 24 hours.

The indicator provides maintenance personnel with a quick reference of the ALT results. The results can also be monitored and benchmarks established for daily results. A decrease in the number of lines tested may indicate equipment out-of-service or the test was disabled. An increase in the number of failed or skipped lines may indicate that further analysis is required.

ATT Indicator

The **ATT Indicator** is only applicable to offices equipped with the Automatic Trunk Test (ATT) feature. The ATT Indicator provides counts on the number of trunks tested, passed, failed, and skipped by the ATT feature for the past 24 hours.

The indicator provides maintenance personnel with a quick reference of the ATT results. The results can also be monitored to determine if ATT is set up properly to run on a nightly basis.

Outage Indicator

The **Outage Indicator** report contains the outage duration for the major DMS components. The outage duration is composed of system busy and man busy outages. The outage duration is reported in hours, minutes and seconds.

The outage indicator reports outage duration on the following components:

- Central Message Controllers (NT40 only)
- Message Switches
- Network Modules
- XPM Peripheral Modules
- Line Concentrating Modules
- Line Modules
- Trunk Modules
- Digital Carrier Modules
- Carriers
- Trunks

The **Outage Indicator** should be used by switch maintenance personnel to follow up on all reported system related outages. The indicator can also be used for system down time reports.

Image Indicator

The **Image Dump Result Indicator** reports on the number of images taken in the last 24 hours and the result of the last Image taken. If no images were taken, the message "No image dump occurred" appears.

The **Image Dump Result Indicator** should be used by switch maintenance personnel daily to ensure that a current Image is available.

PRSU summary information

The Post Release Software Manager (PRSM) is the DMS tool that tracks and maintains patches/PRSUs (Post Release Software Updates). The PRSM applies software fixes distributed after the release of a milestone load. PRSM software replaces PATCHER software, while maintaining and increasing the functionality of PATCHER. The result is a new, high quality software updating tool similar to PATCHER, thus facilitating the transition from PATCHER to PRSM.

A PRSU is distributed after the release of a milestone load. A patch is one type of PRSU. Additional types are planned for introduction in the future.

XPMREX Indicator

The **XPM REX Test Information Indicator** reports on the total number of XPMs in the office and the total number of XPMs not scheduled to run REX.

The **XPM REX Test Information Indicator** should be reviewed to ensure all XPMs in the office are scheduled to run REX.

TABAUDIT

Reports on the number of table audits tested, and passed or failed.

TABAUDIT is a table verification process that can be run prior to making an image tape (approximately 15 days prior to the scheduled application) and periodically after the image tape is made (to verify office data). Errors and inconsistent data identified by TABAUDIT should be corrected by the operating company prior to making the system image tape. This process decreases the need—for Nortel Networks to contact the customer during the dump and restore process—for direction on how to correct table errors.

Options are provided with the TABAUDIT command to verify data in a single table, a range of tables according to table DART, or all the tables within the DMS switch.

For further information on TABAUDIT, see the "Supporting Enhancements" subsection within the *Technical Assistance* tab of this manual. For detailed procedures on the use of the TABAUDIT command and the automatic scheduling AUTOTABAUDIT command, see NTP 297-8991-303, *DMS-100F One Night Software Delivery Process.*

Exhibit A — Output Sample of AMREP

This is an example output of the AMREP generated through a manual request at a DMS-100 site.

```
LOGUTIL:
>open omrs
Done.
EAST_COAST_Y2K      OMRS023 JAN25 17:01:27 5700 INFO OM PERIODIC
REPORT

REPORT NAME:  AMREPORT        REASON:    REQUESTED

CLASS:  HOLDING
START:2000/01/25 16:45:00 THU; STOP: 2000/01/25 17:00:00 THU;
SLOWSAMPLES:         9 ; FASTSAMPLES:          90 ;
ELAPSED TIME:  00/00 00:15:00


==============================================================
***************************************
* MAINTENANCE MANAGERS MORNING REPORT *
***************************************
2000/01/25 17:02:12.968 THU.


OFFICE NAME : RLGHNCY2K
PCL RELEASE : LEC010  (Restart Occurred)

SPMS INDICATORS
===============
    Ofcperf       (office perf)    = 95 (Average performance)
    .....Service (service perf)   = 81 (Below average perf)
    .....Mtcperf (maint perf)     = 90 (Below average perf)
    .....Provres (prov. resource) = 97 (Above average perf)

CALL PROCESSING PERFORMANCE
===========================
    Total Calls        Lost Calls        Completion Percentage
      1322                  0                     100 %

CPU OCCUPANCY
=============
    High Water Mark    Threshold Value    Threshold Exceeded
        0 %                100 %                   0

                    continued
```

```
PM SWACT AND TAKEOVER INFORMATION
=================================
    Pm Type        Man Warm/     Sys Warm/     Man Cold      Sys Cold
                                Takeover      Takeover
                 *** No PM swact/takeover occurred ***


NETWORK INTEG FAIL COUNT
========================
    Fail Count      Total Calls
        10             1322


TRAP / SWERR COUNT
==================
    Swerr Count      Trap Count
        3                1


FM AND OM LOG COUNTS
====================
    FM100       FM101       OM2200
     0           0            0


ALT RESULT
==========
    Total Tested      Total Passed      Total Failed      Total Skipped
        128               89                11                28


ATT RESULT
==========
    Total Tested      Total Passed      Total Failed      Total Skipped
        289              259                24                6


OUTAGE INFORMATION
==================
    H/W Type      Hour Min Sec
    MS              0    5   0
    XPM             1   15   0
    LCM             0   13  20
    LM              0    5   0
    TM              0   18  20
    TRK             4    3  20
    CARR            0   13  20
                              continued
```

```
CM IMAGE DUMP RESULT
====================
    Dump Count     Last Dump Result
    *** No image dump occurred ***


PRSU SUMMARY INFORMATION
========================
    CM    ISN    XPM
    *** PRSU data is unavailable ***


XPM REX INFORMATION
===================
    Total XPM      REX Unscheduled
        8                8


TABAUDIT INFORMATION
====================
Total Tested    Total Passed    Total Failed
    0               0               0


                   *** END ***



================================================================
```

THIS PAGE INTENTIONALLY LEFT BLANK

Technical Assistance – General

Technical assistance is provided through various methods and processes for the Nortel Networks product line. Technical assistance from marketing, customer orders, engineering, planning, installation, cutover, and various in-service support is provided by Nortel Networks. Technical assistance is not only provided through direct contact with Nortel Networks personnel, but through available documentation and various processes for handling technical services and issues. Methods and processes for providing technical assistance are subject to change and may vary from region-to-region; therefore, if any of the topics provided within this section are questionable, consult your local Nortel Networks Customer Support Group for local policies.

This section provides an overview of Nortel Networks technical assistance services and other supporting technical enhancements that provide assistance. The following topics are provided within the following subsections of this tab:

- Technical assistance services
- Emergency plans and escalation procedures
- Maintenance services
- Service Reports (SRs)
- Software application
- Customer Service Computerized Access Network (C-SCAN)
- Customer Information Management (Canada)
- Circuit pack replacement
- DMS-100 warnings and bulletins
- Change application services
- Engineering complaint services
- Outage footprint
- Sherlock data collection tool
- Automatic image dump
- Scheduled patching

Technical Support Services

General

This subsection provides an overview and a brief description of the technical support services, processes, and reporting procedures for maintaining and operating DMS-100F switch products. Services may vary according to local regional policies and will not necessarily be provided (or work) as described within this manual. Contact your Nortel Networks Regional Support Group if more information is needed concerning support services.

The following support services described within this subsection are an integral part of Nortel Networks commitment to assist the operating companies in maintaining DMS-100F switches at their design criteria:

- Technical assistance services
    - Service guidelines
    - Service charges
    - Service Priority Classification
    - TAS for DMS-100F switches
    - TAS for terminals
    - ETAS
- Emergency plans and escalation procedures
    - Emergency recovery documentation
    - Disaster recovery procedures
- Maintenance services
    - Value added documentation
    - Operating company services
- Service Reports (SRs)
    - SR process
    - SR for documentation errors
    - SR flowchart

Nortel Networks internal procedures are in effect for emergency recovery, escalation, patches, and managing software and hardware updates and enhancements.

Technical assistance services

Before escalating a trouble report to Nortel Networks, all local operating company trouble reporting or emergency recovery escalation procedures and policies should have been followed. Nonemergency problems are generally reported through local company maintenance engineering or technical support groups. Upon investigation, nonemergency problems are generally resolved by the customer or reported to Nortel Networks through service reports (SRs) and Engineering Complaints (ECs). SRs and ECs are generally first opened through the Nortel Networks Regional Support Group from the customer. Emergency problems are generally reported through operating company control centers before contacting the Nortel Networks Emergency Technical Assistance Service (ETAS) group. See the *Maintenance Administration* tab for control center acronyms.

Nortel Networks service comprises all actions required to verify the existence of a problem and to ascertain the conditions under which the problem can be duplicated. In response to a problem, the customer is provided with one of the following:

- update or revision
- temporary workaround
- statement indicating that the problem could not be verified and more data is necessary to prove the existence of a problem
- statement indicating that the problem is not of sufficient magnitude to warrant immediate correction, whereupon it will be corrected later. The operating company may request advance application of any required fix, for which charges will apply.
- statement indicating that the system operation meets design intent and that custom modification may be possible
- statement indicating that the problem will not be corrected

Service charges

Users may be billed, following the warranty period, for Nortel Networks technical or maintenance assistance. Any service charge that represents an extension of the operating company's maintenance or administration of its system is deemed to be billable at the published rate.

All requests for technical assistance or miscellaneous services are documented using the service report (SR) described later in this subsection. An SR is used to identify billable services outside the normal functional responsibility of TAS. These calls typically come into TAS as a direct request for a specific service, not as a specific DMS problem that the customer needs assistance in resolving. These are typically functions for which the customer would contract other Nortel Networks organizations or other vendors to perform. They include such items as disk drive recovery, performing product upgrades or installations, setting up initial office translations for a feature/function for a customer, or requests for on-site training, etc.

Customers are encouraged to purchase annual technical support contracts (termed Nortel Networks Service and Support Plans) at a predetermined price, to simplify billing. But individual invoices billed at an hourly rate for each SR opened, are also available.

Service guidelines

Service objectives are related to the severity of a reported problem. It is Nortel Networks policy to respond immediately to critical problems and to restore service to the preincident level in the shortest time possible. Nortel Networks uses all available resources, including Bell Northern Research (BNR) personnel, to restore service in the shortest possible time. Nortel Networks also strives constantly to improve response time for nonservice affecting problem resolution.

Service Priority Classifications

Different problem types require different levels of reaction; therefore, the Service Priority Classification System was designed to establish an interrelationship between problems and the appropriate level of reaction and resolution. The classification system is based upon a problem's direct or potential effect upon subscriber service (i.e., ability to obtain dial tone and make calls).

When a system problem is reported to Technical Assistance Service (TAS) or ETAS, one of six priority classifications is assigned to the trouble report -- E1, E2, E3, E4, MJ, MN -- at that time based on the impact of the trouble report as follows:

- E1 - outage or degradation condition
- E2 - potential outage or degradation condition
- E3 - post-analysis to an E1 condition
- E4 - post-analysis to an E2 condition
- MJ - service affecting
- MN - nonservice affecting

Once a priority has been assigned, the problem is then routed to the appropriate technical response group as follows:

- E1 - remains within ETAS
- E2 - remains within ETAS
- E3 - is always routed to the Outage Follow-up Group
- E4 - may remain within ETAS or be routed to the Outage Follow-up Group
- MJ - may remain in ETAS or be routed to a Customer Service Center (CSC) Product or Account group
- MN - may remain within ETAS or be routed to a CSC Product or Account group

It may also be necessary to involve Nortel Networks Technologies in the resolution of a call report, regardless of the priority.

E1 degradation or outage (Critical)

The following criteria provide guidelines used to establish the priority classification for the E1 degradation or outage:

NOTE: The exact wording of the following criteria has been updated and approved globally in all markets.

- loss of service capability (call processing originations or terminations) for more than 30 seconds.
- any manual or system initiated restart (warm, cold, reload or image reload) which causes a loss of service capability for a period in excess of 30 seconds.
- services degraded for reasons such as, but not limited to:
    — all incoming, outgoing or two-way trunks are lost.
    — a 100% trunk group failure disrupting connections between any switching offices, where the disrupted traffic demand exceeds the alternate routing capability (e.g., ISUP, PRI, PTS, etc.).
    — 10% or more of the total number of subscriber terminals/ports are out-of-service.
    — 10% or more of the total number of trunks are out-of-service, where the disrupted traffic demand exceeds the alternate trunking traffic capability.
    — 64 or more voice or data lines are out-of-service, where a line is defined as one subscriber terminal (e.g., for ISDN, the sum total of "B" and "D" channels without service).
    — consistently slow dial tone (eight second delay or greater).
    — a linkset/routeset/pointcode/subsystem that denies access to network or local services (e.g., E800, ACCS, etc.).
    — failure of 1/2 of a duplicated switch pair (e.g., STP pair).
    — no billing data is being recorded (e.g., MTD, DDU, DPP, etc.).

E2 potential degradation and/or outage (Major)

The following criteria provide guidelines used to establish the priority classification for the E2 potential degradation and/or outage:

- loss of the duplex function for any equipment that is duplicated (e.g., CPU, CM, CMC, MS, LIM, XPM, IOC, NM, etc.).
- loss of the master clock or a network plane out-of-service.
- 50% or more of the equipped magnetic tape units (MTU) or disk drive units (DDU) that are being used to collect billing, are out-of-service.

- more than 50% (but less than 100%) loss of hardware facilities in any area of the DMS that would not create a loss of service, but a degradation (limited) of service with no data loss through the node (e.g., slow dial tone)
- loss of all links within a single linkset.
- loss of duplex recording of billing information.
- inability to dump or initialize an office image
- inability to perform critical maintenance procedures, i.e. REX testing.

E3 follow-up analysis (Major)

The following criteria provide a description of the use of E3 call reports for follow-up analysis:

- may be opened at the discretion of the ETAS engineer or ETAS Duty Manager.
- may be requested by the customer at the discretion of the ETAS Duty Manager.
- contains all important information concerning the outage or degradation, the current status of the switch, and any analysis already performed by ETAS.
- used to document further investigations and analysis to determine the cause of the outage or degradation and steps taken to prevent the same problem in the future.
- should indicate that ETAS has already received telco's approval for closure.

NOTE: ETAS may request or receive telco approval for closure before routing the SR to the Outage Follow-up Group. If closure approval is received from the telco, the ETAS engineer should document in the SR text the closure explanation and telco agent who approved closure, prior to routing.

E4 Follow-up analysis (Major)

The following criteria provide a description of the use of E4 call reports for follow-up analysis:

- may be opened at the discretion of the ETAS engineer or ETAS Duty Manager.
- may be requested by the customer at the discretion of the ETAS Duty Manager.
- may be used by ETAS as a tracking mechanism while monitoring switch stability.
- used to document further investigations and analysis to determine the cause of the potential outage or degradation and steps taken to prevent the same problem in the future.
- contains all important information concerning the potential outage or degradation, the current status of the switch, and any analysis already performed by ETAS.

MJ service affecting (Major)

The following criteria provide guidelines used to establish the priority classification for the MJ service affecting problems:

- Software errors or hardware troubles directly and continuously affecting any subscriber's service or the operating company's ability to collect revenue.

- A problem that will seriously affect subscriber service, as in the above item, at in-service (IS) date.

- MTU, DDU, or SLM problems (excluding regular maintenance and administration).

- Central Control Complex (CCC) or Computing Module (CM) transient errors resulting in a loss of synchronization (more than twice a day).

- Any peripheral module out-of-service.

- Inoperative internal data port or CMC communication link.

- Core equipment diagnostic failures (two or more per day).

- Loss of more than 50% of the links within a linkset or linksets within a routeset, not to exceed 99%.

- Software or hardware faults that only intermittently affect service to one or more classes of subscribers.

- System related documentation errors which categorically result in, or lead to, service impairment.

- Problems where the operating company can show significant impact on plant and traffic operations and upon its ability to plan office extensions.

- Office alarm unit out-of-service.

- Core equipment diagnostic failures (less than two per day).

- CCC or CM transient errors resulting in loss of synchronization (less than two per day).

- Peripheral circuit failures.

- Loss of less than 50% of the LIU7s in a linkset or a routeset.

MN service affecting (Minor)

The following criteria provide guidelines used to establish the priority classification for the MN nonservice affecting problems:

- Service analysis, recorded announcements, operational measurements, maintenance program, or network management problems; or system related documentation inaccuracies, which do not affect call processing.

- Nonservice affecting software inconsistencies.

- Peripheral equipment diagnostic failures, not already defined above, which cannot be corrected by the customer's technicians.

- Test equipment failures for which a backup or manual alternative can be employed.
- Circuit pack testing problems.
- Repetitive CCC transient errors with no loss of synchronization, which cannot be corrected by the customer's technicians.
- Requests to analyze a store dump or a single occurrence initialization.

For additional support on service priority classifications, see NTP 297-0201-015, *North American DMS-100 Service priority classification description.*

TAS for DMS-100F switches

TAS refers to United States LEC TAS (Technical Assistance Service) located at 500PP, Morrisville, North Carolina (for DMS-100 support) or located at the Northern Telecom Plaza, Research Triangle Park, NC. TAS for DMS-100F switches is a centralized group of trained engineers divided into Customer Service Center (CSC) accounts or groups. This helps provide concentrated vertical expertise in each of the several functional areas where problems with the switch are most often reported. Specialty product groups normally become involved in nonemergency problem resolution; however, they also provide backup support to ETAS. Emergency situations often identify problems that require specialized knowledge on specific components of the system. In those instances, ETAS can turn to a specialty group for help.

SL-100, Meridian 1, DMS Mail (SPM/GP), Call Center and other related products are handled out of Richardson, TX (1-800-766-3827).

TAS for DMS-100 terminals

For those needing technical support on DMS-100 terminals or other related products listed below, contact Nortel Networks Customer Response Center at 1-800-251-1758. The following are examples of products that are supported:

- Business sets ("P" phones)
- ACD and add-on module
- M5000 series sets
- MDC console
- Datapath products
- ISDN NT1 and M5000TD-1, M5209T, M5317T, M518T sets
- CLASS products (i.e., Maestro and Lumina)
- SESAME

For Norstar ordering and support, contact 1-800-321-2649.

For addition information on terminals, see the "MDC Terminals" subsection within the *System Products* tab of this manual.

ETAS

Emergency Technical Assistance and Support (ETAS) provides the operating company with immediate and continuous assistance to help resolve E1 or E2 priority emergency problems. ETAS is a centralized group and provides 24 hour, 7 days a week coverage to the operating companies, should an emergency occur.

In the U.S., ETAS is also the key contact for both DMS and non-DMS *disaster* issues. Example of a disaster would be a telephone office destroyed by fire, tornado, or other similar uncontrolled action.

ETAS can be reached directly at (919) 905-8300 24 hours a day, 7 days a week, for emergencies only. For access to both emergency and nonemergency services, you can call the toll-free voice recorded access number (800) 758-4827. In Canada, ETAS can be reached at 613-765-2422, 24 hours a day, seven days a week.

Emergency plans and escalation procedures

Each operating company should develop a plan of action for emergency situations. The plan should be documented and distributed to the involved locations. The plan should include the necessary instructions, authority and follow-up to remove the emergency situations during normal and out of hours. Also include escalation procedures, elapsed time intervals, and a list of management to notify.

Escalation instructions are a key part of the emergency plan. The escalation process alerts key management, in progressive time steps, as warranted by the situation. These escalation steps should be clearly defined in the emergency plan, including elapsed time intervals for the escalation. An informed management team can arrange for the necessary assistance or resources, under the circumstances, to restore the switch to service in the shortest possible time. See the following list of emergency recovery documents as reference.

Emergency recovery documentation

Personnel responsible for emergency recovery of DMS-100F switches should be familiar with NTPs that provide emergency recovery procedures. The following NTPs should be available for current software loads and features that are in-service within your company:

For emergency recovery documentation references, see the "Maintenance, Troubleshooting, and Recovery References" subsection within the *Corrective Maintenance* section of this manual.

Disaster recovery procedures

Nortel Networks commitment is to provide a disaster recovery plan for the telephone operating companies, and to make an extraordinary effort to restore essential communications services to telecommunications systems involved in a disaster.

A disaster is defined as a sudden catastrophic event such as fire, flood, lightning, storm, explosion, tornado, earthquake, hurricane, or any other incident causing damage beyond normal repair to telecommunications facilities. The result is that extensive hardware replacement may be required and a potentially extended outage situation (over 24 hours) exists. Having a predetermined procedure ensures that when disaster strikes a central office, service is restored as quickly and efficiently as possible.

Maintenance services

To assist operating companies with their proactive approach toward maintenance, Nortel Networks Global Professional Services provides special value-added documents and maintenance services. For information on any of the following maintenance services, contact Nortel Networks, Global Professional Services, Manager - Technical Services at 1 (919) 465-0434.

Value-added documents

Special value-added documentation provides tools to assist in maintenance activities and operations. One of those documents is this manual, the *DMS-100F Maintenance & Operations Manual.* Another that supports the DMS-100F switch is the DMS-100F Quick Reference Guide (TAM-1001-018). The DMS-100F Quick Reference Guide is a small pocket-sized document for on-the-job use and a quick reference for such information as:

- Commonly used DMS CI level commands

- Commands for TABLE EDITOR, SFDEV, DMSSCHED SPMS, TABAUDIT, DMSMON, TRAVER, DISPCALL, SHOWAUD, LOGUTIL, DLOG, CLASS, DISKUT, DSKUT, PATCHER, PRSM, OMs, SOC, AUTO-PATCH, and AUTO-MATIC IMAGE DUMP

- Quick references for AIN, CCS7, LNP, ISDN, CLASS, ACD-MIS, CC MIS, SMDI, CompuCALL, REMOTES, DMS-250, and RINGING information

- Tier II support tools for XPMIST, DEBUG, MPCDEBUG, ACDDEBUG, TER-MTRACE, C7TU, SMON, CALLTRAK, XPMTRAK, and REMLOGIN

- Quick references for NTPs, IMs and other documents

- Product Engineering Codes (PECs) for circuit packs

- Hardware shelf diagrams with circuit pack locations

- Circuit pack descriptions

- SuperNode and other block diagrams

- XPM/DTC port and link mapping diagrams

- Keyboard layouts for TOPS MP, MPX, and IWS

- Attendant Console keyboard layouts

- DPP/BMC hardware and DPP commands

- Billing Media Converter (BMC) hardware
- RTIF commands and procedures
- Trunk group type listing (translations)

To order the quick reference guide within North America, call 1-800-684-2273.

Operating company services

Following is a list of operating company services that Nortel Networks Global Professional Services provides:

Control Center Technical and Administrative Analysis and Switch Performance Review — provides an in-depth constructive review of both administrative and technical aspects of an operating company's control center—including on-site review of operating company selected DMS-100F switches. Polling of the selected sites provides performance and maintenance related data that is evaluated. The review identifies strengths and areas of improvement within the center and central office. Additionally, the review provides recommendations and solutions to resolve operations and maintenance issues. The review includes the following areas:

- Site Information
- Personnel
- Communications
- Emergency Recovery
- SCC/NOC Hardware
- Software
- Documentation
- Control Center, Central Office, and Switch Access Security
- Trouble Tracking
- Office Control Logs
- Central Office Environment
- Routine Maintenance
- Circuit Pack Handling and Administration
- Log Message System Administration
- Operational Measurements
- Office Engineering Parameters
- Trunk Maintenance
- Line Maintenance
- Switch Network Maintenance
- Office Results Plan
- Patch Administration
- Organization and Responsibility
- Performance Analysis
- Engineering Parameter Review

- Preventive Maintenance
- Work Pricing
- Priorities
- Work Schedules
- Loading Guides
- Job Descriptions
- Work Force Administration

A verbal feedback session is conducted at the end of the review with the appropriate operating company personnel. Findings on key or critical deficient areas are discussed.

A formal written report is provided detailing all findings during the review period. Documented recommendations are provided to assist the customer in establishing a proactive maintenance program.

DMS-100 Remote Switch Polling and Analysis — is a dial-in access service which polls the switch for selected data that is used to evaluate switch performance and an overall health status. Customers can request that specific problem areas be analyzed. Some of the areas that will be evaluated are:

- Performance Report Utilization
- Analysis of Switch Reports
- Provisioning Tables
- Maintenance tool Usage
- OM Administration
- Log Administration
- Engineering Parameter Setting Review
- Image Administration
- Patch Administration

The service includes a detailed report and recommendations for problem areas.

Standardized Tool Implementation and Workshop — is a service that will implement the following maintenance tools:

- Switch Performance Monitoring System (NTX738)
    - — Output, set up, and scheduling of the SPMS report with the associated trouble shooting
- Operational Measurement Threshold Feature (NTX385)
    - — Customized to switch type, feature set, and office busy hour characteristics
- Focused Maintenance Lines & Trunks (NTX272)
    - — Automated testing program customized for office configuration and requirements
- Automatic Trunk Test (service circuits only) (NTX051)

- — Set up and scheduling of the automated testing solution of the office service circuits
- Killer Trunk (NTX053)
  - — Customized testing and reporting solution based on office patterns and average holding times
- Maintenance Managers Morning Report (NTXJ35)
  - — Provides customized output, according to requirements, indicating switch status (also known as the AM Report)

The Standardized Tool Implementation service provides consistent datafill and activation of the maintenance tools across all DMS switches that are supported by the customer's control center. A customer questionnaire is required for each office prior to implementation. The questionnaire provides the necessary information on log routing, busy hour traffic, office configuration, scheduled automatic test times, and Operational Measurements (OMs). The completed customer questionnaires are used to create a customized program to automatically download datafill to the tables used to implement the maintenance tools.

Upon completion of Standardized Tool Implementation, Nortel Networks will conduct a customized hands-on workshop at the customer's control center. This thirty-two (32) hour workshop ensures that personnel have a complete understanding of tool datafill, tool usage, and associated MAP levels. The Nortel Networks consultant will work directly with maintenance personnel, providing practical experience to complement the workshop.

DMS Trouble Clearing Techniques — is a technical service that allows a customer to identify and correct maintenance issues before service is adversely affected. These procedures utilize automated maintenance tools specifically designed to find customer service problem areas. Trouble clearing techniques is designed to move the customer from a reactive maintenance environment to a proactive maintenance environment.

Once a customer requests this service, a Nortel Networks consultant will hold an Initial Service meeting with the customer detailing customer needs and logistical information. A Nortel Networks consultant will develop a customer specific trouble clearing process using the information obtained from the Initial Service meeting. The consultant will spend one week at the customers's premise to conduct hands-on training and implement the service. The training can either be in a classroom or in a working environment.

Remote Analysis — is a service provided by Nortel Networks after the implementation of the Maintenance Tools. Nortel Networks consultants utilize the existing Maintenance Tools in the switch to perform the Remote Analysis. Nortel Networks consultants provide the customer with maintenance recommendations based on the analysis of the Maintenance Tool output. The Remote Analysis Service is flexible in nature to provide the customer with the maintenance solution that will best meet their needs. The statement of work and frequency of work must be well defined in a con-

tract due to the flexibility of this service. The service is normally provided in two ways, basic and enhanced.

Basic Remote Analysis is the service that is most commonly preferred. Nortel Networks consultants provide the customer with maintenance recommendations based on the analysis of the Maintenance Tool output. Nortel Networks consultants utilize the existing Maintenance Tools in the switch to perform the Remote Analysis.

Enhanced Remote Analysis is normally provided to a customer who does not have any analysis function defined and wishes that Nortel Networks provide total analysis. Enhanced Remote Analysis requires that Nortel Networks have access to the customer switch and OSS. Nortel Networks consultants provide the customer with pack level maintenance recommendations based on the analysis of the Maintenance Tool output and testing. Nortel Networks consultants utilize the existing Maintenance Tools in the switch to perform the Remote Analysis.

Nortel Networks will assist the customer in developing their method of downloading analysis information if necessary. Nortel Networks will develop any tracking logs for customer feedback. The development for this service depends greatly on the contract agreement and need to be addressed in the RFI process on a per service basis.

On-site Assistance/Coaching — is a service that provides on-site assistance/coaching for customer technicians working in DMS switch environment. Includes assistance/coaching for problem detection, resolution, or referral for correction on daily work activities. This service can be provided to both Analysis or Surveillance personnel either in a center environment or in the central office.

The Nortel Networks consultant will coach customer personnel in all or a limited number of the following areas:

- Trouble ticket resolution
- Proactive switch analysis
- Switch log and report questions
- NTP documentation utilization for problem resolution
- Translation error correction
- Existing processes or procedures recommendations
- Troubleshooting techniques
- DMS test tool utilization

Standardized Security Service — is a service that provides a review of the operating company's switch security. Security will be set up based upon information provided by the operating company and recommendations from Nortel Networks. A special program developed by Nortel Networks will be provided to the operating company for implementation on their switches. Nortel Networks lab testing and a VO switch designated by the operating company will provide preliminary program testing before implementation

Service reports

Service reports (SRs) provide an administrative tracking mechanism for Nortel Networks customers and TAS organizations for identifying and resolving problem issues. They are jointly owned by Nortel Networks regional support groups and the TAS Core Speciality Groups. The Nortel Networks internal process of handling SRs results in immediate action. Resolution times are established based upon the service priority level.

SR process

The SR process begins when the telco or a Nortel Networks customer support organization identifies a problem and contacts TAS. General questions or service needs can also prompt the opening of an SR. Customer calls which are addressed in 15 minutes or less may not warrant opening of a SR. This decision will be the responsibility of the individual TAS Account or Product Engineer.

The TAS Engineer, when contacted, will open an SR in the CSDS/e database. Also, Nortel Networks regional support personnel (ex. Technical Assistance Centers, Field Service Engineers) can also open an SR and route it to TAS within the CSDS/e database.

Once opened, an SRID (SR Identification number) is generated by the CSDS/E database. This number is unique and permanent and allows TAS and the Customer to track problems using a common identifying number.

The method employed in contacting the TAS Engineer is any medium that involves communication between TAS and the Customer, where the Customer states the problem and the TAS Engineer acknowledges receipt of the problem. Generally this involves a telephone call from the telco to TAS using 1-800-758-4827.

Normally, the telco's initial contact will be directly to its dedicated account group (known as the 'Account Team') within TAS for first level support. When addressed to the Account Team, many, or all of the initial problems or questions will be resolved at that stage. If the Account Team cannot resolve the issue or if deemed to be a design defect or deficiency, the SR will be routed to the appropriate specialty group (known as the 'Product Team'), or to the appropriate Global Product Support Team within *Technology* for resolution. In general most SRs are expected to be opened and closed by the Account Team. Account Team guidelines for Product Team or *Technology* involvement are the responsibility of the specific Account Team Manager.

SR for documentation errors

When a user finds an error in Nortel Networks documentation, the user should provide the following information to the supporting regional TAS:

- error identification
- document name and issue number
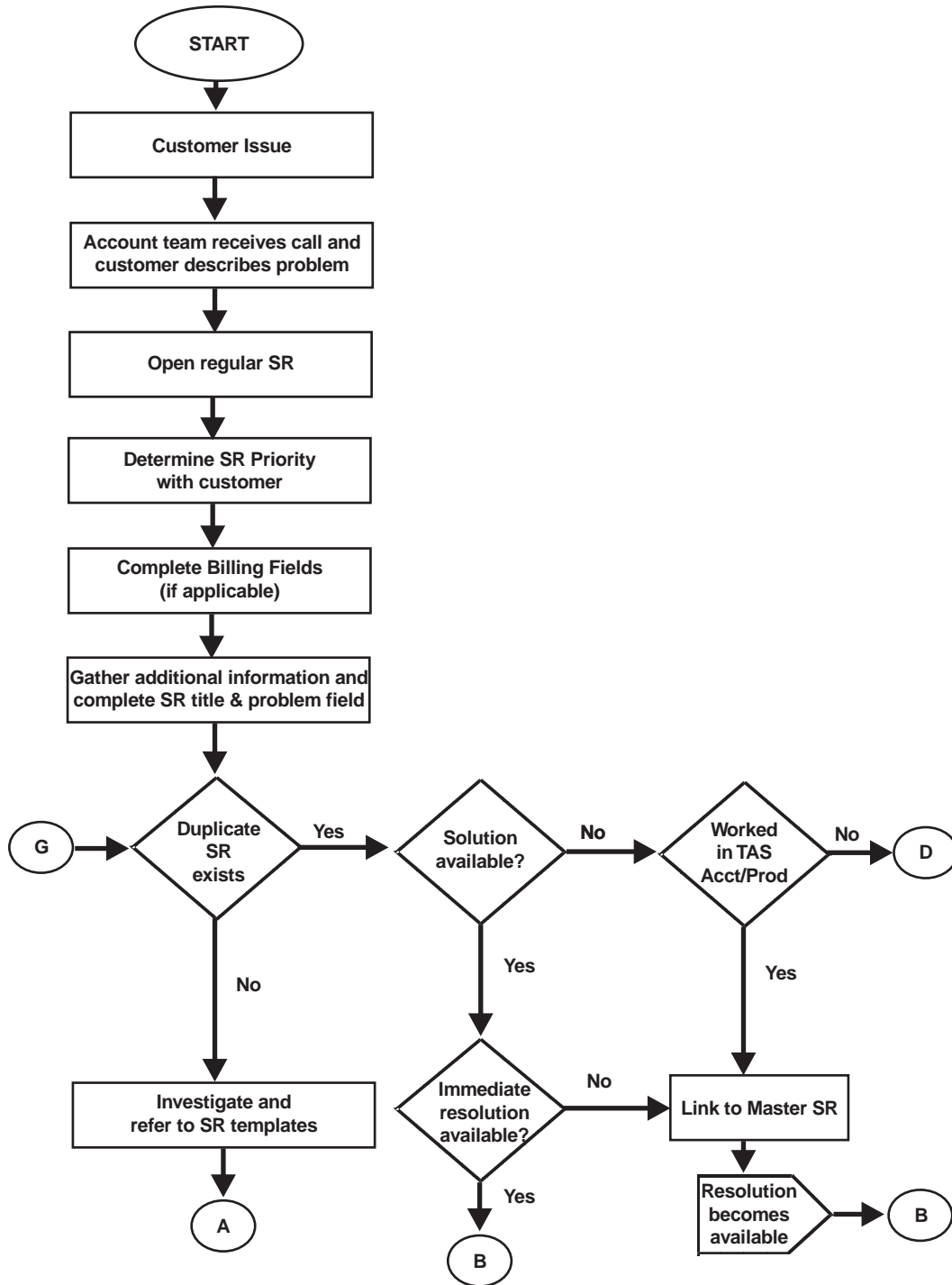- NTP number (if applicable)

- table name and release (if applicable)
- PCL release
- page number.

Once TAS has determined that the latest document reported on has an error, then a SR is opened. A specialty group TAS engineer reviews the SR and analyzes the data pertaining to the problem. If the problem is service affecting or could cause service degradation, then a warning bulletin is prepared. If the SR is related to documentation errors, then it is forwarded to the responsible documentation group where it is reviewed for correction and resolution.

For future deliverable documentation fixes, the engineer must obtain consent from the customer and provide the customer the NTP number, NTP revision level in which the documentation update will be provided, and the associated software release to which the documentation will be tracked before changing the status of the SR.
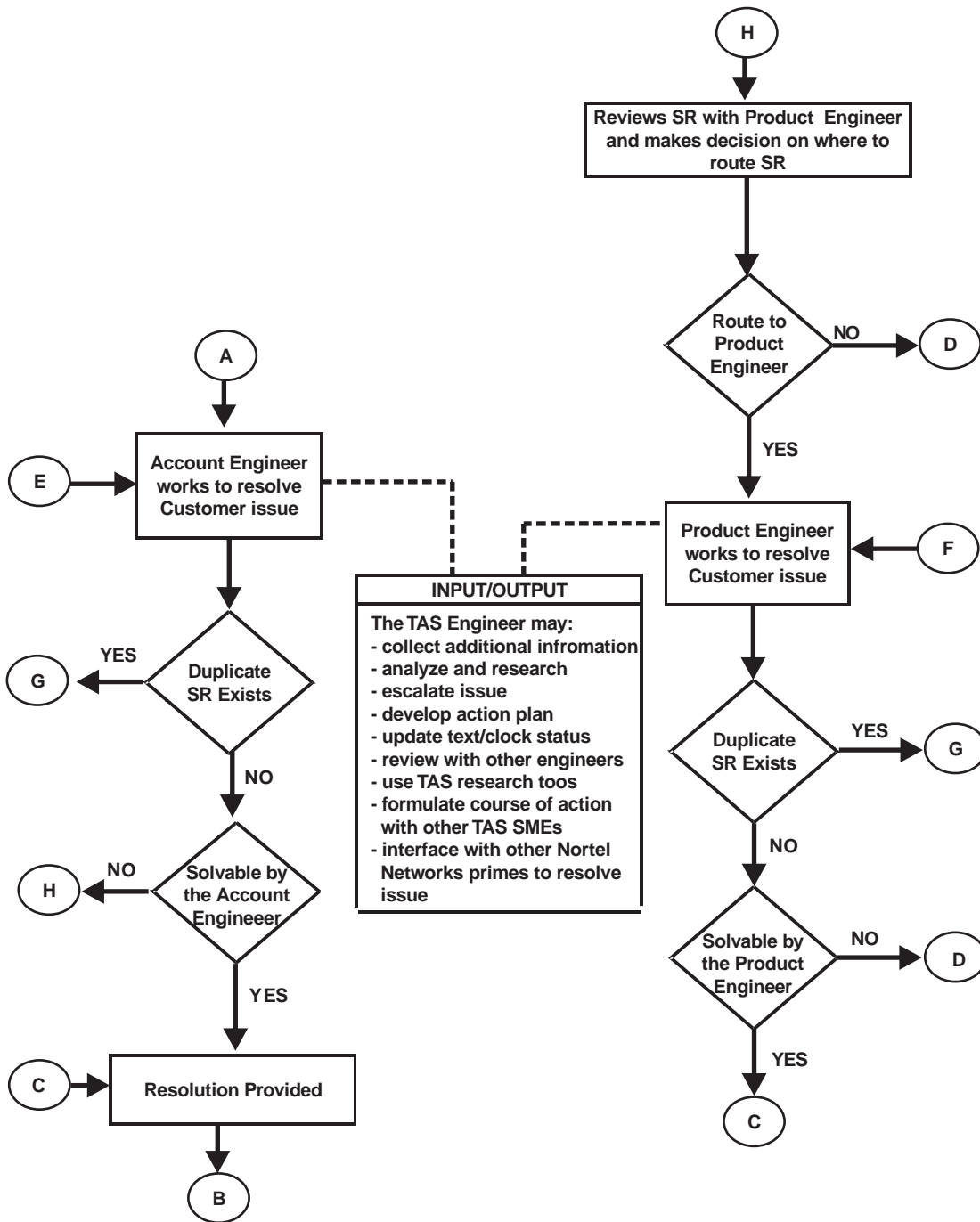
For an overview of the SR process, see the following flowchart.
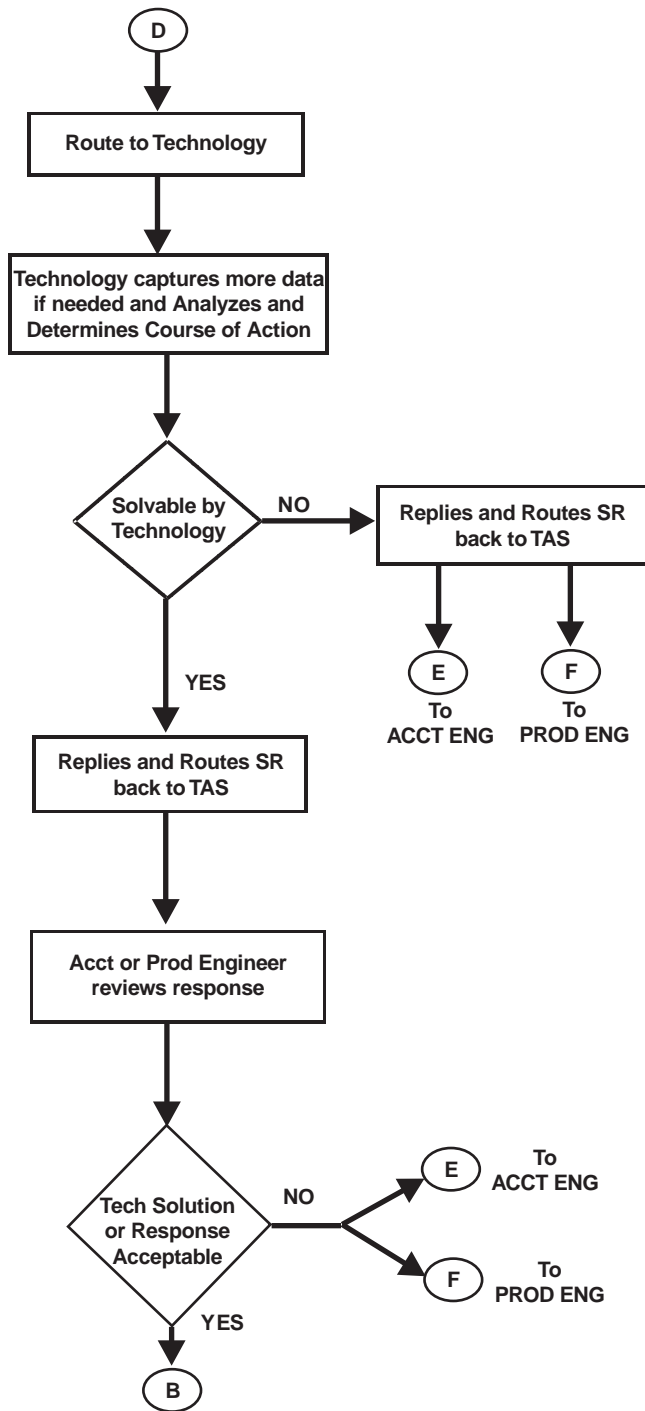
Figure 6-1   Service report flowchart

```
                    ┌─────────┐
                   (  START   )
                    └────┬────┘
                         ▼
              ┌──────────────────────┐
              │    Customer Issue     │
              └──────────┬───────────┘
                         ▼
              ┌──────────────────────┐
              │ Account team receives │
              │ call and customer     │
              │ describes problem     │
              └──────────┬───────────┘
                         ▼
              ┌──────────────────────┐
              │    Open regular SR    │
              └──────────┬───────────┘
                         ▼
              ┌──────────────────────┐
              │ Determine SR Priority │
              │    with customer      │
              └──────────┬───────────┘
                         ▼
              ┌──────────────────────┐
              │ Complete Billing      │
              │ Fields (if applicable)│
              └──────────┬───────────┘
                         ▼
              ┌──────────────────────┐
              │ Gather additional     │
              │ information and       │
              │ complete SR title &   │
              │ problem field         │
              └──────────┬───────────┘
```

Decision: **Duplicate SR exists** — (G) enters. Yes → **Solution available?** No → **Immediate resolution available?**

Solution available? — No → **Worked in TAS Acct/Prod**; Yes → **Immediate resolution available?**

Worked in TAS Acct/Prod — No → (D); Yes → **Link to Master SR**

Duplicate SR exists — No → **Investigate and refer to SR templates** → (A)

Immediate resolution available? — No → **Link to Master SR**; Yes → (B)

Link to Master SR → **Resolution becomes available** → (B)

Continued on next page

SR flowchart continued

H

Reviews SR with Product Engineer and makes decision on where to route SR

Route to Product Engineer — **NO** → **D**

YES

A

Account Engineer works to resolve Customer issue ← **E**

INPUT/OUTPUT

The TAS Engineer may:
- collect additional infromation
- analyze and research
- escalate issue
- develop action plan
- update text/clock status
- review with other engineers
- use TAS research toos
- formulate course of action with other TAS SMEs
- interface with other Nortel Networks primes to resolve issue

Product Engineer works to resolve Customer issue ← **F**

Duplicate SR Exists — **YES** → **G**

NO

Solvable by the Account Engineeer — **NO** → **H**

YES

Duplicate SR Exists — **YES** → **G**

NO

Solvable by the Product Engineer — **NO** → **D**

YES

C → Resolution Provided

B

C

Continued on next page

SR flowchart continued

```
                    ( D )
                      │
                      ▼
            ┌──────────────────┐
            │ Route to Technology │
            └──────────────────┘
                      │
                      ▼
        ┌──────────────────────────┐
        │ Technology captures more data │
        │  if needed and Analyzes and  │
        │ Determines Course of Action  │
        └──────────────────────────┘
                      │
                      ▼
                  ◇ Solvable by      NO      ┌──────────────────┐
                    Technology ──────────────▶│ Replies and Routes SR │
                  ◇                           │    back to TAS     │
                      │                       └──────────────────┘
                    YES                          │            │
                      │                          ▼            ▼
                      ▼                        ( E )        ( F )
        ┌──────────────────┐                   To            To
        │ Replies and Routes SR │            ACCT ENG     PROD ENG
        │    back to TAS     │
        └──────────────────┘
                      │
                      ▼
        ┌──────────────────┐
        │ Acct or Prod Engineer │
        │   reviews response   │
        └──────────────────┘
                      │
                      ▼
                 ◇ Tech Solution     NO         ( E )   To
                   or Response ───────────────▶        ACCT ENG
                   Acceptable ◇
                      │          ───────────────▶ ( F )   To
                    YES                                  PROD ENG
                      │
                      ▼
                    ( B )
```

Continued on next page

SR flowchart continued

B

Reviews Solution with Customer (Prod Eng or Acct Eng as appl)

J

Customer Accepts Solution — **Yes** → **Close SR. Complete Solution Text, Fault Field & other manadatory closing fields**

No

END

Notify affected Acct/Prod Mgr & other involved personnel

Got to Impasse Procedures in TS 710.2

Resolution Becomes Available → **J**

Other Support Services

Software application

Software application procedures include the One Night Process (ONP), Two Night Process, Hybrid process, and SuperNode to BRISC Retrofit. The major steps of the software delivery process are described, beginning with the telephone company's request for new features, and proceeding through the major tasks prior to, during, and after the installation of the new software load into the telephone switch.

One Night Process

The One Night Process (ONP) is an automated software delivery process designed to step the user(s) through the delivery process. High level commands provided with the programs operate at faster speeds. The ONP collapses the normal software delivery time of seven to ten days into one night; therefore, eliminating any data modification restrictions, frozen image capture, and journal file maintenance. If manual intervention is required during the ONP, then an operating company technician and a Nortel Networks Application Engineer will be prompted to perform certain tasks.

For references on the One Night Process, see NTP 297-8991-303, *One Night Process Software Delivery Procedures*.

Software delivery planning and provisioning

For a successful software application, timely completion of activities by the operating company and Nortel Networks must occur. All involved should be informed of the documentation provided with the software application process itself. Be aware of potential hardware problems that can cause software aborts and load reschedules. Before the software update, give special attention to testing all front end memory cards and the monitoring of SuperNode software related logs (CMXXX, MMXXX, MSXXX, TRAPXXX, SWERRXXX etc.). Supporting documentation should be available and read by all personnel assigned to perform the tasks. Customer Service *Warnings and Bulletins* should also be read and reviewed. For a successful software application, it is essential that proper coordination of activities and communications between all responsible personnel be made.

Product Upgrade Manager (PUMA)

In NA006, the Product Upgrade Manager (PUMA) program to automate the delivery of software introduces CHEETAH—the PUMA subsystem devoted to Computing

Module (CM) loading. This program (which also includes the PANTHER subsystem for peripheral module loading) lowers the cost of software delivery and eliminates human errors that can cause service-affecting outages. CHEETAH facilitates CM software loading by:

- Automating 75 percent of the manually administered commands, an enhancement that reduces a One Night Process (ONP) software installation session by 15 to 30 minutes.

- Allowing the use of script files to automate workarounds and bulletins that formerly required craftsperson intervention. This capability reduces the skill level required to administer an ONP installation.

In NA007 ONP automation extends to the premature cancellation—or abort—of an ONP session as the result of an error or other problem. When an abort occurs, an ONP rollback procedure automatically restores the switch to the previous software load, including all values relevant to that load. This change also eliminates a step from the ONP, because the resetting of LOG control data for the new software load is no longer necessary. Additionally, the automation resulting from this enhancement further reduces the required ONP skill level.

Peripheral module loading

The PM upgrade process consists of the following steps:

- administration of the PM upgrade load, patch, and patch cross-reference files

- production of a recommended PM upgrade plan

- execution of the recommended PM upgrade plan A

Panther is a subsystem of Product Upgrade Manager (PUMA) that automates and simplifies the PM upgrade process. Feature AR1713 supports automation of the third phase by providing a framework to support the execution of the plan. This feature provides the following functionality:

- follows the recommended PM upgrade processes and procedures defined in the *Peripheral Module Software Release Document*

- patches the PM software load when required

- follows the upgrade plan generated by the utility PMUPGRADE

- allows the user to start, monitor, control, and abort the PM upgrade process

- allows the user to do the following:

  — perform manual PM upgrades

  — perform automated PM upgrades

  — manually perform automated PM upgrades

- notifies the user of the success or failure of each PM upgrade task

- provides the user with load names, node names, and patches to assist in manual PM upgrades

- allows the user to record the completion of manual PM upgrades

- generates logs that indicate the start of a PM upgrade shift, the end of a PM upgrade shift, the start of a PM upgrade task, and the end of a PM upgrade task

- allows the user to query the current state of the PM upgrade

- allows the user to limit the number of nodes being upgraded concurrently

- allows the user to start a PM upgrade shift, select the upgrade tasks to be executed during a shift, and finish a PM upgrade shift

- allows the user to manually execute an automated task

As of NA008, all Series 2 peripherals and Most Series 3 peripherals can also be automatically loaded now as a result of PANTHER.

C-SCAN

Customer Service Computerized Access Network (C-SCAN) is a computerized information service. The basic version of C-SCAN offers customers an efficient, cost-effective manner to access Nortel Networks customer service information by means of their own computer terminal. It should be noted that WEB sites are being set up and that information in areas such as C-SCANs may move to the WEB.

There are two ways to access the information in the C-SCAN system. For a customer, security is set up so that there is access only to their company data, or to data from other operating companies within the customer's company—as prearranged and authorized. Authorized Nortel Networks employees may view data for any of the operating companies within the system. Once accessed, the customer can view various types of supporting information, such as:

- SR Reports
- Patching Information
- Emergency Recovery (ER) Bulletins
- Emergency Recovery (ER) Warnings
- Alerts
- Maintenance/Service Advisories
- Engineering Complaints
- Installation Documentation
- Senior Management Contacts
- News Flashes
- Baseline Reports
- 88K Change Application Reports (CAPs)

- Software Delivery Bulletins
- Data Exception Reports
- Parm Variance Reports (through NA004 only)
- Product Engineering Codes (PEC)

The Customer Service Computerized Access Network (C-SCAN) is a computerized information service for Nortel Networks customers. Customers must have the following hardware to use C-SCAN:

- a PC or an ASCII terminal
- asynchronous communication through a 1200 or 2400 baud modem
- access to the TELENET long distance network service (other networks are accessible to C-SCAN)

For the basic facility, the subscribing operating company requires a full duplex, asynchronous, dial-in terminal. This terminal may be a line-by-line video display terminal or printer. Access line speed is dictated by the telnet line speed supported in your area.

For the plus facility, the subscribing operating company must have a computer system with the appropriate memory and storage capacity that is UNIX V compatible. This facility also requires that Nortel Networks and the subscriber operating company identify the following information:

- Telco: UNIX host node ID
  UNIX host phone number
- Telco: User ID and password
- Nortel Networks: UNIX node ID
  UNIX node phone number
  User ID and password

SRs on C-SCAN

The SR information is available in both summary and detail reports, and is highlighted by SR indices for quick reference. Besides indices sorted by SR number or CLLI, SR information can be obtained from the C-SCAN databases in the following three forms:

- Detail (CSSC310/RSR004) reports contain detailed information on the tracking of service reports, approximately one page for each report.
- Summary (RSR007) reports contain summaries of service reports, four to six on a page.
- Statistics on SR activity and percent of on time closures.

C-SCAN access features

C-SCAN Basic

C-SCAN Basic allows the subscribing operating company to dial directly into the Nortel Networks-INS customer access computer and view SR, DMS-10 and DMS-100 patch one line summaries, emergency recovery information, or any of the previously mentioned information. This feature is enhanced by menu driven screens with an on-line help facility. To support this feature, the *C-SCAN Users' Guide* is available through your Regional C-SCAN coordinator.

The SR data is secured by each company, while the patch and emergency recovery data is available to all companies that have access.

C-SCAN Plus

C-SCAN Plus allows the subscriber operating company to set up a UNIX data communication environment with Nortel Networks-INS Customer Service. This feature, operating in a UNIX System V compatible environment, uses the UNIX to UNIX Copy Program (UUCP) as the data transport protocol. This system provides a file transfer mechanism between Nortel Networks customer service and subscribing customers.

Operating on a predetermined schedule, the operating company UNIX System V compatible computer automatically dials up the Nortel Networks-INS computer, and initiates the process that transmits the available data files to the operating company computer.

The information on patches is in the form of a brief descriptive summary for each patch. These are called Patch 1-Liners. The Patch 1-Liners are grouped together according to the PCL for DMS-100 products, or the software generic number for DMS-10 products. The PATADM database determines nightly which sites require patches.

C-SCAN and patching

Besides being able to view patch information, C-SCAN can be used by the customer to administer patches. CI level PATCHER commands are used for applying, displaying, and removing patches for SuperNode switches. For information on the "Post-Release Software Manager (PRSM)" that replaces PATCHER, see NTP 297-8991-540, *DMS-100F Post-Release Software Manager (PRSM) Reference Guide.*

See the following subsection "Supporting Enhancements" for further information on the Post-Release Software Manager (PRSM) feature.

Customer Information Management (Canada)

Customer Information Management (CIM) is a software administration package developed by Nortel Networks to help the operating company administer service data to efficiently maintain its DMS family of switches.

This data is transferred from the Nortel Networks regional computer to a personal computer located at the operating company site. The data includes:

- Patch management
- Service Report (SR) management
- Report documents

Patch management

The first module of Customer Information Management (CIM) is Patch Management.

On a nightly basis, the customer's personal computer (PC) automatically dials into the nearest Nortel Networks regional office to transfer data concerning new/changed patches and updated *Inform Lists*.

On the next day, the patch administrator should review the transferred patches and apply comments indicating their applicability to his offices. Such comments could include: "prerequisite patch, please apply," "patch to be applied ASAP," or "not recommended at this time."

These comments are transferred to the Nortel Networks regional computer and appear in the Enhanced Application Procedure File (E-APF). The E-APF that is sent to the site at each patch transfer session shows patch interdependencies and application sequence. Patch comments provides guidance to the patch applicator.

The Inform Lists contain patch information by office and are transferred to the customer PC by CIM as they are updated. Since the PC contains the current Inform Lists, the administrator can view them with ease. In the past, it was necessary to dial into each switch to obtain this information.

Using CIM, the patch administrator can reduce the time spent relaying patch comments by conventional means (i.e., ENVOY, FAX). Since the patch information resides in a database, various queries and reports can be generated using these database capabilities.

Customer Service Report Management

CIM offers the user full Service Report (CSR) capabilities.

On a nightly basis, all new and changed CSRs and Customer Priority Lists (CPL) are transferred through CIM to the customer's PC. As with patch management, the customer is offered a wide choice of new and familiar analytical tools to review the CSR/CPL data.

Maintaining previous CSR capabilities, CIM allows the user to review the coordinator's report, which is a summary of issued CSRs. The user can read the full text of the CSR at any time. As well, statistical reports on Priority and status (OP, AN, CA...) of CSRs, CLLI, or customer can be generated easily.

Additional analytical tools include key word or string searches on the CSR title and problem text. The user can make *ad hoc* queries by choosing from up to 14 fields of information. These fields are: SR Id, Priority, Status, Fault Type, Responsible Department, Problem Code, Change Date, CLLI, City, Site, Equipment Family, Equipment Type, Processor, and Suppid.

Should the user require additional custom queries or reports, CIM supports user-defined applications. The CIM manual shows the reader examples of formulating user-defined applications.

CIM permits the user to access the Service Request (SR) action of the CSR. The progress on the CSR solution can be monitored by the SR action text.

The number of CSRs transferred on CIM can potentially be very large, since most operating companies receive their own as well as CSRs from other operating companies. An archive facility has been built into CIM. The user is able to *archive* closed CSRs to secondary storage without having to expand primary disk storage space. The user can readily *retrieve* information that is archived.

Report documents

CIM also offers report documents.

Report documents are transferred by CIM on a nightly basis as they become available from Nortel Networks. This allows the user to receive and act upon the documents sooner than through the present process of distribution by mail. The following documents are available in CIM:

- Emergency Warning Bulletins (EWBs)
- Product Notification Bulletins (PNBs)
- Customer Advisory Bulletins (CABs)
- Alerts

CIM allows the user the ability to perform various searches on the report documents:

- by type of document (EWB, CAB...)
- by identifier (ALR 00899, EWB 414, ALR CT 900730...)
- by keyword (RLCM, changes in TRKMEM)

This extensive search facility is valuable if, for example, a user wishes to obtain all report documents that may have been issued on a particular topic. Using keyword search, the user is then able to quickly find and read or print all documents relevant to that topic.

With CIM, there is no longer any need to maintain a hard copy filing system of these reports, since they are readily accessible on the PC. Should a hard copy version be required, any document can be printed from the PC with ease.

Circuit pack replacement

This service provides a like-for-like replacement or mail repair service, as well as replacements for selected original equipment manufactured items. Nortel Networks extensively tests all equipment to ensure the highest possible quality of all repair or replacement parts. Nortel Networks battery of tests include: in-service tests, transmission (analog-to-digital conversion) tests, and system level diagnostics. Depending on its complexity, a circuit pack can receive several hundred tests to identify all potential marginal and catastrophic failures. All detected failures must be repaired before the pack can pass inspection. Also, all repaired circuit packs and line cards are updated to the latest Repair Base Line.

Three standard repair service methods are available from Nortel Networks for placing a repair order: Call-In, Fax-In, or Mail-In. Response times for line cards, other circuit packs and miscellaneous are provided on the following page.

Call-In or Fax-In Service

For Call-In or Fax-In Service, once the necessary information has been conveyed to the Service Center via phone or fax, the customer is sent a replacement unit. Within 30 days of receiving the replacement, the customer must send the nonfunctional unit to the Service Center. See the following page for more information on this type of service.

Mail-In Service

For Mail-In Service, the customer must first contact the Customer Service Center. All units should be mailed to the Service Center prepaid, properly secured and with adequate insurance. Nortel Networks will ship the equipment back to the customers with the same standard of care. Upon receipt of the nonfunctional unit, the Service Center will then ship the updated, equivalent circuit pack to the customer. At the present time, there may be a 10% discount applied to the regular mail-in repair price of DMS-100 circuit packs.

Standard repair alternatives

There are three alternative services available with the standard service options. A nominal administrative fee is required for the services.

- Equal Payment Service
- Statement Billing Service
- Repair Plus Service

Equal Payment Service

Nortel Networks totals a customer's repair bills from the last six months to calculate a biannual billing amount. Nortel Networks then determines any anticipated changes in the cost of service over the next six months. The billing amount and anticipated changes are added together to provide the estimated amount of the repair bill for the

next six months. The total is then divided to determine the amount the customer pays each month over the next six months

Statement Billing Service

The customer receives one monthly bill for the previous month's repairs. All repair transactions are itemized, then totaled so the bill is for a single amount, much like a credit card billing. The option of subscribing to repair activity reports that include detailed year to date records of all equipment repairs for each site is offered.

Standard Order

Circuit Packs/Line Cards

Type of Service	Response Time**
General Repair/test	• 5 days
Emergency	• 24 hours
Outage/Degradation	• 4 hours

Miscellaneous Equipment

General Repair/test	• 30 days
Emergency	• 5 days
Outage/Degradation	• 4 hours

Repair Plus Service

Nortel Networks provides reduced repair charges for circuit packs and line cards in this program. We also provide an upgraded replacement to the current design. In addition, NTF (no trouble found) repair performance information is included in our repair service. To receive NTF benefits, customers must subscribe in advance to the NTF service, provide a valid purchase order, and return equipment to Nortel Networks with a repair tag providing diagnostic information.

To help improve the NTF performance within your company, see "Retesting circuit packs" within the "Trouble Repair" subsection of the *Corrective Maintenance* tab. It provides suggestions for testing circuit packs.

Service benefits

- Reduces administrative costs by as much as 75% by using only one invoice per month instead of using multiple invoices

Call-In or Fax-In Service Information

CONDITION:	TIME AVAILABILITY	PHONE NUMBER
•General Replacement	24 Hours	(800) 347-4850
*Emergency Issues during Busines Hours	(8:00a.m.-5:00p.m., EST)	(800) 347-4850
*Emergency after Business Hours	(Weekdays after 5:00p.m. EST, Weekends, Holidays)	(800) 627-8318 or (919) 688-8363

*Emergency Criteria
- An out-of-service condition occurs
- The last spare of a circuit pack has been used
- Northern Telecom's Emergency Technical Assistance Service (ETAS) Center or Field Technical Service (FTS) has so advised.

•Faxed orders	24 Hours	(919) 992-2555

If the order is faxed during business hours (8:00a.m.-5:00p.m., EST, Monday-Friday), the Customer will receive a return acknowledgment within two hours. Orders faxed after business hours will be processed during the next business day.

- Offers very basic to relatively in-depth repair data to aid in spotting trends and reduce expenses
- Offers up to a generous 18 month warranty for circuit packs versus one year with the standard repair service
- Customized services to better help customers meet their individual needs
- Offers prepaid transportation from Nortel Networks to the customer

For more information on repair services, please call or mail:

- 1-(800) 347-4850 Option 1
- Emergency Service Number (800) 627-8318 or (919) 688-8363
- Repair Services FAX number (919) 992-2555
- In Canada, call (416) 454-2808
- Repair Services Mailing Address

  Nortel Networks Plaza Service Center
  4600 Emperor Boulevard
  Morrisville, NC 27560

  Attn. Mail-In Repair Service/Dept. 6677

World Line Card repair attachment

A maintenance enhancement for the World Line Card (WLC) allows for the generation of LINE170 and LINE171 logs that provides measured information for WLC

diagnostic failures. An optional parameter "D" has been added for the DIAG command to allow the logs to be generated with failures. The intent is to provide the log information as an attachment to the card when it is returned for repair. When equipped with WLCs, this should be part of the repair and return procedures.

DMS-100 warnings and bulletins

Warnings

Nortel Networks issues Emergency Recovery (ER) warnings to its customers advising them of potentially serious problems and the steps necessary to avoid them. These warnings are distributed to operating companies as soon as Nortel Networks becomes aware of any problems that can cause an emergency. This information is of an urgent nature that should be handled on an emergency or very high priority basis.

The warning describes the nature of the problem, corrective activity, or workaround actions that should be taken to avoid the problem, including actions that Nortel Networks has taken to correct the problem. Material for warnings includes: *killer* patches, fire and safety hazards, serious call processing problems, deficient procedures, or documentation errors that have caused serious problems. A warning has a priority assigned according to the severity of the problem:

- **Priority 1** (causes service degradation/outage)
- **Priority 2** (may cause service degradation/outage)
- **Priority 3** (does not cause a service impact)

Bulletins

Emergency Recovery (ER) bulletins deal with nonemergency issues that concern the maintenance of the switching equipment. Material for bulletins includes: maintenance activities, revised technical procedures not yet included in standard product documentation, testing procedures, kit information, and nonservice as well as service affecting situations. The bulletin describes the problem, provides a temporary workaround if needed, and corrective action to be taken by Nortel Networks.

There is no charge for the warning or bulletin service. The warnings and bulletins are issued from our regional facilities over C-SCAN. Past issues can be found on Helmsman within PLN-8991-199, *DMS-100F Documentation Warnings and Bulletins.*

Change application services

A *product change* is a modification to an existing product. It can be a simple component change to a complex modification that requires a complete redesign of a circuit.

A Product Change Notice (PCN) is a term used for a written notice that describes a change for a product, such as a circuit pack. Suppliers of equipment are required to submit PCNs to customers for changes on their products. For Bell Operating Compa-

nies (BOCs) that time is generally within 30 days of the release date of the product change.

When a circuit pack change is required, Nortel Networks comprehensive Office Release Record (ORR) database shows offices that are affected. Nortel Networks customer support arranges for new circuit packs of the required release to be shipped to the office. The old release packs are returned so Nortel Networks can verify that the application was a success and to update the database records.

If the NTX120AA Office Hardware Inventory Package (OHIP) is provided in the system features, ORR data can be stored and maintained in the switch rather than the Change Control Log (CCL). It allows customer and Nortel Networks personnel to access the information either locally or from a remote location.

When changes must be performed on-site, the field installers arrange a suitable time with the operating company control center (SCC, NOC, etc.) or site personnel to perform an audit and complete the change application.

Product change classifications

To effectively manage Nortel Networks hardware evolution, the following Bellcore standard classifications apply:

Class 'A'   Correct an inoperative problem

Class 'AC'   Correct an inoperative problem on a conditional basis

Class 'B'   Incorporate design improvements at customer request and cost

Class 'D'   Incorporate new features

Change application procedures

Change Application Procedures (CAPs) describe the procedures and testing requirements necessary for implementing the change. CAPs can be accessed through C-SCAN. Baseline reports providing individual office PCN summaries are also available on C-SCAN. Details on Product Change Kits can be found in Helmsman PLN-8991-103, *Engineering Manuals*.

TR-OPT-000209, *Guidelines for Product Change Notices*

This Bellcore Technical Reference (TR) provides PCN guidelines for BOCs and their equipment suppliers. This document establishes the time frames for delivering and implementing PCNs. Also included are the classifications for PCNs, requirements for Method Of Procedures (MOPs), supplier and operating company responsibilities, and descriptions of the reports and summaries for PCNs.

Engineering complaint services

Engineering Complaints (ECs) are written documents that define a deficiency in a supplier's product. That product could be in various forms, such as software, hard-

ware, safety hazards, design errors, high failure rates, installation errors, shipping and ordering errors, and documentation errors of any kind.

Engineering complaint processing

An engineering complaint form or similar document should have the location and details of the problem clearly defined before it is sent to Nortel Networks. Lack of details can only cause delays in the processing of the ECs.

Engineering complaints are usually mailed to a Nortel Networks Regional Customer Support Services EC Coordinator. An acknowledgment is sent to the customer. If the EC problem cannot be resolved on a regional level, then it is sent to the Nortel Networks Core group for further processing. Generally, within 90 days, Nortel Networks sends a reply to the customer stating what action is to be taken. This could be a request for more time to resolve the problem. Engineering complaint processing will vary depending upon the company contract agreement and policy for handling ECs, and the TR requirements established by Bellcore for the BOCs.

Engineering complaint reports

Nortel Networks provides a report to the customer stating the acceptance or rejection of the EC problem. Status reports are generally provided to the customers on a quarterly basis.

Online customer support

You may access Nortel Networks Customer Support online at www.nortelnetworks.com and then selecting Customer Support. Services available online include:

NOTE: Login may be required. Follow the instructions on the screen.

- Software Distribution

  If you have bought service packages you can obtain software, images, patches or codes to activate their features directly from the Web.

- Customer Service Requests

  Enter, query and track the progress of your trouble tickets and service requests for problems or support issues with Nortel Networks products.

- Keycode Retrieval System

  Retrieve keycodes for Meridian 1 and Business Communications Manager products.

- Service Programs

  Access complete professional services for areas such as AssurancePak Registration, network design and management, Assurance Online, enterprise network management, etc.

- Certification

Nortel Networks Certification Programs that are available include Service Provider and Carrier Solutions, and Enterprise Solutions (Voice & Data) programs.

- Training

  Register for classroom or computer-based training or, in some cases, get online training for some Nortel Networks products.

- Documentation

  Product Bulletins

  Browse or download Nortel Networks product and support documentation from the Web.

- Self Help

  Find the help you need to resolve your issue(s) by browsing published solutions in our database.

- Repair Services

  View and track warranty entitlement information for the products you purchased (available for certain products in some regions).

- Tools

  Retrieve the tools that you need to access newsgroups, drop boxes, searches and News-Flashes.

Supporting Enhancements

This subsection briefly describes some of the supporting feature enhancements for maintaining and operating DMS-100F switches.

These enhancements build more automation into the DMS administrative type activities, faster access to needed information from the DMS switch, and on-line databases.

The following enhancements can help to ensure that tedious and laborious work operations are performed as scheduled with less personnel involvement:

- Post-Release Software Manager (PRSM)
- Table Audit (TABAUDIT)
- System Recovery Controller (SRC)
- Outage footprint
- Sherlock data collection tool
- CC mismatches
- Automatic image dump
- Scheduled patching
- DMS Schedule (DMSSCHED)

Post-Release Software Manager (PRSM)

The Post Release Software Manager (PRSM) is a DMS tool that applies software updates distributed after the release of a milestone load. PRSM software replaces PATCHER software, while maintaining and increasing the functionality of PATCHER. The result is a new, high quality software updating tool similar to PATCHER. The similarities facilitate the transition from using PATCHER to using PRSM.

See NTP 297-8991-540, *Post-Release Software Manager (PRSM) Reference Guide* for information on using PRSM and for support on the transition from using Patcher to using PRSM. Also, see NTP 297-8991-541, *PRSM Basic Commands, Syntax, and Examples (with Patcher Command Comparison)* and NTP 297-8991-542, *Post-Release Software Manager (PRSM) Quick Reference Guide* for other supporting information.

PRSM functionality is controlled either manually or automatically. This allows the user to choose between complete automation and manual intervention.

PRSM manual commands

PRSM CI provides the ability to perform PRSM functions manually. Commands performed in PRSM CI are as follows:

- VALIDATE
- APPLY
- REMOVE
- FREEMEM
- ASSIGN
- DBAUDIT
- FILEAUDIT
- DISADMIN
- PRSMSET
- SETDEF
- SELECT
- SELDEF
- HELP
- AUTOAPP (see automated processes next)
- AUTOPROC (see automated processes next)

PRSM automated processes

PRSM automates certain PRSU maintenance functions through the following processes:

- FILE AUDIT
- AUTOAPP
- STATUS AUDIT
- AUTOPROC (hidden command)

File audit process

The file audit process runs prior to the AUTOAPP process. It searches SFDEV and the devices datafilled in table PADNDEV for new PRSUs and validates them. It also searches for duplicate PRSU files and for missing XPM PRSU files. If such PRSUs are found, the FILEALARM field is set to Y for the PRSU in the PRSM database. The PRSU filename and device information is reported in the PRSM360 log.

AUTOAPP process

The autoapply process (AUTOAPP) can be used to automatically apply certain PRSUs. PRSUs which have been validated, have a CUSTAPP value of Y, a PSTATE value of PRSU_OK, and an AUTOAPP value of Y are eligible to be automatically applied by AUTOAPP. This process runs after the PRSM file audit on the days specified by the MTWTFSS field in table AUTOOPTS.

PRSUs downloaded using PADN or DMSCOM are automatically validated by the PRSM file audit, providing complete automation for most PRSUs. Results of AUTOAPP are reported in the PRSM400 log and the PRSM680 log.

The AUTOAPP process also can be executed manually by the AUTOAPP command.

Status audit process

The status audit process runs after the AUTOAPP process. It ensures PRSM database integrity by running a DBAUDIT. After the DBAUDIT, the status audit searches for any PRSUs which are in alarmable conditions. The alarmable conditions are defined by the datafill in table PRSMALRM. PRSUs that meet any alarmable conditions have the STATALARM field set to Y for the PRSU in the PRSM database. The results of the status audit are reported in the PRSM470 log.

AUTOPROC

This command allows you to start, stop, delay, or query any of the PRSM automated processes (File Audit, Autoapply, Autoinstall, and Status Audit).

The AUTOPROC command includes the following characteristics:

- You cannot start an automated process using the START parameter if any automated process or the PRSM Scheduler is performing work.

- The DELAY parameter cannot be executed successfully for an automated process if the automated process is running.

- The DELAY parameter only affects the automated process when it is executed by the PRSM Scheduler.

- The AUTOPROC ALLSTART command function is not supported. If you want to execute all PRSM automated processes, table AUTOOPTS and AUTOPRSU must be changed to allow the PRSM Scheduler to perform the required work.

- The commands associated with the Autoinstall process are only supported in GSF-specific software loads.

- If the DROPSYNC field is set to "Y" in table AUTOOPTS when the AUTOPROC AUTOAPP START, or AUTOPROC AUTOINST START commands are invoked, the Autoapply or Autoinstall process drops synchronization on the switch before applying or installing post release software updates (PRSU)s.

PRSM terminology

- Post-Release Software Manager (PRSM) - replaces the DMS tool, PATCHER. PRSM applies software fixes distributed after the release of a milestone load.

- Post-Release Software Update (PRSU) - represents a software change necessary for normal maintenance of a DMS-100F office. A PRSU is distributed after the release of a milestone load. A patch is one type of PRSU. Additional types are planned for introduction in the future.

NOTE: A prsuid is the name of a PRSU.

- User - is the human or machine using PRSM through either the CI interface or the machine interfaces provided.

- Destination - represents a single, patchable entity in a DMS-100F office. The term DEST is used interchangeably with destination. For instance, LTC 0 0 is a destination, LTC 0 1 is a destination, and each of the following is a destination:

  — MS 0

  — MS 1

  — LIM 0 0

  — LIU7 15

  — ESA 5

- PRSU Files - are either $PATCH or $DF files.

  — $PATCH file - is more commonly known as a PRSU file. The $PATCH file is the SOS file associated with the prsuid.

  — $DF file - contains a subset of the information contained in a $PATCH file. This subset of information can be used to determine if a PRSU can be applied in an office.

NOTE: By creating a $DF file and validating it, it can be determined if the $PATCH file will apply.

TABAUDIT

TABAUDIT is a table verification process that can be run prior to making an image tape (approximately 15 days prior to the scheduled application) and periodically after the image tape is made to verify office data. Errors and inconsistent data identified by TABAUDIT should be corrected by the telephone company prior to making the system image tape. This process decreases the need for Nortel Networks to contact the customer during the dump and restore process for direction on how to correct table errors.

> **Warning:**
> TABAUDIT can take up to 10 hours to run. The length of time will vary from site to site depending on the number and size of tables. TABAUDIT is not "image safe." Check table AUTOSCHED before defining AUTOTABAUDIT. Do not schedule TABAUDIT to execute at the same time as an auto image.

Nortel Networks recommends that data integrity checking using TABAUDIT be made a regular and ongoing part of normal maintenance procedures. By using the automatic scheduling function this can be accomplished with a minimum of effort.

Sometimes, known error may be encountered when executing TABAUDIT. Look for Nortel Networks TAS bulletins that identify the tables and any fixes if applicable.

For detailed procedures on the use of the TABAUDIT command and the automatic scheduling AUTOTABAUDIT command, see NTP 297-8991-303, *DMS-100F One Night Software Delivery Procedures.*

TABAUDIT enhancement

The TABAUDIT Enhancement feature (AR1917) improves the automated TABAUDIT scheduling capabilities, timeframe specification, and user interface. Use the enhancement if upgrading from Base08 and higher. Feature AR1917 improves the automated TABAUDIT scheduling capabilities, timeframe specification, and user interface. This feature makes the following improvements:

- It makes TABAUDIT easier to use, especially automated TABAUDIT.

- It decreases the number of failed tables and tuples during the table transfer portion of the ONP.

This feature includes the following changes:

- TABAUDIT enables multiple iterations of data checking.

- Some Command interpreter (CI) commands change to include more options. These changes provide users with a more flexible user interface.

- The TABAUDIT architecture changes to make the tool more robust and easier to expand.

System Recovery Controller (SRC)

The System Recovery Controller (SRC) feature was introduced in BCS33. It acts as a high-level intelligence to coordinate system recovery activities, and optimizes the use of system resources needed for recovery following system degradations. The SRC aids in reducing outage time, and decreases the amount of manual intervention that might be necessary.

The SRC coordinates the recovery of nodes in the DMS switch so that when one node is dependant on another for operation, the node which is depended upon must be in-service before a recovery attempt is made on the dependant node. As it progresses

through the dependency hierarchy, the SRC schedules recovery activities to run at appropriate times, thereby reducing the length of outages.

The SRC will make several attempts to recover a node. With each recovery attempt, the SRC performs a more detailed analysis. If necessary, the SRC reloads a node's software and returns the node to service as part of a full recovery process. Reloading a node removes the node from service for a period of time, so the SRC reloads nodes only when required.

For further details on the SRC, see NTP 297-YYYY-545, *DMS-100F Recovery Procedures.*

Outage footprint

Overview

The Outage Footprint Phase II Feature AL0044 in software package NTX001AA provides a method for determining the cause of serious NT40 and SuperNode switch outages. Footprint support for the BNR Reduced Instruction Set Computer (BRISC) is provided in feature AL1587 of the NTXF97AA BRISC Series SuperNode Base software package. The footprint feature has three purposes:

- Provide a history of information that may have led to an outage.
- Take a snapshot of the system when an outage occurs.
- Output outage related information in a human-readable form.

The outage footprint facility (henceforth footprint) operates in three modes:

- Recording
- Snapshot
- Output

Footprint automatically enters the recording mode after a system image reload. In this mode, footprint records traps, mismatches, warm restarts, cold restarts, and software-induced activity switches. These events can help point out the cause of the outage.

This information is stored in DSSAVE. This type of data store survives every type of restart except a system image reload caused by a power loss. For power losses, all recorded information is lost and recording begins again as if the restart is the initial booting of the image. Three recorded events can be viewed by using the DUMP command in the FOOTPRT CI directory.

Footprint enters the snapshot mode when a CC restart occurs. This means footprint copies critical system data, such as some hardware registers and some RAM contents, to a storage area for output after the outage is over. This gives the maintenance support group more information to use when analyzing the outage.

Footprint enters the output mode when requesting outage related information. It displays all the events in the event buffer and displays the snapshot associated with each warm restart, cold restart, and any activity switch restart. The user can have the values in selected system registers decoded into a human-readable form by using the TRNSL command in the footprint CI directory, FOOTPRT.

100 events can be stored in the FOOTPRT file. Storing more events would require using more data store, which may cause problems for more critical data store users.

Reload restarts are not recorded, and a snapshot of the system after a reload restart is not taken. The reason for this is that much of the data placed in the snapshot is lost over a reload restart.

Under certain circumstances, the active CC may fail in its attempt to read the inactive CC's footprint buffer. Hardware problems or a power loss on the inactive CC are two such circumstances.

Footprint commands

Footprint has a CI directory of its own, called FOOTPRT. This makes entering footprint commands easier and faster. Only one user is allowed in the FOOTPRT CI directory at a time. A brief summary of the FOOTPRT commands follows:

>DISPLAY - Displays summary information about any footprint buffer.

> CPU - The active CPU will usually carry a copy of data collected on the mate CPU. The copy can be displayed by specifying the CPU.

>FPBUF - Display event data for any footprint buffer. (see: DISPLAY) BUFFER - Any of the buffers from the display command.

> CPU - The active CPU will usually carry a copy of data collected on the mate CPU. The copy can be displayed by specifying the CPU.

> CLASS - Display only events of this class name. Omitting the class name will display all classes.

> MAXCNT - Number of footprt entries to display. Omitting the count, or entering 0 will display all.

> DETAIL - The brief option will only show the event headers.

>GETMATE - Attempts to transfer a copy of the data collected on the mate CPU (inactive), to the active CPU. You cannot transfer data from the active CPU to the inactive CPU.

>REPORT - Display the registration data of an event or class. Names that are registered in lower case letters need to be enclosed in single quotes so that are not converted to upper case letters by the command interpreter.

> CLASS - Which class name to use. Omitting the class name will select all classes.

> EVENT - Which event name to use. Omitting the event name will select all events in the specified class.

>UNLOCK - Releases the LOCKED buffer so it can be reused by the next event that causes the active buffer to be locked. Once released, the data is not guaranteed to remain in that buffer, and could be destroyed at any point.

Footprint logs

After restarts, the DMS-core generates FP logs for certain conditions. FP logs include the following information:

- a message indicating corruption of FP data
- snapshot data obtained from the active CPU during a restart
- snapshot data obtained from the inactive CPU during a restart
- a message indicating that the initial transfer attempt of the inactive CPU FP data failed
- a message indicating that the second and final transfer of the inactive CPU FP data failed

After a restart, the DMS-core generates a log containing the active CPU snapshot data. If a restart occurs while the CM is out of sync, the DMS-core generates an additional log indicating whether the transfer of the data between the inactive CPU and the active CPU is successful. If the transfer was successful, the log contains snapshot data from the inactive CPU. If the transfer was not successful, the log contains a message indicating the failure of the active CPU to obtain the inactive CPU data.

If a restart occurs while the CM is out of sync, and the initial data transfer from the inactive CPU failed, then the next manual sync attempts a similar transfer. If this second data transfer is successful, the log contains the inactive CPU snapshot data. If the second data transfer of data is unsuccessful, the log contains a message indicating that the second and final attempt to obtain the inactive CPU data has failed.

If an image test fails during a CM REx test, the system attempts to transfer the inactive CPU's footprint buffers to the active side for debugging purposes.

Following are footprint FM logs and triggering information for the SuperNode and SNSE:

NOTE: With BCS33 the log report subsystem 'FP' has been renamed as 'FPRT' to avoid confusion with the file processor (FP) peripheral log reports. So FPRT10_ log report is same as the FP10_ log report prior to BCS33.

FP100/FPRT100   —   ACTIVE CPU FOOTPRINT SNAPSHOT

Footprint snapshot data has been collected from the active CPU. The report is generated after the completion of every restart, except restarts caused by power loss.

FP101/FPRT101   —   INACTIVE CPU FOOTPRINT SNAPSHOT

An out of sync restart occurred, in which the active CPU obtained the FP data from the inactive CPU.

FP102/FPRT102   —   RESTART OUT OF SYNC

An out of sync restart occurred, in which the transfer of the inactive CPU FP data to the active CPU was unsuccessful.

FP103/FPRT103   —   RESTART OUT OF SYNC

The transfer of the inactive CPU FP data failed following the completion of a manual transfer.

FP104/FPRT104   —   RESTART SYNCTXT

An out of sync restart completed, in which the transfer of the inactive CPU footprint data to the active CPU was unsuccessful.

FP105/FPRT105   —   RESTART AND REBOOT SUMMARY

The Footprint (FPRT) subsystem generates this log report after any restart or reboot. It is similar to the FPRT100 log but contains less information as all the information from the FPRT100 is recorded in the FOOTPRINT snapshot event.

Feature AL1976

With BCS33 feature AL1976 provides a footprint utility on the application processor (AP) to record critical system events for maintenance personnel. The following events are collected:

- support operating system (SOS) events
- computing module-specific events that are common to the AP
- events that are specific to the AP only

This feature modifies logs FPRT100, FPRT102, FPRT103, and FPRT104:

- Log FPRT100 is generated when a restart is completed, except those restarts caused by a power loss.
- Log FPRT102 is generated when an out of sync restart is completed, in which the transfer of the inactive CPU footprint data to the active CPU was unsuccessful because data was unavailable.
- Log FPRT103 is generated when a manual sync is completed, in which the transfer of the inactive CPU footprint data was attempted and failed.
- Log FPRT104 is generated when an out of sync restart is completed, in which the transfer of the inactive CPU footprint data to the active CPU was unsuccessful due to data corruption.

User interface, the command REPORT is added to the FOOTPRT level of a MAP terminal. The command is used to do the following:

- turn on and off the recording of one or all AP footprint-specific events
- query the recording status of one or all AP footprint-specific events

Sherlock

Sherlock is a data collection tool that is designed to be used immediately following a service outage. It automatically collects the data that is required to analyze the cause of the failure. Sherlock can be used by only one person at a time. Following is the CI level information from inputting HELP SHERLOCK:

Collect data for service failure analysis.

Parms: <REQUEST> {COLLECT <SERVICE FAILURE> {CORERESTART,

                          CORESWACT,

                          MS,

                          LPP,

                          MSB7,

                          TOPS,

                          MDC,

                          CALLP_MISC,

                          XPM <PM Type> STRING

                            <PMNo> {0 TO 2047},

                          LCM <LCM Type> {ILCM,

                                LCM,

                                LCME,

                                XLCM}

                            <Site> STRING

                            <Frame> {0 TO 511}

                            <Unit> {0 TO 1},

                          NETWORK,

                          AMA}

                <OUTPUT DEVICE> DEVICE name

                <START TIME> STRING

                <END TIME> STRING

                [<OPTIONS>... {NOCOMP,

                        PMDEBUGONLY,

                        WAIT}],

          STOP,

          QUERY}

Sherlock initiates a set of parallel processes that collect all the data available for the specified type of service failure. The data is then sent to a series of temporary files that you cannot access or manipulate unless you stop the Sherlock process before data collection is complete. Once data collection is complete, a data file and a console file are created on the specified storage device, and the temporary files are erased. The data file is named SHRKyymmddhhmmss(Z) and contains the data (Z means the file is compressed). The console file is named SHERLOCK$OUT and contains all the

messages and responses sent to your terminal, and some additional messages, such as time stamps.

CC Mismatches

The CCMNT level of the MAP contains information about CC mismatches, including the number of mismatches in the last seven days, the previous day, and the present day. This provides an indication of how fast an office may be degrading.

Mismatch summary information can also be obtained by using the DMSMON utility command LOGCOUNTS or the CI level MMINFO command described below.

SN/SNSE mismatch logs are generated when the mismatch handler program is invoked. When the matcher circuitry detects a mismatch, the maintenance controller generates a mismatch interrupt. The current values of the status register and the program counter are saved on the interrupt stack, and all hardware is queried for faults.

Once the hardware fault data is collected, the mismatch handler program starts executing. The mismatch handler determines whether it is safe to continue running in sync, which CPU should be active, what component failed and caused the mismatch, and what further recovery action should be taken.

The progress of the mismatch handler is monitored by a set of progress marks. The result of the mismatch analysis is based on which progress mark the handler reaches.

The final action of the mismatch handler is to determine what post-mismatch recovery action to take. Post-mismatch recovery actions include the following:

- No recovery needed. This action is usually seen on transient mismatches.
- Attempt store match. This action is taken for correctable memory errors.
- Attempt copy store. This action is taken when the mismatch handler attempts to spare a memory module and the sparing utilities have not ensured that the store was copied.
- Attempt full sync. This action is always taken because synchronization is usually dropped during mismatch handler execution.
- Complete mate test. This action is taken when a fault has been isolated to a particular component.
- Test mate no sync. This action is taken when synchronization has not been reestablished.
- Indicate self fault. This action is taken when the CPU that is active is known to be faulty, but activity could not be switched.

The data collected, the progress mark reached, and the recovery action that the switch is taking are recorded in the MM100 and MM101 mismatch logs. Once the mismatch recovery action is complete, a postrecovery log is generated. The postrecovery logs are numbered MM110, MM111, MM112, and MM113. These logs tell you the state of the switch after the mismatch.

MMINFO command

MMINFO is a Command Interface (CI) tool that consolidates, manages, and displays mismatch information in an easy to read format. The MMINFO performs the following functions:

- management of the mismatch information database
- generation of MMINFO reports on request

When the user enters a MMINFO CI command, the system records a snapshot of the database. The system copies the snapshot into a local database version. The MMINFO database accommodates a maximum of 20 entries for the Series 20 to 60 SN. The database accommodates a maximum number of 10 entries for the Series 70 SN.

Responding to mismatch logs

The manual action to be taken after a mismatch depends on the type of mismatch detected, and the state of the switch after system recovery is complete.

When postrecovery logs MM111, MM112 and MM113 are generated, the logs provide the specific information concerning where the fault is, and what action to take in order to resolve the fault.

When the MM110 postrecovery log is generated, the system maintenance was able to correct the fault which caused the mismatch, and the switch has been returned to normal synchronous operation. No immediate manual action is required to return the switch to service, but a program to track long-term transient fault occurrences should be developed.

For example, a program to track the number of correctable memory fault errors should be followed before a memory pack is removed from service due to this type of fault. The log module for the MM100 log describes the cause of correctable memory faults and the short-term and long-term limits for the number of acceptable correctable memory faults in different memory configurations.

No action is required if the recommended acceptable rate of occurrences is not exceeded. Once a short-term rate is exceeded, maintenance personnel should determine if the occurrences are randomly distributed among the memory cards, or whether a single card is being consistently flagged. If the correctable faults are random, then the switch should be closely monitored to determine if the 28 day rate is exceeded.

For further details on CC mismatches, see NTP 297-5001-548, *DMS-100F DMS SuperNode and DMS SuperNode SE Computing Module Maintenance Guide* and NTP 297-YYYY-840, *DMS-100F Log Reference Manual.*

TRAPINFO

TRAPINFO is a tool that extracts information about software traps from the log utility and displays the information.

Automatic image dump

Overview

The Automatic Image Dump features F7117 and F7349 in the NTX074AA Disk Data Storage System software package allows for image dumps to be taken automatically for SuperNode switches.

With the introduction of these features the image taking process becomes automated and eliminates the need for human intervention. It also improves efficiency and ensures a current image is always available.

These features allow the customer to schedule image dumps on any day of the week and time defined in table lMGSCHED.

Implementation of this feature requires the datafill of two tables, IMAGEDEV and IMGSCHED, and the use of the CI command AUTODUMP.

Automatic image dump commands

AUTODUMP

The AUTODUMP CI command introduced for use with the scheduled image dump feature has the following sub-commands:

>AUTODUMP <PARMS>

HISTORY	displays the history file for the last scheduled image dump
STATUS	displays information about the last dump taken, indicates if the system is manually turned on or off
ON	turns on the scheduled image dump process
OFF	turns off the scheduled image dump process
MANUAL	starts an image dump on command
RETAIN	change the primary load route updating

STOPDUMP

The STOPDUMP command is used to stop a scheduled image already in progress. There are no other PARMS required with the use of this command.

CCMNT affected

The screen for the CCMNT MAP level is also affected. A new field is provided that displays the current image status and the most recent image volume. If a failure in the automatic image process occurs, a minor alarm is given and DUMP should appear under the CC heading on the MAP.

Automatic image dump tables

IMAGEDEV table

Table IMAGEDEV defines the image file storage devices used in the automatic image dump process. Each tuple in this table consists of two fields, VOLNAME and ACTIVE. This table has a maximum size of four corresponding to the four load routes. Following is the required datafill:

Table IMAGEDEV

FIELD NAME	ENTRY	EXPLANATION
VOLNAME	alphanumeric	VOLUME NAME, enter the name of the disk volume where the image will be dumped.
ACTIVE	Y, N	ACTIVE, enter "Y" if the datafilled volume should be used, or "N" if it should be ignored.

IMGSCHED table

Table IMGSCHED is used to track and schedule the automatic image dump process. Each tuple in this table consists of four fields: DAY, DUMPHOUR, DUMPMIN, and ACTIVE. The table has a maximum size of seven tuples corresponding to the seven days of the week. Below is the required datafill:

Table IMGSCHED

FIELD NAME	ENTRY	EXPLANATION
DAY		alphanumeric DAY OF THE WEEK, the field entries are MONDAY through SUNDAY and cannot be added, deleted or changed.
DUMPHOUR	00 — 23	DUMP HOUR, enter the dump start hour. This is in military time, default is 9:00 p.m.).
DUMPMIN	00 — 59	DUMP MINUTES, enter the dump start minutes. Default is 00.
ACTIVE	Y, N	ACTIVE, enter "Y" if is to be dumped this day, "N" if not.

After the two tables listed above have been datafilled, then you should start the auto-image process. The auto-image process is started by entering the CI command AUTODUMP ON.

Notes and recommendations

If any tuples are not datafilled, the auto-image will not run.

If one volume is defined, the auto-image dumps the image only to that volume.

If more than one volume is defined, then the next image occurs on the next available volume. If the current volume is the last one, the auto-image process will rotate to the top of the table and use the volume defined in the first tuple.

If a tuple is datafilled in either table but the ACTIVE field is set to "N", the auto-image will not run on that day nor use the oldest volume, depending on the table.

Only one image can be scheduled per day without table modification. Only one image can be taken at a time.

Auto-image will not run if DUMP UNSAFE commands or activities are in use. An example would be the automatic line test (ALT).

Starting and stopping of the *journal file* is controlled by the AUTO DUMP process.

The existing DUMP command is not affected by this feature and can still be used.

Some offices may need to increase the size of their disk volumes to accommodate two images. The DDU Image Volume Size Increase feature (F2792) in the NTX074AA software package allows the volume sizes to be increased from 32 megabytes to 64 megabytes.

Scheduled patching

See the Post-release Software Manager (PRSM) feature in the beginning of this sub-section. PRSM software replaces PATCHER software, while maintaining and increasing the functionality of PATCHER

Overview

Scheduled patching features for the CC, CM, MS, XPMs, and Intelligent Service Nodes (ISNs) provide the DMS office with the ability to automatically apply patches with little human intervention. The scheduled patching features is sometimes known as *auto patch*. The operating company still has complete control over the patch process through table control and may select or reject patches and determine method of application, either automatically or manually.

The Automatic Patch Application process is controlled from three tables: PADNDEV, PATSET, and PATCTRL, and one new CI command GETPAT. It is through the

manipulation of these tables that the operating company controls the auto patch feature. Table PATNS was added in BCS35 for the Auto Patch process.

Patching tables

PATNS table

Table PATNS is a table of default nodesets that may be used by auto patcher for patching nodesets or autosets. The table contains the node, nodeset name, device numbers, unit number, and Boolean indication whether each nodeset should be included in the autoset. Table PATNS must be datafilled before tables PATCTRL and PATSET for ISNs.

PATCTRL table

The PATCTRL table contains a list of patches that are available to the switch and the information to control the Automatic Patch Application process. The CI command GETPAT must be entered before table PATCTRL can be updated. This table keeps track of the unapplied patches that have been downloaded and reside on the Store File Device (SFDEV), or the devices specified within table PADNDEV (if NOP software is present). At the scheduled time set in table PATSET, the process awakens to apply the patches listed in table PATCTRL that have been approved for application.

Tuples may not be added or deleted from this table by a user. The only tuple attributes that may be changed by a user are the DATE and the APPROVED fields for CC patches, and the DATE, APPROVED, and ACTION fields for XPM patches.

The following is a list of the tuples for the PATCTRL table; however, reference NTP 297-YYYY-350, *DMS-100F Translation Guides* for current detailed information:

FIELD NAME	ENTRY	EXPLANATION
PATCHID	alphanumeric	PATCH IDENTIFIER, the patch ID given to the patch is entered here.
CAT	ACT, GEN	CATEGORY, the category assigned to the patch is entered here.
TARG	CC,CM,XPM	TARGET, the type of processor to which the patch is applied.
APPLY	Y, N	SAFE TO APPLY, a "Y" indicates the patch is safe to apply, an "N" indicates the patch is not to be applied by the auto application process.
APPROVED	Y, N	TELCO APPROVAL, enter "Y" or "N" to approve or not approve the respective patch for auto application.
DATE	numeric	DATE, enter the date, yymmdd, on which the patch is applied.

ACTION	APPLY_ALL APPLY_ODD APPLY EVEN	ACTION, enter the action to be taken on XPM patches to be applied in the odd, even, or both units of the XPM.
ACK	FAILED, PARTIALLY_APPLIED PENDING, FULLY_APPLIED APPLY_MANUALLY OUT_OF_SEQ MISSING_NEED	ACKNOWLEDGEMENT Enter FAILED to indicate that the action requested under the ACTION field of the table has failed. Enter PARTIALLY_APPLIED to indicate that only partial application has been applied. Enter PENDING to indicate that the patch has been DLCHECKED and placed within the table. Enter FULLY_APPLIED to indicate that the patch is successfully applied. Enter APPLY_MANUALLY to indicate that the patch can be applied manually. Enter OUT_OF_ SEQ to indicate that the patch administration number is out of sequence. Enter MISSING_NEED to indicate that there is a patch missing before the patch can be applied. The default value for this field is PENDING.

PATSET table

The PATSET table is used by the Automatic Patching Application process to establish default values for entries within the table PATCTRL. Tuples may not be added or deleted from this table by a user. However, an EXT (AUTOSUB) file may be used to establish this single tuple table. All the tuple attributes may be altered by a user except for the key field. The user is warned if the scheduled time for auto patch has been changed, or the scheduled time conflicts with the REXTST or auto-image schedules.

The following is a list of the tuples for the PATSET table; however, reference NTP 297-YYYY-350, *DMS-100F Translation Guides* for current detailed information:

FIELD NAME	ENTRY	EXPLANATION
TUPLE	AUTOPTCH	TUPLE, enter "AUTOPTCH" in the field, it is the only a key identifier allowed.
DATE	numeric	DATE, enter the date on which patches are to be applied, yymmdd.
START	numeric	START TIME, enter the start time at that the automatic process is to start (military time).
END	numeric	END TIME, enter the time at which the automatic process is to end (military time).
APPROVED	Y, N	APPROVED, enter the value set for the APPROVED field in table PATCTRL.
XPMVAL	numeric	PERCENT, enter the permissible node application failure rate for XPM patches.
AUTO	Y, N	AUTOMATIC PATCH APPLICATION PROCESS, enter "Y" if the process is to run, enter "N" to disallow the auto process from starting. This tuple may also be set to "N" to stop the Auto Apply process.
PREMON	numeric	PRE-MONITOR TIME, Duration (in minutes) before the auto patch process in which logs are checked.
POSTMON	numeric	POST-MONITOR TIME, Duration (in minutes) after the Auto Patch process in which logs are checked.
THRSHOLD	numeric	THRESHOLD, percentage of log counts taken from pre- and post-application snapshots of logs.
APLNSYNC	Y,N	APPLY-IN-SYNC, Allows auto patch process to run in or out of sync.
STOPFAIL	Y,N	STOPFAIL, Allows the auto patch process to continue or cease the application of patches after a patch has failed to apply.

MAXAPPLY	numeric	MAXAPPLY. Maximum number of patches that can be applied during the auto patch session.

PADNDEV table

The PADNDEV table is used by the Automatic Patching Application process when the NOP software is present. This table list the devices where the patches reside. When the Automatic Patch Application process is initiated, table PADNDEV searches for the patches to be listed in table PATCTRL. The following is a list of the tuples for the PADNDEV table:

FIELD NAME	ENTRY	EXPLANATION
DEVKEY	1, 2, 3	DEVICE KEY, enter the key to the table that indicates the choice of the corresponding device in descending order.
DEVICE	alphanumeric	DEVICE NAME, enter the device name in which patches reside. Only SFDEV or disk volumes are valid device names.

Patching commands

GETPAT command

The GETPAT command searches disk drives and SFDEV for patch files and puts the required patches in table PATCTRL. These are applied later by auto patcher. If GET-PAT finds a patch that is required but is out of sequence so that auto patcher cannot apply it, then the patch is inserted in table PATCTRL with the ACK field set to OUT_OF_SEQ.

AUTOPATCH command

The AUTOPATCH CI command level was introduced in BCS32 and provides the following commands:

COMMAND	DESCRIPTION
START	Allows the user to start the auto patch process by overriding the scheduled start time of auto patch, but does not influence the scheduled start time for the next auto patch session.
STOP	Allows the user to stop the auto patch process from running, and prevents any more patches from being applied during the current Auto Apply session.
CANCEL	Cancels all future auto patch sessions while proceeding with the current auto patch session.

SCHEDULE	Used to schedule the auto patch process START and END times.
QUERY	Allows the user to query the status of the auto patch process. This command shows whether the auto patch process is running, or what time it is scheduled to run.

Auto Patch logs

PCH108

This log summarizes what took place during the auto patch session.

PCH109

This log summarizes what took place when the GETPAT command was executed.

PCH110

This log is output when the auto patch process is generated for information purposes while the auto patch process runs.

PCH111

This log report is output and a major alarm generated if the switch sanity is questionable after the auto patch process has applied patches.

PCH112

This log report is output after an end user executes an AUTOPATCH command that has been canceled, stopped, started, or scheduled by auto patch.

Auto Patch alarms

The following *major* alarms are generated in the EXT level of the MAP if the switch fails sanity checks before or after an auto patch session:

- PRE_AUTOPATCH_SA
- POST_AUTOPATCH_S

Auto Patch setup

The following steps outline the suggested procedures for setting up auto patch:

1. Review the SFDEV for any patches that may require updating.

2. At the CI prompt, enter the GETPAT command if review of SFDEV reveals patches that require updating.

3. Enter table PATCTRL and list all. Review the contents of the table for patches that have "Y" in the APPLY field; these patches are deemed available for automatic application by Nortel Networks.

4. If you concur, change the APPROVED field to "Y" in table PATCRTL. You must also update the DATE and ACTION (XPMs) fields as identified in the PATCTRL table.

5. Before auto patch can run, you must also update and verify table PATSET. The DATE and APPROVED fields must coincide with the DATE and APPROVED fields in table PATCTRL. The XPMVAL field must be datafilled with the node application rate allowed for auto patch on XPMs. This value presently must be set to a minimum of two, even for CC/CM patches.

6. The final field in table PATSET is the AUTO field. This field identifies whether the auto patch process can run or not. If patches are being auto-applied, and there is a need to stop the application of patches, change the "Y" in the AUTO field to "N" to stop the application of patches. Upon datafilling all fields in table PATSET, auto patch is set up to run.

After auto patch has run

After auto patch has run, enter table PATCTRL and list all. If the patch has failed to apply, a store file is created of the console session. The console session of the failed patch is identified in SFDEV by the patch name followed by "$OUT" (RAZ03A27$OUT), a review of this file should reveal the reason for the failure.

NOTES:

1. Before implementing the auto patch features, please review any applicable warnings or bulletins.

2. If you have *auto-image* set up to run, please check the time. Auto Patch will not run during an image, and auto-image will not run during auto patch. Auto Patch process outputs **WARNING MESSAGES** to the user when there may be potential conflicts with scheduling of other maintenance processes, such as the REXTST and auto-image process schedules. If they are scheduled for the same time period, the user is WARNED. Messages are output to all users to warn that the auto patch process is about to run, or has been completed.

3. VO and similar patches require manual applications; therefore, the STAPPLY field in the patch description is set to "N".

4. PATCHER has two fields that are affected by the auto patch feature, AUTO and ST. After the GETPAT CI command has been entered, the patches that are in SFDEV should appear in PATCHER. The AUTO field in PATCHER reflects the contents of the STAPPLY field (Y or N) in the patch description. The ST field in PATCHER should show "DC" (D1Checked). This field should not change until the patch has been updated, either manually or automatically.

5. Ensure that the CC (NT40) or CM (SuperNode) is in sync prior to setting up auto patch.

6. Before starting and after completion of the auto patch process, check for TRAPs, SWERRs, and CC or CM logs to ensure system stability.

Auto Patch precautions

- Ensure that the CCs or CMs are in sync before setting up auto patch.

- Ensure that auto patch does not conflict with REXTST times.

- Auto Patch and auto-image cannot run at the same time.

- Opcode, Debug, VO, and patches requiring manual intervention require manual application since the ST field in the administrative section of the patch is set to "N".

- Auto Patch is not available for use on Link Interface Modules (LIMs), Link Interface Units (LIU7s), Enhanced Networks (ENETs), or Frame Relay Interface Units (FRUIs). These must be patched manually.

- No obsolete patch is allowed to be applied.

DMSSCHED

This tool replaced AUTOSCHED and is used to automatically execute prewritten exec file(s). Users, input file(s) and device name(s), output device(s), and start times are defined using the following commands:

>DMSSCHED   enters the DMSSCHED utility at the CI level

>DEFINE   associates the exec file with the user and defines the output storage device (use NOOUTPUT if no output file is needed)

>START   schedules user login time, day, duration, & periodic logons

>OUTPUT   names the output file and device

>INQUIRE   displays all information on a specified user

>CANCEL   cancels schedule(s) made with the START command

>STOP   forces the immediate logoff of a user that is logged on

>HIST   displays a history of previous DMSSCHED operations

>CLEAR   clears the DMSSCHED history buffer

The system can automatically execute a minimum of one CI command at a given time of day. The system can also automatically save the output to a file. For example, the system can collect logs of a given type during the night without an operator to execute the commands. The user can specify execution as one time only, or as occurring at intervals. The interval is a minimum of one day.

See NTP 297-YYYY-546 for further information on the use of DMSSCHED.

Maintenance Administration

This section describes various key work operations in a DMS environment.

Maintenance and administrative features are available within the DMS-100F system that can improve work operations. Many automated work operations are built into the DMS-100F as features and are not labor intensive. Nevertheless, labor is required to control the features, analyze various outputs, and correct indicated troubles.

The majority of maintenance and administrative work functions for the DMS-100F switches are performed through an access port called a Maintenance and Administration Position (MAP). Several access ports can be assigned for inputting as well as receiving data from the switch. Features within the switch allows for individual port control of input and output data. Security features can be set up for login and logout control of the ports.

Work operations can also be completed from a remote location and centralized to cover more than one DMS-100F switch. Remote MAP terminals can be provided for this purpose. The on-site personnel—generally Tier I support—requirements are reduced significantly, but are not eliminated.

Many companies have maintenance engineering or technical support groups that provide support for administrative functions as well as Tier II technical support to the site or control center. They are usually contacted for assistance with service outage problems, to open up CSRs, engineering complaints, product change audits and issues, and are asked to provide field support for cutovers and assist in solving Tier II type problems.

The maintenance administration described in this section is based on three levels of organization and two tier levels of support:

- Central Office (CO) site—generally Tier I support
- Control centers such as:
    - Switching Control Center (SCC)—Tier I and possibly Tier II support
    - Network Operations Center (NOC)—Tier I and possibly Tier II support
    - Network Reliability Center (NRC)—Tier I and possibly Tier II support
    - Technical Assistance Center (TAC)—Tier I and possibly Tier II support
    - Network Maintenance Center (NMC)—Tier I and possibly Tier II support

- Tier II assistance centers such as:

  — Electronic Switching Assistance Center (ESAC)

  — Technical Assistance Center (TAC)

  — Technical Support Group (TSG)

  — Maintenance Engineering Center (MEC)

  — Digital Support Group (DSG)

These types of center organization are used by many operating companies; however, regardless of the organization structure, all the key activities described in this section should be included.

On-Site Operations

When centralized maintenance is implemented for DMS-100F offices, many of the traditional central office work functions can be moved over to the centralized group; however, some work functions always remain on-site.

Site responsibilities

On-site work activities are performed by Tier I trained personnel—unless a special on-site visit is needed by a Tier II person to clear a problem that cannot be resolved by a Tier I person. See the "DMS Key Work Operation Responsibilities" subsection within this tab for a list of activities performed by Tier I and II persons.

Following are examples of responsibilities for Tier I site personnel or other work forces assigned to perform these responsibilities:

- Clear switch, trunk, and line troubles as received from the control center.
- Perform routine tasks and routine procedures as scheduled and assigned—manually or through a database to automate the process—by the control center.
- Prepare backup office tape image tape on a routine basis.
- Read Dead Office Timer as required by local policy.
- Replenish paper on printer(s).
- Maintain a marked, and proven set of maintenance spare cards.
- Maintain the following office log records:
    — AMA/CDR Tape Log
    — Circuit Pack Replacement/Repair Log for Line Cards
    — Circuit Pack Replacement/Repair Log for Other Cards
- Circuit Pack Replacement (accepting and replacing in-service maintenance spare cards with cards received from repair and return).
- Operate manual answer of dial-up port data sets as required, and restore when dial-up is completed.
- Request technical assistance from the control center as required.
- Refer unsolved service and equipment troubles to the control center for assistance and resolution.

- Perform any miscellaneous work load items requested by the control center.

- Maintain up-to-date documentation (i.e., documentation on CD-ROMs, NTPs, GSs, ISs, EWBs, DMS-100F Maintenance & Operations Manual, DMS-100F Quick Reference Guide). This includes filing documentation and coordinating the need for current documentation. Be aware of enhancements and restructuring that are taking place with Nortel Networks documentation—see the "Nortel Networks Documentation" subsection within the following *Office Administration* section. If necessary, have someone from the Nortel Networks Regional Customer Support Group give a presentation on Nortel Networks documentation or the use of Helmsman CD-ROM.

- Insure security is maintained for the central office and that paper from printers and documentation is properly destroyed or distributed for proper handling. This includes destroying CD-ROMs or recycle old CD-ROMs and jewel cases per "CD-ROM recycling program" on page 8-62.

- Fill out maintenance trouble tickets as needed and keep a historical log of office maintenance activities.

Control Center Operations

The control center for many companies is called a Switching Control Center (SCC), a Network Operations Center (NOC), a Network Reliability Center (NRC), or a Technical Assistance Center (TAC). The control center is a centralized configuration of support systems with features to meet overall surveillance and maintenance requirements of one or more DMS-100F offices—24 hours per day, every day.

Some control centers provide Tier II support for their sites. Tier II personnel require enhanced hardware and software training. In addition, companies with Tier II personnel must have a Technical Information Agreement (TIA) with Nortel Networks to have access to proprietary documentation that supports Tier II functions.

Surveillance, maintenance, and administration activities for Nortel Networks switches can be centralized in the control center operation on a district basis or on a geograpical basis for a larger span of control.

Extending the human-machine interface provides the required real time fault indicators, and access to the machines for maintenance, translation changes, and administrative activities.

Normally, switches (i.e., SMS, SMR, SMU, SMA, RLCM, OPM), are unattended or located in an area staffed with a minimum number of people. Maintenance personnel are dispatched to unattended locations when on-site work activity is required.

Control center responsibilities

The suggested prime areas of responsibility for the control center are:

- Real time surveillance of MAP subsystem alarms for the switch, trunks, links, lines, carrier maintenance alarms, and CCS7 link and alarm analysis.
- Ongoing trouble analysis of OMs for the switch, networks, trunks, links, and lines.
- Ongoing testing of the switch, networks, trunks and lines.
- Operation and management of automatic diagnostic tests such as:
    - Automatic Line Testing (ALT)
    - Automatic Trunk Testing (ATT)

— Killer Trunk (KT) Testing

— Bit Error Rate Performance (BERP) Testing

— Network Fabric (NETFAB) Testing

— Enhanced Network Fabric (ENETFAB) Testing

— XPM Bit Error Rate Tests (XBERT) Testing

— Focused Maintenance for Lines

— Focused Maintenance for Trunks

— BICRELAY testing

NOTE: See the "*Preventive Maintenance*" tab of this manual for details on the maintenance tools listed above.

- Switch network integrity analysis of INTEG, NETFAB, and ENETFAB reports.
- Analysis of system log messages for switch, trunks, and lines.
- Administration of the log message system by controlling the suppression and thresholding of logs, and assuring the highest logging channel baud rate to prevent losing log messages.
- Control of passwords, command screening, and dial-up security for central offices.
- Control of central office security.
- Data modification for routing and translation changes in the trunk network and for customer groups.
- Recording, closing, and control of the following logs:
    — CPU Down-Time Log

    — PM Reload Log

    — Customer Trouble Ticket Log

    — Dial-Up Access Log

    — Trouble Ticket Log

    — Office Alarm Log

    — Office Image Log

    — Spare Data Store Record

    — Office Image and Data Store Available Record
- Controlling and coordinating on-site manually performed routine tasks.
- Changing of office clock times as needed for season changes.
- Providing technical assistance to on-site personnel as required.

- Chairing all major failure and outage investigation meetings.
- Providing remote surveillance and assistance for vendor software and hardware changes.
- Preparing service results plans of all types.
- Initiating Customer Service Reports (CSRs), engineering complaints, and escalating unsolved service problems to maintenance engineering, technical support, and to the Tier II assistance center (i.e., ESAC, MEC, ETAS).
- Identifying documentation problems and reporting them to the vendor.
- Assisting in cutover meetings and preservice testing.
- Identify and recommend DMS-100F training courses.
- Utilizing software support tools and tables such as:
  - Switch network tools (ICTS, NETPATH, NETINTEG, etc.)
  - CALLTRAC
  - CCS7 Test Utility (C7TU)
  - PMIST and XPMIST
  - DEBUG
  - DISPCALL
  - TRAVER
  - DMSMON
  - DMSSCHED
  - SPMS
  - MMINFO
  - TRKSTRBL (TTP level)
  - LNSTRBL (LTP level)
  - Table OMTHRESH
  - Table ALARMTAB
  - Service Monitoring (SMON) for P-phones
- Refer unsolved service and equipment troubles to the control center for assistance and resolution.
- Perform any miscellaneous work load items requested by the control center.
- Maintain up-to-date documentation (i.e., documentation on CD-ROMs, NTPs, GSs, ISs, EWBs, DMS-100F Maintenance & Operations Manual, DMS-100F Quick Reference Guide). This includes filing documentation and coordinating the need for current documentation. Be aware of enhancements and restructuring that are taking place with Nortel Networks documentation—see the "Nortel

Networks Documentation" subsection within the following *Office Administration* section. If necessary, have someone from the Nortel Networks Regional Customer Support Group give a presentation on Nortel Networks documentation or the use of Helmsman CD-ROM.

- Insure security is maintained for the center and that paper from printers and documentation is properly destroyed or distributed for proper handling. This includes destroying CD-ROMs or recycle old CD-ROMs and jewel cases per "CD-ROM recycling program" on page 8-62.

- Fill out maintenance trouble tickets as needed.

In a noncontrol center operation, all the above responsibilities would fall back to the central office personnel. Where a control center or Tier II assistance center does not exist, the operating company normally contacts their Nortel Networks Regional Customer Support Group or ETAS directly for emergency and nonemergency support.

Tier II Control Center Operations

Control centers that provide Tier II DMS operations support are corporate support staffs that assist in problem resolution and escalation that has eluded solution by site technicians, control center personnel, maintenance engineering, or technical support personnel. The Tier II assistance center is usually the prime contact for an office that is out-of-service or experiencing degradation problems. The Tier II assistance center operation is not intended to be a 24 hour operation; however, some companies do provide 24 hour operation through off duty contact and beeper service.

The required real time access is generally provided by dial-up facilities directly to the DMS-100 office or through a control center support system access. With any access method, security should be a prime concern. A supervisor or manager should be assigned security responsibilities for controlling site access.

Tier II assistance center responsibilities

The suggested prime areas of responsibility for the Tier II assistance center are as follows:

- recovery support for service interruptions or outages
- switch access security policies
- direct assistance on switch problems
- Service report (SR) tracking, retesting, and closure
- coordinate maintenance assistance activities with Nortel Networks
- hotlist problems coordination
- advise field of problems, solutions, and workarounds
- participate in trouble investigation meetings
- translations support
- authorized Nortel Networks technical assistance billing and payment
- prein-service checks
    - circuit pack base line
    - patch audit
    - hardware gating DCAs

— office parameters
— translation data
— Service reports (SRs)
— PM loads
— log analysis
— restartability
— bulletins
— OMs
— cutover monitor

- patch control log

- hardware change control

- PCL software application support

- performance analysis and tracking

- extended warranty tracking

- field investigations for outages and loss of AMA

- development of operating company methods and procedures

Tier II software tools

Tier II assistance center personnel should be fully trained in DMS-100F hardware and software. In addition, they should have an excellent working knowledge of these resident and nonresident software tools:

Table 7-1   —   Software Tools

DISPCALL	Displays software errors, audits and traps.
PMIST & XPMIST	Monitor messages to or from peripherals.
DEBUG	Trace points for software debug.
CALLTRAK	Call tracing and monitoring of messages
C7TU	Monitoring CCS7 messages
SMON	Monitoring P-phones
RWOK	Access to restricted tables.
ALTER	Change the contents of an address.
TRACE	Detailed info on call processes.
QUERY	Contents of a module in software.
PMDEBUG	Trace points for PM software bugs.

See the following *Office Administration* tab for a list of proprietary documentation that supports Tier II type control center operations.

DMS Key Work Operation Responsibilities

An overview of the example areas of responsibilities shared by the Tier II only technical assistance centers, control centers with Tier I only technical assistance, and Central Office (CO) Tier I forces is presented in the following chart. Obviously, organizational requirements dictate the assignment of these responsibilities.

NOTE: No attempt is being made to suggest organizational structures, as they are dependent upon geographical location of switches, switch population, and operating company management preferences.

Table 7-2   —   DMS Work Operation Responsibilities

KEY ACTIVITIES	TIER II CENTER	TIER I CENTER	TIER I CO
ETAS/TAS Interface...	Prime	Assist	Assist
Patch Control...	Prime	Assist	Assist
Hardware Change Control..	Assist	Prime	Assist
BCS Application Control..	Prime	Assist	Assist
Translation Support...	Assist	Prime	Assist
Pre-inservice Check..	Assist	Prime	Assist
Solutions & Workarounds (Advise Field)...................	Prime	Assist	Assist
Trouble Escalation (Direct Involvement)...................	Prime	Assist	Assist
Advanced Trouble Testing Techniques......................	Prime	Assist	
Performance Analysis & Tracking..............................	Assist	Prime	Assist
Automatic Trunk Tests.......................................		Prime	Assist
Automatic Line Tests.......................................		Prime	Assist
BERP..		Prime	Assist
NETFAB...		Prime	Assist
Real-Time Switch Surveillance.................................		Prime	
Add or Delete Trunks......................................		Prime	Assist

Continued on next page

Add or Delete Trunk Groups.......................................		Prime	Assist

KEY ACTIVITIES (continued)	TIER II CENTER	TIER I CENTER	TIER I CO
Trunk Logs...		Prime	
Trouble Analysis...................................		Prime	
Log Message Analysis...........................	Assist	Prime	Assist
Performance Analysis.............................		Prime	
Alarm Administration.............................	Assist	Prime	Assist
Translations...	Assist	Prime	Assist
Call Traces..	Assist	Prime	Assist
Trouble Tickets.....................................	Assist	Prime	Assist
Carrier Maintenance..............................		Prime	Assist
Trunk Status...	Assist	Prime	Assist
Take Image..	Assist	Prime	Assist
Trunk Orders...		Prime	Assist
Trunk Coordination with other COs........		Prime	Assist
Framework...		Prime	Assist
Change Circuit Packs		Assist	Prime
Tape Processing.....................................		Prime	Assist
Dead Office Timer.................................		Assist	Prime
Office Routines.....................................		Prime	Assist
Central Office Building Security.............		Prime	Assist
Central Office Access Security...............	Assist	Prime	Assist
Privclassing of commands	Prime	Assist	

Office Administration – General

This section describes various administrative functions associated with the DMS-100F switch. The following subsections are provided for your reference:

Log System Administration

This subsection describes the areas that need administration to control the volume of log messages generated within the DMS-100F switch.

Software optionality control (SOC)

This subsection describes the software optionality control (SOC) tool the operating company can use to purchase and monitor software features that reside within Product Computing-module Loads (PCL).

Log and Control Record Exhibits

Various log and control record forms for documenting DMS-100F maintenance activity are provided as exhibits within the Log and Control Record Exhibits subsection. Examples of various control records, logs, and check lists for power plant maintenance, reviews, and grounding are recorded in NTP 297-1001-350, *DMS-100F Power and Grounding Routine Maintenance Manual.*

Nortel Networks documentation

This subsection describes the publications, drawings, manuals, and other documents that are used to support and maintain accurate design records and capabilities of the DMS-100F switching system. The following areas are covered in this subsection:

- Documentation structure
- Proprietary documentation
- Product documentation catalog
- Site specific documentation
- PCL and PM software release documentation.

Office security

This subsection describes DMS-100F switch features that can be used to secure switch access.

Portable test equipment and tools

This subsection provides a list os suggested portable test equipment and miscellaneous tools that can be used for switch maintenance.

Office parameters

This subsection provides a list of parameters from engineering tables that are related to maintenance features and associated functions.

Store file maintenance and administrative applications

This subsection describes the administration of the DMS-100 store file area and provides exhibits of store file programs associated with maintenance.

Log System Administration

General

A log report is a message generated by the DMS switch whenever a significant event has occurred in the switch or one of its peripherals. A log report may be generated in response to either a system or a manual action.

Log messages are produced within the system to indicate various machine events, such as:

- surveillance status
- maintenance actions
- information items
- alarms and corrective actions

Voluminous amounts of data are produced by the log message subsystem. The log message subsystem comprises over 2200 log message types within over 180 log subsystem groupings.

This subsection will provide information on the administration of log messages using generic features within the DMS-100 switch. Operating companies should be aware that there are special applications and operation systems available through Nortel Networks and other providers that support the management of log messages. One of those is the "Focused Maintenance" feature that is described within the *Preventive Maintenance* tab of this manual.

Most operating companies fail to develop a plan to administer logs. This creates a problem since important log messages are lost within the large volume of informational and low priority logs that should be managed. Maintenance personnel get frustrated with trying to find logs that would support their effort, and therefore, give up on using the logs as a source of information on problems. Efforts are generally placed toward resolving alarms since analyzing a large volume of log messages is time consuming and frustrating.

For details on individual logs and on the structure and variable message data for logs, see the various NTP 297-YYYY-840 PCL log reference documents.

Log administration and control methods

The system has two methods of administering or controlling log messages—one is a temporary method using LOGUTIL subcommands and the other is a permanent one that uses the LOGCLASS and LOGDEV tables. The permanent method is the only one recommended for a controlled data environment since table controls are not interrupted by system reloads as LOGUTIL would be. The permanent basic thresholding or suppressing of logs in LOGCLASS can be *temporarily* superseded by using the LOGUTIL subcommands: THRESHOLD, TIMERESET, and SUPPRESS. The permanent entries in LOGCLASS are not changed by use of the LOGUTIL commands. The use of LOGUTIL commands to control logs—such as thresholding and suppressing logs—is lost with planned or unplanned software reloads.

Nortel Networks does not have an official documented method for administering each log message since each operating company might have different views as to how they want to control log messages. The large volume of log messages from the DMS-100F switch can be very helpful in maintenance operations; however, it can also be ineffective if not administered.

Temporary method

Many operating companies use LOGUTIL commands to manage logs and find they have lost what they have set up after a software reload.

NOTE: LOGUTIL should only be temporarily used for control of logs and not for log administration.

LOGUTIL is a CI increment that allows the operating company to control the routing and retrieval of log reports. Since the log system has a limited amount of storage, only the most recent log reports are accessible through LOGUTIL.

The LOGUTIL program contains commands that allow users to browse within the internal log buffers to obtain information and to implement temporary controls on routing of and generation of log messages. The commands are available at the CI level or at menu levels by typing in LOGUTIL.

The routing and control commands provide the following functions:

- routing of reports to selected input/output devices (IODs) which temporarily supersedes the permanent assignments in tables LOGCLASS and LOGDEV

- interrogating and searching all reports in the various log subsystems

- provides the capability for the operating company to add, change, or delete log reports, and to apply threshold values that limit the basis on which log reports are output.

> **CAUTION:** As previously mentioned, table control is the preferred method of managing the system. Therefore, the use of the CLEAR, FORMAT, RENUMBER, RESET, RESUME, SUPPRESS, SYSLOG, THRESHOLD, TIMERESET commands are definitely not recommended unless there is a clear understanding of the consequences.

Following is a list of LOGUTIL subcommands that provide routing, control, and device information for logs:

>HELP LOGUTIL ....lists LOGUTIL commands.

>LOGUTIL ....access to LOGUTIL commands.

>QUIT or LEAVE ....quits LOGUTIL.

>ADDCLASS.......................adds output report classes to specified primary IOD.

>ADDREP...........................adds more reports to specified primary IOD.

>BACKUP...........................assigns alternative IOD to back up primary IOD.

>CLASS ....assigns report class numbers to specified output reports.

>DELCLASS ....deletes specified report classes with specified IOD.

>DELDEVICE ....deletes specified IOD from receiving log reports.

NOTE: Must use STOPDEV command first

>DELREP............................deletes specified report(s) from specified IOD.

>LISTDEVS........................displays status of each IOD associated with log system.

>LISTREPS......................... SPECIALdisplays a list of special log reports that have special routing or thresholding, and those suppressed.

>LISTREPS SYSLOG ....displays only SYSLOG reports.

>LISTREPS CLASS ....displays a list of reports by log class.

>DUMPLOGS.....................<logname> <log number>display specified log reports in a buffer in the chronological order as they were generated.

>LOGTRACE ....ON/OFF <logname and number>turns ON/OFF the traceback feat. (a SWERR is generated for each rep).

>RENUMBER ....assigns a report number to all report types not assigned.

>LISTROUTE ....displays specified report classes, report names, and IOD, by CLASS, DEVICE, or REPORT.

>LISTNODES ....list all nodes in the switch.

>LISTTIME ....displays log reports on a threshold reset schedule.

>LISTLOGS..........................list all lognames, except SECRET lognames.

>RESET ....resets to zero all threshold values that were applied by THRESHOLD and resumes SUPPRESS reports.

>REROUTE ....reroutes reports from primary IOD to backup IOD.

>RESETROUTE ....restores the temporary routing of output reports.

>RESUME ....resumes the output reports previously suppressed.

>START...............................starts log reports to specified device.

>STOP.................................stops printing of reports on specified device.

>STOPDEV.........................stops the output of reports to the specified device(s).

>STARTDEV ....starts the output of reports to the specified device(s).

>SUPPRESS........................suppresses specified output reports.

>THRESHOLD....................sets a threshold value for specified report(s).

>TIMERESET......................sets a time value for the threshold counter.

The browsing type of commands for the LOGUTIL program are an extremely effective tool for maintenance use. Following is a list of browsing commands:

>OPEN ....access to display log subsystem or SYSLOG buffers.

>FIRST................................displays oldest report in the current log subsystem.

>LAST.................................displays most recent report in current log subsystem.

>FORWARD ....<number or ALL> displays report(s) _after_ current one.

>BACK................................<number or ALL> displays report(s) _before_ current one.

>CLEAR..............................deletes all reports from specified log subsystem buffer.

>FORMAT ....queries or sets the NORMAL or SHORT format in which output reports will be printed.

>TYPE.................................redisplays the report in the current log subsystem buffer that was previously displayed by command LAST, FIRST, BACK, and FORWARD.

Documentation that describes the commands and gives examples of LOGUTIL subcommands and their use can be found in NTP 297-1001-129, *DMS-100F I/O System Description*.

Permanent method

Two tables are provided for implementing the permanent method of log administration—LOGCLASS and LOGDEV.

Table LOGCLASS

Table LOGCLASS provides the following capability:

- allows the capability to assign from 0 to 31 classes to logs for routing

- suppressing of logs
- thresholding of logs
- controlling SYSLOG storage for evaluation of problems

Following is a partial datafill example of table LOGCLASS:

```
TABLE: LOGCLASS

TOP

     REPNAME   CLASS   THRESHLD   SUPPRESS   TUNITS   SYSLOG

--------------------------------------------------------

 LINE 138       0        0          Y          -1       N

 TRK  138       0        0          Y          -1       N

 IOD  304       0        0          N          -1       Y
```

NOTE: Logs suppressed in table LOGCLASS will not be loaded within log device buffers and, therefore, are not available with LOGUTIL or output to a device. They will, however, show up in DMSMON with the HIGHLOGS count because they are in the central device buffers.

Logs can be suppressed in table LOGCLASS to off-load buffers or they could be routed to a class that has no assignment in table LOGDEV—sometimes called a garbage class. The administration of logs using table LOGCLASS should be strictly controlled by both Tier I and Tier II maintenance personnel. If necessary, privclassing commands for both table LOGCLASS and LOGUTIL should be done.

To prevent able LOGCLASS from becoming extremely large in size, an input of "-1" may be used in place of the log message number to represent all other numbers not individually referenced. If a log is assigned a "-1" for a given report name, it must be datafilled before other logs with the same report name—this affects the LISTREP command in LOGUTIL. The following is an example of the sequence for datafill:

> PM -1   (all other messages, excluding PM180 and PM128)
> PM180
> PM128

Please review the NTP 297-YYYY-350, *Translation Guides* before making any entries or changes to table LOGCLASS.

Table LOGDEV

Table LOGDEV selects message groupings by their internal class numbers for routing to terminal devices (max 32), as well as assigning backup devices in case the primary device fails. Terminal devices are assigned in table TERMDEV before table LOGDEV.

Table LOGCLASS interacts with the SCC2_LOGS parameter in table OFCOPT and the parameter LOG_PRIORITIZATION in table OFCENG. Parameter LOG_PRIORITIZATION is related to prioritization of alarmed log messages and is later described under "Log parameters."

In table LOGDEV, only one device can be guaranteed and should be assigned on a device that critical logs would be output on. This would help insure that the device would run under a heavy office load. Table TERMDEV is allowed to have up to five terminal devices assigned as guaranteed terminals

Following is a partial datafill example of table LOGDEV:

```
TABLE: LOGDEV

        DEV            ALT                    CLASSES
FORMAT      PRIORITY  GUAR

-----------------------------------------------------

    MAPPRT             NONE
                                          (0-31)
  STD         N         N

    TTPPRT             NONE
                                          (0-31)
  STD         N         N

    SCCLOG           TLCCLOG
                                    (0-4, 6-8, 10-31)
  SCC2        Y         Y
```

Log parameters

The addition of new features with each software load adds additional load to the log system. Continued efforts are being made in design and new applications to reduce the number of logs and to better control the volume under an overload. During heavy log message conditions the potential exists for losing log messages in the log message system. This is usually seen on logging devices as:

— **WARNING: 100 REPORTS NOT PRINTED.**

One area that records lost logs is within the LOGS OM group. Register LOSTREC records the number of lost log messages and indicates a problem with log administration or the size of the LOGS_CENTRAL_BUFFER_SIZE or the LOGS_DEVICE_BUFFER_SIZE parameter within table OFCVAR.

Three factors contribute to lost logs—log administration, the baud rate of the logging device buffer, and the central log buffer sizes in the switch. Insure maximum log message output and log prioritization (parameter) by checking the office parameters in Table 8-1 on page 8-9, the administration of log routing, thresholding, and suppression.

Table 8-1 — Log message parameters

TABLE	PARAMETER	SUGGESTED	DEFAULT	NOTES
OFCENG	LOG_PRIORITIZATION	Y	Y	Notes 1&3
OFCVAR	LOG_CENTRAL_BUFFER_SIZE	Note 2	2000	Notes 2&3
OFCVAR	LOG_DEVICE_BUFFER_SIZE	Note 2	2000 (SN)	Notes 2&3
OFCVAR	THRESHOLD_IS_SAMPLING	Y	Y	Note 3
OFCVAR	DISKLOGMEMORY	Notes 3&4	Notes 3&4	Notes 3&4
OFCVAR	BUFFER_THRESHOLD_REPORTS	Y	Y	Note 3

NOTE 1. In addition to setting the LOG_PRIORITIZATION parameter in table OFCENG to "Y", assign one logging device as a guaranteed device in table LOGDEV to "Y". Log prioritization insures that log reports with the highest alarm level are output first. Guaranteeing a device insures that logs are given priority during peak traffic periods. It is recommended that this device have all critical logs routed to it.

NOTE 2. Default value is the recommended value; however, if logs are being lost to a device, first consider rerouting unnecessary logs, thresholding and suppressing of logs, increasing device baud rate, and then consider increasing the buffer sizes for the LOG_DEVICE_BUFFER_SIZE and LOG_CENTRAL_BUFFER_SIZE parameters. Before changing the size of the buffers, consult your Design and Maintenance Engineering groups or other maintenance support to insure that there is adequate memory, and that the baud rate is adequate to handle the load.

NOTE 3. See NTP 297-YYYY-855, *DMS-100F Office Parameters Reference Manual*.

NOTE 4. The greater the value of this parameter, the more unformatted logs will be captured by DLOG. The log interception code using this store can often intercept logs that may not be captured by LOGUTIL during problem situations.

Treatment logs

Unmanaged treatment logs can cause the buffers to be overloaded and logs to be lost. Generation of treatment logs (LINE138, TRK138, FRT138 etc.) can be managed through tables TMTCNTL and TMTMAP.

It is highly recommended that treatment logs be managed and set to "N" unless they are needed for analysis. Look at the subtables in TMTCNTL and the individual treatments to determine if the treatment log is needed (set to "Y"). Table TMTMAP for CCS7 treatments can also be set to "Y" or "N" to control generation of logs

Logs and outages

Logs are invaluable as a record for evaluating unplanned reloads and service degradations. The following is a suggested list of information to collect after outages or service degradations:

- CM or MS restarts
- MS clock related outages or SYNCLK problems
- CM activity restarts
- unable to load MS or communicate with it
- call processing degradations or outages
- CCS7 related outages (STP restarts, isolations)
- ENET outages
- XPM outages
- AMA outages

SYSLOG

SYSLOG is a feature that stores SWERR and TRAP logs in a SYSLOG buffer for analysis use after an unplanned office reload. The operating company can also designate selected log reports to be written to the SYSLOG buffer. In the event of a reload, the LOGUTIL buffers are overwritten, but the SYSLOG buffer logs remain for analysis of what caused the reload.

See the SYSLOG field in table LOGCLASS for assigning logs.

SYSLOG is entered through LOGUTIL with the OPEN SYSLOG command. See NTP 297-1001-129, *DMS-100F Input/Output System Reference Manual*, for use of SYSLOG and printing of the SYSLOG buffer.

DLOG

DLOG is used by an operating company or Nortel Networks technical assistance support personnel to use as a debugging tool for evaluation of DMS switch outages or degradations.

The DLOG subsystem (Log Retrieval Facility for E1 Incidents) feature enables logs to be captured on permanent store, including the logs that have been thresholded or suppressed using LOGUTIL commands. The DLOG feature is part of tables DIRP-POOL and DIRPSSYS that supports the Device Independent Recording Package (DIRP). The DIRP utility is used to record unformatted or compact logs on permanent store.

A new feature has been developed to resolve formatting process problems with DLOG. This feature provides a new user interface to the log formatting utility. This interface is in the form of a new Command Interpreter (CI) level called DLOG. Inside this new level, the user has the ability to set up formatting parameters through the use of the DLOG subcommands. These subcommands are:

STATUS .... Displays logs INCLUDED/EXCLUDED, earliest valid start time and previous use information

EXCLUDEALL .... Removes all logs from set of logs to format

INCLUDEALL .... Resets the set of logs to format to all logs

EXCLUDE .... Accepts logs to EXCLUDE from format executed by FORMAT subcommand:

INCLUDE .... Accepts logs to INCLUDE in format executed by FOR-MAT subcommand

FORMAT .... Accepts parameters for date/time range to format

FORMATFILE .... Accepts filename of unformatted DLOG file to format

LISTFILES .... Displays the raw DLOG files recorded in the internal table with their start times and end times

QUIT .... Exits DLOG level

NOTE: It is now possible for the user to capture only PM logs that were generated Friday, April 8 from 10:00 AM to 11:30 AM. The formatting process begins upon entering the FORMAT subcommand.

For further information on DLOG and datafilling DIRPPOOL and DIRPSSYS tables, see NTP 297-YYYY-350, *DMS-100F Translation Guide*.

SCANLOG

SCANLOG is a nonresident software tool that provides the scanning of log files for specific logs and for the elimination of selected logs from large log files, such as DLOG. SCANLOG allows the user to search for logs that meet defined requirements and then place them in a designated file.

SCANLOG can scan 24 hours of logs in about three minutes. Up to four log messages may be searched simultaneously using the SLCLOG command. Logs may be selected with up to ten different fields including time spans.

For those that have access to proprietary documentation, see TAM-1001-014, *SCAN-LOG User Guide*.

Log message routing

Following is an example for log message routing. Utilize it to help in setting up the routing strategy for log messages within your company.

Selecting categories

Log messages should be routed to output devices based on message purpose and areas of responsibility. In many applications, the log messages can be divided into nine groups or categories. Company structural support will dictate the exact number of categories required (the maximum is 31) in table LOGCLASS. The following suggested message routing categories are provided as examples:

0.	D	Default (See Note)
1.	M	Maintenance
2.	L	Lines
3.	T	Trunks
4.	NWM	Network Management
5.	OM	Operational Measurements (traffic)
6.	SA	Service Analysis
7.	ATT	Automatic Trunk Test
8.	SNAC	Switched Network Analysis Center
9.	GENERAL	One Device To Receive All Logs
10.	ISDN	Integrated Service Digital Network
11.	CCS	CCS7 Network Operations Center

NOTE 1. Operating company unassigned logs default to class "0" in table LOGCLASS.

NOTE 2. For more information on log routing, see the appropriate NTP 297-YYYY-840 PCL log reference documents

The following table is an example of message routing—the assignment of specific messages and subsystems groups to specific functional user categories. This table is an example only and is not all inclusive for log messages. However, the concept should be extended to the log messages not addressed at this time.

Table 8-2 — Log Message Routing Examples

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
M	**Alarm Subsystem** ALRM -1
L M, L	**Automatic Line Testing Subsystem** ALT -1 ALT105 FAIL ALT
M	**Automatic Message Accounting Buffer Subsystem** AMAB -1
M	**Automatic Message Accounting Subsystem** AMA -1
ATT	**Automatic Trunk Testing Subsystem** ATT -1
M	**Audit Subsystem** AUD -1
M	**Audit Terminal Subsystem** AUDT -1
M	**Bit Error Rate Test** BERT100
M	**Completion Audit Subsystem** CAUD -1
M	**Central Control Subsystem** CC -1
CCS CCS	**CCS7 MTP Associated & Nonassociated Signaling** CCS -1 C7UP -1
M	**Call Forwarding Subsystem** CFW100 Info No Journal File
M	**Central Message Controller Subsystem** CMC -1
M	**Generic Distributed Data Manager** DDM101 Unable to Download PM DDM102 Unable to Update PM DDM104 Lost Sync with PM

Table 8-2 — Log Message Routing Examples (continued)

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
	Disk Drive Subsystem
M	DDU -1
	Device Independent Recording Program Subsystem
M	DIRP101
	Data Link Controller Subsystem
M	DLC100 Info Controller Error
M	DLC101 Minor Overload
M	DLC102 Major Overload
	External Alarm Subsystem
M	EXT -1
	Focussed Maintenance
T, L	FM100 Trunk Group Exceeded Threshold
T, L	FM101 LCE Exceeded Threshold
	Fiber Multiplex Terminal
M	FMT-1
	Integrity Check Traffic Simulator
M	ICTS-1
	Integrated Business Network Subsystem
M	IBN -1
	Integrated Service Digital Network
ISDN, T	ISDN-1
	Interrupt Subsystem
M	INTP
	Input/Output Audit Subsystem
M	IOAU -1
	Input/Output Device Subsystem
M	IOD -1
	Input/Output Gate Subsystem
G	IOGA -1
	Killer Trunk Subsystem
T	KTRK100 Info KT Report
	Line Maintenance Subsystem

Table 8-2 — Log Message Routing Examples (continued)

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
M, L	LINE100 Pass LN Diag
M, L	LINE101 Fail LN Diag
L	*LINE102 LO ON
L	*LINE103 RTS
M, L	*LINE104 TBL
M, L	*LINE105 TBL
M, L	*LINE106 TBL
L	LINE107 Info
M, L	*LINE108 TBL
T, M, L	*LINE109 TBL
L	*LINE110 TBL FEMF Detected
L	*LINE111 Info FEMF Removed
M, L	LINE112 TBL Stuck Coin
M	LINE113 TBL
M	LINE115 Info
M	LINE117 Info
M, L	LINE118 Fail per Call Test
L	LINE119 Info Calling Line Identifier
L	LINE124 Info Trace-on-Malicious-Call-Initiated
L	LINE125
L	LINE126
ISDN	LINE131
ISDN	LINE145
M	LINE138 Info TRMT
L	*Line 204
	NOTE: (*) Replaced by Focussed Maintenance
	Line Load Control Subsystem
NWM, M	LLC -1
	Lost Message Subsystem
M	LOST -1
	Multi Protocol Controller
M	MPC-1
	Magnetic Tape Drive
M	MTD-1
	Network Maintenance Subsystem
M	NET -1

Table 8-2 — Log Message Routing Examples (continued)

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
	Network Operations (SCC MAP)
M	NOP114 Restart
	Northern X-25 (LINK)
M	NPAC210 Minor Overload
M	NPAC212 Major Overload
	Network Management Subsystem
NWM	NWM -1
	Operational Measurements Printing Subsystem
ALL	All Routing Categories (1-10)
1-11	OMPR250 Info Clock Change
1-11	OMPR2xx Info OM Report
	Operational Measurements Reporting Subsystem
ALL	All Routing Categories (1-10)
1-11	OMRS100 Info Clock Change
1-11	OMRS0xx Info Periodic Report
OM NOTE	NOTE: Since log messages within the subsystem are being split to various routing categories, each log must be assigned individually.
	Operational Measurement Subsystem
M, OM	OM 2113 Info OM Tape
M	OM 2200 Info OM Threshold Exceeded
M, OM	OM 2300 Info OM Accumulated Store Error
	Patch Subsystem
M	PCH-1
	Pending Order Subsystem
M	PEND 100 Pending Order Audit
	Peripheral Module Subsystem
M	PM -1
	Service Analysis Subsystem
SA	SA -1 Info SA Summary
	Switched Network Analysis Subsystem
SNAC	SNAC 100 TBL
SNAC	SNAC 101 TBL
M, SNAC	SNAC 102 TBL
M, SNAC	SNAC 103 TBL

Table 8-2   —   Log Message Routing Examples (continued)

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
	Software Error Subsystem
M	SWER (NOTE: Always Class 0)
	Synchronizable Clock Subsystem
M	SYNC -1
	SS7 Mass Trunk Conversion
T	TKCV100 Trunk Conversion Trouble
	Traffic Operator Position Subsystem
M	TOPS -1
	Trunk Subsystem
T	TRK101 FLT Group-Alarm
T	TRK102 FLT Group-Alarm
T	TRK103 FLT Group-Alarm
T	TRK104 INF Group Ok
T	TRK105 Info ONI-Function-Transferred
T	TRK106 Fail
T	TRK107 Pass
T	TRK108 Pass
T	TRK109 Fail
T	TRK110 SBSY Lockout On
T	*TRK111 FLT Routing Trouble
T	*TRK112 OK Lockout Off
T	*TRK113 FLT Trunk Trouble
T	*TRK114 FLT DP Reception TRBL
T	*TRK115 FLT DP Permanent Signal
T	*TRK116 FLT MF Reception Trouble
T	*TRK117 FLT MF Permanent Signal
T	*TRK118 FLT ANI Reception Trouble
T	*TRK119 FLT ANI Reception Trouble
T	*TRK120 FLT ONI Trouble
T	*TRK121 FLT Outpulsing Trouble
M, T	*TRK122 Fail Integrity Trouble
T	*TRK123 Fail PP CC Communication
ATT, T	TRK124 Fail TL102 Aborted
ATT, T	TRK125 Pass TL102 Passed
ATT, T	TRK126 Fail TL102 Failed
ATT, T	TRK127 Pass TL100 Passed

Table 8-2 — Log Message Routing Examples (continued)

ROUTING CATEGORY	LOG MESSAGES AND SUBSYSTEM GROUP
ATT, T	TRK128 Fail TL100 Failed
ATT, T	TRK129 Fail TL100 Failed
ATT, T	TRK130 Pass TL100 Passed
ATT, T	TRK131 Fail TL100 Failed
ATT, T	TRK132 Pass TL103 Passed
ATT, T	TRK133 Fail TL103 Failed
ATT, T	TRK134 Pass TL104 Passed
ATT, T	TRK135 Fail TL104 Failed
ATT, T	TRK136 Fail TL104 Failed
M	TRK138 Info Treatment
T	TRK139 Pass Tlnss Passed
T	TRK140 Fail Tlnss Failed
T	TRK141 Pass Tlsyn Passed
T	TRK142 Fail Tlsyn Failed
T	TRK143 Pass TL E-M Passed
T	TRK144 Fail TL E-M Passed
T	TRK145 Pass TL RP2 Passed
T	TRK146 Fail TL RP2 Failed
T	TRK147 RTS State-Change-by Rotl
T	TRK148 Mbsy State-Change-by-Rotl
M	TRK151 Inf Bluebox Detection Active
M	TRK152 Inf Bluebox Detection Cleared
M	TRK153 Inf Bluebox Call Detected
M	TRK154 Inf Bluebox Call Disconnect
M,T	TRK155 Info D911 Origination
T	TRK156 Pass TL-LPA-Passed
T	TRK157 Fail TL-LPA-Aborted
T	TRK158 Fail TL-LPA-Failed
T	*TRK162
T	*TRK182
T	*TRK183
	NOTE: (*) Needs to be routed to garbage class in table LOGCLASS if using Focused Maintenance

Software Optionality Control

Introduction

Software optionality control (SOC), part of the DMS Evolution (DMSE) product delivery process, facilitates the definition and delivery of product computing module loads (PCL). Once the new PCL is loaded, all the features it contains can be activated by the customer as needed without a software reload.

All functionality in a PCL is categorized as either base or optional. Base functionality is available for use immediately. Optional functionality is grouped into commercial units called SOC options, which can be purchased by operating companies. SOC options correspond to functional groups or functions. Optional functional groups and their optional capabilities may be activated, managed, and tracked without a software reload or restart using Software Optionality Control (SOC).

Rather than ordering a software delivery to get a new function, the network provider simply orders the authorization, or the Right-to-Use to enable the function. For functions that are managed through SOC, Nortel Networks sends software passwords that allow the customer to activate or deactivate the function at will.

The traditional INFORM report listed all the software loaded onto the switch. This report will still be provided, and will still indicate which software is loaded. However, because PCLs include all generally available functions—whether or not right-to-use has been obtained for all those functions—the INFORM report cannot indicate which software is licensed for use. For this purpose, a new tracking mechanism has been provided through the Software Optionality Control (SOC) utility.

Functional overview

SOC provides the following capabilities:

- provides an interface through which operating company personnel disable and enable options
- maintains a database of option interdependencies which ensures that no option is activated or deactivated unless it is safe to do so
- tracks the state of SOC options (on or idle)
- generates reports with status information about SOC options
- provides a mechanism for counting and limiting the usage of DMS

- services and resources
- defines and tracks options that are not controlled by SOC

Phases of operation

SOC has three phases of operation: software application, restart, and normal operation.

Software application

Software application is the phase during which the PCL is installed on the DMS switch. During a software application, SOC ensures that SOC options in the new software load inherit their settings from the previous software load. After a software application, all SOC options remain in their specified states (on or idle) until a state change is requested through the SOC user interface.

Restarts

During warm and cold restarts, SOC retains its database information, including the states, RTU settings, usage counts, and usage limits of options. However, an option in an error condition that recovers by changing its state during the restart may not return to its original state. In this case, SOC generates a message stating the new state of the option and the option's explanation of why it changed.

Normal operation

During normal operation, SOC periodically audits options to ensure that their current states and usage levels match the states and usage levels recorded for them in the SOC data tables. During these audits, SOC also verifies that dependency requirements for options are being met. SOC answers queries from other software about the state of options, and processes SOC user requests during normal operation.

User requests consist of database information queries, RTU or usage limit assignments, and requests to change the state or usage threshold of an option. Database information requests include queries about SOC option order codes, names, RTU settings, states, usage counts, and usage limits. SOC retrieves the information in the SOC database and formats it. The user can then either view the information on the MAP terminal or route the information to a file.

SOC options

There are three types of SOC options:

- state
- usage
- combo

A state option has a Right to Use (RTU) setting (yes or no) and a state (on or idle). The RTU setting must be yes in order for a user to change the state of an option. A

usage option has a usage limit (hard, soft, or monitored) and a current usage. It has no state and its RTU is determined by its usage limit. If the limit is zero then the RTU is no, or if the limit is greater than zero then the RTU is yes. A combo option has both a usage limit and a state (on or idle), and its RTU is determined by its usage limit. SOC manages options in three ways. An option can be:

- controlled
- tracked
- pending

SOC controls the state or usage of controlled options. Tracked options, on the other hand, are not controlled by SOC. The RTU settings and usage limits of these options are only recorded by SOC. Tracking options allows SOC to provide a complete record of the RTU status of all options in a PCL. A pending option is a place holder for an option that does not exist in the current software load but will exist in a future one. Pending options allow the operating company to preconfigure an upcoming option either in the on state or with a certain usage limit. The options in the new load are automatically set to the state or usage limit assigned to them as pending options. A pending option with an RTU of *yes* before the application of the new software load configures an option in the on state; a pending option with an RTU of *no* configures an option in the idle state.

Key codes

A key code is an alphanumeric password that Nortel Networks gives to the operating company, which allows the operating company to assign RTU to an option, to remove the RTU from an option, or to assign a new usage limit to an option. A unique key code is used for each operation for each option in a DMS office.

What you can do with SOC

The user interface for SOC consists of CI commands on the MAP terminal. The ASSIGN, SELECT, DBAUDIT and REMOVE commands allow you to:

- assign RTU to an option
- remove RTU from an option
- assign a usage limit to an option
- assign RTU or usage limits to a group of options using a key code file
- assign the on or idle state to an option
- assign a warning threshold to a usage option
- generate a report about one or more options in a PCL
- perform an audit of the SOC database

For detailed procedures on the use of the SOC utility commands, see NTP 297-8991-901, *DMS-100F Software Optionality Control User's Manual.*

Assigning and removing the RTU option

ASSIGN RTU command

When an operating company purchases a state option, Nortel Networks gives the operating company a password called a key code for the option. Once the key code is known, the ASSIGN RTU command can be used to grant the operating company permission to change the state of the option.

You can assign RTU to a group of options by applying the ASSIGN KEYS command to a key code file. This file, supplied by Nortel Networks, contains a list of order codes and key codes for the options. NTP 297-8991-901 describes how to assign RTU and usage limits to or remove the RTU from a group of options in a key code file.

The ASSIGN RTU command can be used with state options only. The RTU of usage and combo options is controlled by assigning the usage limit of the option. NTP 297-8991-901 provides a step-action procedure on how to assign RTU to a single option, and also describes how to assign a usage limit to an option. Software optionality control (SOC) generates a SOC504 log if the RTU application is successful or a SOC505 log if the RTU application is not successful.

REMOVE RTU command

The REMOVE RTU command allows operating company personnel to remove the RTU from a state option, thereby preventing any subsequent state changes for that option. An option that is controlled by software optionality control (SOC) must be in the idle state before you can remove its RTU. You can remove the RTU for a tracked option or a pending option at any time.

The REMOVE RTU command applies to state options only. To achieve the same functionality for a usage or combo option, you assign a usage limit of zero. NTP 297-8991-901 provides a step-action procedure on how to remove RTU to a state option. If the procedure is successful a SOC504 log is generated. If the procedure is not successful a SOC505 log is generated.

SOC User's Manual

NTP 297-8991-901, *DMS-100F Software Optionality Control User's Manual* is designed for operating company managers, engineers, planners and maintenance personnel who are activating, deactivating, or defining parameters for software optionality control (SOC) options. This manual contains procedures for assigning and removing the Right to Use (RTU) for an option, changing the state of an option, assigning a usage limit or a warning threshold to an option, displaying information about options in a product computing module load (PCL), and performing an audit of the SOC database.

Log and Control Record Exhibits

Following are various log and control forms developed for operating company use. They are not official forms and only should be used where no official forms are available. Utilize the forms for your benefit and adjust any form information to meet your needs.

The exhibits are followed with an explanation of the purpose of the form, the format, and provide remarks and documentation references when applicable. These references are in no way all inclusive and additional information may be found in the appropriate documentation. The exhibits also include a copy of the forms—use them for your benefit.

Exhibits

A. **CPU Downtime Log**

B. **PM Reload Log**

C. **Dial-up Access Log**

D. **Patch Control Log**

E. **AMA/CDR Tape Log**

F. **Circuit Pack Replacement/Repair Log — Line Cards**

G. **Customer Trouble Ticket Log**

H. **DMS-100F Trouble Log**

I. **ETAS Referral Trouble Log**

J. **Office Alarm Log**

K. **Office Image Log**

L. **DMS Control Record**

M. **DMS Maintenance Ticket**

N. **Office Journal Book**

Exhibit A   —   CPU Downtime Log

OFFICE_____   SOFTWARE LOAD_____

A		B	C	D	E	F	G	H	J	K
STOPPED CALL PROCESSING		INITIATED BY				DOWN-TIME IN SEC-ONDS	PREVIOUS HOUR		CALLS NOT SERVED F(G+H) 3600	EXPLANATION
		MAN		SYS						
DATE	TIME	COLD	WARM	COLD	WARM		MIN	NORIG		
TOTAL										

Exhibit A — CPU Down Time Log (continued)

Purpose

— Record CPU Downtime (Warm, Cold and Reload Initializations)

— Means of Prorating # of Calls Not Served During Downtime

— Track Processor Performance and Trend Information

— Input to Service and Performance Results Plan

A CPU downtime log is recommended at the site or within the control center. Logs will in most cases allow reconstruction of events leading up to an outage. Patterns in the total switching network cannot be developed by logs, however, radio station contests and many other external forces may cause multiple outages which can be seen using manual logs that include time and duration of not just CPU down time but service degradations as well.

Recommended Log Format

Suggested format includes the following items:

— Office Name

— Date

— Start Time

— Stop Time

— Total Down Time

— Type: Manual, System

— Degree: Warm, Cold

— Explanation/Purpose

— Technician Initials

— Remarks/Referral Information

Remarks

To determine the cause of the warm restarts, contact Nortel Networks Technical Support. Verify OM group CPU (SYSCINIT) or for SuperNode, group CM (CMSCINIT, CMMCINIT). Check logs CC107, INIT, and SWCT103. The following OM group CPU registers should be used to evaluate CPU problems:

MTCHINT; TRAPINT; CPUFLT; SYSWINIT; SYSCINIT; SYNCLOSS; MSYLOSSU; and SSYLOSSU

See office engineering parameters MAX_WARM and MAX_COLD in table OFC-STD. Also, see RECOVERY_INTERVAL_AFTER_WARMCOLD and RECOVERY_INTERVAL_AFTER_RELOAD parameters in table OFCENG.

Exhibit A — CPU Down Time Log (continued)

Detailed Preparation Guide

Column Headers	Description
OFFICE	Enter the office name
SOFTWARE	Enter the PCL software load
DATE	Enter the year, month and day of each call processing stoppage. One stoppage is recorded per line.
TIME	Enter the hour and minute of each call processing stoppage.
INITIATED BY MANUAL SYSTEM	Indicates whether the stoppage was manually or system originated. Enter "X" in required column. Cold/Warm Cold/Warm
Down time in seconds	The elapsed time that the system was not call processing, calculated as follows:

Cold & Warm Restarts	The difference in seconds between the time indicated in the CC107 printout and the time from the last log message prior to the restart.
	
	Example:
	***CC107 DEC09 12:22:15 4201 INIT WARM RESTART
	Reason = 50 PC = 4B5250 PTA = 00001689
	Program Wake Proc Module Procedure
	
	Difference Between:
	    (CC107) 12:22:15
	    (Last Log Msg) 12:21:41
	    Elapsed Time 34 sec

CPU Reloads	**Description**
	The difference in seconds between the time indicated in the immediately preceding log message printed or in SYSLOG, whichever is more current.
	
	Example
	*CC100 DEC13 21:05:28 4474 FAIL STORE TEST PSI MOD 1
	FCODE = OOOC CONTR = OOOF COMMN = 0003
	CARD_TEST = 7FFF, 7FFF, 7FFF
	
	System Image Reload
	***SOS RELOAD restart no. 1 @ ???-00
	00:00:00
	
	***CC107 DEC12 21:10:59 1101 INIT RELOAD RESTART
	REASON = 2 PC OOOBOEBB PTA 00001331
	PROGRAM MODULE PROCEDURE
	
	Difference Between:
	    CC107 21:10:59
	    CC100 21:05:28
	    Elapsed Time 331 sec

Exhibit A — CPU Down Time Log (continued)

Detailed Preparation Guide

Column Headers	Description
	Note 1: If there is no CC107 printed or in SYSLOG for the restart, the difference between the two available log messages immediately surrounding the restart will be used.
	Example: PM116 DEC08 03:20:27 6309 INFO PP-REPORT-DUMP TM80
	Activity Switch ***SOS COLD Restart No. 5 Dec-08 00:00:00
	NET102 DEC08 03:24:42 3301 EXC INTEGRITY DGN Elapsed Time = 03:24:42 minus 03:20:37 = 245 seconds
	Note 2: Printouts used in CPU Down Time calculations are to be retained with the service report plan and made available to support groups upon request.
PREVIOUS HOUR OMs NIN & NORIG	Enter the readings of the NIN and NORIG OMs for the hour preceding the initialization.
CALLS NOT SERVED	Calculate as shown by multiplying Column F times the sum of column G and H, then dividing by 3600.
EXPLANATION	Provides the reason for call processing stoppage or the trouble symptoms encountered. The action taken should be recorded (i.e. referred to ETAS CSR#XXX). Reference to any other supporting documentation should also be recorded. Use more than one line for explanation if necessary.
TOTAL	At month end, add columns B, C, D, E, F and J for transcription to other forms, e.g.. service report plan.

Exhibit B   —   PM Reload Log

OFFICE _____

DATE	START TIME	END TIME	TOTAL DN. TIME	PM		TECH INIT.	REASON FOR RELOAD
				TYPE	#		

Exhibit B — PM Reload Log (continued)

Purpose

Identify Peripheral Module (PM) outages for the purpose of:

— Tracking PM Performance

— Compiling Trend Analysis Data

Recommended Log Format

Suggested format includes the following items:

— Date

— Start Time

— Stop Time

— Total Down Time

— PM Type and Number

— Reason, Explanation, or Purpose

— Technician's Initials

References

OM group PM1 registers PM single-unit faults.

OM register PM1FLT is incremented when the system removes a PM from service because of a persistent fault that is detected during system-initiated diagnostics.

PM1FLT counts the faults for all PM cards except for P-side and C-side interface cards. Once a fault is counted by PM1FLT, the register does not count the same fault again during subsequent retesting when system diagnostics attempt to clear the fault.

PM2 provides information on the performance of dual-unit peripheral modules (PM) of type IPML (without node numbers). PM2 also collects data for the single-unit very small remote (VSR) PMs.

Suggest referencing logs PM128 and PM181.

For information on OM groups PM1 and PM2, see NTP 297-YYYY-814 for PCL loads and higher. For information on PM128 and PM181 logs, see NTP 297-YYYY-840 for PCL loads and higher.

Exhibit C — Dial-up Access Log

OFFICE _____

Dial-up Access Log							
	TIME		**REQUESTED INFORMATION**				
DATE	**LOG IN**	**LOG OUT**	**BY**	**ORGANIZATION**	**TEL NO.**	**REASON**	**ACTUAL ACTIVITY**

Exhibit C — Dial-up Access Log (continued)

Purpose

Track and control dial-up access to the DMS switch.

Dial up access logs enhance the security of the switch. All requests for access should be screened and logged. Since disconnected users may be left active or processes may be left running after logout, knowing who was logged in on a particular port as well as what they were doing is extremely important.

All dial-up access ports should be arranged for customer controlled access. This control may consist of manual answer on the data set, call transfer to a restricted centrex group, access through a central minicomputer system, or a dial back feature. All dial-up accesses should be logged. Periodic checks should be made to ensure that all dial-up access is being controlled by responsible personnel, whether it is through a control center or within the switch.

Recommended Log Format

Suggested format includes the following items:

— Date
— Log In Time
— Log Out Time
— Requested by Initials (Organization)
— Call Back #
— Reason for Access
— Actual Activity
— I (Initials of Person Giving Access)

Recommendation

It is recommended that the CI level LOGINCONTROL feature be used to assist in controlling the use of dial-up ports into the switch. This feature allows the automatic disabling of a port after disconnect by a user, as well as limiting the time and number of attempts at logging into an enabled port.

Remarks

Log entries should be made for all requests whether granted or not.

Exhibit D — Patch Control Log

	DATE		APPLICATION			
PATCH ID	**DOWN LOADED**	**APPLIED**	**NAME**	**ORIG**	**CALLBACK NUMBER**	**REMARKS**

Patch Control Log

Exhibit D — Patch Control Log (continued)

Purpose

To monitor the application of patches and to record associated data.

Patch control logs should include date, name of downloader, and number of patches. Logging this information allows follow up if they are not applied in a timely manner. It is also a flag to indicate new peripheral patches which should be applied against PM loads as soon as possible.

Recommended Log Format

Suggested format includes the following items:

— Patch I.D.

— Date downloaded

— Date applied

— Application

— Name/Organization

— Callback number

— Remarks (i.e., nature of patch, problems, call report #, etc.)

Remarks

Log entry to be generated and updated with any patch activity.

Exhibit E — AMA (CDR) Tape Log

DATE	TIME	INIT	VOL/FILE to TAPE	MTD# SER#	NUMBER OF RECORDS	LAST PARALLEL	ACTIVE VOL/FILE

Exhibit E — AMA (CDR) Tape Log (continued)

Purpose

To document preparation of (AMA) CDR data for transmittal to down stream processing.

Due to the revenue involved with AMA, accurate data such as date, volume name, file name, block sizes, and tape drives used to DIRPCOPY should be kept. Retrieving lost or mutilated data depends on the availability of this information.

Recommended Log Format

Suggested format include the following items:

— Date

— Time

— Initials

— Volume/File to Tape

— MTD # and Serial #

— # of Records

— Last Parallel File Block #

— Active Volume/File

— Remarks (Identify any unusual events, i.e., time change troubles, condition of tape, etc.)

Remarks

May or may not be required. Duplicate information may be contained on (AMA) CDR transmittal form.

Exhibit E — AMA (CDR) Tape Log (continued)

DATE	TIME	INIT	VOL/FILE to TAPE	MTD# SER#	# RECORDS	LAST PAR	ACTIVE VOL/FILE
6/17	0730	JAM	D000AMA4 U860617000033AMA	1 TX555	38461	2170	D010AMA1 A860618000035AMA

                                *1   *2   *3   *4

where file U860617000033AMA was copied to tape serial # TX555 on drive 1

DIRP101 JUN18 00:00:00 1700 INFO DIRP_FLOW_FLOW_LOG REASON = 14 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0003 SOS_FILE_ID = A003 0008 0005
    TEXT1 = SCHEDULED OG ROTATE INITIATED, RECORDS: 38428   PARM1 = 1303
    TEXT2 = VOL: D000AMA4, FILE: A860617000033AMA, ROTATE: PARM2 = 0036

DIRP101 JUN18 00:00:01 1900 INFO DIRP_FLOW_LOG REASON = 15 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0003 SOS_FILE_ID = A003 0008 0005
    TEXT1 = SCHEDULED OG ROTATE COMPLETED, RECORDS: 38461   PARM1 = 1305
    TEXT2 = VOL: D000AMA4, FILE: A860617000033AMA, ROTATE: PARM2 = 0036

DIRP101 JUN18 00:00:01 2000 INFO DIRP_FLOW_LOG REASON = 17 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0003 SOS_FILE_ID = A003 0008 0005
*3   TEXT1 = LAST PARALLEL FILE BLOCK NUMBER: 2170   PARM1 = 0
    TEXT2 = LAST ACTIVE FILE BLOCK NUMBER: 1305   PARM2 = FFFF

DIRP101 JUN18 00:00:01 2300 INFO DIRP_FLOW_LOG REASON = 12 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0006 SOS_FILE_ID = A081 0017 0001
    TEXT1 = SCHEDULED INC ROTATE INITIATED, RECORDS: 0   PARM1 = 0
*4   TEXT2 = VOL: D010AMA1, FILE: A860618000035AMA, ROTATE: PARM2 = 0036

DIRP101 JUN18 00:00:01 2400 INFO DIRP_FLOW_LOG REASON: 16 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0006 SOS_FILE_ID = A081 0017 0001
    TEXT1 = NEXT PARALLEL FILE BLOCKNUMBER: 2171   PARM1 = 0
    TEXT2 = NEXT ACTIVE FILE BLOCK NUMBER: 1   PARM2 = FFFF

DIRP101 JUN18 00:00:02 2600 INFO DIRP_FLOW_LOG REASON = 13 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0006 SOS_FILE_ID = A081 0017 0001
    TEXT1 = SCHEDULED INC ROTATE COMPLETED, RECORDS: 1   PARM1 = 1
    TEXT2 = VOL: D010AMA1, FILE: A860618000035AMA, ROTATE: PARM2 = 0036

DIRP101 JUN18 00:00:11 2800 INFO DIRP_FLOW_LOG REASON - 21 SSYS# = 0000
    SSNAME = AMA POOL# = 0003 VOLUME# = 0003 SOS_FILE_ID = A003 0008 0005
*2   TEXT1 = FILE CLOSED, RECORDS: 38461   PARM1 = 1305
*1   TEXT2 = VOL: D000AMA4, FILE: U860617000033AMA, ROTATE: PARM2 = 0036

Response received during dump to tape using DIRPAUTO:
END OF FILE REACHED
  1305 BLOCKS COPIED
0 BLANK BLOCKS ENCOUNTERED
0 I/O ERRORS ENCOUNTERED
0 INCORRECTLY FORMATTED BLOCKS ENCOUNTERED

Exhibit F — Circuit Pack Repair Log

SWITCHING CENTER_____   PERIOD_____

MTCE TKT. NO.	FAILED PACK		TROUBLE INDICATION	REQUISITION		WAYBILL		DATE REPLACE-MENT REC'D	DAYS TO TURN AROUND	IN SERV.		CIRCUIT PACK LOCATION
	CODE	SERIAL		NUMBER	DATE	NUMBER	DATE			OK	FL	

Exhibit F — Circuit Pack Repair Log (continued)

Purpose:

To record information concerning card replacement for the purpose of tracking and building patterns for line cards and line drawers, documenting turnaround time associated with card returns, and providing spare pack inventory and audit information.

Recommended Log Format:

Suggested format includes the following items:

— Maintenance Ticket Number

— Failed Pack Code (PEC) and Serial Number

— Trouble Indication

— Requisition Number and Date

— Waybill Number and Date

— Date Replacement Received

— Days to Turn Around

— In-service Test OK or Fail

— Circuit Pack Location

Recommendation

Use this log for logging line cards only. Use to track patterns to line drawer problems or track specific types of line card problems. Use other copies of this log for recording all other types of line cards.

Remarks:

Line logs LINE170 and LINE171 provide measured information for WLC diagnostic failures. An optional parameter "D" has been added for the DIAG command to allow the logs to be generated with failures. The intent is to provide the log information as an attachment to the card when it is returned for repair.

Exhibit G — Customer Trouble Ticket Log

OFFICE _____

		Customer Trouble Ticket Log							
TICKET NO.	**TELEPHONE NO.**	**REPORT TIME**			**LEN**	**CA/PR**	**TROUBLE**		**REF'D**
		DATE	**REC'D**	**CC**			**REPORT**	**FOUND**	

Exhibit G — Customer Trouble Ticket Log (continued)

Purpose

To record customer reported "troubles" for the purpose of taking corrective action and monitoring trend data.

Recommended Log Format

Suggested format includes the following items:

— Ticket number

— Telephone number

— Date/Time Received

— CC — Customer commitment time

— LEN — Line Equipment Number

— Cable facility

— Trouble reported

— Trouble found

— Referral information

Remarks

Some of these items may duplicate log and ticket entries currently in place, therefore should be weighed against existing procedures.

Exhibit H — DMS-100F Trouble Log

DATE	MTCE TKT. NO.	REPORT			DN. CCT. NO., EQUIPMENT		REPORT DETAILS	DESP TO	TROUBLE FOUND	TIME OK	CLOSE OUT TO	DISP. CODE
		TIME	BY	SER								

OFFICE_____

YEAR _____ MONTH_____

PAGE_____OF_____

Exhibit H — DMS-100F Trouble Log (continued)

Purpose

To record or identify equipment irregularities or failures for the purpose of taking corrective action and monitoring trend data.

Recommended Log Format

Suggested format includes the following items:

— Date Trouble Received
— Maintenance Ticket Number
— Report Time, Reported By, Their Serial #
— Customer Number, Circuit Number, or Equipment Number
— Reported Trouble
— Dispatched Trouble to
— Trouble Condition Found
— Time O.K.
— Closed Out To (Initials)
— Disposition Code (i.e. Code 5, 7 & 8, etc.)

Remarks

Some of these items may duplicate log and ticket entries currently in place, therefore should be weighed against existing procedures.

Exhibit I — ETAS/TAS Referred Trouble Log

TKT NO.	TROUBLE DESCRIPTION	ETAS/TAS REFERRAL				TROUBLE CLEARANCE			REMARKS
		PRIOR-ITY	CALL NO	DATE	TIME	ACTION TAKEN	DATE	TIME	

Exhibit I — ETAS/TAS Referred Trouble Log

Purpose

To maintain a record of DMS-100F trouble conditions referred to ETAS/TAS for resolution.

Recommended Log Format

Suggested format includes the following:

— Ticket No. —Serial number in office

— Trouble Description

— ETAS Referral Priority, Call Number, Date, Time

— Trouble Clearance Action Taken, Date, Time

— Remarks including CSR number or Engineering Complaint

Remarks

Perform periodic follow up with ETAS/TAS as required and record each event in a chronological log.

Exhibit J — Office Alarm Log

OFFICE _____

		ALARM LEVEL				RCVD BY	DISPOSITION	
DATE	**TIME**	**CRIT**	**MAJ**	**MIN**	**DESCRIPTION**		**FOUND**	**REF'D TO**

The table title "Office Alarm Log" spans the full width above the column headers.

Exhibit J — Office Alarm Log (continued)

Purpose

To record system reported alarm conditions for the purpose of taking corrective action and monitoring trend data. These are alarms separate from the MAP alarms.

Recommended Log Format

Suggested format includes the following items:

— Date

— Time

— Alarm Level (critical, major, minor)

— Description of alarm

— Received By

— Disposition — Found (yes/no), Referred To:

Remarks

Follow locally established alarm procedures. See NTP 297-1001-122, *DMS-100F Alarm System Description.*

Exhibit K — Office Image Log

OFFICE _____

DATE	**TIME**	**INIT**	**DISK VOL TAPE ID**	**IMAGE NAME**	**COPY**	**TEST**	**OFF-SITE IMAGE SENT**	**ACTIVE JOURNAL FILE**

The table title is **Office Image Log**.

Exhibit K — Office Image Log (continued)

Purpose

To maintain a record of office images and to assure that the most current image is available and used when required.

Generation of system image and journal file rotation should be coincident. Date, volume, file name, and comments should be kept. Problems encountered during image should be logged under the comment area. Disk read/write problems can start as intermittent failures. Noting this can make early detection of disk problems possible.

Log Format

— Date
— Time
— Initials
— Disk Volume/Tape I.D.
— Image Name
— Copy
— Test
— Off-site Image Sent (Date)
— Active Journal File

Remarks

See the *Preventive Maintenance* tab and the "Routine Tasks" subsection for tables listing the image routine and references to publications for procedures.

Tape should be labeled with appropriate information. Archiving of images on a weekly basis should be required of all sites. Journal files should be done as well. A series of at least three tapes using a grandfathered tape method is usually preferred. In addition, images should be retained remotely either in a control center or other secure area. Due to the possibility of intentional disruption of call handling as well as destruction of system images, maintaining an image remotely is excellent insurance. When the image is sent off-site for archiving, note the date in the Off-site Image Sent column.

Exhibit L — DMS Control Record for Operational Measurement Data

Yearly	Monthly Day	OM Registers																			
	1																				
JAN	2																				
	3																				
FEB	4																				
	5																				
MAR	6																				
	7																				
APR	8																				
	9																				
MAY	10																				
	11																				
JUN	12																				
	13																				
JUL	14																				
	15																				
AUG	16																				
	17																				
SEP	18																				
	19																				
OCT	20																				
	21																				
NOV	22																				
	23																				
DEC	24																				
AVG	25																				
PER YEAR	26																				
	27																				
	28																				
	29																				
	30																				
	31																				
ACTUAL	7 DAY																				
	14 DAY																				
	21 DAY																				
	28 DAY																				
	MONTHLY																				
BOGEY	DAILY																				
	7 DAY																				
	14 DAY																				
	21 DAY																				
	28 DAY																				
	MONTHLY																				

Exhibit L — DMS Control Record (continued)

Purpose

Provides a record for recording daily, weekly, and monthly key OM data on the same form. Using a second form monthly data can be summarized for 12 consecutive months. Also record related bogey information for analysis of data by day, week, and month.

Log Format

—Office

—Period (month or year records)

—Yearly - use these lines when recording month data

—Monthly/Day - use these lines for recording day data

—Actual - record week/month totals

—Bogeys - record daily/weekly/monthly bogeys.

Remarks

Record key OM register field descriptions, one per block across top of form. Several sheets may be required to record all the data. See the *Preventive Maintenance* tab and the "Operational Measurements" subsection for a list of OM registers to track for maintenance areas.

Also, see the "SPMS" subsection in the *Performance* tab for a list of OM groups and their registers.

Reference NTP 297-YYYY-814, *Operational Measurements Reference Manual* for a complete list of OMs.

Exhibit M — DMS Maintenance Ticket (Front and Back

DMS MAINTENANCE TICKET			
SU	DATE	TIME	TKT
REPT BY			
DN/TRK GRP/EQ			
LEN/TRK			
CA. PR./CXR			
OTHER EQ.		CLASS	
REPORT			
TEST			
REFER TO	DATE	TIME	
COMPLETION			
CLOSE TO	DATE	TIME	RSB CODE	QTY
ANALYSIS CODE			SPECIAL STUDY	

NOTES			
WORK TIME	ACCT CODE	INITIALS	DATE

Exhibit M — DMS Maintenance Ticket (continued)

Purpose

— To record relevant trouble report data, subsequent investigative data, and corrective activity until the report is closed out.

— To record administrative information.

— Used in conjunction with Customer Trouble Ticket Log (Exhibit G)

Ticket Format

— SU: Switching Unit (NNX or CLLI)

— DATE & TIME

— TKT: Numbered serially

— REPT BY: Source of Report

— DN/TRK GRP/EQ (Directory #, Trunk Group or Equipment)

— LEN/TRK (Line Equip or Trunk Member)

— OTHER EQ. & CLASS

— REPORT (Trouble Condition Reported)

— TEST (Trouble Condition Tested)

— REFER TO (Initials), DATE & TIME

— COMPLETION (What was found & corrective action)

— CLOSED TO, DATE, TIME, RSB CODE & QUANTITY

— ANALYSIS CODE & SPECIAL STUDY

— NOTES: Additional space as required for Report, Test, Completion, or Other Data

— WORK TIME TALLY (Time Spent & Codes, etc.)

Remarks

Write up a DMS Maintenance Ticket for each reported trouble/investigation. All tickets should be serialized and accounted for.

Exhibit N — Office Journal Book

Purpose

To record maintenance activities in a chronological manner.

Journals are used to log information pertaining to any central office maintenance activities or other events. Entries for PM outages and initialization can also be kept here for patterning. Journals allow shifts to pass on information about office activity, and problems that have been identified and corrective action that has taken place.

All sites may not benefit from this type of log, but most manned sites prefer to keep one.

Journal Format

— DATE, TIME

— Technicians's Initials

— Short Narrative Format

Remarks

A Journal Book with lined pages, or a spiral bound notebook is used. Journals are available through corporate stationary supply channels, or from local office supply stores. A structured format is not generally used.

Nortel Networks Documentation

This subsection describes the publications, drawings, manuals, and other documents that are used to support and maintain the DMS-100F switching system. Included is information on the Product Computing-module Load (PCL) documentation structure. Following is a sample of information provided in this subsection:

- Documentation structure
- Proprietary documentation
- Product documentation catalog
- Site specific documentation
- Software software release documentation
- Value added documentation

For information on value added documentation, such as this manual, see the *Technical Assistance* tab and information under "Maintenance Services."

Documentation structure

Two types of standard documentation are provided with DMS-100F systems: Modular Documentation System (MDS) documents and Nortel Networks Publications (NTPs). The NTPs are documented as "publications" or "practices" but will be called "publications" within this subsection. The MDS documents are associated with Nortel Networks product engineering codes (PECs), but the NTPs have their own 10-digit numbering system not related to the PEC.

Modular Documentation System (MDS)

The MDS structure of the documents complements the modular nature of the system. The functions of MDS are as follows:

- To produce documents whose contents satisfy the specific needs of frequent users, and the general needs of all users.
- To be technology independent (i.e., changes in the technology used in the product must not affect the documentation system).

- To provide a document identifier (prefix) which relates to the type of information contained within the document, and to aid a user when searching for a specific type of information.

- To provide a document identifier that relates to the product identifier, and to aid a user in the search for information on a product.

Characteristics of MDS

MDS has a "top down" structure. Documents are stratified to conform to each level of the product structure (i.e., system, subsystem, module).

MDS documents describe a product as a module. A module in this case is one that stands alone in its internal functions and whose interface with the rest of the system (input and output signals, and connections) are defined within the terms of this module. As a result, the module and its documentation can be changed as required without affecting the rest of the system.

MDS document identifiers

Each hardware product of the DMS 100 Family is identified by a unique Product Engineering Code (PEC). A PEC consists of eight characters and has a specific structure:

(Prefix)	(Base)	(Suffix)
NT	NANN	XX
NT	AANN	XX

Where: NT is Northern Telecom (now Nortel Networks)

N is numeric

A is alphabetic

X is alphanumeric

Examples of PECs are NT0X25AA, NT4X25BH and NT6X10AC.

- Prefix — The prefix NT is assigned to all codes, thereby identifying this item as a Nortel Networks product.

- Base Code Group — Uniquely identifies a family of products. Associated hardware documents bear an identical base code.

- Suffix — A two character suffix uniquely identifies each member within a family of products. It is assigned in sequence: AA, AB, AC, and 01, 02, 03. Combination alphanumeric suffixes are allowed, but are not presently used.

The documents prepared to support each PEC are identified in a similar manner:

(Prefix)	(Base)	(Suffix)	(Stream)	(Issue)
AA	NANN	XX	NN	NN

- Prefix — The alphabetic prefix identifies each type of document. An Interconnect Schematic has the prefix IS, Assembly Drawing is AD, General Specification has the prefix GS, and Module structure has the prefix MS.

- Base Code — The base code is identical to the associated PEC.

- Suffix — If the suffix is present, it will be the same as the suffix of the PEC. Some documents are written for more than one very similar PEC. Such an example is GS6X17, which is applicable to the NT6X17AA, NT6X17AB, NT6X17AC and the NT6X17AD.

- Stream — The Stream of a document is changed when major revisions to the features or operations of the PEC are involved, but would remain unchanged for minor enhancements or refinements to a product.

- Issue — The issue of the document is changed whenever minor revisions, corrections or improvements are made to a product or document.

Nortel Networks Publications (NTPs)

NTPs are issued to document all aspects of the family of DMS-100 switches and basically cover the following disciplines:

- Administration
- Engineering
- Installation and Testing
- Operations
- Maintenance
- Translations
- Provisioning

Nortel Networks is in an ongoing effort to redesign and restructure NTPs through a program called DMS documentation evolution (DMSE). Restructuring of NTPs to meet customer requirements has resulted in many NTPs being transferred to newer or other existing NTPS. Some have been canceled or discontinued.

Documentation was restructured with the Product Computing-module Load (PCL) delivery. The PCL documentation structure allows delivery of PCL specific documentation to the customer. This significantly reduces the volume of documentation delivered, while increasing the usability of the documentation received.

Reference NTP 297-8991-001, *DMS-100 Family Product Documentation Directory* for a complete list of available NTPs, and NTP 297-8991-002, *DMS-100 Cancellation Cross-reference Directory* for NTPs that have been canceled or replaced by other NTP documents.

PCL documentation structure

The Product Computing-module Load (PCL) structure follows the BCS36 release of documentation. PCL documentation has reduced the volume of documentation by

eliminating duplication and by the restructuring of similar information into fewer documents.

For some documents that were canceled, the resulting pieces were distributed among several documents in an effort to improve organization and simplify the task of finding information.

All DMS-100F NTPs are identified by a ten-digit number that is divided into three blocks as follows:

297-YYYY-ZZZ

- The first three digits denote the DMS-100 Family of NTPs.
- The layer number—YYYY—denotes the PCL product.
- The last three digits, ZZZ, are called the suffix and denotes the type of NTP.

The following is a list of PCL layer numbers and their associated products:

PCL layer number	PCL or product	PCL name or product name
8001	LEC	U.S. Stand-alone DMS-100/200
8003	LECA	U.S. Stand-alone DMS-100/200 (GSF)
8011	CDN/CDNB	Canadian Stand-alone DMA-100/200
8013	CDNA	Canadian Stand-alone DMS-100/200 (GSF)
8021	LET/LETB	U.S. DMS-100/200 TOPS Combination
8023	LETA	U.S. DMS-100/200 TOPS Combination (GSF)
8031	LTT/LTTB	Canadian DMS-100/200 TOPS Combination
8033	LTTA	Can. DMS-100/200 TOPS Combination (GSF)
8041	UK/EUR	European DMS-100
8051	ABSM	Advanced Business Services (ABSM = Australia, China, and CALA)
8061	ABSK	Advanced Bus. Services (ABSK = IDC Only)
8071	ATVB	Can. Stand-alone DMS-100/200 AUTOVON
8073	LAVB	U.S Stand-alone DMS-100/200 AUTOVON
8101	STPBASE	Signaling Transfer Point Base
8111	STPMDR7	Signaling Transfer Point MDR7
8121	STPSEAS	STP Signaling Eng & Admin System
8201	RLCM/OPM	RLCM/OPM
8211	OPAC	Outside Plant Access Cabinet
8221	RSC	Remote Switching Center
8231	SCM-100S	Subscriber Carrier Module-100S (SLC-96)
8241	SCM-100U	Subscriber Carrier Module-100U (Urban)
8251	SCM-100A	Subscriber Carrier Module-100A (Access)
8261	RSCS Model A	RSC-SONET Model A (DS1)
8263	SCM-100A	Subscriber Carrier Module-100A Maint. Manual
8271	RSCS Model A	RSC-SONET Model A (PCM30)
8281	RSCS Model B	RSC-SONET Model B (DS1)
8291	RSCS Model B	RSC-SONET Model B (PCM30)

8301	SCM-100SR	Subscriber Carrier Module-100S Remote
8311	Host XPM	Host Extended Peripheral Module
8321	XPM	Extended Peripheral Module (DS1)
8331	XPM	Extended Peripheral Module (PCM30)
8341	TOPS MS	TOPS Operator Position Sys Msg Switch
8401	TOPS	TOPS (Stand-alone Global)
8411	USTOPS	TOPS (Stand-alone U.S.)
8421	CDNTOPS	TOPS (Stand-alone Canadian)
8501	SCP	Service Control Point
8991	PCL com/misc	PCL common and miscellaneous

The following is a list of PCL suffix numbers:

Suffix	NTP type
350	Translations Guide
543	Alarm and Performance Monitoring Procedures
544	Trouble Locating and Clearing Procedures
545	Recovery Procedures
546	Routine Procedures
547	Card Replacement Procedures
550	XPM Maintenance Manual (remote only, layers 8201-8331)
599	Feature Description Manual
801	Peripheral Module Software Release
805	Hardware Description Man. (PCL com/misc only, layer 8991)
808	Service Order Reference manual (SERVORD)
814	Operational Measurements Reference Man. (all PCLs & SPM)
840	Log Reports Reference Manual
855	Office Parameters Reference Manual
856	Software-to-Data Cross-reference

For further information on PCL documentation, see NTP 297-8991-001, *DMS-100 Family Product Documentation Directory* and NTP 297-8991-002, *DMS-100 Cancellation Cross-reference Directory.*

General Specifications (GSs)

General specifications contain hardware descriptive information pertaining to the purpose, function, and system interrelationship (input/output). These documents are written to address the shelf or circuit pack level for maintenance purposes.

Assembly Drawings (ADs)

Products that are the assembly of various elements may be pictorially displayed on an AD. The AD, created by equipment design or mechanical design, is required for manufacturing to assemble and inspect the product and for on-site installation and maintenance.

There are two types of nonproprietary ADs as follows:

- Mechanical Assembly Drawings — These drawings show the construction of frames, shelves, and other miscellaneous equipment.
- Structural Assembly Drawings — These drawings illustrate the placement of circuit packs in a drawer, drawers in a module, and modules in a frame.

Interconnect Schematics (ISs) or Functional Schematics (FSs)

The FS applies to electromagnetic equipment and has now been largely replaced by the IS. The FS illustrates functional interconnections between subassemblies of the product.

The IS describes connectivity between modules by using block diagrams in which functional blocks are joined by lines. Each line represents a set of connections. Detailed connections are identified in tabular form using separate tables to group similar connections. Notes are used as required to supplement the block diagram and detailed tabular information.

Cabling Assignments (CAs)

A CA drawing defines the specific interconnections among products within a system. It includes information on both the originating and terminating ends of a cable, the specific type of cable, and the number of leads required.

CA drawings also describe drop lengths of cables and pin-to-pin connections between frames, and are used to engineer offices. CAs are one of the key documents used in the creation of job specifications. The CA drawings are necessary documentation for the assembly plant, installer and customer.

Development Release Units (DRUs)

For PCL loads, Development Release Units (DRUs) are the equivalent of DDOCs for the older BCS loads.

These documents provide information describing new features as they are added to the DMS-100F of systems. Each DRU is assigned a feature number and title. Issue numbers and revision dates, as appropriate, are also included.

DRUs include, as appropriate, the NTPs affected, a functional description, system log message changes, operational measurement changes, data schema changes, man-machine interface changes, and any engineering changes required with the new feature.

Tier II documentation

Tier II documents provide more detailed technical software information than documentation normally supplied with a DMS-100F system. Such documentation is identified by an appropriate proprietary statement on the documents. For a complete list and description of the Tier II documents and packages that can be ordered, see NTP

297-8991-001, *DMS-100 Family Product Documentation Directory.* Following is a list of those documents:

- TAM-1001-001, Index of Technical Assistance Manuals (TAMs)
- TAM-1001-002, TAS NON-RES Tool Listing Technical Assistance Manual
- TAM-1001-003, DISPCALL User's Guide
- TAM-1001-004, PMDEBUG Technical Assistance Manual
- TAM-1001-007, PMIST Technical Assistance Manual
- TAM-1001-008, DEBUG Technical Assistance Manual
- TAM-1001-011, Data Layout Reference Manual
- TAM-1001-012, CALLTRAK User Guide
- TAM-1001-013, MPCDebug User Guide
- TAM-1001-014, SCANLOG User Guide
- TAM-1001-015, C7TU Technical Assistance Manual
- TAM-1001-018, DMS-100F Quick Reference Guide
- TID-1001-000, Program Documentation Index (PDI)
- TID-1001-001, Central Control Software Program Listing (NT40)
- TID-1001-006, PROTEL Reference Manual
- TID-1001-007, DMS-100F CCC Guide 1 Machine Architecture
- TID-1001-008, DMS-100F CCC Guide 2 User's Manual
- TID-1001-009, XPM Assembler User's Manual
- TID-1001-010, XPM PASCAL Manual
- TID-1001-012, DMS-100 Synchronizable Clock Debug Software
- TID-1001-013, DMS-100 Debugging and Measuring Tools: A Survey
- TID-1001-014, DEBUG and SWERR Monitors
- TID-1001-015, New Peripheral Debugging
- TID-1001-016, IOQUERY - User's Guide
- TID-1001-017, Network Integrity Fault Analysis Guide
- TID-1001-019, Circuit Schematics (CS)
- TID-1001-020, Functional Description (FD)
- TID-1001-022, Assembly Drawings (PAD)
- TID-1001-023, DMS-100F Interface Compatibility Reference Guide
- TID-1001-024, XPM Peripheral Software Program Listings
- TID-5001-001, DMS SuperNode Software Program Listings
- TID-5001-002, DMS-100F System Description

- TID-5001-003, BRISC Software Program Listings
- IM-1001-001, DMS-100 Customer Installation Manuals

DMS-100 Installation Manual

The DMS-100 Customer Installation Manual (IM) contains all the installation methods available to install and commission the DMS-100 switch. All installation methods previously contained in the following manuals have been incorporated into one manual:

- IM925 DMS-100 Installation Manual
- IM926 User Guides
- IM940 Vendor Equipment Manual
- IM964 Dynamic Network Control (DNC) Manual
- IM966 Data Packet Network (DPN) Manual

Product documentation directory

The Product Documentation Directory is a catalog that describes documentation available to users of the DMS-100F of switching products as well as other related products. The directory also provides ordering information and price listings.

- NTP 297-8991-001, *DMS-100 Family Product Documentation Directory*

Documentation media

Nortel Networks DMS-100F documentation is available in paper, and electronic formats. The electronic format is Helmsman CD-ROM. The "User documentation," which is shipped with the switching system, is a mixture of paper and CD-ROM. Software listings of each specific generic program are available in PROTEL CD-ROM form.

Documentation ordering

Documentation can be ordered in three distinct ways:

1. Call 1-800-684-2273 Option 2.

2. Both standard and job related documentation can be ordered through the NT86XX questionnaire or NT ACCESS at the Customer Information (CI) ordering phase of an initial or extension to a switch.

3. Operating companies may purchase additional documentation by submitting a purchase order for specific documents or document packets to the Nortel Networks merchandise order specialist. This is usually done through a documentation coordinator within the operating company.

CD-ROM recycling program

Nortel Networks has developed a CD-ROM recycling program in some market areas to recycle materials whenever feasible. Its Reclamation Facilities use reliable outlets for recycling compact discs and the clear jewel cases. Please recycle older discs when they are no longer needed. If you have any questions about this program, please call your regional Helmsman coordinator. In the U. S., you may call the Reclamation Facility directly: 1-919-687-3928 (within Nortel Networks, call 6-262-3928.)

The procedure for recycling is listed below.

1. CD-ROM user collects a minimum of 10 CD-ROMs. CD-ROM user packages the material and ships it to the Recycling Center. Sender is responsible for packaging and shipping costs. (CD-ROMs do not need to be well cushioned.)

CD-ROM recycling program in the United States

via U. S. Postal Service

> Wesbell Recycling Center
> CD-ROM Recycle Program
> P. O. Box 15009
> Durham, North Carolina 27704
> *(Please, no more than five pounds.)*

via UPS or other direct delivery:

> Wesbell Recycling Center
> CD-ROM Recycle Program
> 1431 East Geer Street
> Durham, North Carolina 27704

via Nortel Networks internal mail:

> Wesbell Recycling Center
> CD-ROM Recycle Program
> Dept. 8800/Geer

CD-ROM recycling program in Canada

via external mail:

> Philip Recycling Center
> CD-ROM Recycling Program
> 200 Brock Street
> Barrie, Ontario
> L4M 2M4

2. The Recycling Center collects the materials until an adequate quantity for shipment to a recycler is reached. The Recycling Center is responsible for packaging and shipment costs.

3. The recycler receives the CD-ROM material in pre-approved minimum quantities.

Site specific documentation

Office job related record drawings and documentation are provided with the delivery of any initial or extension for a DMS-100F switch. The following documentation is site specific:

Document Index (DI)

The DI is an index of all standard job related documents provided for each office and includes the issue of each document supplied.

Office Inventory Record (OIR)

The OIR contains the list of all the components of a customer office, the quantity, and the release. Input is from job specifications and on-site equipment audits. The OIR is used for keeping track of the contents of a particular office, change control, and extended warranty service.

Office Feature Record (OFR) (D190)

The OFR contains a short description of each PROTEL software subsystem resident in a particular office and a list of feature packages provided in the software load.

Job specifications

The main function of the job specification is to list the materials needed to assemble and install a job. There are three types of job specifications: material requirement, configuration, and cable. After the job specification has been used by manufacturing to assemble the job, and by the installer to install the job, it is no longer required since the job drawings contain all the information about the contents of the office.

Job drawings

Job drawings are office records generated by customer engineering job specifications, JIM, or 88K orders. Job drawings are permanent records of what equipment is in a particular office and indicate the location of components when the positioning is variable. A breakdown of the drawings for a standard job would consist of: up to 20 job drawings, four facility drawings showing floor plan, lighting, cable racks and ceiling inserts, one Distributing Frame (DF) drawing, and one transmission drawing.

Common systems drawings

These drawings portray equipment that is not unique to DMS-100F equipment, but is nevertheless part of the installation (i.e., power, cable racking).

Purchased items documents

These documents are for equipment that Nortel Networks obtains from other manu-facturers (TTYs, tape drives, etc.). This documentation is normally in the form of manuals provided with the equipment.

Software release documentation

Product Computing-module Load (PCL) release document

The DMS-100 Family software release document is supplied for each Software Stream. The release document provides software feature information pertinent to the new software load.

A status of PRELIMINARY means the final feature content of the software release has not been finalized and features may be added or deleted without notice. A status of STANDARD indicates that the feature content of the software release is firm.

A FEATURE CONTENT section provides information concerning DMS-100 Family System features associated with software releases. Each office configuration is cus-tomized to meet Telco/Carrier requirements. Only features NEW or CHANGED in the release(s) covered by the document are included. Cross-reference tables make it more efficient to find information. A description of the tables precedes them.

The following sections provide information necessary to support changes applicable to the new software release:

- Functional Descriptions (FN) — summarizes the functions of the feature
- Data Schema (DS) — indicates major additions/changes to the Data Schema table
- Logs (LG) — indicates major additions/changes to the LOGs
- Office Parameters (PARM) — indicates major additions/changes to the PARMs
- Operational Measurements(OM) — indicates major additions/changes to the OM groups
- Man-Machine Interface (MM) — indicates major additions/changes to the LOGs
- Office Parameters (PARM) — indicates major additions/changes to the Service Order
- Automatic Message Accounting (AM) — indicates major additions/changes to the AMA

PM software release documentation

The NTP 297-8981-599, *DMS-100F North American DMS-100 Peripheral Module Software Release Document* is used to update the software in North American DMS-100 family peripheral modules (PM) and hardware types. This document provides

load names, update procedures, and other release-specific information. It may be used by maintenance technicians with a range of experience in switching, PM software, and PM software updating.

Companies may have company-specific and office-specific policies regarding PM updates. Review these policies, and resolve any differences between the policies and this document before beginning the PM update process.

Customer Support documentation

Documentation is available at the Nortel Networks website located at URL www.nortelnetworks.com/. Select Customer Support, Documentation. You may search, personalize, and save documents for future reference.

Helmsman Express online

DMS-100F Helmsman online documentation is available via the Nortel Networks website at www.nortelnetworks.com/. Select Customer Support, Documentation, Region and Language, Online Documentation. Product Family is Switching Products, and Product is DMS-100/200 Local switching Systems. Helmsman Express Login, Registration, and Training are on the right side of the screen.

Value added documentation

To assist operating companies with their proactive approach toward maintenance, Nortel Networks Global Professional Services provides special value added documents and maintenance services. For information on value added documents or maintenance services, see the ''Technical Support Services'' subsection within this manual or contact Nortel Networks, Global Professional Services, Manager - Technical Services at 1 (919) 465-0434.

Office Security

General

In today's environment, with the challenge of illegal access to computer systems, the security of our telephone network should be one of the highest priorities within any communications company. There is a need to safeguard telephone service to the customer, AMA billing records, credit card numbers, communications equipment, and databases by restricting access only to authorized personnel. These safeguards require constant monitoring and 24 hour year-round commitment.

Some safeguards have been described in previous areas of this manual. Those safeguards dealt with office images, maintaining office logs for AMA tapes and dial-up access, and retaining hard copies of translation tables, office parameters, and SFDEV files. In addition to those safeguards, this subsection describes security features and safeguards for:

- Dial-up access
- Human-machine access
- Input command screening
- Audit trail
- Dial-up access ports

All dial-up access ports should be arranged for customer controlled access. This control may consist of manual answer on the data set, call transfer to a restricted centrex group, access through a central minicomputer system, or a dial back feature. All dial-up accesses should be logged (see the Dial-Up Access Log form within the previous "Log and Control Record Exhibits" subsection). Periodic checks should be made to ensure that all dial-up access is being controlled by responsible personnel, whether it is through a control center or within the switch.

LOGINCONTROL command

It is recommended that the CI level LOGINCONTROL feature be used to provide security for the use of dial-up ports into the switch. This feature allows the automatic disabling of a port after disconnect by a user, as well as limiting the time and number of attempts at logging into an enabled port.

This can be a valuable enhancement to switch security and reduces the possibility of ports being left in an accessible state. We suggest LOGINCONTROL responsibility be under control of security supervisor or manager. You may consider privclassing LOGINCONTROL for additional security. More is provided on the LOGINCON-TROL command later within this subsection.

Human-machine access

The following are general security safeguards regarding human-machine access:

- Log out I/O devices (i.e., MAPs, PRTs) during extended periods when not in use and unattended.

- Change user passwords every month or more frequently.

- Follow local procedures for disposing of printout paper, documentation, and CD-ROM.

Input command screening

All commands should be privilege classed (PRIVCLASS) to restrict commands to selected users and all commands should be DUMPSAFE or DUMPUNSAFE as required. It is suggested that the PRIVCLASS screening process be controlled only by the control center (i.e., SCC, NOC, NRC). More is provided later within this sub-section.

Security log

When the parameter TABLE_ACCESS_CONTROL is set to "Y" and table CUST-PROT is datafilled, a security log is generated each time a table is changed. It records who, when, and what was changed. See table CUSTPROT later within this subsection.

Access control for tables

When equipped with the appropriate software, it is possible to control who may change translation data by using table CUSTPROT. Three levels of security may be provided: read only, update, and all privileges. TABLXXX logs produce an audit trail if they are set up in the log system.

Log trails and security alarms

Any security log reports described within this subsection may be alarmed if desired. Various alarm levels for the SECU and TABL logs may be assigned by using table AUDALARM. The security logs can be used as an audit trail for regular and unauthorized operations. More is provided later within this subsection.

Reference information

The following should be used as reference for supporting the material within this sub-section:

NTP 297-YYYY-350, *Translations Guides*

NTP 297-1001-129, *DMS-100F Input/Output Reference Manual*

NTP 297-YYYY-855, *Office Parameters*

NTP 297-1001-822, *DMS-100F Commands Reference Manual*

NTP 297-YYYY-840, *Log Reference Manuals*

NOTE: Where there is a conflict between this document and the listed Nortel Networks Publications (NTPs), the NTP shall take precedence.

Security software packages

One or more of the following software packages must be present in the switching system to implement enhanced security:

- NTX292AB (BASE0001) Enhanced Security Package (Password Encrytion)
- NTX292BA (BASE0001) Enhanced Security Package (Non Encrytion)
- NTX293AA (BASE0001) Enhanced Security Package II (Auto Dial Back)

Office security parameters

The following office parameters are associated with the Enhanced Office Security Software Packages NTX292AB, NTX292BA, and NTX293AA:

ENHANCED_COMMAND_SCREENING Table OFCOPT

This parameter should have a value of "Y" if the switching unit has the Enhanced Security with Password Encryption software NTX292AB.

The feature associated with this parameter allows commands to be assigned any subset of 31 classes. Command screening then becomes a matter of ensuring that a user's command classes have a nonempty intersection with the classes of any command they wish to use.

+ **Change requires a New Software Load.**

ENHANCED_PASSWORD_CONTROL Table OFCOPT

This option should be set to "Y" if the switching unit has the Enhanced Password Control feature NTX292AB/NTX292BA.

If set to Y, it creates the following parameters in table OFCENG:

EXPIRED_PASSWORD_GRACE
MIN_PASSWORD_LENGTH
PASSWORD_LIFETIME

Use of the Enhanced Password Control feature disables all automatic login features.

This feature must have a value of "Y" in order for the Automatic Dialback feature (NTX293AA) to function properly.

+ **Change requires a New Software Load.**

MONITOR_TABLE_ACCESS parameter in Table OFCOPT

This option specifies whether the switching unit has the Security Table Enhancement feature (NTX292AB/NTX292BA).

The operating company can activate or deactivate this feature by changing the value of parameter TABLE_ACCESS_CONTROL in table OFCVAR.

The operating company may activate or deactivate this feature on a table basis by changing the value of fields READPROT, UPDTPROT or ALLPROT in table CUST-PROT.

+ **This option can only be changed by Nortel Networks.**

+ **Activation requires a cold start.**

PASSWORD_ENCRYPTED parameter in Table OFCOPT

This parameter specifies whether the SHOWPW command is to be suppressed or not. The command SHOWPW is not optional and is available in switching units with the Password Encrytion feature (NTX292AB).

+ **Activation requires a new load**

DIALBACKPW_ENCRYPTED parameter in Table OFCOPT

This parameter is required in a switching unit with the Automatic Dial Back Feature (NTX293AA) and specifies whether the SHOWDBPW (show dial back password) command is to be suppressed or not.

+ **Activation requires a new load**

MODEM_DIALBACK_CONTROL parameter in Table OFCOPT

This option specifies whether automatic dial back is allowed on MODEMS.

The Enhanced Password Control feature (NTX292AB/BA) is required for dial back to function properly.

The LOGINCONTROL command is used to specify whether a modem is to be used as an answer modem or a dialout modem when DIALBACK is active.

Table DIALBACK stores the *dialback* related data.

+ **Activation requires a new load**

SUPPRESS_USERNAME parameter in Table OFCOPT

This appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

This parameter specifies if the user name is suppressed during MAP VDU and printer sessions.

Set the parameter to "Y" if the user name is to be suppressed.

DEFAULT VALUE(N)

+ **Activation immediate**

EXPIRED_PASSWORD_GRACE parameter in Table OFCENG

This appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

The number of logons for which a password may be used if the password is older than the value of parameter PASSWORD_LIFETIME.

MINIMUM -0
MAXIMUM -32767
DEFAULT -3

+ **Activation immediate**

MIN_PASSWORD_LENGTH parameter in Table OFCENG

This parameter appears only if the switching unit has the option
ENHANCED_PASSWORD_CONTROL in table OFCOPT set to "Y" and the

Enhanced Security Package (with Password Encryption software package NTX292AB) is present.

This parameter specifies the minimum number of characters allowed for logon passwords.

MINIMUM -0
MAXIMUM -16
DEFAULT -6

+ **Activation immediate**

PASSWORD_LIFETIME parameter in Table OFCENG

Appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

Determines the duration, in number of days, for which a password may be used.

MINIMUM-0
MAXIMUM-32767
DEFAULT-30

+ **Activation immediate**

TABLE_ACCESS_CONTROL parameter in Table OFCVAR

This parameter is required if the switching unit has the "Security Table Enhancement" feature office option MONITOR_TABLE_CONTROL set to "Y" in table OFCOPT.

This parameter allows the operating company to activate or deactivate the feature by changing the value of this parameter.

When this parameter has the value of "Y", the operating company can activate or deactivate this feature on a table basis by changing value of fields READPROT, UPDTPROT or ALLPROT in table CUSTPROT.

+ **Activation immediate**

Associated data tables

The following tables are associated with *enhanced security* as described in NTP 297-YYYY-350, *Translations Guides.*

Table TERMDEV

This table lists the assignments for terminal devices. Table TERMDEV provides the ability to PRIVCLAS a terminal device restricting the device to a specific set or class of commands specified in table CMDS. There can be any combination of classes between zero through 31 or all.

This table also stipulates the type of modem that is connected to the corresponding port and thus determines which set of procedures are used for controlling the modem.

Where the Enhanced Password Control (Automatic Dialback) feature is present, the type of modem must be specified.

Access to table TERMDEV can be restricted by datafilling table CUSTPROT.

> **WARNING**
> *Be aware that a lockout condition exists if all the commands are "PRIVCLASSed" out for all users and terminals.* The only way out is to use the userid called ADMIN. An ADMIN userid is neither displayed nor restricted in any way. It is always available, provided the ADMIN password is known and the terminal is not in the "autologin" mode.

Table CMDS

Office parameter ENHANCED_COMMAND_SCREENING determines if the feature is turned on. This office parameter may be set only once: that is, at datafill time.

When office parameter ENHANCED_COMMAND_SCREENING is turned on, the table is automatically datafilled by the system.

The table is initially datafilled with default values.

> **WARNING**
> If tuples are added to this table through table control, a **RESTART** is required to activate the change, particularly if the tuple is deleted and then readded. To avoid a **RESTART**, modify the tuples in table CMDS using the CHANGE or REPLACE command (or via the PRIVCLAS command) instead of the DELETE and ADD commands.

The PRIVCLAS command allows for setting multiple command classes.

Four fields are present in table CMDS that specifies whether command use or command abuse is to be logged or alarmed. Those fields are:

LOGONUSE	Y or N	Enter Y when a log is to be created on every use of this command. **Default value is N.**
USEALARM	CR, MJ, MN, or NA	Enter the type of alarm to raise on every use of this command. **Default value is No Alarm (NA)**
LOGABUSE	Y or N	Enter Y when a log is to be created when

a user with the wrong command set tries
to use this command.
Default is N.

ALRMABUS CR, MJ, Enter the type of alarm to raise when
      MN, or NA a user with the wrong command set
             tries to use this command.
             Default value is No Alarm (NA).

Table CUSTPROT

This table defines the command class of users able to read, change and add or delete tuples respectively for each table assigned in the switching unit.

The initial input for table CUSTPROT is automatically produced by table control, and maintains this value unless changed by the operating company. The initial values produce by table control for privilege classes are 15.

The privilege class that has the **read** protect capability is allowed to read, but <u>not</u> allowed to update, add, or delete tuples from the table.

The privilege class that has the **update** protection capability is allowed to read and update, but not allowed to add or delete tuples from the table.

The privilege class that has the **all** protection capability, is allowed to read, update, add, or delete tuples from the table.

All completed or aborted attempts to access a table is recorded in the form of log reports for examination later.

The log reports are generated on a per table basis when attempting to read a tuple and have it displayed, and on a tuple basis when attempting to write the tuple.

The log TABLXXX that is introduced by this feature is a *secret* log. All *secret* type logs are automatically routed to SYSLOG.

Following are the fields and associated datafill:

TABNAME alphanumeric   **TABLE NAME. Entry is equal to the table name.**

READPROT 0 - 30   READ PROTECT. Enter the privilege class that is allowed to read this table.

UPDTPROT 0 - 30   UPDATE PROTECTION. Enter the privilege class that is allowed to read the table and update tuples. Not allowed to add or delete tuples from the table.

ALLPROT	0 - 30	ALL PROTECTION. Enter the privilege class that is allowed to read, update, add or delete tuples from the table.
VALACC	OFF, ALL, or WRITE	VALID ACCESS. If the switching unit has the security Enhancements Feature, and TABL101 logs are required, enter WRITE, if TABL100 and 101 logs are required, enter all, otherwise if the feature is not provided, or logs TABL100 and 101 are not required, enter OFF.
DENACC	OFF, ALL, or WRITE	DENIED ACCESS. If the switching unit has the security Enhancements Feature, and TABL103 logs are required, enter WRITE, if TABL102 and 103 logs are required, enter all, otherwise if the feature is not provided, or logs TABL102 and 103 are not required, enter OFF.

Table AUDALARM

This table is used to specify the alarm level for SECURITY log reports, which are *secret*. These reports are secure, that is, seeing them and manipulating them is restricted. The operating company can specify alarm levels to flag these reports.

Alarms can be specified in the following two ways:

- For report of the valid or invalid use of commands, the operating company can specify whether a report and alarm are to be generated for each command separately. This is specified in table CMDS.

- For other reports, the operating company can optionally specify an alarm level for each report separately. This is specified in table AUDALARM.

Secret alarms are not printed by log devices. To aid the operating company in determining the cause of alarms, any time a *secret* report causes an alarm, a nonsecret log is generated by the alarm system. This nonsecret log only reports that an alarmed secret report has occurred.

Tuples can not be added or deleted from the table with LOGUTIL. Tuples are added automatically by the log system at restart time, and each log report has the alarm level set to **no alarm** by the default. The only valid user operation on this table is to change the alarm level on an existing tuple.

Following are the fields and associated datafill.

LOGREP	alphanumeric (16 char)	LOGREP. This is the key field in the form `logname$report number'. Only lognames and report numbers of *secret* logs are keys to their table.
ALARM	NA, MN, MJ, or CR	ALARM LEVEL. This sets the alarm to raise whenever the report is logged.

Table DIALBACK

The Automatic Dial Back table enhances the security of dialup ports (Requires feature package NTX293AA).

The special DIALBACK login sequence is performed only if the correct hardware and firmware are available, and the DIALBACK flag associated with the modem is set.

The LOGINCONTROL command permits the operating company to turn DIAL-BACK on or off for a specific port as well as change three dial-out related values:

- Number of rings per dial back attempt
- Number of dial back attempts
- Type of dial line.

Command DIALBACKPW allows the operating company to change DIALBACK passwords. This should be a privileged command to prevent security violations.

Table LGINCTRL

The Login Control (LGINCTRL) table is provided to enable the login control data to be dumped and restored during the software application process. This enables data to be preserved between software loads. This table is an extension to table TERMDEV that controls the addition or deletion of tuples for table LGINCTRL.

The operating companies can change the tuples if they so desire, but it is **highly recommended** that they use the CI command LOGINCONTROL.

Associated Commands

Following are the commands associated with the "Enhanced Office Security" software packages:

PASSWORD

>**PASSWORD [username] newpw**

Changes a user's own password. Only the ADMIN user can change another user's password. (see Note 1)

Where:

username   is an 8-character (max.) name, defined by the operating company. Use SHOW USERS command to display a list of current usernames. Required only when ADMIN user is changing another user's password.

newpw   is the new password that is to replace the current password associated with the username. Password characteristics are controlled by the following parameters (default values) in table OFCENG:

*MIN_PASSWORD_LENGTH	6 characters
*PASSWORD_LIFETIME	30 days
*EXPIRED_PASSWORD_GRACE	3 LOGONS (See Notes 2 and 3.)

Responses:

PASSWORD: ENTER NEW LOGON PASSWORD

Explanation: Normal system prompting before newpw is entered.

PASSWORD: ENTER YOUR CURRENT PASSWORD TO VERIFY

Explanation: Normal system prompting after valid newpw has been entered.

PASSWORD FOR YYYYYYYY HAS BEEN CHANGED. IT MUST BE CHANGED AGAIN WITHIN 30 DAYS **(default value)**.

Explanation: Normal response when the new password has replaced the old password.

PASSWORD: SORRY THAT PASSWORD SHOULD BE AT LEAST 6 CHARACTERS LONG **(default value).**

Explanation: A new password has been entered that does not conform to the office parameter MIN_PASSWORD_LENGTH. Select a proper password and reenter it.

*****Warning*****

YOUR LOGON PASSWORD HAS NOT BEEN CHANGED IN 30 **(default value)** DAYS. YOU HAVE 3 **(default value)** MORE LOGON SESSIONS TO CHANGE YOUR PASSWORD AFTER WHICH YOU WILL *NOT* BE ABLE TO LOGON

Explanation: Reminder to a user at LOGIN time that office parameter PASSWORD LIFETIME has been exceeded, and that EXPIRED_PASSWORD_GRACE parameter is in effect.

Notes:

1. PASSWORD is only present and active when the enhanced security software package is provisioned, and the ENHANCED_PASSWORD_CONTROL parameter in table OFCENG is set to TRUE.

2. PASSWORD should first be entered alone. The system then prompts the user to enter NEWPW.

3. PASSWORD must be used periodically to change passwords. Users are automatically reminded to change their passwords when PASSWORD_LIFETIME has expired. The new password must be different from the old password.

PERMIT

>PERMIT

[user name] [parmlist]

Assigns command classes, previously defined by PRIVCLAS, to specified users. It also alters previous assignments to a user, or defines new users.

Where:

username	An 8 character (max) name for a user class that is defined by the operating company. Use SHOW USERS command to display a list of current usernames.
password	The DMS user password that is to be associated with the username. Required when a user initially logs on. Passwords are defined by the operating company. The number of characters permissible in a password is governed by the parameter MIN_PASSWORD_LENGTH in table OFCENG, if ENHANCED_PASSWORD_CONTROL is true.
parmlist	Consist of additional parameters that are entered using the following syntax: [priority][stksize][lang][cmd_clas]

Where:

priority	Value 1 to 4 (default =4). Sets the priority level of the user's process.
stksize	Sets the number of words of memory that are assigned to the specified user's processes at log on. The range available is 1500 to 10,000 (default = 4000).
lang	Values: FRENCH, GERMAN. Selects the language of input commands and system outputs. If human-machine interface is required in a language other than default value (ENGLISH),

then

set in the DEFAULTLANGUAGE field of table OFCENG. Bilingual human-machine interface software must be provided.

cmd_clas Command class number(s) value 0 to 30, NONE, or ALL (default = NONE. Terminal designation associated with each of 31 class numbers are entered in the COMCLASS field of table TERMDEV, and are assigned by the operating company.

PRIVCLAS

>PRIVCLAS ALL

 [cmd_name][mod_name]   [cmd clas][cmd_lst]

Adds, changes, or deletes the privilege class for specified command(s) or program module(s). Lists all current privilege commands and their classes. Sets DUMPSAFE state for specified command(s) or module(s).

Where:

ALL provides a display listing all command and module names, with their assigned command class(es) and DUMPSAFE states. Unrestricted commands are not listed. **Default value if PRIVCLAS only is entered.**

cmd_name is the name of any valid DMS-100 Family command. Specifies command name to be assigned privilege class(es) and DUMPSAFE state.

modname is the name of the program module that is to be assigned a privilege class, or the name of the module in which the specified cmd_name resides. Also referred to as "increment" (INCR).

cmd_clas specifies the class number to be assigned to a cmd_name or mod_name. Also used to set DUMPSAFE state. Used with systems having regular command screening.

Values:

0 to 30: terminal designations associated with each of the 31 class numbers are entered in COMCLASS field of table TERMDEV and are assigned by the operating company

NONE: deletes any privilege class already assigned, so that any user can execute the specified cmd_name.

DUMPSAFE: sets the specified cmd_name, or commands associated with a specified mod_name, to DUMPSAFE.

DUMPUNSAFE: sets the specified cmd␣name or mod name to DUMPUNSAFE (cannot be executed during office image production).

cmcl_lstis   Used only when the enhanced command screening feature is turned on. Specifies a list of command classes to be assigned to a cmd_name or mod␣name. Also sets DUMPSAFE state for the specified command classes.

Syntax

DUMPSAFE ALL_clas ... DUMPUNSAFE_ L

ALL: used instead of cmd clas... (0 to 30) clears all previously assigned command classes.

LOGINCONTROL

>LOGINCONTROL Control LOGIN access to consoles.

Parms: <Console name>

(ALL, <Action> (QUERY) <Full/Brief> (FULL, BRIEF),

    ENABLE,
    DISABLE <Time> (FOREVER, MINS< Minutes> (1 TO 32767)),

    AUTODISABLETIME <Time> (FOREVER, MINS <Minutes>
                  (1 TO 32767)),
    MAXLOGINTIME <Time> (FOREVER, SECS <Seconds>
                  (1 TO 32767)),
    MAXIDLETIME <Time> (FOREVER, MINS <Minutes>
                  (2 TO 546)),
    LOGINRETRIES <Num Retries> (1 TO 32767),
    OPENCONDITIONFORCEOUT <True/False> (TRUE,FALSE),
    DISABLEON <Add/Set/Remove>   (ADD,
                                    SET,
                                    REMOVE)
    DISABLEON <Set>   (LOGINFAIL,
                                    LOGINTIMEOUT,
                                    IDLETTMEOUT,
                                    LOGOUT,
                                    OPENCOND,
                                    DIALBACKLOGINFAIL,
                                    DIALBACKCALLFAIL,
    DIALBACK <State> (OFF, ANSWER, DIAL),
    DIALOUT <Max Calls> (1 TO 7)
    [<Dialtype> (AUTO, PULSE, TONE)]

Command descriptions

>QUERY

Displays the current settings and current state of a console (port). The **BRIEF** option causes only the current enable state and the current user to be displayed. The **FULL** option displays the state of all options that can be set by the other parameters.

>ENABLE

Allows login attempts on a port to be accepted by the system.

>DISABLE

Causes the system to refuse any login attempt.

The optional subparameter, **DISABLETIME**, specifies how long the port is unavailable for logins. Default is **FOREVER.**

NOTE: Currently logged in ports cannot be disabled. If the LOGINCONTROL command is used to set ALL ports disabled, only those ports that are not currently logged in are disabled.

>AUTODISABLETIME

Determines how long a port is disabled if it is disabled automatically by the system. **Default is FOREVER.**

>MAXLOGINTIME

Determines the maximum time a user my take to login on a specific port. If the timeout is exceeded, the login sequence is canceled and the port is optionally disabled (see DISABLEON parameter). **Default is 60 seconds.**

>MAXIDLETIME

Determines the maximum time a user may leave a port unattended. If timeout is exceeded, the user is forced out and the port is optionally disabled (see DISABLEON parameter). **Default is FOREVER.**

>LOGINRETRIES

Determines the number of times a user has to login correctly before the login sequence is canceled. If the login sequence is canceled, the port may also be optionally disabled (see DISABLEON parameter). **Default is 4.**

>OPENCONDITIONFORCEOUT

Indicates that the user at the reported terminal should be logged out when a line open condition is detected. The port may optionally be disabled.

>**DISABLEON**

Determines the events that cause a port to be automatically disabled. The DIS-ABLEON parameter takes two subparameters. The first subparameter is either ADD, SET, or REMOVE that specifies what to do with the second subparameter, which is any number of entries from the following list:

LOGINFAIL — The port is to be disabled if the user cannot supply a valid userid and password in MAXLOGINRETRIES attempts.

LOGONTIMEOUT — The port is to be disabled when the login sequence of a user is canceled when the user takes more than **MAXLOGINTIME** to login.

IDLETIMEOUT — Specifies that the port is to be disabled when an idle user is forced out on that port.

LOGOUT — Specifies that the port is to be disabled upon the user logout.

OPENCOND — Specifies that the port is to be disabled if the user is logged out due to the detection of a line open condition.

DIALBACKLOGINFAIL — Specifies that the port is to be disabled upon a dial back login failure.

DIALBACKCALLFAIL — Specifies that the port is to be disabled upon a failed dial back call.

>**DIALBACK**

Disables DIALBACK for specified port or enables the port as a dial-out or answer modem.

>**DIALOUT**

Sets the maximum number of rings the modem is to wait for an answer before aborting the call, the maximum number of dial back calls that the modem will attempt, and the line type associated with the modem (dial pulse or tone).

NOTE: The number of characters in the commands and parameters for LOGINCONTROL have been deliberately exaggerated for security reasons.

Examples

To enable a port:

>LOGINCONTROL DIALUP1 ENABLE

To enable all ports:

>LOGINCONTROL ALL ENABLE

To disable a port temporarily:

>LOGINCONTROL DIALUP1 DISABLE MINS 10

To set a port to force out a user if the user has been idle for ten minutes:

>LOGINCONTROL DIALUP1 MAXIDLETIME MINS 10

To set the port to disable if the user does not login in two attempts:

>LOGINCONTROL DIALUP1 LOGINRETRIES 2

>LOGINCONTROL DIALUP1 DISABLEON LOGINFAIL

To turn off disable on IDLETIMEOUT for all terminals:

>LOGINCONTROL ALL DISABLEON REMOVE IDLETIMEOUT

To set the disable options of a port to a specific list:

>LOGINCONTRL DIALUP1 DISABLEON SET LOGINFAIL
 IDLETIMEOUT LOGOUT

To turn off all disable options for a port:

>LOGINCONTROL DIALUP1 DISABLEON REMOVE LOGINFAIL
 IDLETIMEOUT LOGOUT LOGINTIMEOUT

To display current settings:

>LOGINCONTROL ALL QUERY

To forceout a terminal when a line open condition is detected:

>LOGINCONTOL DUALUP1 OPENCONDITIONFORCEOUT

To set the terminal to disable if a line open condition exists:

>LOGINCONTROL DIALUP1 OPENCONDITIONFORCEOUT
DISABLEON ADD OPENCOND

To turn off all disable options for a terminal:

>LOGINCONTROL DIALUP1 DISABLEON REMOVE LOGINFAIL
 IDLETIMEOUT LOGOUT LOGINTIMEOUT OPENCOND

Login banner

Login banner is a feature—NTXS07AA—that displays a banner immediately follow-ing a successful login. The banner will appear after a successful login—on the initial login, not a remote login—and will survive all restarts. The customer can define the banner by using the SETBANNER command to replace the current login banner with a user-defined banner file. The user banner file may be no longer than 22 lines, 80 characters per line. A file that exceeds this limit will be truncated before being cop-ied. The user banner file must not be blank or have its first 22 lines blank. A blank file

will not be copied. The device where the user banner file is stored, and the name of that file must be provided. The device on which the user file is located must be listed so that SETBANNER can locate that file.

It is suggested that the customer PRIVCLAS the SETBANNER command using the CMDS table. Until the customer replaces the default login banner text, it will read:

"This is a private database. All activity is subject to monitoring. Any UNAUTHORIZED access or use is PROHIBITED, and may result in PROSECUTION."

Log SOS600

Log SOS600 is a new log that informs the customer that a hung login process has been killed. It captures status information of the login process and provides ideas of why the login process hung.

Associated logs

The following SECUXXX and TABLXXX logs are associated with the enhanced office security software packages:

SECU101

The Security (SECU) subsystem generates this report when a valid user logs on or off a terminal using normal login or logoff procedures.

SECU102

Generated when a user attempts to login on a terminal using an invalid identification or password.

SECU103

Generated when one user forces another user off the terminal they are logged in on.

SECU104

Generated when a user changed the commandset class for a privileged command or the automatic logging of command use or abuse in table CMDS.

SECU105

Generated when one user changes the password for another user.

SECU106

Generated when a user with the proper command class set issues a command datafilled in table CMDS, and the command is executed.

SECU108

Generated when a user without the proper command class set attempts to access a table, and the table is not accessed.

SECU109

Generated when a valid user logs on a terminal using Priority Login (PLOGIN) procedures.

SECU110

The security (SECU) subsystem generates this report when a user attempts a Priority Login (PLOGIN) on a terminal using an invalid identification or password.

SECU111

The security (SECU) subsystem generates this report when a user changes the command class set for a terminal defined in customer data table TERMDEV.

SECU112

Generated when one user adds or changes the security profile for another user.

SECU113

Generated when an attempt is made to login on a terminal that is not enabled.

SECU114

Generated when a console is manually enabled or disabled.

SECU115

Generated when the maximum login time specified by the LOGINCONTROL command is exceeded, and the terminal is disabled.

SECU116

The Security (SECU) subsystem generates this report when the maximum number of invalid login attempts specified by the LOGINCONTROL command is exceeded, and the console is disabled.

SECU117

Generated when a terminal is automatically enabled by the system as specified by the LOGINCONTROL command.

SECU118

Generated when a user is idle too long or a line open condition is detected. The user is automatically logged off the terminal, and the terminal is disconnected, depending on the terminal's security profile defined in table TERMDEV and by LOGINCON-TROL.

SECU119

The Security (SECU) generates this report when a terminal is disabled by the system after the user has logged out, or the terminal has been busied out.

SECU120

Generated when a user attempts to login on a dialup terminal using an invalid identification or password.

SECU121

Generated when a valid user logs on a dialup terminal using normal login procedures.

SECU122

Generated when an attempt to logon on a dialup terminal fails.

SECU123

Generated when an attempt to login on a dialup terminal succeeds, the dialback call is successful, and the login is completed.

SECU124

Generated when a user changes the dialback password for a user.

SECU125

Generated when dialback is enabled for a dialup terminal.

SECU126

Generated when dialback is disabled for a dialup terminal.

SECU127

Generated when a START, STOP, REMOVE, or OVERRIDE command is used in the Automatic Line Testing (ALT) MAP levels. This log is also generated when changes are made to the start field.

SECU128

Generated when the system of ADMIN user activates of deactivates the AUTOLOG feature.

SECU129

Generated when the AUTOLOG CLASS command is issued by the ADMIN user.

TABL100

The table subsystem generates this report to indicate that an authorized user has accessed the customer data table in read mode, and displayed a tuple. It is generated once per table entry.

TABL101

Generated to indicate that an authorized user has accessed the specified customer data table in write mode. This report is generated once per tuple update.

TABL102

Generated to indicate that an unauthorized user has attempted to access the specified customer data table. This report is generated once per table entry attempt only.

TABL103

Generated to indicate that an unauthorized user has accessed the customer data table in write mode. This report is generated once per tuple update.

For details on the SECUXXX and TABLXXX logs, including examples and action to take, see NTP 297-YYYY-840, *Log Reports Reference Manual.*

Arrangement of user classes

Switch *users* should be organized into classes that define a specific set of functions they are required to perform. These functional needs in turn dictate the command requirements for each user class. The assignment of user commands and table access is made flexible to meet telephone company operational requirements. The rule is: the division of tasks shall provide the purpose for each users' class.

The following are the names and descriptions for some typical users' classes:

Administration (ADMIN)

Provides the user with unlimited access from any device to all command classes (see PRIVCLAS). ADMIN is assigned the highest priority level. The password associated with ADMIN cannot be displayed, and cannot be changed by any other user.

See NTP 297-1001-129, *DMS-100F Input/Output System Reference Manual.*

Switch Maintenance (SMTCE)

Enables the user to maintain the DMS switch by performing regular maintenance and fault correction for the following:

- Central Control/Computer Module (CC/CM)
- Central Message Controller/Message Switch (CMC/MS)
- Input/Output Device (IOD)
- Network Module (NM)
- Peripheral Module (PM)

The SMTCE user also performs all data base changes to administer the switch. SMTCE monitors the switch status, runs diagnostic programs, and replaces equipment. This class has commands associated with table editor and the Support Operating System (SOS). SMTCE class also includes control center positions for analyzers and office control responsibilities.

Trunk Maintenance (TMTCE)

Enables the user to perform regular maintenance and fault correction for trunk circuits, trunk facilities, and trunk translations (maintenance and input). The user monitors the trunk status, runs diagnostic programs, and performs hardware tests.

The TMTCE use is limited to the input commands available only to the user's class. TMTCE has only those commands associated with testing and maintaining trunks and trunk facilities. The user has access to the table editor commands, but is restricted in the changing of specific tables as required by the position profile. The TMTCE functions are performed from a Trunk Test Position (TTP). This class of user also includes the control center position for trunk analysis control responsibilities.

Network Management (NM)

Enables the user to make optimum use of available facilities and equipment by exercising routing control over traffic oriented switch resources. The user monitors traffic levels, applies manual controls, adjusts automatic controls, and receives Operational Measurement (OM) traffic reports (OMPR/OMRS).

NM has interactive capabilities to execute only those input commands assigned to its class. The user is allowed data table query capabilities, but is restricted to changes for specific data tables.

Dial Administration (DADMIN)

This class enables the user to monitor OM traffic reports. DADMIN can alter OM scheduling, assignments, and thresholds.

The DADMIN user has access to the table editor repertoire of commands when altering data associated with OMs. Full data table query capabilities are also afforded the user (in particular, traffic register assignment and readings).

Service Analysis (SA)

Enables the user to monitor, on a random basis, customer dialed and operation assisted toll calls to obtain information on the quality of service provided by the equipment and personnel.

The SA user has access to the table editor repertoire of commands, but is screened on a table basis to change only those data tables associated with this class. The SA user has access to the SAselect area of the MAPCI commands.

Technical Assistance Center (TAC)

The TAC, or equivalent technical support group (i.e., ESAC), enables the user to monitor unattended switching units and provide technical assistance to switching center personnel as required. The TAC is a centralized maintenance group of highly trained and experienced personnel.

This user class has interactive capabilities to execute all input commands that are applicable to switch maintenance.

Emergency Technical Assistance Service (ETAS)

Nortel Network's ETAS provides assistance to customers TAC groups when they are having difficulty correcting switching problems.

This user class is restricted to those input commands required for system interrogation, data dumps, etc. No machine operating parameters—including tables OFCOPT, OFCENG, OFCVAR, OFCSTD, CUSTPROT, TERMDEV, CMDS, AUDALARM, and equipment inventory tables—should be allowed to be altered from this position.

Line Maintenance (LMTCE)

Enables the user to monitor the status of line cards, run diagnostics on line cards, sectionalize troubles, test and diagnose troubles with the office, query and change subscriber data, and schedule automatic line card diagnostics.

Repair Service Bureau (RSB)

Enables the user to sectionalize troubles, test and diagnose facility troubles, schedule Automatic Line Insulation Testing (ALIT), receive ALIT outputs, and query or change subscriber data.

Traffic Administration (TA)

Enables the user to receive automatic periodic summary reports of traffic statistics accumulated by the switching system. These reports reflect traffic peg counts, overflows, usage of the switching units, and OMs. The TA user can modify the schedule and output of these reports.

Minimum security implementation

There are four key areas in implementing minimum security: (1) passwords, (2) ports, (3) tables, and (4) commands.

Listed below is a step by step example for implementing minimum security in the DMS-100F. The scheme is to reserve classes 1 thru 13 for commands and 15 thru 29 for tables. Classes 14 and 30 are reserved for the Administrator (ADMIN). Class assignment is flexible and any command or table can be assigned any or all of the 31 allowable classes.

Commands are automatically written into table CMDS, upon their first use, with a class of 0. Therefore, command class 0 should not be assigned to a user after all user classes have been designated.

Steps 1 & 2 show the office parameters associated with *enhanced security.*

1. Check the following parameters in table OFCOPT for correct settings as listed:

Table OFCOPT:

ENHANCED_COMMAND_SCREENING= Y
ENHANCED_PASSWORD_CONTROL= Y
SUPPRESS_USERNAME   = Y
MONITOR_TABLE_ACCESS   = Y

2. Check the following parameter in table OFCVAR for the correct setting as listed:

Table OFCVAR:

TABLE_ACCESS_CONTROL   = Y

Step 3 shows the recommended settings for password security.

3. The following tuples in table OFCENG set the parameters associated with user passwords, provided are the recommended minimum and maximum values (These parameters appear only if the table OFCOPT parameter ENHANCED_PASSWORD_CONTROL is set to "Y"):

PARAMETER	MINIMUM	MAXIMUM
PASSWORD_LIFETIME	30	90
MIN_PASSWORD_LENGTH	4	8
EXPIRED_PASSWORD_GRACE	1	4

Steps 4 & 5 shows the use of the command LOGINCONTROL and how to secure port access.

4. Review the existing *login control* parameters set for all ports. Input the following command to print out these parameters:

>LOGINCONTROL ALL QUERY FULL

5. Set *login control* parameters for all ports. For more information on the LOGIN-CONTROL command, see NTP 297-1001-822, *Commands Reference Manual*. Also, see NTP 297-1001-129, *DMS-100F Input/Output Reference Manual.* The following are the suggested *login control* parameters:

>LOGINCONTROL ALL DISABLE (disables all idle ports)
>LOGINCONTROL ALL AUTODISABLETIME FOREVER
>LOGINCONTROL ALL MAXLOGINTIME SECS 60
>LOGINCONTROL ALL MAXIDLETIME MINS 15
>LOGINCONTROL ALL LOGINRETRIES 3
>LOGINCONTROL ALL DISABLEON SET LOGINFAIL
>LOGINTIMEOUT IDLETIMEOUT

NOTE: A secret log SECUXXX is generated

Steps 6 thru 13 show an example of restricting ports and users to table access.

6. Print a hard copy of tables CUSTPROT and TERMDEV and the SHOW USERS command. These will be needed for reference with the remaining implementation examples.

7. Logout and login as the ADMIN user.

NOTE: Be aware that a lockout condition exists if all the commands are "Priv_class" out for all users and terminals. The only way out is to use the userid called ADMIN. An ADMIN userid is neither displayed nor restricted in any way. It is always available, provided the ADMIN password is known and the terminal is not in the autologin mode.

---

8. Review table TERMDEV for devices that should be restricted access to tables.

9. Change field COMCLASS from ALL to 0 1 2 3 4 5 6 7 8 9 10 11 12 13 15.

10. Review SHOW USERS printout for users to be restricted from tables.

11. Using the command PERMIT, change the command class of the users to be restricted from ALL to 0 1 2 3 4 5 6 7 8 9 10 11 12 13 15.

12. Enter table CUSTPROT and change the entries for the following tables and fields. (Default values for this table are 15, 15, 15, OFF, OFF).

TABLE	UPDTPROT	ALLPROT	VALACC	DENACC
OFCENG	28	29	WRITE	WRITE
OFCSTD	28	29	WRITE	WRITE
OFCOPT	28	29	WRITE	WRITE
OFCVAR	28	29	WRITE	WRITE
CUSTPROT	30	30	WRITE	WRITE
CMDS	30	30	WRITE	WRITE
AUDALARM	30	30	WRITE	WRITE
TERMDEV	30	30	WRITE	WRITE
DIALBACK	30	30	WRITE	WRITE
LGINCTRL	30	30	WRITE	WRITE

13. Assign class 28 to users that are allowed to update the above tables and assign class 29 to those users allowed complete access to the above tables.

NOTES:

1. Assigning WRITE to field VALACC and DENACC provides a secret log TABLXXX. When an authorized user writes to the above tables a TABL101 log is generated. A TABL103 log is generated when an unauthorized user attempts to write to the above tables.

2. Class 30 is reserved for ADMIN.

Steps 14 thru 16 show the restriction of specific command to specific users.

---

14. Access table CMDS and perform the following changes to fields LOGONUSE, USEALARM, LOGABUSE, and ALRMABUS:

COMMAND	**LOGONUSE**	**USEALARM**	**LOGABUSE**	**ALRMABUS**	**CLASS**
ENGWRITE	Y	NA	Y	NA	13
JFFREEZE	Y	MJ	Y	CR	14
LOGINCONTROL	Y	NA	Y	NA	13
MODEDIT	Y	MJ	Y	MJ	13
PRIORITY	Y	NA	Y	NA	13
PROIRITY	Y	NA	Y	NA	13
PRIVCLAS	Y	NA	Y	NA	14
PRIVERAS	Y	NA	Y	NA	14
RESTART	Y	CR	Y	CR	13
RESTARTBASE	Y	CR	Y	CR	13
RWOK	Y	NA	Y	MN	13
SHOWDBPW	Y	NA	Y	NA	14
SHOWPW	Y	NA	Y	NA	14
SLEEP	Y	MJ	Y	MJ	13
SLEEPTIL	Y	NA	Y	NA	13
PERMIT	Y	NA	Y	NA	14
UNPERMIT	Y	NA	Y	NA	14
LOGUTIL:					
OPENSECRET	Y	NA	Y	NA	14

15. Using the command PRIVCLAS, assign the above commands to their respective class.

```
>PRIVCLAS ENGWRITE $ 13
>PRIVCLAS OPENSECRET LOGUTIL 14
```

16. Assign command class 13 to those users allowed the above commands.

```
>PERMIT [USERNAME] [PASSWORD] 1 4000 ENGLISH 0 1 2 3
4 5 6 7 8 9 10 11 12 13 15
```

NOTES:

1. The fields LOGONUSE and LOGABUSE set to "Y" causes the following two logs to be generated: TABL106 for valid command use, and TABL107 for invalid command use.

2. Class 14 is reserved for ADMIN.

Step 17 shows the assignment of an EXT alarm and log to specific secret logs that are not alarmed in tables CMDS and CUSTPROT.

17.Enter table AUDALARM and change the following records:

LOGREP	ALARM	REASON
SECU$103	MN	one user forces another out
SECU$107	MJ	command abuse
SECU$111	MN	changes to port class in table TERMDEV
SECU$124	MJ	DIALBKPW changed for a user

NOTES:

1. The alarm generated by a secret log or commands use or abuse turn themselves off after approximately 15 seconds.

2. An EXT108 log is printed for critical alarms, an EXT107 log is printed for major alarms, and an EXT106 log is printed for minor alarms. EXTXXX log reports are not generated for "NA" (No Alarm).

Security recommendations

It is extremely difficult to provide specific security recommendations without knowledge of a company's requirements. Below are general recommendations that provide basic security for the DMS-100F switches. It is recommended that security measures be implemented to safeguard switch integrity.

1. PRIVCLASS all devices and user passwords according to the needs of the device and user.

2. Establish password aging.

3. Change the password for user ADMIN and it should be known only by the office and/or control center supervisor.

4. All dialup modems should be set to DISABLE upon logout.

5. Institute a manual log form of all requests for dialup access. A sample log form can be found in this section following the "Office Evaluation" subsection. When a request for dialup access is received, the requester should be called back to verify the validity of the their phone number.

6. PRIVCLASS all sensitive data tables such as:

    CUSTPROT
    OFCENG
    OFCVAR
    OFCOPT
    OFCSTD
    TERMDEV
    CMDS
    AUDALARM

7. Restrict access command use by user need. The following commands should only be available to the switch administrator (ADMIN):

> SHOWDBPW
> SHOWPW
> PERMIT
> UNPERMIT
> PRIVCLAS
> PRIVERASE

8. All I/O devices (MAPS, TTPs, LTPs, etc.) should be logged out during extended periods when not in use and unattended.

9. User passwords should be changed every three months or more often.

10. Local procedures should be followed for disposing of printout paper, documentation, and CD-ROMs. This may require recycling or shredding to meet local and Technical Information Agreement (TIA) security requirements.

Nortel Networks security service

To assist operating companies with their switch security, Nortel Networks Global Professional Services Group provides a **Standardized Security Service**. There is a nominal charge for this service.

This service provides a review of the operating company's switch security. If an operating company requests this service, security will be set up based upon information provided by the operating company and recommendations from Nortel Networks. A special program developed by Nortel Networks will be provided to the operating company for implementation on their switches. Nortel Networks lab testing and a VO switch designated by the operating company will provide preliminary program testing before implementation.

For further information on this service or obtaining this special service, see the "Technical Support Services" subsection within this manual or contact Nortel Networks, Global Professional Services, Manager - Technical Services at 1 (919) 465-0434.

Portable Test Equipment and Tools

Portable test equipment

Portable test equipment and tools selection is an area that is generally dependent upon maintenance methods, individual company policies, and local budgets. Local policies for pooling test equipment may be desirable. Most portable test equipment and tools are optional tools needed for performing preventive and corrective maintenance. Some tools are essential to prevent damage during the removal and insertion of equipment, as well as personal safety.

The Trunk Test Position (TTP) contains two identical jack fields connected in parallel, one on each side of the VDU. Each jack field has four appearances, each appearance with two jacks, one for transmitting and one for receiving. Three of the jack appearances are connected to jack-ended trunks by the Main Distribution Frame (MDF). Jack-ended trunks connect circuits under test to portable test equipment, which may be used when tests other than those provided by internal switch equipment are required.

The following lists of portable test equipment and tools are _suggested_ for DMS-100F switch maintenance. Before ordering any test equipment, check for the latest model and other features that may better suit your needs. Also, verify that the testing features needed are available within the DMS switch. Additional portable test equipment may be required to support fiber-optic and span line equipment.

NOMENCLATURE	MANUFACTURER	MODEL#	QTY
Digital Multimeter	Fluke	806A	1
DMM Carrying Case	Fluke		1
Oscilloscope (Dual Channel 100-MHz)	Hewlett-Packard	HP1740A	1
Test Mobile	Hewlett-Packard	HP10007A	1
Voltage Probe	Hewlett-Packard	HP100041A	1
Current Probe	Hewlett-Packard	HP1110A	1
Probe Tip Kit	Hewlett-Packard	HP10035A	1
Probe Tip Extender Kit	Hewlett-Packard	HP10037A	1
Feed through Adapter	Hewlett-Packard	HP10100B	1
Transmission Measuring Set	Hewlett-Packard	HP3551A	1
Signalling Display— DP/MT/DTMF	Northeast Electronics	2763	1
Strip Chart Recorder	Gould	220	1

Card insertion/removal/extender tools

Line card tools

Line card removal and insertion tools are necessary to prevent damage to line cards as well as preventing personal injury due to possible burns from components on the line card. It is recommended that a minimum of two line card insertion and removal tools be ordered for an office. Two additional tools should be ordered for each 10K of equipped lines. The following specialized tools are required for inserting and removing cards in line drawers as follows:

- LCM DRAWERS:

    Line Card Insertion/Withdrawal Tool (3")
    QTH56A (Apparatus Code)
    A0298291 (Common Product Code)

    Line Card Insertion/Withdrawal Tool (6")
    QTH58A (Apparatus Code)
    A0313317 (Common Product Code)

- LM DRAWERS:

    Small grip tool for 3 inch or larger cards is described as follows:

    Card Removal Tool
    QTH57A (Apparatus Code)
    A0298292 (Common Product Code)

    Large grip tool for 4 inch or larger cards is described as follows:
    NT tool ITA9953

Circuit pack extender

One NT5X54AA Circuit Pack Extender is recommended for the DMS-100F switch.

Minibar switch kit

If any DMS-100F office is equipped with the NT2X46AB Minibar Switch and NT2X50 Driver Card currently being used for Metallic Test Access (MTA), then it is recommended that a QKG1B Minibar Switch Kit be ordered. Newer offices are being equipped with a NT3X09BA 8X8 Metallic Access Card as a replacement for NT2X46AB/NT2X50 arrangements. Where the NT3X09BA is equipped, then the minibar switch kit will not be needed. See PLN-8991-104, *DMS-100F Provisioning Guides* for more details on provisioning of the MTA cards.

Common tools

Common tools (i.e., screwdrivers, pliers etc.) are available through Nortel Networks by ordering the NT0X58AA General Office Maintenance Tool Set, or can be purchased locally if desired.

Office Parameters

Some engineering parameters that are set incorrectly can have a serious affect on customer service. Many control the use of maintenance features and tools. Others control the availability of software and hardware resources. Obviously, parameters are very important for maintaining good switch performance and customer service.

The following parameter tables are addressed within this subsection.

OFCENG table

OFCSTD table

OFCOPT table

OFCVAR table

Since the above data tables can seriously affect the operation of the DMS-100F switch, it is recommended that the table data entries be verified periodically. Hard copies of office parameter data tables should be retained and verified for accuracy before the in-service date and after each of the following: software updates, patch insertion, cold restart, warm restart, and changes in office operations.

It is highly recommended that engineering parameters for all offices within an operating company be compared for consistency of timing values and maintenance features. A maintenance or technical support group should have primary responsibility for reviewing existing and new parameters and making changes. The group responsible should include other departments involved with traffic engineering, outside plant, service orders, etc.

The following tables list <u>selected</u> maintenance office parameters that can have an effect on switch maintenance—including parameters that impact the switch's capability to handle log messages. Included are Nortel Networks recommended settings and default data table settings.

> ⚠ **CAUTION:** Since parameters are subject to changes, and in some cases they are canceled, it is recommended that NTP 297-YYYY-855, *Office Parameters (PCL loads and higher)* be referenced before changing any settings.

Table 8-3 — Table OFCENG Parameters

PARAMETER	SUGGESTED VALUE	DEFAULT VALUE	REMARKS
ALLOW_RINGING_ON_TIP_SIDE			Note 1
CABLE_LOCATE_TIMEOUT	180	180	
CABLE_SHORT_TIMEOUT	180	180	
COMMAND_SCREEN	Y	N	Note 2
COPP_RELAY_OPEN_TIME	80	80	
DM_HIT_TIME		40	Note 3
ENHANCED_DEAD_SYSTEM_ALARM	Y	N	
EXPIRED_PASSWORD_GRACE	3	3	Note 2
GLOBAL_CUTOFF_ON_DISCONNECT	Y 80 Y	N 80 N	Note 4
GUARANTEED_TERMINAL_CPU_SHARE	2	2	
IMMEDIATE_RING_ENABLE	Y for US	N	Note 6
LOG_PRIORITIZATION	Y	N	Note 5
LN_LONG_PARTIAL_DIAL_TIME	63	63	Note 7
LN_SHORT_PARTIAL_DIAL_TIME	24	24	
LN_PERM_SIG_TIME	125	125	
MAX_MADN_MEMBERS_PER_LSG	Note 8	4	Note 8
MIN_PASSWORD_LENGTH	6	6	Note 2
PASSWORD_LIFETIME	30	30	Note 2
PRINT_NET102_LOGS	Y	Y	
RECOVERY_INTERVAL_AFTER_RELOAD	10	10	
RECOVERY_INTERVAL_AFTER_WARMCOLD	2	2	
RLCM_ESAENTRY_BADCSIDE	5	5	
RLCM_ESAENTRY_BADLINK	6	6	
RLCM_XPMESAEXIT	6	6	
RSC_ESAENTRY_BADCSIDE	5	5	
RSC_ESAENTRY_BADLINK	0	0	
RSC_XPMESAEXIT	6	6	
SET_TO_UNBALANCE	Y	N	
SILENT_SWITCHMAN_TIMEOUT	100	100	

1. If ALLOW_RINGING_ON_TIP_SIDE is set to yes, it allows for ringing on either the TIP & RING side of the line for multiparty lines using NT6X17 line cards, or for ringing with NT6X19 message waiting cards. If this feature is being used, then consider setting up BICRELAY testing.

2. See the "Office Security" subsection in this tab for a description.

3. When under provisioned, operator positions will more likely be taken out of service for carrier conditions that are not service affecting.

4. Very important for service, see NTP 297-YYYY-855 for a description.

5. Very important to insure alarmed logs are not lost. See "Log System Administration" subsection within this tab for information on this parameter.

6. Very important for service, see NTP 297-YYYY-855 for a description and country suggestions.

7. Must be at least two units higher than LN_SHORT_PARTIAL_DIAL_TIME parameter.

8. For IBN and RES switching units in the United States, the recommended value is 1, and is set to 1 during the process for initial offices.

Table 8-4 — Table OFCSTD Parameters

PARAMETER	SUGGESTED VALUE	DEFAULT VALUE	REMARKS
FREEZE_ON_REINIT	N	N	
MAX_COLDS	1	1	
MAX_LOCKED_TRAPS	10	10	
MAX_SANITY_TIMEOUTS	10	10	
MAX_WARMS	1	10	
MTCBASE_EXTRAMSG	1024	100	
PM180	N	N	Note 1
TRAP_THRESHOLD	1000	1000	
XPM_PARITY_THRESHOLD	*	20	Note 2

1. If needed, the command XPMLOGS can be used to QUERY, ENABLE, or DISABLE the reporting of PM180 log messages for individual XPMs

2. Indicates the values are office dependent. For the XPM_PARITY_THRESHOLD value, it is recommended that a suggested value of one (1) be met for service improvement and high speed data requirements. See the *Preventive Maintenance* tab and the "Network Maintenance" subsection for network maintenance topics before changing any value.

Table 8-5 — Table OFCOPT Parameters

PARAMETER	SUGGESTED VALUE	DEFAULT VALUE	REMARKS
AMREP_ACTIVE	Y	Y	
CCS7_H0H1_RCP	53	53	
CKT_LOC	Y	Y	
DIALBACKPW_ENCRYPTED		N	Note 1
DIS_LKD_CKT	Y	Y	
ENHANCED_COMMAND_SCREENING	Y	N	Note 1
ENHANCED_PASSWORD_CONTROL	Y	N	Note 1
ERL_SPT	Y	N	
KEYSET_SRT	Y	N	
LOOP_BACK	Y	N	
MONITOR_TABLE_ACCESS	Y	N	
NOISE_MEAS	Y	N	
NRTEST	Y	N	
PASSWORD_ENCRYPTED	Y	N	Note 1
SUPPRESS_USERNAME	Y	N	Note 1
XPM_MATE_DIAGNOSTICS_AVAILABLE	Y	N	Note 2

1. See the "Office Security" subsection in this tab for a description.

2. See NTP 297-YYYY-855 for the XPM_MATE_DIAGNOSTICS_AVAILABLE parameter description and hardware requirements for implementing.

Table 8-6 — Table OFCVAR Parameters

PARAMETER	SUGGESTED VALUE	DEFAULT VALUE	REMARKS
BUFFER_THRESHOLDED_REPORTS	Y	Y	
CIRCUIT_TEST_NUMBER_MESSAGES	10	10	
CUTOFF_ON_DISC_TIME	255	255	
CWT_TONE_LENGTH	3	3	
DISKLOGMEMORY	128	128	
E911_PSAP_DISCONNECT_TIME	16	16	
E911_PSAP_OFFHK_ALARM_TIME	0	0	
LCDREX_CONTROL	Y * * * * 2	N 1 0 3 0 2	Note 1
LINE_CARD_MONITOR	Y	N	
LOG_CENTRAL_BUFFER_SIZE	See Note 2	2000	Note 2
LOG_DEVICE_BUFFER_SIZE	See Note 2	2000 (CM)	Note 2
LOG_OFFICE_ID	Note 3	$	Note 3
NETFAB_SCHEDULE_ENABLED	Y	Y	
NETFAB_SCHEDULE_TIME	Note 4	2	Note 4
NODEREX_CONTROL	Y * * * *	Y 1 30 3 30	Notes 1 & 4
PER_CALL_GND_LOOP_TEST	Y	N	
SIG_TEST	Y	N	
SYSLOG_ACCESS	N	Y	
TABLE_ACCESS_CONTROL	Y	N	
THRESHOLD_IS_SAMPLING	Y	Y	
TRKLPBK_TIMEOUT_IN_MINUTES	20	20	
WLC_0VERVOLTAGE_REPORTING	See Note 5	Y	

1. Schedule REX testing as required.

2. This setting can be the cause of lost log messages. See "Log System Administration" subsection within this tab for more information on these parameters.

3. Usually set to office CLLI name.

4. Schedule as not to conflict with other automated schedules.

5. Look for any Warnings or Bulletins before changing.

Store File Administration

Store file device (SFDEV)

The DMS-100F system permits the user to create, edit, file, and execute sets of MAPCI input commands for generating *custom programs*, storing patches, and storing and executing pending orders (POs). The creation and editing of such files can be performed using the store file device (SFDEV)—commonly called *store file*.

The store file system allows a user to input user created routines or to temporarily store files copied from magnetic tape or disk. The selected store file is then executed by maintenance personnel using store file commands. The store file can be erased if desired. Before any command in SFDEV is executed, newly created commands should be checked (using PRINT) for any obvious errors, and to ensure that call processing is not affected. Use the commands LISTSF or LISTSF ALL to view store files.

SFDEV is meant only to be used as a temporary storage medium. Frequently used files should be copied to disk and accessed from the disk volume file. Infrequently used files should be copied to disk or magnetic tape, and when required, copied from disk or tape to the store file. SFDEV should be purged periodically to remove obsolete information. DMS-100F supervisors and technicians must be aware of the contents of SFDEV. A hard copy should be obtained regularly and any redundant, outdated, or suspicious files be investigated. Verify if any store files are set up in AUTOSCHED (described later) and are being utilized.

> **CAUTION:**
> Before SFDEV programs are executed for the first time, obtain a hard copy print. Verify the commands and subsequent action to ensure no detrimental switch activity occurs.

The Pending Order (PO) subsystem provides the means for storing and manipulating orders—such as service orders (SO) and data modification orders (DMO)—previously created by the user. The SFDEV and AUTOSCHED commands are used to manipulate the PO subsystem.

For further information on SFDEV and its commands, including details on the SFDEV commands used with the Pending Order subsystem, see NTP 297-1001-360, *DMS-100F Basic Translations Tools Guide.* Also, see NTP 297-1001-822, *Commands Reference Manual*.

Store file commands

>EDIT	creates a new file or enters an existing file
>READ	CI level command used to run a specified store file
>ERASESF	CI level command that erases a specified store file
>FILE dev_type file_name	refiles the file to a specified device (SF if not specified) with any updated information and exits EDIT
>LISTSF	lists the files in SFDEV that the user created
>LISTSF ALL	lists all the files contained in SFDEV
>LISTSF INFO ALL	list all the files contained in SFDEV
>LISTSF <user>	list files for a specific user
>INPUT n	used to add line(s) to a store file ("Enter" twice ends input)
>DOWN n	moves the pointer down one line or specified # (n) of lines
>UP n	moves the pointer up one line or specified # (n) of lines
>FIND 'string'	moves <u>down</u> the file to line <u>beginning</u> with 'string'
>VERIFY	displays all, or any part of line at terminal after processed
>DELETE	deletes line or number of lines as specified
>CHANGE 'old' 'new'	change characters as defined within parameters
>TOP	takes pointer to the EDIT: line within the store file
>END	takes pointer to the bottom line within the store file
>LINE n	moves the pointer to the specified line number
>TYPE n	displays one line or lines according to specified parameters
>SAVE SFDEV	saves existing store file device without exiting the editor (EDIT mode)
>PRINT	print the specified store file
>QUIT	exits from store file editor (EDIT mode)

AUTOSCHED utility

AUTOSCHED subcommands provide the ability to execute an SOS exec file at a predetermined time. This utility has been replaced with the DMS Schedule (DMSSCHED) tool that is described in the "Supporting Enhancements" subsection of this manual.

THIS PAGE INTENTIONALLY LEFT BLANK

Training

General

This section briefly summarizes various Nortel Networks training courses for maintaining and operating the DMS SuperNode System and other DMS-100 Family switches—including courses for advanced training. Included in this section is a list of curriculum paths, some of which are specific to maintenance and operations. Use the Nortel Networks website, discussed below, to find course details for each curriculum path.

Formal DMS SuperNode System technical training is essential to ensure the availability of qualified technicians for up-to-date maintenance and operation of new and preexisting switch features. Candidates completing Nortel Networks Customer Information and Training Services training should receive every opportunity to practice their new skills on the job to become wholly proficient.

Training Information

Information on Nortel Networks Customer Support and Training Services courses can be accessed in several ways:

- Via the Nortel Networks Customer Support online website.
- Through Nortel Networks Customer Support and Training Services's Fax-on-Demand service, accessed via 1-800-NT-TRAIN, option 3. This service provides course descriptions, scheduling information, order forms, location maps and hotel rates—that are faxed directly to your machine.

Online training/certification information

Online information for Nortel Networks training and certification programs can be found at www.nortelnetworks.com select Customer Support, and Training.

The new Nortel Networks Certification Program allows candidates to choose the certifications that best meet individual and business needs. Six certification programs cover Sales, Network Design, and Technical Support for the broad range of Nortel Networks voice and data products.

Scheduling

To schedule Nortel Networks Customer Training and Documentation Services courses, contact your company's training coordinator. If your company does not have a training coordinator, call 1-800-NT-TRAIN (1-800-688-7246) and select option 1.

Training Options

Training to operate and maintain the DMS-100 Family of switches is offered through four Nortel Networks Technical Training Centers, located in Raleigh, North Carolina; Sacramento, California; Brampton (Toronto), Ontario; and Montreal, Quebec. On-site training is also conducted per customer request. Due to the hands-on exposure required for some courses, not all can be offered on-site. Course scheduling is developed based on customer need and training staff availability.

Nortel Networks Customer Training and Documentation Services use alternative media for many of its training courses: Computer-Based Training (CBT), Remote Access Learning (RAL), self-paced workbooks and video, and combinations of several media types. Alternative media training provides greater flexibility for the customer and allows you to train at your site, at your convenience. Travel expense and time away from work are also greatly reduced when alternative training methods are used.

Customer Account Representatives

Customer Training and Documentation Customer Account Representatives serve as liaisons between our customers and the Customer Information and Training Services Centers. They provide training recommendations and global marketing strategies to match customer needs. To speak to one of our Customer Account Representatives, call 1-800-NT-TRAIN.

Advanced Training

Advanced technical training courses have been developed by Nortel Networks Customer Training and Documentation. They are intended to meet the needs of the personnel directly responsible for Tier II maintenance and advanced technical support for the DMS SuperNode System switches. Individuals such as Electronic Switch Assistance Center (ESAC) personnel, are prime candidates for this advanced training. See the TAS related curriculums next and use Advisor for details.

Curriculum Paths

Curriculum paths will help you determine which courses to take in order to receive the training you need. Curriculum paths can, and do, periodically change. Use www.nortelnetworks.com select Customer Support, Training, Curriculum Path to see the current courses for each curriculum path. The following curriculum paths existed at the time that this document was last updated:

AccessNode
Installation
Maintenance
ACD/NACD
ADAS Plus
Agent Portal
AIN/LNP
B&AS
BWA Technician
CAMS
CCMIS
CCS7/CLASS
CDMA
Administrative Personnel
Cell Site Technician
Delta Path
Design Engineer
Management Personnel
Network Design Technician
Optimization Engineer
Switch Technician
System Database
Commerce Manager
CVX 1800
Data Network Solutions
Directory One
DMS SuperNode
and DMS-500 End User
Hardware Maintenance (ENET and JNET)
Hardware Maintenance (ENET only)
Installation
MDC Translations
Planning and Engineering
Product Hardware Maintenance
Software Support (Course 1900 Specific)
Software Support (Course 1901 Specific)
Software Support (Course 1902 Specific)
Software Support (Course 1903 Specific)
Software Support (Course 1904 Specific)
Software Support (TAS) (2)
Translations
DMS
Technology (Canada & International)

DMS-10
   End User
   Hardware and Software Maintenance
   Installation
   Planning and Engineering
   Translations
DMS-100
   Wireless Hardware Maintenance (AMPS/TDMA)
   Wireless Hardware Maintenance (CDMA)
   Wireless Translations (AMPS/TDMA)
   Wireless Translations (CDMA)
DMS-250
   Hardware Maintenance (ENET and JNET)
   Hardware Maintenance (ENET only)
   Planning and Engineering
   Translations
DMS-300
   Gateway Switch Operations and Translations
DMS-500
   Hardware Maintenance
   MDC Translations
   Planning and Engineering
   Translations (DMS SuperNode functionality)
   Translations (DMS-250 functionality)
GDA
Global Server
Global Services Platform (GSP) Translations
GSM
   BSS Datafill Engineer
   BSS System Acceptance Engineer
   Database Administrator
   Manager Overview
   Network Design Engineer
   OMC-R Controller
   OMC-R Database Administrator
   Radio Site Verfication Engineer
   RF Engineer and Cell Planner
   RF Field Engineer and Technician
   Switch Technician
Intelligent Call Management Planning and Engineering (DMS SuperNode and DMS-500)
ISDN
   Integrated Services Digital Network (ISDN) for DMS

LION
    LION Intercept
    LPS
MDC
Modify Line Data
Modify Subscriber Data
Multimedia Messaging Overview
Networks Training
Navigation Services
OC-12/OC-48 Installation and Commissioning
OC-192 and Advanced Optics
OPTera
    Long Haul
    Metro
Passport
    Carrier
Preside
    CSA
    Preside
Radio
Shasta
SuperNode Data Manager
SuperNode Translations
TDMA
    Administrative Personnel
    Cell Site Technician
    Delta Path
    Management Personnel
    Network Operations
    North American Switch Technician
    Performance Engineer
    System Database
    System Planner
TOPS
TransportNode
    and AccessNode Overview
    Express
    OC-12 and OC-48 OAM&P
    OC-12 and OC-48 OAM&P (cont'd)
Universal Edge
    9000
    IMAS
Versalar 25000

Voice Navigation System
WebDA

Training policies

Online information for Nortel Networks Training Policies can be found at
www.nortelnetworks.com select Customer Support, Training, Training Policies. Policy
topics include:

- Block Booking
- Cancellation
- Class Participation
- Courseware Copyright
- Confirmation
- Course Access
- Inclement Weather
- Merchandise
- Miscellaneous
- Onsites
- Payment
- Prerequisites
- Prework
- Registration
- Resident Buyout Classes
- Sexual Harassment
- Substitution
- Travel Arrangements
- Weapon-Free Policy

NOTE: Check the website for current policy information.

User Index

Synopsis

This user index is provided to help the user of this manual find various topics. Each topic is referenced to the section and page number(s) within this manual. Using the table of contents in the first tab, and the user index in the last tab of this manual, should direct the user to the topic(s).

Become familiar with the topics listed to assist in finding information for future references. Use the referenced section and page number(s) (i.e., 2-25 is section two, page 25) to find the subject matter. The section number, followed by the page number, can be found at the top of each page. The section titles are identified at the top of the page, and on the colored tabs (furnished with the document) as follows:

Table of Contents

Introduction

Preventive Maintenance

Corrective Maintenance

System Products

Performance

Technical Assistance

Maintenance Administration

Office Administration

Training

User Index, References, Acronyms, and Notes

Numerics

88k   3-40

A

Abbreviations and Acronyms   10-27
AIN
    call progression marker   4-335
    commands   4-336
    logs   4-337
    maintenance   4-336
    operation   4-335
    overview   4-332
AINTRACE command   4-337
ALT   1-12
    references   2-137
ALT (Also, see Line Maintenance)   1-12
ALT Indicator   5-56
ATT   1-13
ATT (Also, see Trunk Maintenance)   1-13
ATT Indicator   5-57
Automatic image dump   6-47
    Commands   6-47
    recommendations   6-49
    Tables   6-48

B

Babbling device   4-393
Babbling line   1-13, 2-138
Balance tests   2-136, 3-17
Balance tests (Also, see Line Maintenance)   2-136
Basic Rate Interface (BRI) (See ISDN Access Interfaces)   4-103
BCSMON   1-4, 1-18
BER   2-267
BER Testing Guidelines   2-252
    BER testing criteria   2-255
    BERP testing procedures for lines   2-255
    BERP testing procedures for trunks   2-257
    BERT preparation   2-253
    NETFAB testing procedures   2-258

D

F

H

I

K

L

M

N

O

P

R

T

U

V

W

X

References

This subsection was provided to support documentation references for the MOM. This subsection is being retired in this issue of this document. This is being done because document restructuring has caused this subsection to become obsolete.

Restructuring of NTPs has evolved into the current Product Computing-module Loads (PCLs) documents.

See the *"Office Administration"* tab and the "Nortel Networks Documentation" sub-section within this manual for information on Nortel Networks PCL documentation restructuring. For further details on documentation structuring, see NTP 297-8991-101, *DMS-100 Product Documentation Directory* and NTP 297-8991-002, *DMS-100F Cancellation Cross Reference Directory*.

Abbreviations and Acronyms

Abbreviations are shortened forms of words, terms, phrases, or units of measurement (such as fig. for figure, abbr. for abbreviation, and in. for inch). They are used in place of the whole word either by convention, for convenience, or to save space.

Acronyms are abbreviations derived from the initial letters or from parts of a compound term (such as telco for telephone company and DMS for Digital Multiplex System).

Where appropriate, such as in the "ISDN Maintenance" subsection, an "ISDN list of terms" was added to provide more definition than an abbreviation and acronym list could provide. Whether abbreviations or acronyms are in a list or not, they are usually defined with the first appearance in the text of each subsection of this manual. The exception would be for abbreviations or acronyms that are well known—such as telco, DMS, MAP, CPU, I/O, CLASS, POTS, ISDN, CCS7.

Following is a summary of the abbreviations and acronyms associated with this manual and the DMS-100F switch documentation. Although the list of abbreviations and acronyms is comprehensive, it is not all inclusive since new features with related abbreviations and acronyms are always under development.

A good reference to have at hand for terms, acronyms, and abbreviations is NTP 297-1001-825, *DMS-100F Glossary Of Terms and Abbreviations Reference Manual.* This document is kept up to date with new terms and changes to existing terms, abbreviations, and acronyms.

List of DMS-100F Acronyms

1-9

1FR	Single Party Flat Rate
1MR	Single Party Measured Rate
1W	One-way Trunk
2B1Q	Two Binary One Quaternary
2W	Two-Way Trunk: Two-Wire Circuit
3WC	Three Way Calling
4W	Four-Wire Circuit
800+	800 Plus Service (Telecom Canada Service)

A

A	Ampere
A/C	Attendant Console
A/D	Analog-to-Digital
A/R	Alternate Route
A&M	Additions & Maintenance
AAB	Automatic Answer Back
AABS	Auxiliary Alternate Billing Service; Automated Alternate Billing Service
AAP	Audible Alarm Panel
AB	A & B Signaling Bits on Digital Channels
ABNN	Add Bridged Night Number
ABBT	Automatic Board-to-Board Testing
ABH	Average Busy Hour
ABS	Average Busy Season
ABSBH	Average Busy Season Busy Hour
AC	Alternating Current; Attendant Console
ACB	Automatic Call Back; Account Code Billing

ACCS	Automatic Calling Card Service
ACCV	Automatic Calling Card Validation
ACD	Alarm Control and Display; Automatic Call Distribution
ACG	Automatic Call Gapping
ACH	Attempts per Circuit per Hour
ACM	Address Complete Message
ACMS	Advanced Call Management Server
ACO	Address Complete Message; Alarm Cut Off
Act	Activate
ACT	Advanced Communications Terminals Division
ACTS	Automatic Coin Toll Service
ACU	Acknowledgement Unit; Automatic Callback Unit
ADACC	Automatic Directory Assistance Call Completion
ADAS	Automated Directory Assistance Service
ADC	Analog/Digital Converter
ADDR	Address
ADPCM	Adaptive Differential Pulse Code Modulation
ADS	AudioGram Delivery Service
ADSL	Asymmetric Digital Subscriber Line
ADTS	Automatic Data Test System
AILC	Asynchronous Interface line Card
AIM	Asynchronous Interface Module
AIN	Advanced Intelligent Network
AINT	Adjacent Intermediate Node Translator
AINTCC	Automated Intercept Call Completion
AIOD	Automatic Identification of Outward Dialing
AIS	Alarm Indication Signal Automatic Intercept System
AIX	Advanced Interactive Executive
ALC	Asynchronous Line Card
ALCK	Alarm Checking Access

ALGOL	Algorithmic Language
ALIC	Asynchronous Line Interface Card
ALIT	Automatic Line Insulation Test
ALM	Alarm
ALSC	Alternate Line Screening Code
ALT	Automatic Line Testing
ALU	Arithmetic and Logic Unit
AM	Access Module
AMA	Automatic Message Accounting
AMATPS	AMA Teleprocessing System
AMI	Alternate Mark Inversion; Automatic Modem Insertion
AML	Actual Measured Loss; Addition Main Line
ANA	Automatic Number Annc.
ANI	Automatic Number Identification
ANIF	Automatic Number Identification Failure
ANSI	American National Standards Institute
AOCR	Automatic Out-of-Chain Reroute
AOSS	Auxiliary Operator Services Signaling
AOSSVR	Auxiliary Operator Service System Voice Response
AP	Application Processor
API	Application Programming Interface
APS	Attended Pay Station
APU	Application Processing Unit
AQ	Autoquote
AR	Automatic Recall
ARQ	Automatic Repeat-Request
ARS	Alternate Route Selection; Audio Response System
ARU	Audio Response Unit
ASCII	American Standard Code for Information Interchange
ASP	Application Service Part
ASPA	Automatic Message Accounting Specialized Processing Application
ASQ	Automated Status Query
ASR	Automated Speech Recognition

Assoc	Associated
ASST	Assistant
ASTM	American Society for Testing and Materials
ASU	Acknowledgment Signal Unit; Application Specific Unit
ASYNC	Asynchronize, Asynchronous
AT	Access Tandem
ATB	All Trunks Busy
ATC	Access Tandem Connection; Access To Tandem Carrier
ATD	Atlanta Transmission Division; Audio Tone Detection
ATM	Asynchronous Transfer Mode
ATME	Automatic Transmission Measuring Equipment
ATMS	Automatic Transmission Measurement System
ATP	Access Transport Parameter
ATRS	Automatic Trouble Reporting System
ATT	Automatic Trunk Testing
AUD	Automatic Dial
AUL	Automatic Line
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network
AUX	Auxiliary
AVD	Alternate Voice/Data
AVT	AUTOVON Termination
AWC	Area Wide Centrex
AWG	American Wire Gauge
AWT	Average Work Time

B

B	Bearer; Byte
B/G	Battery/Ground
B8ZS	Bipolar Eight Zero Substitution
B911	Basic 911
BAF	Bellcore Automatic Message Accounting (AMA) Format
BAT	Battery

BBF	Blue Box Fraud		BMS	Buffer Management System
BBG	Basic Business Group		BNC	Billing Number Code
BBHCA	Billing Busy Hour Call Attempts		BNF	Backus Nuar Form
BCD	Binary-Coded Decimal		BNM	Business Network Management
BCI	Backward Call Indicators		BNN	Bridged Night Number
BCP	Bell Canada Practice		BNR	Bell-Northern Research
BCR	Bell Communications Research (Bellcore)		BNS	Billed Number Screening
			BOC	Bell Operating Company
BCS	Batch Change Supplement		BORSCHT	Battery (feed), Overvoltage (protection), Ringing, Supervision Coding (decoding), Hybrid & Testing
BCSMON	BCS Monitoring			
BCU	Battery Charging Unit			
Bd	Baud; (Pronounce as "B sub-d") Bd Channel - A DS0 channel that carries low speed, packet switched data; Bd Link - A DS0 link that carries statistically multiplexed D-channel Packet Data		BOT	Beginning of Tape
			BPI	Bits Per Inch
			BPS or bps	Bits Per Second
			BPV	Bipolar Violation
			BRA	Basic Rate Access (ISDN Service) Replaced with BRI
			BRCS	Business and Residential Communications System
Bellcore	Bell Communications Research; Now Known as Telcordia		BRI	Basic Rate Interface
			BRISC	BNR Reduced Instruction Set Computing
BER	Bit Error Rate			
BERP	Bit Error Rate Performance		BSM	Billing Services Management
BERT	Bit Error Rate Tester		BSN	Backward Sequence Number
BERTL	Bit Error Rate Test Line		BSRF	Bell System Reference Frequency
BERTTIME	Bit Error Rate Testing Time			
BGID	Business Group ID		BSY	Busy
BH	Busy Hour		BSY/RTS	Busy/Return To Service
BHC	Busy Hour Calls		BVL	Busy Verification Line
BHCA	Busy Hour Call Attempts		BX.25	Bell Version of X.25 Machine-to-Machine Protocol
BHCV	Busy Hour Call Volume			
BHH	Busy Half-Hour			
BI	Bus Interface			
BIC	Bus Interface Card			
BISYNC	Binary Synchronous Communications			
bit	Binary Digit			
BITS	Building Integrated Timing Supply			
BIX	Building Interoffice Crossconnect			

C

C-side	Core Side
C	Celsius
CA	Cable Assignment Cable
CAC	Carrier Access Code
CAD/CAM	Computer-Aided Design/Computer-Aided Manufacture

BLK	Block
BLV	Busy Line Verification
BMC	Billing Media Converter
BMMI	Bilingual Man/Machine Interface

CALLTRF	Call Transfer		CCT	Central Control Terminal Circuit
CALRS	Centralized Automatic Loop Reporting System		CCV	Calling Card Validation
CAMA	Centralized Automatic Message Accounting		CCW	Cancel Call Waiting
			CDAR	Customer Dialed Account Recording
CAMS	Centralized Alarm Management System		CDC	Coin Detection Circuit Customer Data Change
CAROT	Centralized Automatic Reporting On Trunks		CDF	Coin, Dial Tone First
			CDIR	Country Direct
CARPAC	Carrier Pretest and Cutover		CDM	Customer Data Modification
CAS	Call Accounting Subsystem		CDN	Called Party Number
CASE	Customer Assistance Service Enhancements		CDO	Community Dial Office
			CDP	Customized Dial Plan
CATV	Community Antenna Television		CDPA	Called Party Address
CBK	Changeback		CDR	Call Detail Recording
CBQ	Call-Back Queuing		CDS	Call Disposition Summary
CBsy	C-Side Busy		CED	Cook Electric Division
CBT	Computer Based Training		CEI	Comparably Efficient Interconnection
CC	Central Controller; Common Control; Country Code		CENTREX	Centralized PBX
			CEPT	European Conference of Postal and Telecommunications Administrations
CC-PP	Central Control-Peripheral Processor			
CCAN	Calling Card Account Number		CF3P	Conference Circuits (3 Ports)
CCB	Call Condense Block		CFA	Configuration Acknowledge
CCC	Central Control Complex; Clear Channel Capability		CFB	Call Forwarding – Busy
			CFD	Call Forwarding – Don't Answer
CCF	Coin, Coin First		CFF	Call Forward – Fixed
CCH	Completions per Circuit per Hour		CFI	Call Forwarding – Intragroup
			CFNA	Call Forwarding – No Answer
CCI	Computer Consoles Incorporated		CFRA	Call Forward – Remote Access
CCIS	Common Channel Inter-office Signaling		CFS	Call Forwarding – Station
			CFT	Call Forwarded - Timed
CCIS6	Common Channel Inter-office Signaling 6		CFU	Call Forwarding – Universal
			CFW	Call Forwarding
CCITT	International Consultative Committee on Telegraphy & Telephony (see ITU-T)		CFWVAL	Call Forwarding Validation
			CGA	Carrier Group Alarm
			CGB	Circuit Group Blocking
CCN	Calling Card Number		CGPA	Calling Party Address
CCS	Common Channel Signaling Hundred Call Seconds		CH	Call Hold
			CHD	Card Issuer Identifier
CCS7	Common Channel Signaling No.7		CHG	Change
			CI	Command Interpreter; Customer Information
CCSA	Common Control Switching Arrangement			

CIC	Carrier Identification Code; Circuit Identification Code		CND	Calling Number Delivery
CICS	Customer Information Control System		CNDB	Calling Number Delivery Blocking
CIP	Critical Indicator Panel; C-Bus Interface Paddle Board; Carrier Identification Parameter		CO	Central Office; Call Originating
			COAM	Centralized Oper., Admin.,& Mtce. for LBR
CIR	Circular Hunting; Committed Information Rate		COD	Cut-Off on Disconnect
CKT	Circuit		CODEC	Coder/Decoder
CLASS	Custom Local Area Signaling Services		COER	Central Office Equipment Report
CLD	Called Number		CONF	Conference
CLEC	Competitive local Exchange Carrier		Cong	Congestion
			COOT	Combined Operator–Office Trunk
CLF	Clear Forwarding		COS	Class of Service; Corporation for Open Systems
CLI	Calling Line Identification			
CLID	Calling Line Identification Display		COSMIC	Common Systems Main Interconnecting
CLIDN	Calling Line Identification Directory Number		COSMOS	Computer System for Mainframe Operations
CLIF	Calling Line Identification through Flash		COT	Central Office Terminal; Continuity Signal; Customer Originated Trace
CLLI	Common Language Location Identifier			
CLNET	Calling Line Number Exclusion Table		COTS	Commercial Off-The-Shelf (as in "We've quoted COTS prices")
CLT	Call Trace		COV	Changeover
CM	Computing Module (SuperNode); Central Memory; Control Module; Central Maintenance		CP	Call Processing; Central Processor; Circuit Pack
			CPA	Congestion Parm Acknowledge
			CPB	Call Processing Busy
CMC	Central Message Controller; Cellular Mobile Carrier		CPC	Calling Party's Category
			CPE	Customer Premises Equipment
CMOS	Complementary Metallic Oxide Semiconductor		CPG	Call Progress
			CPI	Characters Per Inch; Computer-to-PBX Interface; C-Bus Interface Paddleboard
CMR	CLASS Modem Resource			
CMS	Call Management Service		CPID	Call Processing ID
CMX	Concentration Module Extension		CPM	Central Processor and Memory
CN	Calling Number; Charge Number		CPU	Central Processing Unit; Call Pickup
			CR	Carriage Return
CNA	Calling Number Announcement; Customer Name and Address		CRC	Cyclical Redundancy Check
CNC	Customer Network Change		CRT	Cathode Ray Tube (Terminal)

CS	Call Seconds; Call Supervisor
CSA	Canadian Standards Association; Carrier Service Area
CSB	Channel Supervision Bit
CSC	Cell Site Controller
C-SCAN	Customer Service Computer Access Network
CSCC	Coordinated State Change Control
CSDC	Circuit Switched Digital Capability
CSDDS	Circuit Switched Digital Data Service
CSDN	Circuit Switched Digital Network
CSE	Customer Service Expert
CSM	Channel Supervision Message
CSR	Customer Service Report (see SR)
CSS	Customer Support System
CSU	Customer Service Unit
CT	Control Terminal; Call Transfer
CTD	Carrier Toll Denial
CTM	Conference Trunk Module
CTS	Carrier Transit Switch; Clear to Send
CTX	Centrex
CUG	Closed User Group
CUIF	Control Unit Interface
CW	Calls Waiting
CWI	Call Waiting Indication; Call Waiting Intragroup
CWID	Call Waiting Identification Display
CWT	Call Waiting
CX	Composite Signaling
CXR	Carrier
CXR	Call Transfer

D

D	Delivery (Date); Duplicate anchor; Digit
D/A	Digital-to-Analog
D30	30-Channel Digital CC Data Link
DA	Directory Assistance
DACC	Directory Assistance Call Completion
DACS	Digital Access and Cross-Connect System
DAMA	Demand Assignment Multiple Access
DAO	Digits as Outpulsed
DAS	Directory Assistance System
DAT	Digital Audio Tape
DAV	Data Above Voice
DAVLC	Data Above Voice Line Card
DB; dB; db	Decibel
DB	Database
DBIC	Data Enhanced BIC
DBMS	Database Management Systems
DBS	Data Base Services
DC	Data Collection; Direct Current; Document Controller
DCBU	Directed Call Pick-up Non Barge In
DCC	Destination Code Cancel; Digital Cross-Connect
DCE	Data Circuit-Terminating Equipment; Data Communications Equipment; Distributed Computing Environment
DCH	D-Channel Handler
DCLU	Digital Carrier Line Unit

DCM	Diagnostic Control Module; Digital Carrier Module		DISALM	Display Alarm
DCM-B	Digital Carrier Module-Basic		DISC	Disconnect
DCMPAC	Digital Carrier Module Pretesting and Cutover		DISCTRL	Display Control
			DIST	Distribution
DCM-R	Digital Carrier Module-Remote		DITCH	Digital Trunk Controller for CCS7
DCM-S	Digital Carrier Module-Slave		DIU	Digital Interworking Unit
DCP	Data Communications Processor; Design Change Proposal		DLC	Data Line Card; Data Link Controller; Digital Loop Carrier
DCPX	Directed Call Pick-up Exempt		DLH	Distributed Line Hunt
DCR	Dynamic Controlled Routing		DLM	Digital Line Module
DCS	Digital Cross-Connect Systems		DLP	Data Link Processor
DD	Data Dictionary; Direct Dial		DLTU	Digital Line and Trunk Unit
			DM	Digital Modem
DDD	Direct Distance Dialing		DMA	Direct Memory Access
DDL	Data Description Language		DMI	Digital Multiplex Interface
DDO	Direct Dialing Overseas		DMO	Data Modification Order
DDS	Dataphone Digital Service; Digital Data Services		DMODEM	Digital Modem
			DMS	Digital Multiplex System
DDU	Disk Drive Unit		DMSC	DMS Catalog Sheet
DDUOS	Disk Drive Unit Out of Service		DMSE	DMS Evolution
Deact	Deactivated		DMS-X	Internal Signaling Protocol
DES	Digital Echo Suppressor		DMT	Digital Multiplex Terminal
DESA	Dual Emergency Stand Alone		DN	Directory Number
DEST	Destination		DNA	Dynamic Network Architecture
DF	Distribution Frame		DNC	Dynamic Network Control; Dynamic Network Controller
DFI	Direct Fiber Interface			
DFMS	Digital Facility Management System		DND	Do Not Disturb
			DNG	Dynamic Network Gateway
DFS	Dual Function Switch		DNH	Directory Number Hunt
DFT	Distributed Function Terminal		DNIC	Digital Network Interconnecting
DG	Differential Gain		DNS	Dynamic Network Services
DGT	Digitone		DNT	Directory Number Translator
DIALAN	DMS Integrated Local Area Net.		DNX	Digital Network Cross-Connect
DID	Direct Inward Dialing		DOC	Dynamic Overload Control
DILEP	Digital Line Engineering Program		DOD	Direct Outward Dialing
			DOJ	Department of Justice
DIMA	Direct Inward Mobile Access		DOR	Denied Originating
DIN	Denied Incoming		DOV	Data Over Voice
DIP	Dual In-Line Package		DP	Dial Pulse
DIRP	Device Independent Recording Package		DPC	Destination Point Code
			DPN	Digital Packet Network
DISA	Direct Inward System Access		DPO	Dial Pulse Originating

DPO	Dial Pulse Originating
DPP	Distributed Processing Peripheral
DPP	Distributed Processing Peripherals
DPR	Datapath Profile
DPT	Dial Pulse Terminating
DPX	Datapath Loop Extension
DQT	Display Queue Threshold
DR	Distinctive Ringing
DRAM	Digital Recorded Announcement Machine
DRCC	Dual Remote Cluster Controller
DRE	Directional Reservation Equipment
DRTU	Digital Remote Test Unit
DS	Data Schema; Data Set; Data Store; Data Stream; Digital Signal; Downstream
DS0	Digital Signal Level 0, A Channel
DS1	24 Channel Digital Carrier System
DS30A	30 Channel Digital Peripheral Link
DSA	Dial Service Assistance
DSCWID	Call Waiting Display with Disposition
DSI	Data Stream Interface; Digital Speech Interpolation
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Loop Access Multiplexer
DSM	Direct Signal Monitoring
DSN	Data Set Name; Double Shelf Network
DSP	Down Stream Processor
DSS	Digital Switching Systems; Direct Station Selection
DSX	Digital Cross-Connect
DTA	Digital Trunk Array; Digital Test Access
DTC	Digital Trunk Controller

DTC7	Digital Trunk Controller for CCS7
DTCI	Digital Trunk Controller for ISDN
DTE	Data Terminal Equipment
DTF	Dial Tone First
DTH	Digital Test Head
DTL	Diode Transistor Logic
DTMF	Dual-Tone Multifrequency
DTR	Data Terminal Ready
DTSR	Dial Tone Speed Recording
DTT	Digital Trunk Testing
DTU	Data Terminating Unit; Digital Test Unit; Digital Tone Unit
DU	Data Unit
DUAQ	Dial-Up Autoquote
DUV	Data Under Voice
DVM	Digital Voltmeter
DVS	Data Voice System
DWS	Dialable Wideband Service
DX	Duplex
DXMS	Distributed Extended Multi-processor System

E

E	Erlang (36 CCS)
E/W	Equipped With
E&M	E Lead & M Lead Signaling
E1	Emergency Switch Degradation
E800	Enhanced 800 Service
E911	Enhanced 911
EA	Equal Access
EABS	Exchange Alternate Billing Service
EADAS	Engineering and Administrative Data Acquisition System
EADAS/DC	Engineering and Administrative Data Acquisition System/Data Collection
EADAS/NM	Engineering and Administrative Data Acquisition System/Network Management

EBAF	Extended Bellcore AMA Format		EMDR	Expanded Message Detail Recording
EAEO	Equal Access End Office		EMER	Emergency Restart
EAIT	Equal Access Intermediate Tandem		emf	Electromotive Force
EAO	Extended Area Office		EMI	Electromagnetic Interference
EAOS	Exchange Access Operator Service		EML	Expected Measured Loss
EAOSS	Exchange Access Operator Services Signaling		EMPC	Enhanced Multi-Protocol Controller
EAP	Equal Access Plan		ENET	Enhanced Network
EAS	Extended Area Service		ENFIA	Exchange Network Facilities for Interstate Access
EBAF	Expanded Bellcore Automatic Message Accounting Format		ENS	Emergency Number Services
EBCDIC	Extended Binary-Coded Decimal Interchange Code		EO	End Office
EBO	Executive Busy Override		EOC	Embedded Operations Channel
EBS	Electronic Business Set		EOF	End of File
EBX	Executive Busy Override Exempt		EOP	End of Program
ECA	Exchange Carrier Association		EOT	End of Tape; End of Transmission
ECD	Error Control Device		EOV	End of Volume
ECMA	European Computer Manufacturers Association		EPROM	Erasable Programmable Read-Only Memory
ECSA	Exchange Carrier Standards Association		EPSCS	Enhanced Private-Switched Communication Service
ECU	Environmental Control Unit		ERL	Echo Return Loss
EDRAM	Enhanced Digital Recording Announcement Machine		ERLC	Extended Range Line Card
EEPROM	Electronically Erasable Programmable Read-Only Memory		ERWT	Expensive Route Warning Tone
			ES	Echo Suppressor; Error Second
EF&I	Engineer, Furnish & Install		ESA	Emergency Stand-Alone
EFS	Error Free Seconds		ESAC	Electronic Switching Assistance Center
EIA	Electronic Industries Association		ESB	Emergency Service Bureau
EIS	Expanded Inband Signaling		ESC	Echo Suppressor Control
EISP	Enhanced ISDN Signal Processor		ESD	Electrostatic Discharge
EIU	Ethernet Interface Unit		ESF	Extended Super Frame
EKTS	Electronic Key Telephone Service		ESL	Essential Service Line
ELN	Essential Line		ESMA	Expanded Subscriber Carrier Module-100A
EM	Electromagnetic; Electromechanical		ESMU	Expanded Subscriber Carrier Module-100 Urban
			ESN	Electronic Switched Network; Emergency Service Number
			ESP	Essential Service Protection; Enhanced Service Provider
			ESS	Electronic Switching System

ESTU	Enhanced Services Test Unit
ESU	End-of-Status Update
ESZ	Emergency Service Zone
ET	Exchange Terminal; Exchange Termination; Exchange Terminator
ETAS	Emergency Technical Assistance service
ETN	Electronic Tandem Network
ETS	Electronic Tandem Switching; Enhanced Time Switch
EUTT	End User Testing of Trunks
EWP	Electronic White Pages
EXB	Extension Bridging
EXT	Eternal Alarm
EXTN	Extension

F

F	Fahrenheit
Fbus	Frame Transport Bus
FA	Fuse Alarm
FAC	Facility
FACS	Facility Assignment and Control System
FADS	Force Administration Data System
FAST	First Application System Test
FAX	Facsimile
FCC	Federal Communications Commission
FCI	Feature Code Indicator
FCTD	Full Carrier Toll Denial
FD	Functional Description
FDM	Feature Description Manual; Frequency-Division Multiplex
FDX	Full Duplex
FEATID	Feature Identification
FEXT	Far-End Cross Talk
FGA	Feature Group A
FGB	Feature Group B
FGC	Feature Group C
FGD	Feature Group D

FIB	Forward Indicator Bit
FISU	Fill-in Signal Unit
FIU	Facilities Interface Unit
FM	Focused Maintenance; Force Management
FMT	Fiber Multiplex Terminal
FN	Feature Node; Functional Description
FNPA	Foreign Numbering Plan Area
FNT	Free Number Termination
FO	Fiber Optic
FOTS	Fiber Optic Transmission System
FPE	Feature Processing Environment
FR	Force Release
FRIU	Frame Relay Interface Unit
FRS	Flexible Route Selection
FS	Frequency Shift; Functional Signaling; Functional Specification
FSK	Frequency Shift Keying
FSN	Forward Sequence Number
FSP	Frame Supervisory Panel
FSR	Frequency Selective Ringing
FTM	Fiber Transport Management
FTP	File Transport Protocol
FTS	Fax-Thru Service
FTS 2000	Fed. Telecom. System (2000)
FVR	Flexible Vocabulary Recognition
FX	Foreign Exchange

G

G	Giga (billion)
GA	General Availability
GAP	Generic Address Parameter
GBH	Group Busy Hour
Gbyte	Gigabyte
GDA	Global Database Access
GFCI	Ground Fault Circuit Interrupter
GFD	General Feature Description

G	Giga (billion)
GOS	Grade of Service (noun); Grade-of-Service (adj.)
GPF	General Planning Forecast
GPIC	Per-Group Primary InterLATA Carrier
GR	Generic Requirements
GRD	Ground
GRP	Group
GSF	Generic Service Framework
GSM	Global System for Mobile Communications
GT	Global Title
GTI	Global Title Identifier
GTT	Global Title Translation
GUI	Graphical User Interface

H

H/W	Hardware
H Date	Installation Start (Date)
HADS	HOBIC Administrative Data System
HD	High Day
HDBH	High Day Busy Hour
HDLC	High-Level Data Link Control
HDR	Header
HDX	Half Duplex
HEX	Hexadecimal
HF	High Frequency
HG	High-resistance Ground
HIE	Host Interface Equipment
HIF	Host Interface
HIS	Host Interface Shelf
HLD	Hold
HLIU	High-Speed Link Interface Unit
HLL	High-Level Language
HMI	Human-Machine Interface
HNPA	Home Numbering Plan Area
HOBIC	Hotel Billing Information Center
HOC	Host Office Collector
HOTL	Hand Off Threshold Level

HP	Hewlett-Packard Corporation
HPR	High Performance Routing
HRX	Hypothetical Reference Connection
HSDA	High Speed Data Access
HSDU	High Speed Data Unit
HSM	High Speed Modem
HT	Holding Time
HTRF	Hard-to-Reach Flag
HTRP	Hard-to-Reach Peg
HU	High Usage
HX	HALT
Hz	Hertz

I

I/O	Input/Output
I/F	Interface
I/C	Incoming
IAC	Integrated Access Controller; ISDN Access Controller
IAM	Incoming Address Message; Initial Address Message
IAP	Internet Access Provider
IB	In-Band; In-Band Signaling
IBERT	Integrated Bit Error Rate Tester
IBM	International Business Machines Corporation
IBML	Interbay Message Link
IBN	Integrated Business Network
IC	Integrated Circuit; Inter-exchange Carrier; InterLATA; In Charge
IC-XPT	Incoming Crosspoint
ICAN	Individual Circuit Analysis
ICB	Integrated Collector Bus
ICI	Incoming Call Identification
ICL	Incoming Line; Inserted Connection Loss
ICM	Intercom

ICNPA	Interchangeable Numbering Plan Area		INWATS	Inward Wide-Area Telephone Service
ICS	Integrated Carrier Systems		IOC	Independent Operating Company; Input/Output Controller
ICTS	Integrity Check Traffic Simulator			
ICUP	Individual Circuit Usage and Peg Count		IOE	Input/Output Equipment
			IOM	Input/Output Module
ID	Identification; Identifier		IOS	Integrated Office Systems International Organization for Standardization
IDDD	International Direct Distance Dialing			
IDF	Intermediate Distribution Frame		IP	Initial Period; Internet Protocol; Intelligent Peripheral
IDOC	Internal Dynamic Overload Control			
IEC	Inter-Exchange (InterLATA) Carrier		IPC	Interperipheral Connection; Interprocessor Communications; Intelligent Peripheral Controller
IEEE	Institute of Electrical and Electronics Engineers			
IFP	International Free Phone		IPF	Integrated Processor and Frame Bus Interface
IID	Interface Identifier			
ILC	IBERT Line Card		IPH	Integrated Packet Handler
ILD-R	ISDN Line Drawer for Remotes		IPL	Initial Program Load
ILLP	Inter link-to-Link Protocol		IPM	Interruptions Per Minute; Impulses Per Minute
ILTC	ISDN Line Trunk Controller			
IMC	Interface Module Cabinet; Inter-Module Communications		IPML	Interperipheral Message Link
			IR	Integrated Release
IMH	Intelligent Mismatch Handler		IRTU	Integrated Remote Test Unit
IML	Incoming Matching Loss		IS Date	In-Service (Date)
IMR	Individual Message Register		ISA	Integrated Services Access
IN	Interlata		ISC	International Switching Center
INB	Installation Busy		ISDD	Incoming start-to-dial delay (OM Group)
INC	Incoming; Industry Numbering Committee; International Carrier			
			ISDN	Integrated Services Digital Network
INFO	Information		ISDN UP	ISDN User Part
INI	Initialized State		ISE	Intelligent Services Environment
INode	Integrated Node (SSP and STP)		ISG	ISDN Service Group
INPA	Interchangeable Numbering Plan Area		ISLC	ISDN Line Card
			ISLM	Integrated Services Line Module
INR	Information Request Message		ISM	Integrated Services Module
INIT	Initialize		ISN	Integrated Services Node; Intelligent Services Node
INS	Integrated Network Systems			
INSV	In Service		ISP	ISDN Signaling Pre-processor; Internet Service Provider
INT	Intercept			
INV	Inverter Unit		ISS	Intelligent Services Switch
			ISTB	In-Service Trouble

ISU	Initial Signal Unit
ISUP	ISDN User Part; Integrated Signaling User Part
IT	Intertoll
ITB	Incoming Trunk Busy
ITC	Information Transfer Capability
ITS	Integrated Test System
ITT	International Telephone and Telegraph Corporation
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union (formerly the CCITT)
IVD	Integrated Voice and Data (Lines)
IVDT	Integrated Voice-Data Terminal
IVR	Integrated Voice Response
IVS	Interactive Voice Subsystem
IWS	Intelligent Workstation
IWSS	Intelligent Workstation Subsystem
IXC	Interexchange Carrier

J

JF	Junctor Frame; Journal File
JIP	Jurisdiction Information Parameter
JNET	Junctored Network

K

K	Kilo (1000 or 1024)
KBD	Keyboard Dialing
kbps	Kilobits per second
KBps	Kilobytes Per Second
KBYTES	Kilobytes
K-date	Installation Complete (Date)

Khz	KiloHertz
KP	Keypulse; Keypad
KSR	Keyboard Send/Receive
KT	Killer Trunk
KTS	Key Telephone System

L

LADT	Local Area Data Transport
LAMA	Local Automatic Message Accounting
LAN	Local Area Network
LAP	Link Access Protocol
LAPB	Link Access Procedures Balanced
LAPD	Link Access Procedures D-Channel
LASS	Local Area Signaling Service
LATA	Local Access and Transport Area
LBR	Large Business Remote
LBS	Load Balance System
LC	Line Card
LCA	Line Concentrating Array
LCC	Line Class Code; Link Common Control
LCD	Line Concentrating Device; Liquid Crystal Display
LCDR	Local Call Detail Recording
LCE	Line Concentrating Equipment
LCGA	Local Carrier Group Alarm
LCM	Line Concentrating Module
LCME	Line Concentrating Module Enhanced
LCMI	ISDN Line Concentrating Module
LD	Long Distance
LDA	Long Distance Alerting
LDN	Listed Directory Number
LDS	Local Digital Switch

LDT	Line Digital Trunk; Line appearance on a Digital Trunk		LNR	Last Number Redial
			LMOS	Loop Maintenance Operations System
LEAS	LATA Equal Access System		LNP	Local Number Portability
LEC	Local Exchange Carrier		LO	Lockout
LED	Light-Emitting Diode		LOADPM	Load Peripheral Module
LEN	Line Equipment Number		LOC	Location Code
LET	Local Exchange with TOPS		LOF	Loss of Frame Loss of Framing
LF	Low Frequency			
LG	Log (Message)		LPIC	IntraLATA Primary Interexchange Carrier
LGA	Line Group Array			
LGC	Line Group Controller		LSLD	Signaling Link Deactivation
LGCI	Line Group Controller ISDN		LP	Loop
LGE	Line Group Equipment		Lpbk	Loop Back
LGP	Link General Processor		LPC	Linear Predictive Coding
LID	Line Inhibit Denied		LPIC	Line-based Primary InterLATA Carrier
LIDB	Line Information Database			
LIM	Link Interface Module		LPO	Local Processor Outage
LINEATTR	Line Attribute		LPP	Link Peripheral Processor
LInh	Local Inhibit		LRN	Location Routing Number
LION	Line Information for Open Networks		LRS	Loop Reporting System
			LS	Line Switch
LIS	Link Interface Shelf		LSAC	Signaling Link Activity Control
LIU	LAN Interface; Link Interface Unit		LSB	Least Significant Bit
			LSC	Line Screening Code
LIU7	Link Interface Unit for CCS7		LSDA	Signaling Data Link Allocation
Lk	Link		LSDU	Low-Speed Data Unit
LkSet	Linkset		LSI	Large-Scale Integration
LLC	Line Load Control; Lower-Layer Compatibility		LSLA	Signaling Link Activation
			LSPI	Local Service Provider Identification
LLSC	Link Set Control			
LM	Line Module; Load Management; Local Maintenance		LSSGR	LATA Switching System Generic Requirements
			LTC	Line Trunk Controller
LMAS	Local Maintenance and Administration System		LTCI	Line Trunk Controller ISDN
			LTID	Logical Terminal Identifier
LMB	Line Maintenance Busy		LTP	Line Test Position; Link Termination Processor
LME	Line Module Equipment			
LMOS	Loop Maintenance Operations System		LTPDATA	Line Test Position Data (test level)
			LTR	Load Transfer
LMS	Line Message Service; Link Message Switch; Local Message Service		LTU	Line Test Unit; Loop Test Unit
			LU	Line Unit
LN	Line			
LNA	Link Number Acknowledge			

LW	Leave Word

M

MAC	Medium Access Control
MAD	Maintenance Advisor (replaced by term MAX)
MADN	Multiple Appearance Directory Number
Man	Manual
MAP	Maintenance and Administration Position
MAX	Maint & Administrative Expert
MB	Maintenance Busy; Make Busy
MBA	Multi Bridge Arrangement
Mbps	Megabits Per Second
Mbyte	Megabyte
MBS	Meridian Business Service
MCA	Multiple Call Arrangement
MCC	Master Control Center
MCCS	Mechanized Calling Card Service
MCD	Minimum Call Duration
MCLC	Multi Circuit Line Card
MCM	Maintenance Control Module
MCO	Manual Changeover
MD	Manufacture Discontinued
MDC	Meridian Digital Centrex
MDF	Main Distribution Frame; Main Distribution Facility
MDII	Machine Detected Inter-office Irregularities
MDR	Message Detail Recording
MDR7	Message Detail Recording for CCS7
Mega	Million
MF	Multi-Frequency
MFADS	Mechanized Force Administration Data System
MFJ	Modification of Final Judgment
MFR	Multi-Frequency Receiver

MI	Marketing Information System
MIB	Management Information Base
MIC	Modem Interface Card
min	Minimum
MINS	Minutes
MIS	Management Information Systems
ML	Maintenance Limit
MLH	Multi-Line Hunting
MLT	Mechanized Loop Test; Multi-Line Test; Multiple Line Test
MMB	Man-Made Busy
MMI	Man-Machine Interface
MMS	Memory Management System
MNA7	Multiple CCS7 Network Addresses
MOS	Metallic Oxide Semiconductor
MP	Multi-purpose Position; Master Processor; Maintenance Processing
MPC	Multi-Protocol Converter; Multiple Power Controller
MPL	Maximum Power Level
MPSC	Multi Protocol Serial Controller
MRFF	Master Reference Frequency Frame
MR	Message Rate
MRVT	Message Transfer Part Routing Verification Test
MS	Message Switch (SuperNode)
MSA	Mobile Serving Area; Message Service Application
MSB	Message Switch and Buffer; Most Significant Bit
MSB7	Message Switch & Buffer for CCS7
MSBI	Make Set Busy-Intragroup
MSDA	Multi Speed Data Access
msg	Message
MSI	Medium Scale Integration
MSU	Message Signal Unit
MTA	Metallic Test Access
MTBF	Mean Time Between Failures

MTC	Magnetic Tape Controller; Maintenance		NCL	Non-Computing Module Load
MTCE	Maintenance		NCOS	Network Class of Service
MTD	Magnetic Tape Drive		NCP	Network Control Point; Network Control Program
MTM	Maintenance Trunk Module		NCTE	Network Channel Terminating Equipment
MTP	Message Transfer Part			
MTS	Message Telecommunications Service Message Transport System		NDCOS	Network Data Collection Operations System
MTTR	Mean Time to Restore		NE	Near End; Network Element; Network Equipment
MTU	Magnetic Tape Unit			
MTX	Mobile Telephone Exchange		NEBS	Network Equipment Building Standards
MU	Message Unit			
MultiSUN	Multi-Sending Unit		NEC	National Electric Code; Nippon Electric Company
MUM	Multi-Unit Message			
MUMR	Multi-Unit Message Rate		NEL	Next Event List
MUX	Multiplex		NENA	National Emergency Number Association
MUXER	Multiplexer			
MVL	Morrisville		NEMA	National Electrical Manufacturers' Association
MVP	Multi-line Variety Package			
MWI	Message Waiting Indication		NEXT	Near-End Crosstalk
MWT	Message Waiting		NFF	No Fault Found

N

NA	Not Available; Not Applicable		NI	Network Indicator
			NI-1,2,3	National ISDN-1,2,3
NACK	Negative ACKnowledgment		NIC	National ISDN Council; Network Interface Card
NAG	Node Assessment Graph			
NANP	North American Numbering Plan		NIS	Network Interface Specification
			NIT	Non-Initializing Terminal
NAS	Network Attendant Services		NIU	Network Interface Unit
NAV	Network Applications Vehicle		NM	Network Module
NBAS	Network-Based Answering Service		NMA	Network Monitoring & Analysis
			NMB	Network Management Busy
NBEC	Non-Bell Exchange Carrier		NMC	Network Management Center; Network Message Controller
NBOC	Network Building Out Capacitor			
NBOR	Network Building Out Resistor		NMOS	N-Channel Metal Oxide Semiconductor
NC	Normally Closed; Network Congestion; Network Connection			
			NMS	Network Maintenance Services
			NNX	N=Number 2-9, X=Number 0-9 (general code for central office)
NCEO	Non-Conforming End Office (not Equal Access ready)		NO	Normally Open
			NOA	Nature of Address; Network Operations Architecture
			NOC	Nature of Connection; Network Operations Center

NOH	No Receiver Off-Hook Tone
NOP	Network Operations Protocol
NORGEN	Network Operations Report Generator
NOS	Network Operations System
NOTIS	Network Operations Trouble Information System
NPA	Numbering Plan Area
NPD	Numbering Plan Digit
NPE	New Peripheral Evolution
NPI	Numbering Plan Indicator
NRC	Network Reliability Council
NREAD	Network Ring Again
NSC	Number Services Call
NSG	Network Subgroup
NSP	Network Service Part
NSR	Network Software Release
NSS	Network Signaling Services; Network Support Systems
NSSD	Network Support Systems Division
NT	Northern Telecom
NT1	Network Termination One
NT DA	Nortel Directory Assistance
NTE	Network Terminal Equipment
NTF	No Trouble Found
NTI	Northern Telecom Incorporated
NTMOS	Network Traffic Management Operations System
NTP	Nortel Networks Publication; Nortel Networks Practice; Nortel Networks Plaza
NTS	Network Transport Services; Number Translation Services
NTT	No-Test Trunk
NUC	Nailed-Up Connection
NWM	Network Management
NXX	N=Number 2-9, X=Number 0-9; The Office Exchange Code

O

OAM OA&M	Operation, Administration and Maintenance
OAM&P	Operations, Administration, And Maintenance Processor; Operations, Administration, Maintenance, and Provisioning
OAP	Open Automated Protocol
OAU	Office Alarm Unit
OBCI	Optional Backward Call Indicators
OBH	Office Busy Hour
OC	Operator Centralization; Optical Carrier
OCC	Other Common Carrier
OCN	Original Called Number
ODM	Office Data Unit Modification
OEM	Original Equipment Manufacturer
OFFL	Off-Line
OFZ	Office Traffic Summary
OG	Outgoing
OGT	Outgoing Trunk
OHD	Off-Hook Delay
OHQ	Off-Hook Queuing
OIA	Open Information Access
OIU	Office Interface Unit
OLI	Originating Line Information
OLNS	Originating Line Number Screening
OM	Operational Measurement
OMAP	Operations and Maintenance Application Part
OML	Outgoing Matching Loss
OMRS	Operational Measurement Reporting System
ONA	Open Network Architecture
ONAL	Off-Net Access Line
ONI	Operator Number Identification
ONP	One Night Process
OOF	Out of Frame
OOS	Out of Service

OPAC	Outside Plant Access Cabinet
OPC	Originating Point Code
OPDU	Operation Protocol Data Unit
OPEN	Open Protocol Enhanced Networks
OPM	Outside Plant Module
OPP	Open Position Protocol
OPR	Operator
OPS	Off-Premise Station
OPX	Off-Premise Extension
ORB	Office Repeater Bay
ORDB	Operator Reference Data Base
OS	Operating System; Operations System
OSC	Operator Service Center; Operator Services Code
OSF	Open Systems Foundation
OSI	Operator Services Information; Open System Interconnection
OSI Model	Open System Interconnection Reference Model
OSNC	Operator Services Network Capability
OSNM	Operator Service Node-Maintained
OSO	Origination Screening Office
OSS7	Operator Services Signaling System No. 7
OSS	Operations Support System; Operator Services Signaling
OSSAIN	Operator Services Signaling Advanced Intelligent Networking
OSSGR	Operator Services Systems Generic Requirements
OSSP	Operations Support System Plan (Bellcore; NT's is NOA)
OTC	Operating Telephone Company
OUTWATS	Outward Wide-Area Telephone Service
OW	Order Wire

P

P-side	Peripheral Side
PABX	Private Automatic Branch Exchange
PAD	Packet Assembler/Dis-assembler
PAM	Pulse Amplitude Modulation
PAMS	Preselected Alternate Master/Slave
PAQS	Provisioning and Quotation System
PARS	Personal Audio Response System
PARMS	Parameters
PAX	Private Automatic Exchange
PBX	Private Branch Exchange
PC	Peg Count; Personal Computer; Point Code; Process Controller
PCB	Printed Circuit Board; Process Control Block
PCC	Point Code Critical
PCI/F	Personal Computer Interface
PCL	Product Computing-module Load
PCM	Pulse Code Modulation
PCP	Port Call Processing
PCR	Preventive Cyclic Retransmission
PCS	Personal Communications Services
PCU	Power Control Unit
PDAB	Partial Dial Abandon
PDC	Physical Distribution Center; Power Distribution Center; Product Distribution Center
PDN	Packet Data Network; Primary Directory Number
PDP	Programmable Digital Processor
PDTO	Partial Dial Time Out

PE	Peripheral Equipment; Phase Encoded; Processing Element
PEC	Product Engineering Code
PEFS	Percent Error-Free Seconds
PERM	Permanent
PH	Packet Handler
PIC	Primary InterLATA Carrier; Point in Call; Presubscribed Inter-exchange Carrier; Polyethylene–Insulated Conductor; Pulp Insulated Cable
PICS	Plug-In Control System
PIN	Personal Identification Number
PL/1	Programming Language One
PLR	Pulse Loop Repeater
PM	Peripheral Module
PMB	Peripheral Module Busy
PMBX	Private Manual Branch Exchange
PODP	Public Office Dialing Plan
POF	Pending Order File
POI	Point of Interface
POP	Point of Presence
Pos	Position
POTS	Plain Old Telephone Service; Plain Ordinary Telephone Service
PP	Peripheral Processor
PPSN	Public Packet Switched Network
PR	Processor Reset
PRA	Primary Rate Access (ISDN Service)
PRE	Prepayment Coin Telephone
PRI	Primary Rate Interface
PRK	Call Park
PRL	Privacy Release
PROM	Programmable Read-Only Memory
PROTEL	Procedure Oriented Type Enforcing Language
PRSM	Post Release Software Manager
PRU	Program Resource Unit

PS	Permanent Signal; Power Supply; Program Store
PSAP	Public Safety Answering Point
PSDC	Packet Switched Digital Capability
PSDN	Packet Switched Digital Network
PSDS	Packet Switched Data Service
PSIDE	Peripheral Side
PSIU	Packet Switch Interface Unit
PSLINK	Peripheral Side Link
PSTN	Public Switched Telephone Network
PTE	Partitioned Table Editor
PTS	Proceed to Select; Proceed to Send; Public Telephone System; Per-Trunk Signaling
PTT	Post, Telegraph and Telecommunications
PVC	Permanent Virtual Circuit
PVN	Private Virtual Network
PWAC	Present Worth of Annual Charges
PWM	Pulse Width Modulation
PWR	Power
PX	Private Exchange

Q

Q	Quarter
Q.921	Layer 2 Data Link Protocol
QAM	Quadrature Amplitude Modulation
QMIS	Queue Management Information System
QMS	Queue Management System
QMS CASE	QMS Customer Assistance Service Enhancements
Quasi	Quasi-Associated
Quest411	Nortel's National DA offering

R

R/W	Read/Write
R	Ring
RA	Recorded Announcement
RADR	Receiver Attachment Delay Recorder
RAG	Ring Again
RAI	Remote Alarm Indication
RAM	Random Access Memory
RAMP	Remote Access Maintenance Positions
RAMS	Repair Access Management System
RAO	Regional Accounting Office; Revenue Accounting Office
RAS	Route Accounting Subsystem
RBOC	Regional Bell Operating Company
RC	Recording Completing Regional Center
RCA	Remote Cluster Array
RCC	Remote Cluster Controller
RCD	Record
RCER	Remote Call Event Record
RCF	Remote Call Forwarding
RCGA	Remote Carrier Group Alarm
RCT	Remote Concentrator Terminal
RCU	Radio Control Unit
RDAT	Receive Data
RDBMS	Relational Database Management System
RDLM	Remote Digital Line Module
RDOC	Remote Dynamic Overload Control
RDR	Remote Dump and Restore
RDT	Remote Digital Terminal
RDW	Record Descriptor Word
REA	Rural Electrification Administration
REC	Receive
RECT	Rectifier
REL	Release

REM	Remote Equipment Module
RES	Residential Enhanced Service; Resume
REX	Routine Exercise
RF	Radio Frequency
RFA	Recurrent Fault Analysis
RFF	Request For Feature
RFI	Radio Frequency Interface
RG	Ringing Generator
RGI	Ringing Generator Interface
RHC	Regional Holding Company
RInh	Remote Inhibit
RISC	Reduced Instruction Set Computing
RL	Ring Lead
RLC	Release Complete; Remote Line Controller
RLCM	Remote Line Concentrating Module
RLM	Remote Line Module; Remote Load Management
RLS	Release
RLT	Release Line Trunk
RM	Resource Module
RMAS	Remote Memory Administration System
RMB	Remote-Made-Busy; Remote-Make-Busy
RMC	Remote Maintenance and Control; Remote Maintenance Center
RME	Remote Miscellaneous Equipment
RMM	Remote Maintenance Module
RO	Receive Only; Remote Office
ROH	Receiver Off-Hook
ROM	Read-Only Memory
RONI	Remote Operator Number Identification
ROTL	Remote Office Test Line
RPO	Remote Processor Outage
RR	Re-Route
RRU	Remote Resource Unit

RS	Rate Step; Recommended Standard; Remote Surveillance
RS-232C	Recommended Standard #232 — Communications (the industry standard for a 25-pin interface)
RSB	Remote Switching Bay; Repair Service Bureau
RSC	Remote Switching Center; Routeset Critical
RSC-S	Remote Switching Center-Sonet
RSM	Remote Switching Module; Routeset Major
RST	Remote Supervisor Terminal
RSU	Remote Switching Unit
RSUS	Requested Suspended Service
RT	Remote Terminal; Ringing Tone
RTA	Remote Trunking Arrangement
RTAN	Remote Test Access Network
Rte	Route
RteSet	Routeset
RTM	Ready To Manufacture
RTO	Ready To Order
RTOIS	Ready To Order In-Service
RTONIS	Ready To Order Not In-Service
RTP	Research Triangle Park
RTS	Remote Test System; Request To Send; Return To Service
RTU	Right to Use
RU	Recording Unit
RVDTS	Revertive Call Destination Traffic Separation

S

S/R	Send/Receive
S/W	Software
SA	Service Assistance
SAC	Special Access Code; Special Area Code

SADS	System Administration Data System
SAID	Speech-Activated Intelligent Dialing
SAM	Subscriber Access Module; Subsequent Address Message
SAP	Service Activation Parameter
SAPI	Service Access Point Identifier
SARTS	Switched Access Remote Test System
SAS	System Administration Services; Switched Access System
SBA	Single Bridge Arrangement
SCA	Single Call Arrangement
SCAMA	Super Centralized Automatic Message Accounting
SCC	Specialized Common Carrier; Switching Control Center
SCCP	Signaling Connection Control Part
SCCS	Switching Control Center System
SCI	Subscriber Carrier Interface
SCL	Speed Calling Long List
SCLC	SCCP Connectionless Control
SCLLI	Short Common Language Location Identifier
SCM-100A	Subscriber Carrier Module-100 Access
SCM-100S	Subscriber Carrier Module-SLC-96 Interface
SCM-100R	Subscriber Carrier Module — DMS-100 Rural
SCM-100U	Subscriber Carrier Module — DMS–100 Urban
SCM	Subscriber Carrier Module
SCMG	SCCP Management
SCMR	Subscriber Carrier Module Remote
SCOC	SCCP Connection-Oriented Control
SCP	Service Control Point (Same as SDB)
SCRC	SCCP Routing Control
SCS	Speed Calling Short List

SCSI	Small Computer System Interface		SL	Signaling Link; Subscriber's Loop
SCU	System Control Signaling Unit		SLC	Subscriber Line Carrier; Subscriber Loop Carrier; Signaling Link Code
SCWID	Spontaneous Call Waiting Display		SLIC	Subscriber Line Interface Circuit
SD	Schematic Drawing; Send Digits; Signal Distributor		SLM	System Load Module; Switching Link Management
SDB	Services Database		SLS	Signaling Link Selection
SDIG	Short Diagnostics		SLT	Setup Logical Terminal
SDK	Software Development Kit		SLU	Subscriber Line Usage
SDL	Signaling Datalink		SLUS	Subscriber Line Usage Study
SDLC	Synchronous Data Link Control		SMA	Subscriber Carrier Module-100 Access
SDM	DMS SuperNode Data Manager		SMAS	Switched Maintenance Access System
SDN	Secondary Directory Number		SMDI	Simplified Message Desk Interface
SDOC	Selective Dynamic Overload Control		SMDR	Station Message Detail Recording
SEAC	Signaling Engineering And Administration Center		SMH	Signaling Message Handling
SEAS	Signaling Engineering And Administration System		SMR	Subscriber Module Remote
			SMS	Software Management System
SEQ	Sequential		SMSA	Standard Metropolitan Statistical Area
SERVORD	Service Order			
SES	Service Evaluation System; Severe Error Seconds		SMSR	Subscriber Module Slc-96 Remote
SF	Service Feature; Single Frequency; Store File; Superframe		SMSS	Switch Maintenance Services System
			SMU	Subscriber (premises) Module Unit
SI	System International (Metric System)		SN	Subscriber Number
SIE	Emergency Alignment Status Indicator		SNA	Systems Network Architecture
			SNAC	Switching Network Analysis Center
SILC	Selective Incoming Load Control		SNAP	Standard Network Access Protocol
SIN	Normal Alignment Status Indicator		SNID	Signaling Network Identifier
SIO	Serial Input/Output; Service Information Octet		SNM	Subsystem Network Management; Signaling Network Management
SIOS	Out of Service Status Indicator		SNMP	Simple Network Management Protocol
SIT	Special Information Tone			
SITE	Traffic and dial tone speed recording, remote sites (OM Group)		SNR	Stored Number Redial; Subsystem Normal Routing Message
SIU	Out of Alignment Status Indicator			

SO	Service Order; Switching Office		SSN	Subsystem Number
SOC	Software Optionality Control; Service Oversight Center (as in FTS 2000 NOC/SOC)		SSP	Service Switching Point; Special Service Protection
			SSR	Switch Status Report
SOD	Stringing of Digits		ST	Signaling Terminal; Start Signal; Stop Pulsing Signal (End-of-Pulsing Signal)
SOE	Standard Operating Environment			
SONET	Synchronous Optical Network		ST7	Signaling Terminal 7
SOP	Service Ordering Processor		STA	Signaling Terminal Array
SOS	Software Operating System		STAI	Signaling Terminal Access Interface
SOST	Special Operator Service Traffic			
SP	Signaling Processor; Signaling Point		STB	Signaling Terminal Buffer
			STBY	Standby
SPB	Special Billing		STC	Signaling Terminal Controller
SPC	Stored Program Control		STD	Standard; Subscriber Trunk Dialing
SPCS	Stored Program Controlled Switch			
			STI	Signaling Terminal Interface
SPG	Single Point Ground		STIF	Signaling Terminal Interface
SPID	Service Provider Identification		STINV	Signal Terminal Inventory (table)
SPM	Service Peripheral Module; Spectrum Peripheral Module		STM	Signaling Traffic Management
			STOR	Send to Outside Resource
SPMS	Switch Performance Monitoring System		STP	Signaling Transfer Point
			STR	Selective Trunk Reservation; Special Tone Receiver; Send To Resource
SP MUX	Serial Parallel Multiplexer			
SPOAMI	Single Point OA&M For ISDN Node			
			STS	Serving Translation Scheme
SQA	Software Quality Assurance		SU	Signaling Unit
SR	Service Report; Special Report; Speech Recognition		SUS	Suspend
			SVC	Switched Virtual Circuit
			SW	Switch
SRDB	Selective Routing Database		SWACT	Switch Activity
SRL	Singing Return Loss		SWR	Software Register
SRM	Signaling Route Management		SX	Simplex Signaling
SRU	Shared Resource Unit		SXS	Step-by-Step
SRS	Statistics Repository Subsystem		SYN	Synchronous Idle Character
SS	Signaling System; Special Service; Station-to-Station		SYNC	Synchronized; Synchronous
			SYSB	System Busy
SS#7	Signaling System No. 7 (International version)		SYSDATA	System Data
			SYSINIT	System Initialization
SS7	Signaling System No. 7 (North American version)		SYSLOG	System Log
			SYSMON	System Monitor
SSC	Subsystem Critical		SYU	Synchronization Unit
SSM	Special Services Module			

SZ	Seize
SZD	Seized

T

T	Tip
T1	Digital Carrier Line Facility at the 1.544 Mbps DS1 Rate
T-Link	Rate Adaption Protocol up to 64 Kbits
T/R	Tip/Ring
T&C	Time & Charges
TA	Terminal Adapter; Test Access; Termination Attempt; Toll and Assistance
TABS	Talking Alternate Billing System
TAC	Technician Access Controller; Trunk Access Control; Technical Assistance Center
TADS	Traffic Administration Data System
TAFAS	Trunk Answer From Any Station
TAMI	Tops Administration And Maintenance Interface
TAN	Test Access Network
TAS	Technical Assistance and Support
TASI	Time Assigned Speech Interpolation
TAT	Termination Attempt Trigger
TAU	Test and Alarm Unit
TBD	To Be Determined
TBI	Transaction Bus Interface
TC	Terminal Controller; Test Code; Toll Center
TCAP	Transaction Capabilities Application Part
TCAS	T-Channel Administration System
TCBC	Traffic Changeback Control
TCM	Time Compression Multiplexing

TCOC	Traffic Changeover Control
TCOS	Traveling Class of Service
TCP/IP	Transmission Control Protocol/Internet Protocol
TCRC	Traffic Routing Congestion Control
TCS	Test Control System
TCTS	Trans-Canada Telephone System
TDAS	Traffic Data Administration System
TDF	Trunk Distribution Frame
TDM	Time Division Multiplexing
TDR	TOPS Call Detail Recording
TE	Terminal Equipment
TEHO	Tail-End Hop-Off
TEI	Terminal Endpoint Identifier; Terminal Equipment Identifier
TELEX	Teletypewriter Exchange Service
TFA	Transfer Allowed
TFC	Transfer Control
TFMI	Traffic Mix Information
TFP	Transfer Prohibited
TFR	Transfer Restricted
TFRC	Traffic Routing Congestion Control
TFS	Trunk Forecasting System
TG	Trunk Group
TGB	Trunk Group Busy
TICS	TOPS InterLATA Carrier Service
TID	The Terminal ID of the Agent
TIDF	Trunk Intermediate Distribution Frame
TIRKS	Trunk Integrated Records Keeping System
TL-1	Transaction Language 1
TL	Transmission Link
TLAC	Transfer Link Activity Control
TLP	Transmission Level Point; Test Level Reset Point
TLWS	Trunk and Line Work Station
TM	Trunk Module
TME	Trunk Module Equipment
TML	Tandem Matching Loss

TMS	Trouble Mgmt. Systems (for FTS-2000); Tops Message Switch
TNDS	Total Network Data System
TNN	Trunk Network Number
TNS	Transit Network Services
TO	Traffic Order
TOD	Time-of-Day
TOPS	Traffic Operator Position System
TOPS MP	TOPS Multi-purpose Position
TOPS MPX	Connectivity with IBM DA
TOPSVR	Traffic Operator Position Voice Response
TOS	Taken Out of Service; Trunk Offer Start
TP	Test Position; Toll Point; Transaction Portion
TPC	TOPS Position Controller; Terminal Position Controller; TOPS Programmable Switch
TR	Technical Reference; Test Ring
TRCC	Traffic Routing Congestion Control
TRAVER	Translation and Verification
TRD	Timed Release Disconnect
TRK	Trunk
TRKGRP	Trunk Group
TS	Time Switch; Toll Switching
TSFC	Traffic Signaling Flow Control
TSM	Transport Services Management
TSMS	Traffic Separation Measurement System
TSP	Terminal Service Profile
TSPS	Traffic Service Position System
TSRC	Traffic Signaling Route Control
TSS	Trunk Servicing System
TST	Test; Time-Space-Time
TSW	Time Switch
TTC	Terminal Test and Configuration; Terminating Toll Center

TTL	Transistor-Transistor Logic
TTP	Transmission Test Position; Trunk Test Position
TTT	Transmission Test Trunk
TTU	Test Trunk Unit
TTY	Teletypewriter
TWC	Three-Way Calling
TWOOT	Two-Way Operator Office Trunks
TWX	Teletypewriter Exchange

U

UAS	Unavailable Second
UBM	Unsuccessful Backwards Failure Message
UCD	Uniform Call Distributor Universal Call Distributor
UDT	UNITDATA Message
UDTS	UNITDATA Service Message
UIB	User Interaction Base
UL	Underwriter's Laboratory, Inc.
UNBAL	Unbalanced
UNDN	Unassigned Directory Number
UP	User Part
USAA	United States Assurance Association
USI	User Services Information
USP	Usage Sensitive Pricing
USTA	United States Telephone Association
UTR	Universal Tone Receiver
UUI	User-to-User information

V

V	Volt
VAC	Volts Alternating Current
VAD	Voice Activated Dialing
VAPD	Voice Activated Premier Dialing

VAPN	Virtual Access to Private Networks
VAS	Value Added Service; Voice Activated Services
VB	Voice Band
VBD	Voice Band Data
VCXO	Voltage Controlled Crystal Oscillator
VDC	Volts Direct Current
VDS	Voice Prompt Development System
VDT	Video Display Terminal
VDU	Video Display Unit
VER	Verify
VF	Voice Frequency
VFG	Virtual Facility Group
VFL	Voice Frequency Link
VGB	Virtual Group Busy
VIR	Variable Initial Rate
VLAN	Virtual Local Area Network
VLC	Voice Line Card
VLL	Virtual Leased Line
VLSI	Very Large Scale Integration
VMS	Voice Message System
VMX	Voice Message Exchange
VNL	Via Network Loss
VO	Verification Office; Validation Office
VOC	Video Operations Center
VOL	Volume Label
VPU	Voice Processing Unit
VQ	Voice Quote
VS	Virtual System
VSN	Voice Service Node
VT	Video Terminal

WAN	Wide Area Network
WATS	Wide Area Telephone Service
WD	Wiring Diagram
WE	Write Enable
WECO	Western Electric Company
WNZ	World Numbering Zone

X

X.25	CCITT-defined network layer protocol used in packet switching
XBAR	Crossbar
XBERT	XPM-based Bit Error Rate
xDSL	Digital Subscriber Line Technology
XFER	Transfer
XLCM	Peripheral Line Concentrating Module
XMIT	Transmit
XMS	Extended Memory Specification; Extended Multiprocessor System
XPAM	Transmit Pulse Amplitude Modulation
XPM	XMS-Based Peripheral Module; Extended Peripheral Module
XPM PLUS	XPM Product Life Upgrade Strategy
XPT	Crosspoint

Z

ZBTSI	Zero Byte Time Slot Interchange
ZCS	Zero Code Suppression

W

W	Watts; Width
WACK	Wait Acknowledge
WAHT	Weighed Average Holding Time

User's Notes

Add your own personal maintenance and operations notes. CD-ROM users print to use.

DMS-100 Family

All Product Computing-Module Loads

Maintenance and Operations Manual

Address comments to:

Nortel Networks

Global Professional Services

Technical Services

Dept. 1773, MDN MS49D030F5

2520 Meridian Pkwy Durham, NC 27713

NORTEL
NETWORKS ™