297-1001-129

DMS-100 Family

Input/Output System

Reference Manual

BASE13 and up Standard 06.06 September 2000

NORTEL NETWORKS™

DMS-100 Family

Input/Output System

Reference Manual

Publication number: 297-1001-129
Product release: BASE13 and up
Document release: Standard 06.06
Date: September 2000

Published in the United States of America

Publication history

September 2000

BASE13 and up Standard 06.06

- Converted document to FrameMaker + SGML and updated references in document.
- deleted references to SYSLOG as a command.

August 1999

BASE13 and up Standard 06.05

- explanation for stksize given in Chapter 5

April 1998

BASE03 and up Standard 06.04

- editing changes

BASE03 and up Standard 06.02

- made minor corrections to commands

BASE03 and up Standard 06.01

- made changes to login procedures after restarts

Contents

About this document vii
When to use this document vii
How to check the version and issue of this document vii
References in this document vii
What precautionary messages mean viii
How commands, parameters, and responses are represented ix
Input prompt (>) ix
Commands and fixed parameters x
Variables x
Responses x

1 Introduction 1-1
Application 1-1
Software Identification 1-1
Command Format Conventions 1-1

2 Input/Output Hardware 2-1
Input/Output Controller 2-2
Device Controllers 2-3
IO User Classes 2-5
Trunk Maintenance (TMtc): 2-6
Network Management (NWM): 2-6
Dial Administration (DAdm): 2-7
Service Analysis (SA): 2-7
Technical Assistance Center (TAC): 2-7
Emergency Technical Assistance Service (ETAS): 2-7
Line Maintenance (LMtc): 2-7
Repair Service Bureau (RSB): 2-8
Traffic Administration (TA): 2-8
International Switch Maintenance Center (ISMC): 2-8
International Transmission Maintenance Center (ITMC): 2-8
International Service Coordination Center (ISCC): 2-8
Network Management Control (NWC): 2-8

3 Input Control Software 3-1
Remote Access Security Control 3-1
Automatic Dialback Active 3-1
Security and Access Control 3-1
Enhanced Security Active 3-2

Enhanced Security Inactive. 3-2
Automatic Logout 3-3
Command Screening 3-6
Enhanced Command Screening Active 3-6
Enhanced Command Screening Inactive 3-7
ADMIN User 3-7
Show-Password Feature 3-9
Dumpsafe State 3-9
Priority Map Terminal 3-9

4 Output Control Software 4-1
Log System Interface 4-1
SYSLOG 4-4
Critical Message Prioritization 4-5
Guaranteed Background Schedule 4-5
Secret Logs 4-6
Report Routing 4-7
Basic Permanent Routing 4-7
Temporary Routing Commands 4-8
Report Thresholding 4-9
Thresholding Types 4-9
Threshold Values. 4-10
Disposition of Unprinted Thresholded Reports. 4-10
Temporary Thresholding 4-12
Thresholding for INIT and TRAP Logs 4-12
Logs Format_Offices with Enhanced Core 4-12

5 Man-Machine Interface 5-1
Types of MMI 5-1
Bilingual Man-Machine Interface 5-1
Parameters and Responses 5-2
Common Commands 5-2
Prompting 5-2
Security and Access Control MMI 5-3
Command Screening MMI 5-12
Report Routing MMI 5-25
Search and Display (Browse) MMI 5-42

List of terms 55

About this document

When to use this document

This publication describes the hardware and software aspects of the DMS-100 Family Input/Output (I/O) system. This manual contains details of the command syntax the user requires to perform the I/O functions. This manual contains details of the machine responses that occur because of these commands.

How to check the version and issue of this document

Numbers like 01.01 indicated the version and issue of the document.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. If the first release of a document is 01.01, first release of the same document is 02.01 in the *next* software release cycle.

The second two digits indicate the issue. The issue number increases for each revision of the document that is released in the *same* software release cycle. The second release of a document in the same software release cycle is 01.02.

This document applies to all DMS-100 Family offices. More than one version of this document can be present. To determine if you have the most current version of this document and organization of documentation for your product, refer to the release information in *DMS-100 Family Guide to Northern Telecom Publications,* 297-1001-001.

References in this document

The user requires references listed as requirements to understand this publication. References listed as informative contain information on other items in this publication, but are not necessary. References are entered at the correct places in the text.

Note: The documents listed can be present in more than one version. Refer to *Product Documentation Directory* 297-8991-001 to determine the release code of the version compatible with a specified release of software.

Prerequisite references for this publication are:

- *System Description*, 297-1001-100

Informative references for this publication are:

- *Product Documentation Directory*, 297-8991-001
- *Commands Reference Manual*, 297-1001-820
- *Basic Translations Tools Guide*, 297-1001-360
- *Provisioning Guide*, PLN-8991-104
- *Translations Guide*, 297-YYYY-350
- *Office Parameters*, 297-YYYY-855
- *Log Report Reference Manual*, 297-1001-840
- *Trunks Maintenance Guide*, 297-1001-595
- *Hardware Description Manual*, 297-8991-805

What precautionary messages mean

The types of precautionary messages that NT documents use include attention boxes and danger, warning and caution messages.

An attention box identifies information is required for the correct performance of a procedure or task or for the correct interpretation of information or data. Danger, warning and caution messages indicate possible risks.

Examples of the precautionary messages follow.

ATTENTION
Information required to perform a task

ATTENTION
Before you install a DS-1/VT Mapper, deprovision the DS-3 ports that are not used. If the ports are provisioned, DS-1 traffic is not carried through the DS-1/VT Mapper.

DANGER
Possibility of personal injury

DANGER
Risk of electrocution
Open the front panel of the inverter only if fuses F1, F2, and F3 are not present. The inverter contains high-voltage lines. The high-voltage lines are active until the fuses are removed. You risk electrocution.

WARNING
Possibility of equipment damage

DANGER
Damage to the backplane connector pins
Align the card before you seat the card. This action prevents bending of the backplane connector pins. Use light pressure to align the card with the connectors. Use the levers on the card to seat the card into the connectors.

CAUTION
Possible service interruption or degradation

CAUTION
Possible loss of service
Make sure that you remove the card from the inactive unit of the peripheral module. Removal of a card from the active list causes the loss of subscriber service.

How commands, parameters, and responses are represented

Commands, parameters and responses in this document conform to the following conventions.

Input prompt (>)

An input prompt (>) indicates the following information is a command:

```
>BSY
```

Commands and fixed parameters

Commands and fixed parameters the user enters at a MAP terminal appear in uppercase letters:

```
>BSY CTRL
```

Variables

Variables appear in lowercase letters:

```
>BSY CTRL ctrl_no
```

The user must enter letters or numbers that the variable represents. A list that follows the command string describes each variable.

Responses

Responses correspond to the MAP display and appear in a different type:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

The following excerpt from a procedure shows the command syntax that document uses:

At the MAP display

1 To manually busy the CTRL on the inactive plane, type

>BSY CTRL ctrl_no

and press the Enter key.

where

ctrl_no
is the number of the CTRL (0 or 1)

Example of a MAP response:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

1 Introduction

Application

The information in this publication applies to offices with Base13 software.

The information in this publication applies to offices with a Base release greater than Base13, if the information is not issued again. The application of all Northern Telecom Publication (NTP) editions that apply to Base releases is in *Product Documentation Directory* 297-8991-001.

Software Identification

A Base release number identifies software that applies to a DMS-100 Family office. A Northern Telecom (NT) Product Engineering Code (PEC) identifies the software. *Provisioning Guide* PLN-8991-104 and Office Feature Record D-190 describes the BCS number and the PEC. Office feature Record D-190 describes the meaning of the BCS number and PEC.

To display the Base number and PEC for the NT feature packages available in a specified office, type:

>PATCHER;INFORM LIST;LEAVE

Enter this command string at a MAP (maintenance and administration position) terminal.

Command Format Conventions

In this publication, a standard system of notes describes system commands and responses. The notes indicate the order in which command elements, the

punctuation, and the options appear. When the standards do not apply, the text provides an explanation.

Table 1-1

Convention	Meaning
CAPITAL letters or special characters	Show constants, commands or keywords that the system accepts when the user enters the constants, commands, or keywords as written.
lowercase letters	Show a user- or system-supplied parameter. Descriptions appear for each parameter.
Brackets {} or []	Enclose optional parameters. A vertical list in brackets indicates the user can select one or more of the parameters.
Underlined parameter	Is a default. If the user does not enter a selection, the system acts as if the user entered the underlined parameter.
Underscore that connects words	Treat the words as one item. For example, pm_type or #_one_two.
...	Indicates repeated steps or items.
In addition, the following standards are used.	
n (lowercase n)	Is a number from 0 to 9.
a (lowercase a)	Is a letter from A to Z.
h (lowercase h)	Is a hexadecimal integer from 0 to F.

Special features are used when the associated software package is provisioned and installed. The following features are available:

Table 1-2 (Sheet 1 of 2)

Feature	In Package
Auto LOGIN	NTX001
Automatic Dial Back	NTX293
Bilingual Human-Machine Interface (HMMI)	NTX066
Critical Message Prioritization	NTX001
Enhanced Command Screening	NTX292
Note: The DISPLAYPHONE is a trademark of Northern Telecom.	

Table 1-2 (Sheet 2 of 2)

Feature	In Package
Guaranteed Background Schedule	NTX000
MAP support for DISPLAYPHONE *	NTX001
Password and Access Control	NTX292
Priority MAP Terminal	NTX001
Show Password (SHOWPW) Command	NTX001
Secrecy	NTX100
Note: The DISPLAYPHONE is a trademark of Northern Telecom.	

2 Input/Output Hardware

Input/Output (I/O) hardware consists of controllers and I/O Devices (IOD) which enable the operating company to maintain, operate and administer the DMS switch. This hardware is in the *Product Documentation Directory*.

The MAP provides communication between the user and the DMS switch. Through the MAP, the Human-Machine Interface (MMI) inputs commands, runs tests, requests information and displays messages or reports. For details of the MAP refer to *Commands Reference Manual*.

Note: MAP is a trademark of Nortel (Northern Telecom).

In addition,the DISPLAY PHONE terminal (F5439) receives full MAP support. The difference between the standard MAP position and the DISPLAYPHONE terminal is the line editing control function. The user implements the line editing control function with the cursor movement keys and the control key sequences as follows:

Table 2-1 (Sheet 1 of 2)

Down Arrow	Refreshes the input line.
Up Arrow	Allows character insertion at the cursor position.
Right Arrow	Advances the cursor one character position to the right for each depression. The cursor advances until the cursor reaches the end of the current input line.
Left Arrow	Backs up the cursor one character position to the left for each depression. The cursor backs up to the beginning of the input line.
CONTROL U	This key sequence causes the system to delete the contents of the input line (refer to Note).
CONTROL E	This key sequence causes the system to delete the input line. The sequence deletes the input from the current cursor position to the end of the input line (refer to Note).

Table 2-1 (Sheet 2 of 2)

CONTROL X	This key sequence turns off the result of the Up Arrow (refer to Note).
?	Retrieves the previous input line. The DMS remembers the current line and the two previous lines.

Note: The key sequence, CONTROL , means that the user presses and holds the Control key while the user enters the character.

A printer is an IOD. A printer provides printed copies of reports and can be used for MMI. Magnetic tape and disk recording devices are IODS that store and retrieve data.

Input/Output Controller

The Input/Output Controller (IOC) is the hardware entity that provides the interface between the Central Control Complex (CCC) and the IOD (refer to Figure 2-1). The CCC side of the IOC connects through a pair of 32-channel, 2.56 Mb/s serial data links (designated DS30), to the Central Message Controllers (CMC) and to the Central Processing Units (CPU) in the CCC.

Each CMC has 70 serial data ports to which the DS30 data links are assigned in pairs. Some of these ports are assigned to the IOC. Other ports are assigned to the network message controllers (NMC) in the two planes of the switching network.

Offices with BCS16 and higher software can have a maximum of 12 pairs of ports. These ports are assigned to links to a maximum of 12 IOCs (0 to 11). In this configuration, the number of pairs of ports available for assignment to NMC reduces to a maximum of. If less than 12 IOCs are required, the number of ports available for assignment to NMC increases.

Data in the peripheral equipment assignment tables controls CMC port assignments to IOC and NMC. The format of the maintenance displays on the MAP depends on which BCS or Base release number is in effect. The format of the maintenance display shows the status of the IOC units.

The other side of the IOC provides common parallel data and address buses. Up to nine (numbered 0 to 8) Device Controllers (DC) connect to these address buses and common parallel data. The I/O message controller handles the flow of data and routes the data to the addressed DC.

The I/O message controller and the DC are circuit cards that plug in to the backplane of the IOC shelf. Single-bay I/O equipment (IOE) frames contain the IOC shelves. For more details of the IOC, refer to *Hardware Description Manual*.

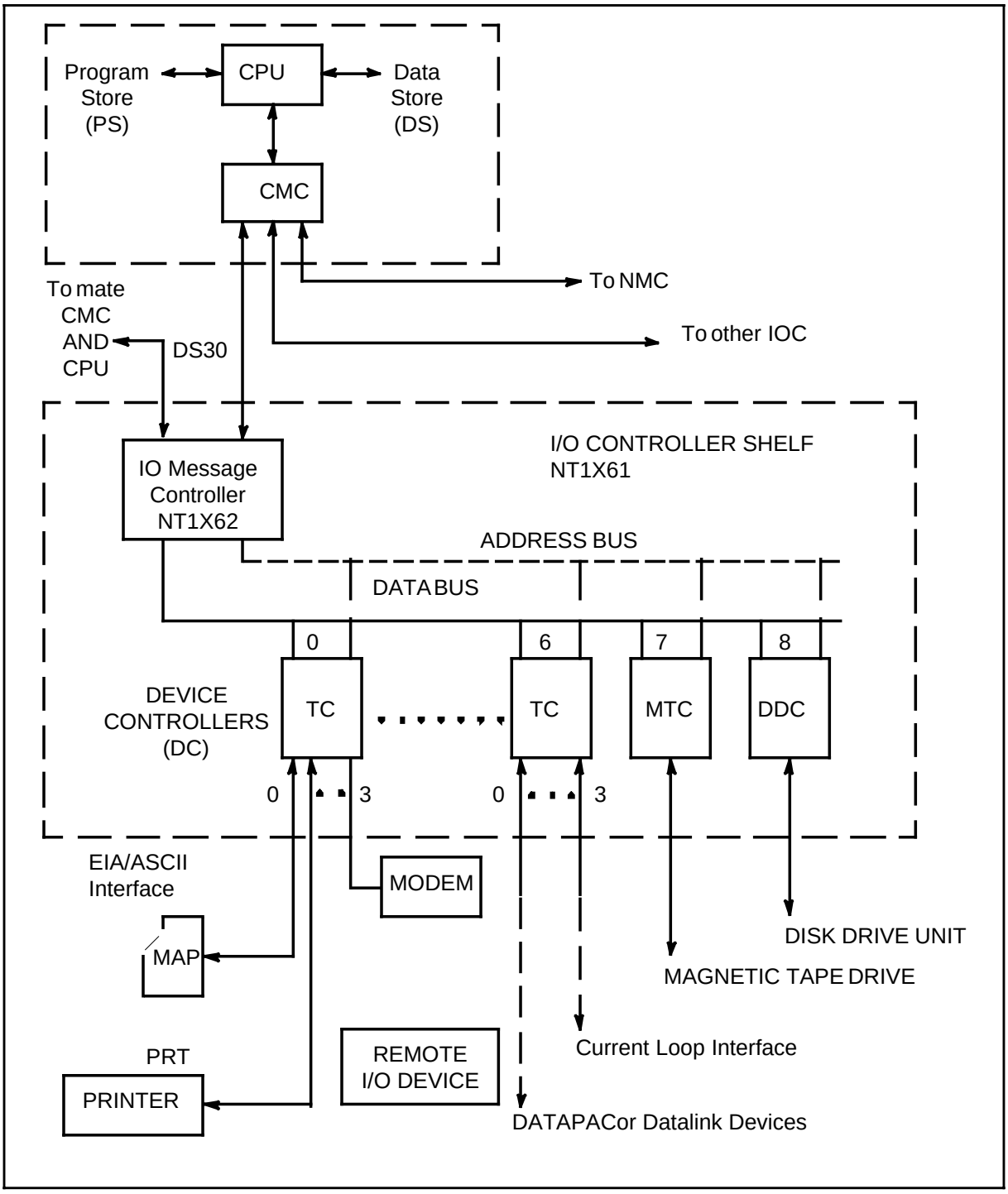
Device Controllers

The DC converts the characteristics of the IODs to the common data bus format in the IOC. This process requires three types of DC circuit cards. The number of DCs that the process uses depends on the number of IOCs in service. The number of DCs also depends on the number of IODs in use. Part of the office engineering process provisions the DC circuit cards. The applications of the three DC types are as follows:

- Disk Drive Controller (DDC). The DDC interfaces the Disk Drive Unit (DDU) with the IOC data bus. The DDC allows commands input at the MAP to control the DDU. The DDC provides read/write facilities for

retrieval and storage of data on magnetic disks. For details of the DDU, refer to *Hardware Description Manual*.

Figure 2-1 Relationship of DMS-100 Family System to I/O Devices



- Magnetic Tape Controller (MTC). The MTC interfaces the Magnetic Tape Drive (MTD) with the IOC data bus. The MTC allows commands input at the MAP to control the MTD. The MTC provides read/write facilities for retrieval and storage of data on magnetic tapes. Refer to GS1X68 for details of the MTC.
- Terminal Controller (TC). The TC are circuit cards with many purposes. The TC can interface up to four IODs per card with the IOC data bus. The IODS connect to four ports. The user can set the configurations of these ports to match the characteristics of the IOD that connect to that port. Refer to GS1X67 for more details of the TC. Port configurations can be programmed. Entries in table TERMDEV can set the port configurations to one of the following:
  - — The EIA/ASCII for an IOD (MAP or PRT) within 50 ft (15m) of the IOE frame. The EIA/ASCII also connects to a modem for operation with remote devices.
  - — Current Loop for IOD within 1200 ft (366m) of the IOE frame.

Data the user enters in the IOD table assigns the correct DC for each IOD. Other characteristics like baud rate and port configuration are also assigned in these tables.

The I/O devices and their associated data tables are as follows:

- Magnetic Tape Drives - table MTD
- Disk Drive Units - table DDU
- Visual Display Unit - (part of MAP), printers (PRT), or modem to a remote PRT - table TERMDEV
- DATAPAC - table DPACDEV
- Data Link Controller - DLCDEV.

Note: The DATAPAC is a trademark of Bell Canada

IO User Classes

The I/O users must organize into classes that define a set of functions that these users must perform. These operating requirements dictate the IOD requirements for each user class. The arrangement of I/O user classes is flexible to meet operating company operational requirements. This arrangement makes sure the division of tasks serves the purpose of each user class. In addition, this arrangement makes sure the division of tasks does not interfere with the functions of other users.

The selection of the type and quantity of IOD for each user class function depends on operating company requirements. The selection forms part of the office engineering process. Refer to Information on the *Provisioning Guide*.

Names and descriptions for some I/O user classes are as follows:

- Administration (ADMIN): provides the user with access that is not limited, from any IOD to all command classes (refer to PRIVCLAS). ADMIN has the highest priority level (refer to PERMIT). The password that associates with ADMIN is not displayed. Other users cannot change the password (refer to COMMAND SCREENING).
- Switch Maintenance (SMtc): allows the user to maintain the DMS switch. SMtc performs maintenance and corrects faults for the following:
  - — Central Control (CC)
  - — Central Message Controller (CMC)
  - — Input/Output Devices (IOD)
  - — Network Modules (NM)
  - — Peripheral Modules (PM)

The SMtc user also can perform database modifications to administer the switch, monitor the switch status, run diagnostic programs and replace equipment. The user can execute all input commands that associate with the Table Editor and the Support Operating System (SOS).

Trunk Maintenance (TMtc):

The TMtc permits the user to perform maintenance and correct faults for trunk circuits and trunk facilities. The user monitors the trunk status, runs diagnostic programs and performs hardware tests.

The TMtc user has access to the collection of input commands available to this user class only. Only commands that apply to testing and maintenance of trunks and trunk facilities are permitted. This user has access to the Table Editor set of commands but cannot manipulate tables. A *Trucks Maintenance Guide* performs the TMtc functions.

Network Management (NWM):

The NWM allows the user to make use of available facilities and equipment. The user applies routing controls over traffic-oriented switch resources. The user monitors traffic levels, applies manual controls, adjusts automatic controls and receives traffic reports.

This user class can execute input commands assigned to the user class. The user has data table query abilities, but cannot make changes to some data tables.

Dial Administration (DAdm):

DAdm allows the user to monitor traffic reports and operational measurements (OM) of the switching unit. The user can alter OM scheduling, assignments and thresholds.

This user class can execute commands that are assigned to the user class only. The DAdm user can access the Table Editor collection of commands when the user alters data that associates with OM. In addition, the user has full data table query abilities. These abilities include traffic register assignment and readings.

Service Analysis (SA):

The SA allows the user to monitor customer dialed and operator assisted toll calls at random. The user can monitor these calls for information on the quality of service the operating company equipment and personnel provide.

This user class can execute commands assigned to the user class only. The SA user can access the Table Editor set of commands. The SA user is screened based on tables, to control changes to data tables that associate with this class only.

Technical Assistance Center (TAC):

The TAC allows the user to monitor switching units that are not attended and to provide technical help to switching center personnel. The TAC is a central operating company plant maintenance group.

This user class can execute all the input commands that apply to Switch Maintenance.

Emergency Technical Assistance Service (ETAS):

The ETAS provides help to Switch Maintenance or TAC personnel when personnel cannot correct switching problems. Northern Telecom provides the ETAS service.

The ETAS users have a user class of ALL. The ETAS users can perform operations to help TAC personnel.

Line Maintenance (LMtc):

The LMtc allows the user to perform the following:

- monitor the status of line cards
- run diagnostics on line cards
- sectionalize troubles
- test and diagnose problems within the office

- query and change subscriber data
- schedule automatic line card diagnostics

Repair Service Bureau (RSB):

The RSB allows the user to perform the following:

- sectionalize troubles
- test and diagnose facility troubles
- schedule Automatic Line Insulation Testing (ALIT)
- receive ALIT outputs
- query or change subscriber data

Traffic Administration (TA):

The TA allows the user to receive automatic periodic summary reports of traffic statistics the switching system accumulates. These reports reflect traffic peg counts, overflow, use of the switching unit and Operational Measurements. The TA user can modify the schedule and output of these reports.

International Switch Maintenance Center (ISMC):

The ISMC allows the user to maintain the switch. The user performs maintenance and corrects faults for most subsystems. The ISMC function is like the function of the Switch Maintenance user class and is for DMS-300 International offices only.

International Transmission Maintenance Center (ITMC):

ITMC allows the user to perform maintenance fault correction for the Trunks Subsystem and trunk facilities. The ITMC function is like the function of the Trunk Maintenance user class but, for DMS-300 offices only.

International Service Coordination Center (ISCC):

The ISCC allows the user to monitor the quality of service the operating company personnel and equipment provide. The ISCC function is like the Service Analysis user class and is for DMS-300 offices only.

Network Management Control (NWC):

The NWC allows the user to make use of available facilities and equipment. The user applies routing controls over traffic-oriented switch resources. The user monitors traffic levels, applies manual controls, adjusts automatic controls and receives traffic reports. The NWC function is like the NWM user class and is for DMS-300 offices only.

3 Input Control Software

Input control software, in the CCC, performs the following functions:

- passwords and user identifications control security and access
- assignment of selected commands to classes of I/O users, appropriate to the tasks screens commands
- optional software packages implements special input control features

Remote Access Security Control

The presence and state of activation of Automatic Dialback Feature (part of NTX293) determine the security methods that control Remote Access to the I/O system. Figure 3-1 illustrates the differences.

Automatic Dialback Active

The MODEM_DIALBACK_CONTROL field in OFCO3-1M, 3-1M, PT controls the application of the Automatic Dialback feature. Set this field to Y (yes) at the time of office entry to activate the feature. The operating company cannot change this field when the field is set.

When a remote user logs in, the system initiates a request for dialback ID and password. The system disconnects the modem and attempts a callback to the remote user. The elapsed time between the modem disconnect and the completion of the return call can vary from 40 s to 120 s. The length of the directory number and the type of the modem used for the callback determine the time elapsed.

If the callback is successful, the user must logon again. The user must not use the BREAK key at this time. Access to the I/O system and access for an onsite user are the same. The state of activation of the Enhanced Security Feature determines the final logon requirements.

Security and Access Control

Security involves the use of passwords to make sure that only authorized users have access to the I/O system. The presence and state of activation of the *Enhanced Security Package* determine the methods used to control the validity

and assignments of passwords. Figure 3-1 illustrates the remote access control. Figure 3-2 illustrates the onsite security and access control scheme.

Enhanced Security Active

The ENHANCED_PASSWORD_CONTROL field in OFCOPT controls the application of the enhanced security feature. Set this field to TRUE at the time of office entry to activate the feature. The operating company cannot change this field when the field is set.

The system compares the password the user enters at a terminal (IOD) with entries in OFCENG. The system takes this action to make sure the password complies with the following:

- minimum password length
- password lifetime (not expired)
- expired password grace

If the password grace expires, the grace period before password renewal is not exceeded. Use the PASSWORD command to make changes.

The Enhanced Security Package includes the LOGINCONTROL command. The LOGINCONTROL command is active when the user sets the ENHANCED_ACCESS_CONTROL field in OFCOPT to TRUE at the time of office entry. LOGINCONTROL sets the conditions for designated terminals to logon. Terminals can be allowed or disabled manually or automatically for specified periods of time or indefinitely.

When a logon attempt meets all the enhanced security package standards, the system gives access to the command interpreter (CI) level. The system records problems with security standards and automatic allowing or disabling in the security (SECU) log subsystem. The SECU logs are SECRET (refer to SECRET LOGS). The system only displays the SECU logs to users with authorization to use the OPENSECRET command.

Enhanced Security Inactive.

When the user sets ENHANCED_PASSWORD_CONTROL field (OFCOPT) to FALSE, the enhanced password control feature is not present. The enhanced password control feature includes the PASSWORD command and associated parameters in OFCENG. The ENHANCED_ACCESS_CONTROL field (OFCOPT) is set to FALSE. The LOGINCONTROL command is not present. Set these fields to FALSE at the time of office entry. The user cannot change these fields without the permission of Northern Telecom personnel.

The LOGIN scheme that is not enhanced is active. Refer to Figure 3-1, "Remote Access Security Control" on page 3-4. Enter the user name and password at the terminal for the LOGIN scheme that is not enhanced. Security

consists of an automatic check to make sure that the user name and password are valid. If valid, the CI level receives access.

Automatic Log-in.

The AUTOLOG-IN feature allows permanent users which use a terminal or users which use the terminal often, to logon quickly. This user does not need to enter a password. The AUTOLOGIN is applied to a terminal when the device name in the TERMDES field of Table TERMDEV matches the user name. (Refer to PERMIT). When the user enters the user name, the terminal logs in. For security, AUTOLOGIN is assigned to local terminals, not to dial-up or remote terminals. The operating company must make sure the device names at terminals that are not local, do not match valid user names. If a match occurs, an AUTOLOGIN that is not authorized can result.

Automatic Logout

The AUTOLOGOUT feature increases security. This feature automatically logs out idle logged-on terminals, after a preset period of time that the terminal is idle. This action reduces the risk that users which are not authorized misuse terminals that are logged-on and not attended.

The AUTOLOGOUT is active when the user sets the AUTO_LOGOUT field in Table OFCOPT to TRUE. To set the idle period for each terminal device, enter the time (in minutes) into the IDLE-TIMEOUT field of Table TERMDEV. If the user enters zero minutes against a terminal, AUTOLOGOUT does not affect that terminal. The minimum period at any other time is five min.

The AUTOLOGOUT is inactive for all terminals when the user sets the AUTO_LOGOUT field to FALSE.

Figure 3-1 Remote Access Security Control

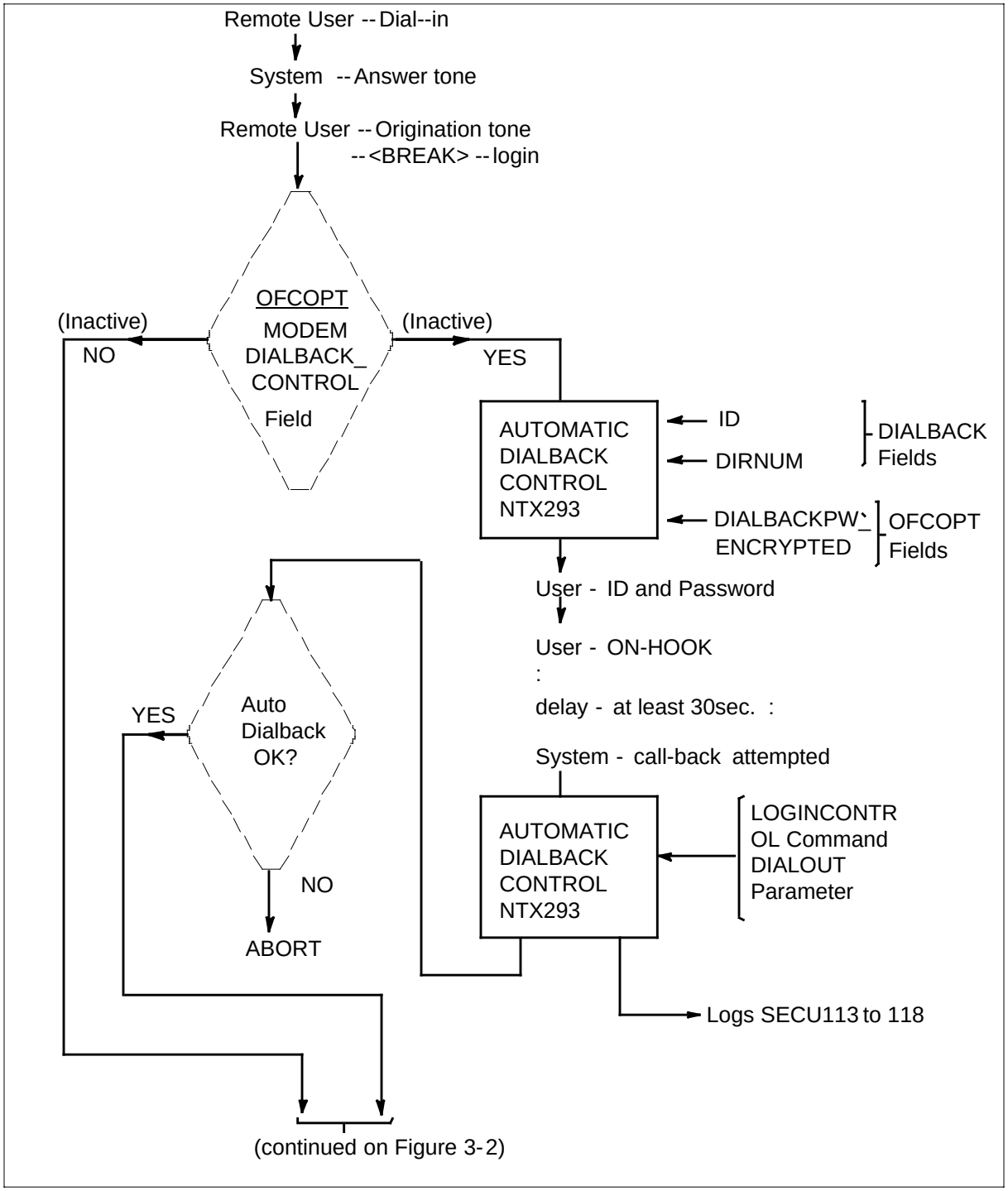
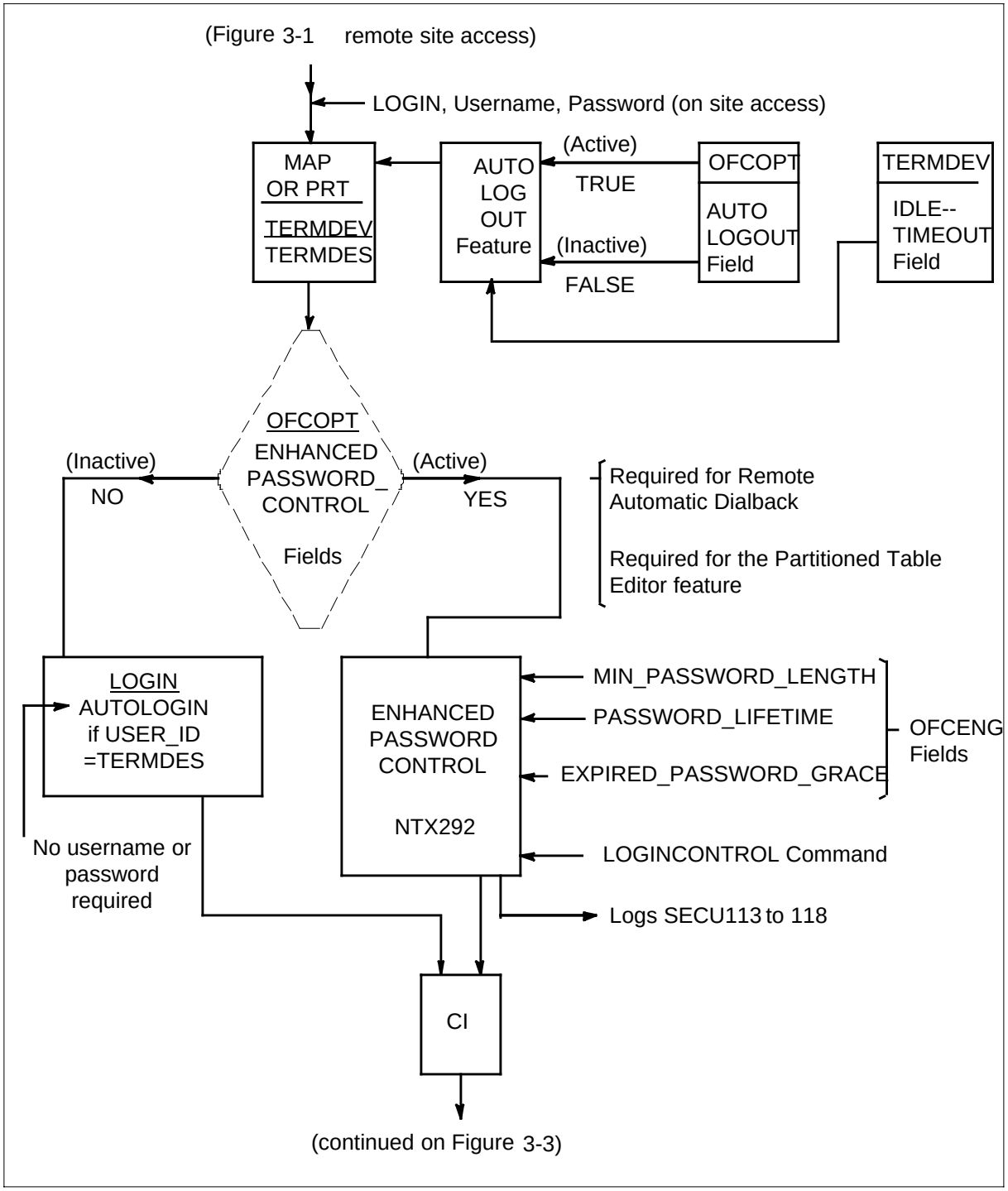


Figure 3-2 Remote Access Security Control



Command Screening

Command screening makes sure that terminals are used for their assigned tasks only. For example, a terminal assigned to service orders does not need access to commands that a network management terminal uses. Refer to Section , "Input/Output Controller" on page 2-2 , which describes the division of tasks between groups of users.

Each command is associated with one of 31 command class numbers. These numbers range from 0 to 30. The operating company management uses the PRIVCLAS command to assign this number. The management assigns the command class number to users and terminals through the PERMIT command. The user enters the acceptable command class numbers for each terminal in the COMCLASS field of Table TERMDEV. The SHOW USERS command displays the command class numbers.

The effective command class of a user is the intersection of the command class of the user and of the terminal. The PERMIT command sets the command class of the user. The field COMCLASS in Table TERMDEV determines the command class of the terminal. If the effective command class is empty, the user cannot logon to the terminal. You cannot perform commands when logged on to the terminal.

The command classes of users and terminals can be set to allow users to logon but not logoff. Users cannot logoff because the effective command class of the users does not permit this action. These users must be logged off by a user like ADMIN. The ADMIN user can use the FORCE logoff command to force the user to logoff. Provide all users and terminals with the command class of the logoff command to avoid this condition.

The result is to make sure that only authorized users can use designated classes of commands on designated terminals. Commands without assigned class numbers do not have restrictions. The user can enter changes to command class assignments at any time. These changes can take effect immediately. The response to PRIVCLAS acknowledges these changes. The changes are stored until a restart occurs. Examples of restarts include warm, reload, or cold. After a restart occurs, changes are implemented.

The use of command screening depends on the Enhanced Security Package (NTX292) software. The presence of software and the state of activation of enhanced command screening feature determines command screening. (Refer to Figure 3-3, "Command Screening Scheme" on page 3-8)

Enhanced Command Screening Active

The ENHANCED_COMMAND_SCREENING field in Table OFCOPT controls the application of this feature. When active, this field is set to TRUE at the time of office entry. The operating company cannot change this field

when the field is set. The result on the command screening scheme is as follows:

- PRIVCLAS - can assign up to 31 class numbers for each command
- PERMIT - cannot change passwords, but can create new passwords
- PASSWORD - can change passwords

Enhanced Command Screening Inactive

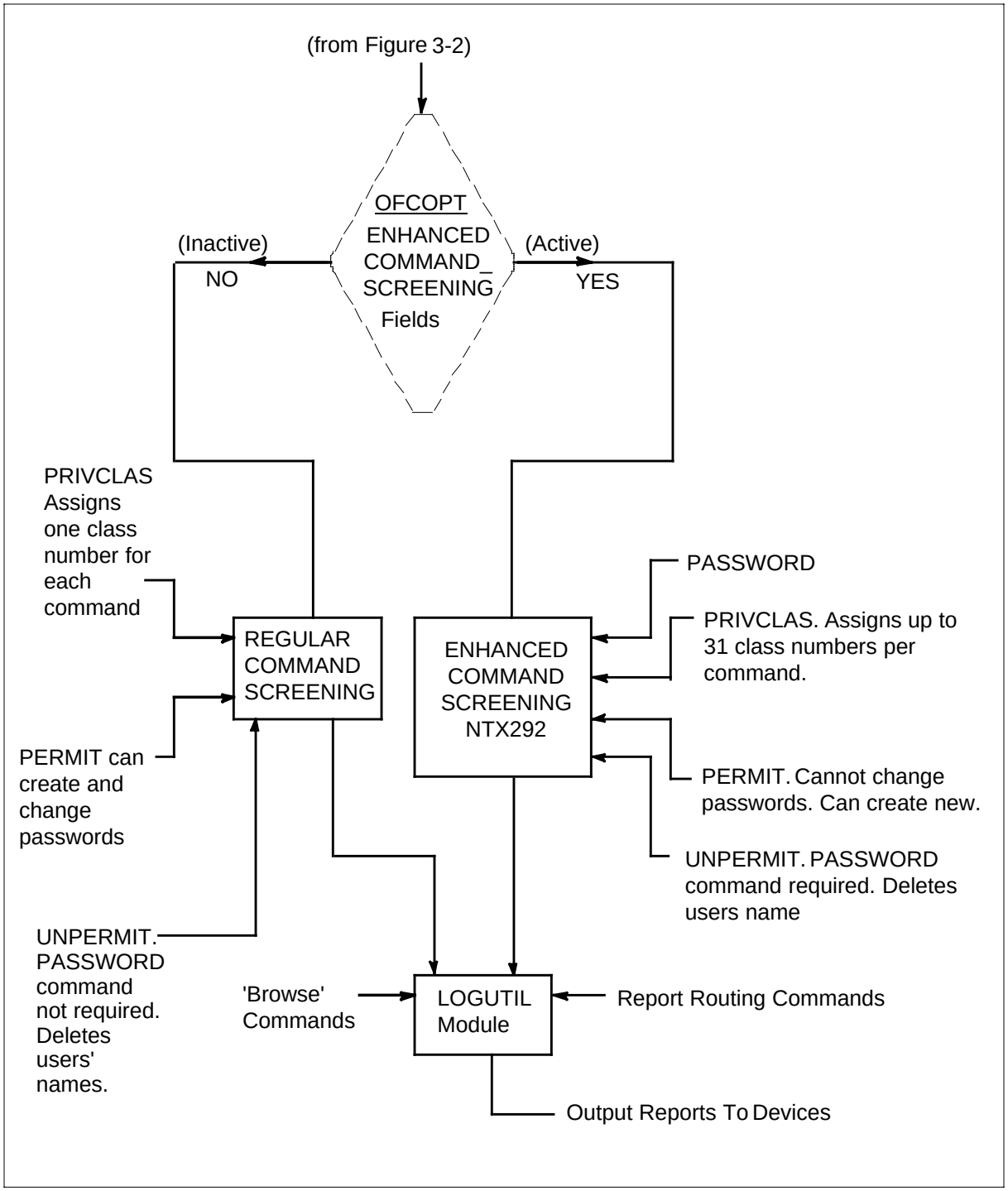
When the ENHANCED_COMMAND_SCREENING field is set to FALSE, the enhanced command screening feature is inactive. Normal command screening is active. The purpose of command screening is the same, but the following affect its use:

- PRIVCLAS - can only assign one class number for each command
- PERMIT - can change passwords and create new passwords
- PASSWORD - is not present

ADMIN User

The user class ADMIN is not subject to command screening. The user class ADMIN has access through any terminal and can use any command. The system only displays the password assigned to ADMIN (refer to PERMIT) to the ADMIN user. Only the ADMIN user can change the password. The ADMIN use must change the ADMIN password from time to time. Change the ADMIN password after a new Base release is loaded. Representatives of two different management functions must verify, record, and store the ADMIN password.

Figure 3-3 Command Screening Scheme



Show-Password Feature

The Show-Password (SHOWPW) feature allows any user to obtain a display of the current password of the name of this user. The user obtains this display through PASSWORD or PERMIT commands. The SHOWPW is available when the PASSWORD_ENCRYPTED field in Table OFCOPT is set to FALSE. If the SHOWPW feature is not available, the PASSWORD_ENCRYPTED field is set to TRUE. Only the ADMIN user can obtain a display of passwords of other users. The PASSWORD_ENCRYPTED field is set at the time of office entry. The operating company can not change this field when the field is set. The operating company can only change the field with permission from Northern Telecom. The SHOWPW does not depend on the presence of any other features.

Dumpsafe State

Command screening restricts the entry of commands that overwrite and change protected data store during office image production (DUMP). The system designates commands the user can enter as DUMPSAFE. The system designates commands the user cannot enter as DUMPUNSAFE.

The PRIVCLAS command, with parameters DUMPSAFE or DUMPUNSAFE, sets the DUMPSAFE state for each command. The operating company defines the DUMPSAFE states before the office goes into service. The user cannot execute a DUMPUNSAFE command when DUMP is in progress.

If an office has ENHANCED_COMMAND_SCREENING feature active, the DUMPSAFE states of all commands are in Table CMDS. In any other condition, datafill PRIVCLAS ALL for a display of commands or modules (increments) and the DUMPSAFE states of the commands or modules.

Priority Map Terminal

The priority MAP terminal feature is part of Feature Package NTX001. The priority MAP feature allows the ADMIN class user to use the ADMIN password to LOGON at any authorized MAP. This feature allows improved terminal response. This feature performs diagnostic procedures and corrective procedures. This feature performs these procedures when a high call processing occupancy of 60 percent or more can reduce terminal response time.

Chapter 4, "Output Control Software" on page -1 describes guaranteed background scheduling for up to six other tasks.

4 Output Control Software

Output control software operates through the log utility module (LOGUTIL). The LOGUTIL provides the mechanism for the implementation of the log system commands. These commands perform the following functions:

- Routes reports to selected Input/Output Devices (IODs). This function overrides the permanent assignments in the data tables LOGCLASS and LOGDEV for a short time.
- Interrogates and searches all reports in the log subsystems.
- Enable operating company personnel to add, change or delete reports. Enable operating company personnel to apply threshold values to limit how the system outputs reports.

In addition to LOGUTIL, there are a number of optional software packages present that can apply Special logging features.

Log System Interface

Separate DMS subsystem software creates output reports. The LOGS file is a history file that receives output reports. The LOG system stores this report information in a log buffer for the specified subsystem. The system can also forward the output report to an output device. The report routing subsystem controls the how the system routes reports. The *Log Report Reference Manual* contains a list and descriptions of current log reports.

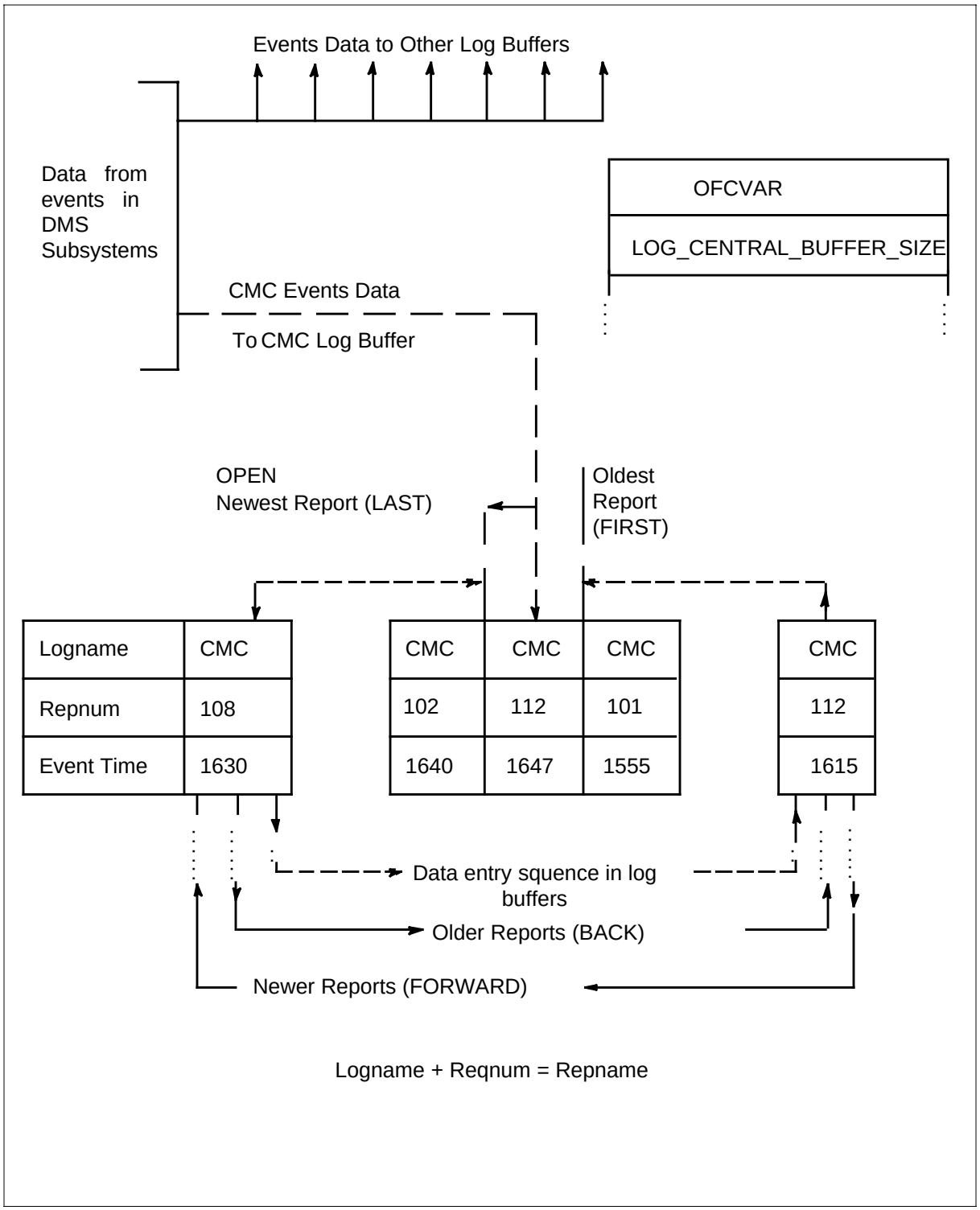
The log buffers are large enough to hold several hours of subsystem reports at peak output rates. The value of office parameter LOG_CENTRAL_BUFFER_SIZE in table OFCVAR (default value = 2000) determines the number of reports that the buffers can hold.

Figure 4-1, "Schematic Image of Normal Log Buffer" on page 4-3, is a schematic design of a normal log buffer. The example describes the log buffer that stores data from events in the CMC subsystem.

Each type of event in a log subsystem has a report number (REPNUM). The REPNAME consists of LOGNAME and REPNUM (example: CMC112). The

REPNAME identifies reports in the log system. Reports are entered in the order in which the system generates the reports.

Figure 4-1 Schematic Image of Normal Log Buffer



In the example, the system generates report CMC112. The report is entered in the CMC log buffer at event time 1647 hours. The CMC log buffer also contains older reports that occur at different times to a maximum of 1555 hours. A report at 1555 hours is the oldest log for which the buffer has space. The buffer in this example contains a previous CMC112 report that occurred at 1615 hours. The user can use the appropriate commands to select one of the two CMC112 reports to display. The user can use commands to browse through a selected log subsystem buffer to examine the contents of a report.

When a subsystem buffer is full, the next report that the system generates displaces the oldest report. In the example, the next report after 1647 hours is entered in the buffer location that contains report CMC101 (1555 hours). The system replaces and loses report CMC10 if itdoes not route the report to a data storage device. If the system routes this report to a data storage device, the system retains the report.

As the system generates reports, the 1647 CMC112 report becomes older until 1647 CMC112 becomes the oldest report. The newest report replaces the oldest report. The actions that occur in the other log buffers are like the actions that occur here.

Several commands (browse commands) allow operating company personnel to interrogate the contents and details the of the reports in the log buffers. The functions of these commands include:

- selection of a specified log subsystem (OPEN) for display
- display of the newest or oldest report (LAST, FIRST)
- display of the newer (BACK) or older (FORWARD) entries in a log buffer
- deletion of the reports in a specified log buffer (CLEAR)
- display of the log names defined in the LOG system (LISTREPS) and
- selection of the normal or an abbreviated form of a report for display (FORMAT).

SYSLOG

The SYSLOG feature allows the operating company to designate log reports for recovery after the system performs an office reload. The designated reports are written into the SYSLOG buffer and the LOGUTIL buffer. If a reload occurs, the LOGUTIL buffers are overwritten. The designated reports remain in SYSLOG.

The log reports in SYSLOG, and the SWERR and TRAP logs contain information about the state of the system before the last reload. This information is a problem solving aid if a problem occurs after reload.

The user enters the LOGUTIL command and the OPEN SYSLOG command to activate SYSLOG. After entering the OPEN SYSLOG command the reports can be displayed by using the FIRST, LAST, BACK, FORWARD or TYPE commands. If SYSLOG contains a SECRET logname, only the non-secret lognames are displayed. SECRET lognames are accessabile only to those authorized to use the OPENSECRET command. More information on these commands can be found in Chapter 5, Man-Machine Interface, of this publication.

Critical Message Prioritization

The LOG_PRIORITIZATION field in OFCOPT controls the activation of this feature. The feature is active when this field is set to Y. The feature is not active when the field is set to N.

This feature provides an additional method to set the order in which the system outputs log reports to a specified log device. When this feature is not active (N), normal log operation is in effect. The system stores reports in order in log buffers. Figure 4-1, "Schematic Image of Normal Log Buffer" on page 4-3 illustrates the storage process.

When the feature is active (Y), four log prioritization buffers are present, in addition to the normal log buffers. Each buffer represents one of the log alarm levels. Alarm levels are critical, major, minor, and no alarm. Alarm level also categorizes reports. The system stores reports in the correct buffer in order.

To apply the feature to specified log devices, table LOGDEV contains an additional field called PRIORITY. This field is present when the feature is active. When this field contains Y on the same line as a device that the DEV field indicates, the log prioritization buffers sends reports to the device. The buffers send the reports with the highest alarm level first. The system outputs reports with the same alarm level in order from the correct buffer. A device that DEV field indicates, that has N on the same line in the PRIORITY field, outputs reports in normal order.

Current log reports in the normal and prioritization buffers, that have associated alarm levels, are copied into a special log buffer. The special log buffer is SAVLOG. The result of the SAVLOG command is the system saves the critical data that contains the alarm level information. The system saves this information during a restart. The system preserves this information through the restart until three min after restart occurs.

Guaranteed Background Schedule

Of the many tasks performed in the system, some are grouped as background tasks. These tasks include terminal functions, control of logs, system audits, maintenance audits, and MAP control. The creation of groups of background

processes causes increased delay in terminal response under heavy load conditions.

This feature (part of NXT000) allows some tasks to have a number limit so that specified tasks run more than other tasks.

The operating company uses parameter GUAR in tables TERMDEV and LOGDEV to assign tasks that must be guaranteed. These tasks can be one of the following:

- Network Management MAP or Port
- Switching Control Center System (SCCS) MAP
- Local MAP
- Service Analysis (SA) Position or interface
- ETAS reserved device
- Log device

Secret Logs

A SECRET log is a type of log that a user cannot access through the OPEN command. The user must use a separate OPENSECRET command to access a SECRET log. Command classes like ADMIN can use the OPENSECRET log. Privileged classes that the PRIVCLAS command defines and the CMDS table contains, can use the PRIVCLASS command.

The purpose of the SECRET log is to keep track of security-related events. The SECRET log tracks security-realated events while the log makes sure that only authorized users view these occurrences. These events are entered in the security series of logs, (SECU) and (TABL). These logs provide reports on the items that follow:

- Valid use of LOGIN and LOGOUT (SECU101, SECU109).
- Invalid LOGIN attempts, like not correct or expired password, or not authorized user class (SECU102, SECU110).
- Forceout of users (SECU103).
- Change of password (SECU105).
- Addition of a user_name with the PERMIT command. This command identifies new user_name (SECU112).
- Use of PRIVCLAS command to change the parameters for a command_name. A change in the way the system logs command use/abuse (SECU111, SECU104).
- Privilege problem (not correct privilege class) when the user uses commands (SECU107,108).

- Valid use of commands (SECU106).
- Authorized user accesses a table, reads and displays the first horizontal row of the table (TABL100).
- Authorized user accesses a table and writes to a horizontal row of the table (TABL101).
- Not authorized user attempts access to a table (TABL102).
- Not authorized user accesses a table and writes to a horizontal row of the table (TABL103).

The system cannot print SECRET logs on any device. The user can access SECRET logs through the use of the OPENSECRET command. An authorized OPENSECRET user can use the LOGUTIL commands, except CLEAR and SUPPRESS, to display SECRET logs on the MAP display.

A user that is not authorized cannot view SECRET logs. Each report can have an associated alarm of a specified level. Entries in table AUDALARM associate the alarm level with a specified SECRET LOGNAME and REPNUM.

The system prints not secret log reports (EXT series) on the device of the user. The system prints the reports to notify a user, not authorized to see SECRET logs, of an associated alarm. The EXT report only records the occurrence of a SECRET log message and alarm. The EXT report does not contain additional information about the cause of the alarm.

The system outputs log EXT 106 for minor SECRET alarms, EXT 107 for major alarms, and EXT 108 for critical alarms. When the authorized user receives one of the logs, the user can use the OPENSECRET command. The OPENSECRET command allows the user to view the contents of the SECRET log, and the cause of the alarm.

Report Routing

The routing and reporting subsystem routes reports from the log system buffers to an IOD. The system prints, displays, and stores reports at the IOD. Three data tables and LOGUTIL control commands control this subsystem. These data tables provide basic permanent routing. The LOGUTIL commands can change basic routing for a short time.

Basic Permanent Routing

Entries in data tables LOGCLASS, LOGDEV, and TERMDEV establish basic routing. Figure 4-2, "Report Routing Scheme" on page 4-11 describes how the fields in these tables interact. Figure 4-2 describes the relationship of the fields to the I/O hardware. These tables have several other fields that do not connect to basic report routing. Basic routing can change through the Table Editor only.

LOGCLASS.

Every log report that the system can generate has a report class number. For example, in Figure 4-1, "Schematic Image of Normal Log Buffer.", you enter log report CMC112 in the REPNAME field. On the same line, you enter report class number 7 under CLASS field. All other reports in the log system are assigned report class numbers in the same way.

The assigned function of the IOD normally governs the assignment of output report classes. The use of report classes to classify output reports prevents conflict between different operating groups within an operating company. These operating groups have different responsibilities in the operating company organization. Consult the representatives of all operating groups to make sure that the assignment of report classes meets the requirements of each group.

The operating company gives the assignment of reports to classes to Northern Telecom. Northern Telecom enters data through input forms 2320, the Log Device Table Record, and 2321, the Log Class Table Record.

LOGDEV

Every IOD that connects to the IOC is entered in the DEV field. Every IOD is entered to indicate availability for use as a primary IOD. The field ALT contains the names of IODs available for backup use if the primary device is not in service. In the example, PRT1 is assigned to primary service and PRT2 to backup. On the same line, the report class number 7 (assigned in LOGCLASS) is entered in the CLASSES field. When a report with class number 7 (like CMC112) is output, the system routes the report to PRT1 under normal conditions. The system routes the report to PRT2 under backup conditions. The number of reports a device must handle can be very large. The office parameter LOG_DEVICE_BUFFER_SIZE in table OFCVAR can change to accommodate the larger number of reports.

TERMDEV

The names of all the IOD that connect to the DMS-100 system are entered in the TERMDES field. The IOCNO and the IOCKTNO that control the device are entered on the same line, against each device name. The IOC-0 and IOCKT 20 and 21 control PRT1 and PRT2. Through this mechanism, log report CMC112 emerges on the assigned printer PRT1. Other IODs, for example, the MAP and MTD are assigned to associated IOC circuits through entries in this table.

Temporary Routing Commands

The system makes temporary routing changes through the routing commands. These commands override the permanent entries in LOGCLASS and TERMDEV that control routing. The routing commands do not change the permanent entries. The permanent entries remain available for a return to permanent routing. The user can use the RESETROUTE command to restore

permanent routing. A system restart can restore permanent routing. The routing commands, and the entries these commands affect are as follows (Refer to Figure 4-2):

- ADDREP - adds more reports to the reports that the system has routed to a specified IOD.
- DELREP - deletes reports that the system has routed to a specified IOD.
- ADDCLASS - adds more report classes to the reports assigned to a specified IOD.
- DELCLASS - deletes report classes from the reports assigned to a specified IOD.
- CLASS - sets class numbers for selected reports.
- DELDEVICE - deletes a specified IOD from use in the log system.
- REROUTE - reroutes all reports assigned to specified primary IOD, to their backup devices. For example, if the user enters REROUTE PRT1 report CMC112 prints on PRT2 and not PRT1.
- RESETROUTE - deletes all temporary routing and returns to the permanent routing data in the LOGCLASS and LOGDEV tables.

Report Thresholding

Thresholding controls the quantity of reports sent to an IOD. Entries in office parameter table OFCVAR set the basic permanent values that select the type of thresholding. Entries in parameter table OFCVAR set the type of reports that are not printed. The OFCVAR table sets the basic parameter values as follows.

Thresholding Types

The two types of thresholds that can apply to the printing of reports are high water mark and sampling. The THRESHOLD_IS_SAMPLING field in table OFCVAR selects the threshold types as follows:

- High Water Mark Active when THRESHOLD_IS_SAMPLING is set to N. When the threshold value is reached, the system prints all instances of specified reports that occur after the threshold is reached. For example, if the threshold number is 5, only the 6th, 7th, 8th...reports are printed by the system.
- Sampling Active when THRESHOLD_IS_SAMPLING is set to Y. When the threshold value is reached, the system prints the specified report. The count returns to zero and starts again. For example if the threshold number is 5, then the system prints the 5th, 10th, 15th... reports.

Threshold Values.

The threshold values that apply to high water mark and sampling purposes are set in the THRESHOLD and TUNITS field of table LOGCLASS. These settings produce the following effects:

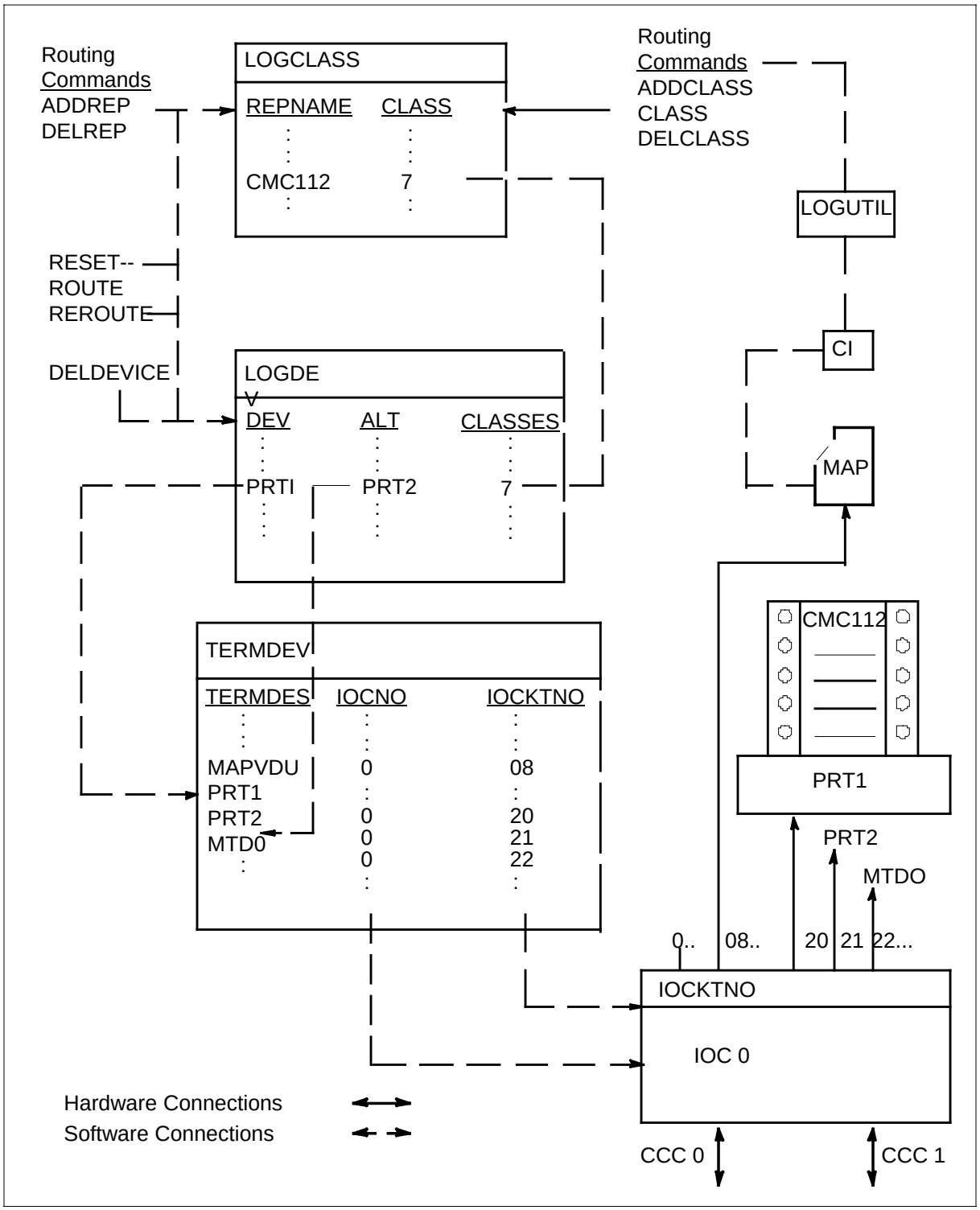
- The THRESHOLD field is the count number that provides the threshold value. This value controls the quantity of reports the system does not print. The examples in the previous description specify a value of 5. The full range of values is 0 to 255.
- The TUNITS field is the time in minutes that determines when the THRESHOLD counter must be reset to zero. The timing period can indicate if the rate of report generation is too high. For example, assume that TUNITS is specified as 15 min and the threshold is a high water mark with a THRESHOLD value of 5. If more than five reports are received in 15 min, the system prints all future instances of the specified report. If less than five reports are received, the system does not output reports during the 15 period. If TUNITS is set to zero, the number of reports does not affect the THRESHOLD counter. The THRESHOLD counter resets when the number of reports reaches the set count number.

The THRESHOLD and TUNITS values are applied to separate reports through the entry of the values on the same line. The values are entered opposite the report name under the REPNAME field. The Table Editor can change values.

Disposition of Unprinted Thresholded Reports.

The system can keep or discard reports that the system does not print because of thresholding action. The system keeps the reports in the log buffer. The BUFFER_THRESHOLDED_REPORTS field in table OFCVAR controls the condition of thresholded logs. If this field contains Y, the system retains the thresholded reports in the log buffer. The user can access the reports through the LOGUTIL commands. If this field contains N, the system does not enter the reports in the log buffer, and discards the reports. The system does not print a report when Y is entered in the SUPPRESS field of table LOGCLASS opposite the REPNAME. When N is entered, SUPPRESS does not affect reports.

Figure 4-2 Report Routing Scheme



Temporary Thresholding

Entries in tables OFCVAR and LOGCLASS apply permanent basic thresholding. Use of the LOGUTIL commands THRESHOLD, TIMERESET and SUPPRESS can for a limited time override the permanent basic thresholding. Temporary entries do not change permanent entries. The permanent entries remain available for a revision to permanent thresholding.

These commands can apply temporary values to selected REP-NAMES. The value range for the THRESHOLD command is the same (0 to 255) as that of the THRESHOLD field in LOGCLASS. The TIMERESET command has the same effect as the TUNITS field in LOGCLASS. The limit of the range of the TIMERESET command is 0 to 9999.

The SUPPRESS command can suppress a report that the SUPPRESS field in table LOGCLASS does not suppress.

The user uses the RESET command to restore permanent thresholding. The system can restore permanent thresholding at a system restart. The RESET command also returns to zero all values that THRESHOLD and TIMERSET apply. The RESET command resumes the generation of reports that the SUPPRESS command suppresses.

Thresholding for INIT and TRAP Logs

Permanent thresholding through OFCVAR and temporary thresholding through LOGUTIL commands cannot apply to the INIT and TRAP log subsystems.

Four fixed parameters in table OFCSTD control thresholding for these logs. The values for these parameters are set at the time of office data entry, and cannot change. Consult Northern Telecom personnel to change parameters after these parameters are rest.

These logs contain information for Northern Telecom personnel to use for fault analysis and debugging purposes.

Logs Format_Offices with Enhanced Core

The switch identification part of the log headers expands. The expansion occurs in the log headers of all logs that the system generates in offices that have Enhanced Core. The switch identification part expands to include a three-character node name and a three-digit node number.

This expansion facilitates identification of the source of the logs when the system prints logs from different nodes. This expansion facilitates identification when the system prints logs on the same output device. Refer to parameter ECORE_FORMAT of table OFCVAR, and to *Log Report Reference Manual*, 297-1001-840.

5 Man-Machine Interface

Man-Machine Interface (MMI) describes the methods used to enter commands and command syntax. The MMI describes the system responses to commands as the responses appear on the MAP display or printer. Examples appear on the MAP display to illustrate complicated syntax. Usage notes indicate details that can affect the MMI procedures.

Types of MMI

The MMI in the input/output (I/O) system performs the following functions:

- Security and Access Control
- Command Screening
- Report Routing
- Search and Display (Browse) of log reports
- The instructions include MMI special features for the group.

The instructions contain notes that describe the conditions under which the features are active.

The MMI for each group appear in a list in alphabetical order by basic command name. The list appears in the left hand box on the command description page.

Bilingual Man-Machine Interface

The Bilingual Man-Machine Interface (BMMI) is a feature that permits a user to select another language, or a default language. The user selects a language for commands, displays and printouts. The BMMI is available when software package NTX066AA is present.

The DEFAULT_LANGUAGE field of table OFCENG specifies the default language. The default value is set to ENGLISH but can change to FRENCH or GERMAN to suit operating company requirements.

You can require the MMI in a language other than the default language. The setting of the parameter lang of the following commands is the value for that language:

- PERMIT
- STARTDEV
- REROUTE

Commands that associate with the BMMI command interpreter (BMMICI) are used to enter data. The operating company personnel uses these commands to enter data that specify the output language, and load the BMMI database file. Enter BMMICMDS to obtain access to these commands.

Parameters and Responses

Parameters and responses that apply to more than one command appear by item number in tables. Item numbers reference the parameters and responses. These item numbers appear in the descriptions of the associated commands. Table 5-44, "Common parameters" on page 5-51 contains the descriptions of common parameters. Table 5-45, "Common command responses" on page 5-52 contains the text of common responses.

The parameter description, Where, describes the parameters that are different to a command. Different responses appear in capital letters in the, Responses, description. An explanation can follow.

Common Commands

The following common commands enable the user to obtain information about I/O command syntax. These commands enable the user to cancel an input that is not correct, and start again.

- **HELP**. The user uses this command with the name of the command for which information is required. This command causes a list to appear. This list contains the correct command syntax and parameters.
- **ABORT**. If the user experiences problems during the entry of a command, the user must enter ABORT. Then the user must enter the original command again.
- **QUIT**. The user uses this command to change from the current display to the previous command directory.

Prompting

The prompt character > appears before each response to a command. If parameters are left out, or are not entered correctly, the response prompts the user as to the type of error. The response can list the correct parameters to enter.

Security and Access Control MMI

This group consists of the following commands:

- LOGINCONTROL

```
LOGINCONTROL ALL QUERY            BRIEF      io_dev  FUL
             ENABLE
             DISABLE              disabtime
             AUTODISABLETIME      disabtime
             MAXLOGINTIME         logintime
             MAXIDLETIME          idletime
             LOGINRETRIES         numretry
             OPENFORCEOUT         TRUE
                                   FALSE
             DIALBACK             OFF
                                  ANSWER
                                  DIAL
             DIALOUT              numcallsdialtype
             DISABLEON            parm 1       parm 2
```

- PASSWORD

  controls LOGIN access. This group specifies the input/output device (IOD) for LOGIN use and sets the conditions for the devices that are not for LOGIN use. Refer to Note 1 on page 5-7

Where:

- ALL

  applies LOGINCONTROL to all IODs. Refer to Note 9 on page 5-8.

- io_dev

  applies LOGIN-CONTROL to a specific IOD. Refer to description in Table 5-44, "Common parameters" on page 5-51

- QUERY

  displays the current LOGINCONTROL settings and state of the IOD

- BRIEF

  displays the current enable state of the IODs, and the name(s) of the logged in user(s)

- FULL

displays the same information as BRIEF, and the state of all other LOGINCONTROL parameters

- ENABLE

  allows the system to accept LOGIN attempts from the specified device(s). Refer to Note 2 and Note 4 on page 5-8.

- DISABLE

  sets a disable period disabtime during which the system refuses LOGIN attempts from the specified device(s). Refer to Note 3, Note 4 and Note 9 on page 5-8.

- AUTODISABLETIME

  sets a disabtime to device(s) that the system disables. Refer to Note 5 on page 5-8. This command The MMI can be required in a language other than the default language does not apply to devices that the system disables after a restart.

- disabtime

  specifies in minutes the length of time the system refuses LOGIN to the disabled device(s). Default value is FOREVER.

- MAXLOGINTIME

  sets a limit logintime, to the time specified device(s) user(s) take to LOGIN. If the time exceeds the limit, that device is disabled. Refer to Note 6 on page 5-8.

- logintime

  specifies the time limit, in seconds, for MAXLOGINTIME. The default value is 60 s. FOREVER is a value.

- MAXIDLETIM

  sets a limit idletime to the time that specified device(s) can be left logged-on and not in use. If the time exceeds the limit, the user is logged-off by the system. Refer to Note 3 and Note 7 on page 5-8.

- idletime

  specifies time limit in minutes for MAXIDLETIME. Default value is FOREVER.

- LOGINRETRIES

  sets a limit to the number of times numretry that a user can enter a correct user-name and password. The user must enter the correct user-name and password before the user device is disabled. Refer to Note 8 on page 5-8.

- numretry

specifies the number of retries for LOGINRETRIES. The default value is four retries.

- OPENFORCEOUT

  causes the activation (true) or deactivation (false) of logoff of the specified IOD when an accidental disconnect occurs.

- TRUE

  enables OPENFORCEOUT logoff

- FALSE

  disables OPENFORCEOUT logoff

- DIALBACK

  specifies if the device(s) must have dialback disabled, or be a dialout or answer modem

- OFF

  disables DIALBACK for the specified device(s)

- ANSW

  enables the device(s) as an answer modem

- DIAL

  enables the device(s) as a dial

- DIALOUT

  limits the number of dialback call attempts NUMCALLS, before the call is aborted. This command also limits the line type, dialtype, for the modem.

- NUMCALLS

  specifies the number of dialback attempts, value = 1 to 7

- dialtype

  specifies the line type for the modem, value AUTO, PULSE or TONE

- DISABLEON

  determines what cause(s) the system to disable the specified device(s)

- parm 1

  specifies the method of application for the events that parm 2 lists. Consists of one of the following entries:

— ADD

adds the DISABLEON events that parm 2 must select, to events assigned to the specified device(s)

— SET

changes the earlier DISABLEON event settings to the settings that parm 2 selects

— REMOVE

deletes the DISABLEON events that parm 2 selects from the event settings assigned to the specified device(s)

- parm 2

selects the DISABLEON events to add, change or delete. This can consist of one or more of the following entries:

— LOGINFAIL

disables the device(s) if the user fails to enter a correct user name and password. The user must enter the correct user name and password in the maximum number of retries that numretry specifies.

— LOGINTIMEOUT

does not allow device(s) to be logged-on if the user takes longer than logintime to LOGON specifies

— IDLETIMEOUT

disables device(s) if the user is logged off by the system because idletime exceeds the limit

— LOGOUT

a log-off event disables the specified device(s)

— OPENCOND

disables the specified device(s) to all users if OPENFORCEOUT logs out the users

— DIALBACKLOGINFAIL

disables the device(s) if a failed dialback logon occurs

— DIALBACKCALLFAIL

disables the device(s) if a failed dialback call occurs

Responses
DONE

Responses

Meaning: Response to a LOGINCONTROL command, correct entry and execution.

Action: There is no action required.

```
DONE Num calls set to 1 for all ports.
```

or

```
DONE No change to some parts.
```

Meaning: Responses to command LOGINCONTROL ALL DIALOUT 1

Action: There is no action required.

```
DONE Num calls set to 1 and dialtype to PULSE for this port
```

or

```
Flags have no meaning for this port.
```

Meaning: Responses to command LOGINCONTROL RMT1 DAILOUT 1 PULSE

Action: There is no action required.

```
THE LOGINCONTROL COMMAND IS NOT AVAILABLE
```

Meaning: The enhanced access control feature is not provisioned or is inactive Refer to Note 1.

Action: There is no action required.

```
io_dev... ENABLED
          DISABLED
```

Meaning: Response to LOGINCONTROL command in which the IOD is enabled or disabled.

Action: There is no action required.

```
CANNOT DISABLE, THAT CONSOLE IS LOGGED IN
```

Meaning: An attempt to disable a logged-in io_dev (console)

Action: There is no action required.

Note 1: The LOGINCONTROL command is present and active when the enhanced security software package NTX292AB is provisioned. The ENHANCED_ACCESS_CONTROL and ENHANCED_PASSWORD_CONTROL fields in table OFCENG must be set to TRUE.

The LOGINCONTROL command affects terminal device data in table LGINCTRL. Although the user can change this data, the LOGINCONTROL command can be used for this data change only.

Note 2: You must apply the ENABLE command to all devices near the MAP of the DMS-100 switch.

Note 3: Remote and dial-up devices must have MAXIDLETIME. Devices that are not remote, and are not near the MAP, must have DISABLE when not in use.

Note 4: The system generates Log SECU113 when an attempt to logon on a disabled device occurs. The system outputs Log SECU114 when a user enables or disables a device.

Note 5: The system generates Log SECU117 when the system enables a device.

Note 6: The system generates Log SECU115 when a device is disabled because MAXLOGINTIME exceeds the time limit.

Note 7: The system generates Log SECU118 when a device is logged off or disabled because MAXIDLETIME exceeds the time limit.

Note 8: The system generates Log SECU116 when a device is disabled because the specified number of LOGINRETRIES exceeds the limit.

Note 9: You cannot disable logged on devices. If LOGINCONTROL ALL DISABLE is entered, devices that are not logged in are disabled only.

Examples:

1. Describes the use of the QUERY parameter to obtain information on the status of the DIALUP2 device that Emergency Technical Assistance Service (ETAS) uses.

   LOGINCONTROL DIALUP2 QUERY FULL command

   CONSOLE DIALUP2 ENABLED. USER: ETAS1. AUTODISABLE TIME 10MIN, LOGIN TIMEOUT 60 SECS, MAX IDLE TIME FOREVER, LOGIN RETRIES 4. SET TO DISABLE ON: LOGIN FAILURE, LOGIN TIMEOUT, LOGOUT response.

2. Describes how to set a value for the LOGINRETRIES parameter.

   LOGINCONTROL DIALUP2 LOGINRETRIES 2 command

   DONE response

3. Describes how to set the disable options for a device to a specified list.

   LOGINCONTROL DIALUP2 DISABLEON SET LOGINFAIL IDLETIMEOUT LOGOUT command

DONE response

4. Describes how to delete all the disable options for the specified device that appears in example 3.

   LOGINCONTROL DIALUP2 DISABLEON REMOVE command

   DONE response

   allows the user to change password. The ADMIN user can change another user password only. Refer to Note 1 on page 5-21.

Table 5-1

PASSWORD [username] newpw

Where:

- username

  a maximum of eight characters that the operating company defines. Use SHOW USERS command to display a list of current usernames. Required when ADMIN user changes another user password.

- newpw

  the new password that must replace the current password for the username. The following parameters default values, control password characteristics:

  — MIN_PASSWORD_LENGTH - six characters

  — PASSWORD_LIFETIME - 30 days

  — EXPIRED_PASSWORD_GRACE - 3 LOGONS

  These parameters appear in table OFCENG.

Refer to Note 2 and Note 3 on page 5-8.

Table 5-2 (Sheet 1 of 2)

Responses
PASSWORD: ENTER NEW LOGON PASSWORD **Meaning:** Normal system prompts occur before entry of newpw. **Action:** There is no action required.
PASSWORD: ENTER YOUR CURRENT PASSWORD TO VERIFY **Meaning:** Response to LOGINCONTROL command in which IOD is enabled or disabled. **Action:** There is no action required.

Table 5-2 (Sheet 2 of 2)

Responses

`PASSWORD FOR OPERATOR IS CHANGED`
`PASSWORD MUST CHANGE IN 30 DAYS`
 	
Meaning: Normal response when the new password replaces the old password.
 	
Action: There is no action required.

`PASSWORD: SORRY THAT PASSWORD MUST BE AT LEAST SIX CHARACTERS LONG` **Meaning:** A newpw is entered that does not conform to the office parameter MIN_PASSWORD_LENGTH. Select the correct password and enter the password again. **Action:** There is no action required.

DANGER

Password expires in 30 days

You have not changed your LOGON password in 30 days. You have three more logon sessions to change your password before access to the system is blocked.

Note 1: The PASSWORD command is present and active when the enhanced security software package is provisioned. The ENHANCED_PASSWORD_CONTROL field in table OFCOPT must also be set to TRUE.

Note 2: The user must first enter the PASSWORD command alone. The system prompts the user to enter a newpw.

Note 3: The user must use the PASSWORD command to change passwords. The system reminds users to change passwords when the PASSWORD_LIFETIME expires. The new password must be different from the old password.

Table 5-3

Responses
Meaning: Note to a user at LOGIN time that office parameter PASSWORD_LIFETIME exceeds the limit, and that EXPIRED_PASSWORD_GRACE parameter is in effect. **Action:** There is no action effect.

Command Screening MMI

This group consists of the following commands:

- PERMIT
- PRIORITY
- PRIVCLAS
- SETPRIV
- SHOW
- UNPERMIT.

Table 5-4

PERMIT	username password [parmlist]

assigns command classes, that PRIVCLAS defines, to specified users. Alters previous assignments to a user, or defines new users. Refer to Note 5 on page 5-14.

Where:

- username

  a maximum of eight characters for a user class, that the operating company defines. Use SHOW USERS command to display a list of current usernames.

- password

  the DMS user password that must associate with the username. This password is required when a user first logs on. The operating company defines passwords. The number of characters allowed in a password depends on, if the enhanced password control feature is on or off. The use

of this parameter depends on, if the enhanced password control feature is on or off. Refer to Note 1, Note 2 and Note 3 on page 5-10.

- parmlist

  has additional parameters that a user enters with the following syntax:

  `> [priority][stksize][lang][cmd_clas]`

  Where:

  — priority

  value 1 to 4 default = 4. Sets the priority level of the user processes. Refer to Note 4 on page 5-13.

  — stksize

  sets the number of words of memory assigned to the user processes specified at logon. The available range of stksize is 2000 to 10000. The default range is 7000. The range of assigned as required. Refer to Note 4 on page 5-13

  — lang

  values: FRENCH, GERMAN. Selects the language of input commands and system outputs. Selects the input language if MMI is required in a language other than the default value ENGLISH. You can set the default language in the DEFAULTLANGUAGE field of OFCENG. BMMI software must be present.

  — cmd_class

  value 0 to 30, or ALL. Command class number(s). The user enters terminal identification for each of the 31 class numbers in the COMCLASS field of table TERM-DE. The operating company assigns terminal identification. Refer to Note 4 and Note 5 on page 5-14.

Table 5-5

Responses
`YOU MUST SUPPLY A PASSWORD WHEN YOU CREATE NEW USERS` **Meaning:** The password parameter is left out. No action taken. **Action:** There is no action required.
`PERMIT - - USE THE PASSWORD COMMAND TO CHANGE PASSWORDS` **Meaning:** In a system that has enhanced password control, an attempt to change a password with the PERMIT command occurs. **Action:** There is no action required.

Refer to Table 5-45, "Common command responses" on page 5-52, item 6, for other responses to this command.

Examples:

1. Produces a new user name and password, and assigns priority 3 and stacksize 5000.

   PERMIT USER1 FRED 3 5000

2. Changes the priority in example 1 from 3 to 4.

   PERMIT USER1 4 5000

   Note: do not repeat the password if the username is the same.

Note 1: The enhanced password control feature is active when the correct software is present. Also, the ENHANCED_PASSWORD_CONTROL field in data table OFCOPT must be set to TRUE. This field is set first at datafill time, and cannot change. Enhanced password control is inactive when the associated field is set to FALSE.

Note 2: Enhanced_Password_Control: TRUE active.

Data table OFCENG. Parameters that affect password characteristics take effect:

- MIN_PASSWORD_LENGTH - one to 16 characters, default value six
- PASSWORD_LIFETIME - one to 32767 days, default value 30
- EXPIRED_PASSWORD_GRACE - default three LOGONS

The PASSWORD command takes effect and must be used to change passwords.

Use the PERMIT command to define new users and new user passwords, and change parameters other than password.

Note 3: Enhanced_Password_Control: FALSE inactive.

Data table OFCENG. Parameters that affect password characteristics do not appear. Password length has a limit of eight characters. There is no expiration time for passwords.

The PASSWORD command does not appear.

The user uses the PERMIT command to change passwords and related functions.

Note 4: When the user uses the PERMIT command, the system counts parmlist parameter values as default values. The user can request that the system not count parmlist parameter values as default values. When you must change the cmd_clas to a value that is a priority value, like 1, 2, 3 or 4.

Use SHOW USERS to determine the current priority level. The user enters PERMIT with the priority level and cmd_clas value.

Note 5: With the parameter cmd_clas, you can assign the following:

1. a privilege class to a user for access to commands
2. a privilege class for access to one or more system data tables.

Note 6: The operating company personnel must be careful during the definition of command classes in table TERMDEV with command PRIVCLAS. The operating company personnel must be careful during the definition classes of access to tables in table CUSTPROT. Personnel must make sure that the same class is not used two times. Personnel can use the same class one time for commands in TERMDEV and one time for tables in CUSTPROT. If personnel are not careful, a user can obtain access to a prohibited table or command.

CAUTION

Briefly state reasons for the caution

Enter the reasons for the caution: a caution informs the reader of a risk of service interruption.

Before the BCS32 load:

1. When ENHANCED_PASSWORD_CONTROL is set INACTIVE:
   - WARM RESTART: the systems logs in the users

     Note: the term users refers to the users which logon the DMS system before the RESTART.

   - COLD or RELOAD RESTART: the system logs in the operator. The other users do not receive a message.
2. When ENHANCED_PASSWORD_CONTROL is set ACTIVE:
   - WARM RESTART: Users receive Please Login message.
   - COLD or RELOAD RESTART: The operator receives the Please Login message. The other users do not receive a message.

With BCS32 and higher loads:

1. When ENHANCED_PASSWORD_CONTROL is set INACTIVE:
   - WARM RESTART: the system logs in the users.
   - COLD or RELOAD RESTART: the system logs in the operator. Users receive a Please Login message.
2. When ENHANCED_PASSWORD_CONTROL is set ACTIVE:
   - WARM, COLD or RELOAD RESTART: users receive a Please Login message.

Table 5-6

PRIORITY	ON CLEAR OFF

causes improved terminal response of the MAP where you entered PRIORITY. Refer to Notes.

Where:

- ON

  implements improved terminal response for the authorized user

- CLEAR

  clears priorities from other processes that have assigned priority as a result of previous use through the priority MAP. Refer to Note 3 on page 5-13.

- OFF

  resumes normal operation

Table 5-7 (Sheet 1 of 2)

Responses
USER HAS PRIORITY **Meaning:** The user enters the PRIORITY ON command for the first time. **Action:** There is no action required.
PRIORITY EXTENDED **Meaning:** The user enters the PRIORITY ON command for the second or the next time. **Action:** There is no action required.
PRIORITY IS STARTED

Table 5-7 (Sheet 2 of 2)

Responses
Meaning: Another user operates a priority MAP. **Action:** There is no action required.
`PRIORITY CLEARED FROM ALL PROCESSES EXCEPT THE USER PROCESS`
Meaning: The user enters PRIORITY CLEAR after PRIORITY ON. The system executes the PRIORITY CLEAR command. **Action:** There is no action required.
`PRIORITY CLEAR MUST BE PERFORMED FROM THE PRIORITY USER`
Meaning: The user enters PRIORITY CLEAR. The user did not enter PRIORITY ON first. Another user did not enter PRIORITY ON. **Action:** There is no action required.
`NORMAL OPERATION RESUMES`
Meaning: Response follows the entry and execution of PRIORITY OFF. **Action:** There is no action required.
`COMMAND FAILS`
Meaning: An error in PRIORITY command syntax occurs or SETPRIV command is not entered. **Action:** Use HELP_name> to check the correct syntax. Enter the correct command and parameter again.
`CANNOT ALLOCATE MAILBOX FOR COMMAND RESPONSE`
Meaning: Temporary software condition. **Action:** Enter the correct command and parameter again after a short period.

Note 1: Use this command in emergency conditions when you require current switch information. All terminals except for designated MAP positions and Emergency Technical Assistance Service (ETAS) dial-up ports must be privclassed to prohibit the use of this command.

Note 2: When call processing occupancy exceeds 60% use of this command by the ADMIN user class provides faster terminal response. Refer to Guaranteed Background Schedule on page 27.

Note 3: The normal prompt character > changes to PREF> when PRIORITYON is in effect.

Note 4: Use the PRIORITY CLEAR command if many users have guaranteed background process status. If many users have this status, the

advantage of PRIORITY to the ADMIN user MAP dissipates. Enter the QPRIO command to display the number of guaranteed background processes.

Note 5: The system outputs Log SOS102 when you use PRIORITY ON, CLEAR, or OFF.

PRIVCLAS	ALL [cmd_name] [mod_name] [cmd_class / cmd_lst]

adds, changes, or deletes the privilege class for specified command(s) or program module(s). Lists all current privilege commands and associated classes. Sets DUMPSAFE state for specified command(s) or module(s). Refer to Note 1 on page 5-16

Where:

- ALL

  provides a display listing all command and module names, and assigned command class(es) and DUMP-SAFE states. Commands that are not restricted do not appear in the list. Default value if the user enters PRIVCLAV only.

- cmd_name

  is the name of a valid DMS-100 Family command. Specifies the command name that you must assign privilege class(es) and DUMPSAFE state.

- mod_name

  is the name of the program module that you must assign a privilege class. The name of the module in which the specified cmd_name resides. Refer to Note 2 on page 5-16. Increment (INCR) is another name for mod_name.

- cmd_clas

  specifies the class number that you must assign to a cmd_name and/or mod_name. You use the cmd_clas to set DUMPSAFE state. You use cmd_clas with systems that have normal command screening. Refer to Note 1 and Note 3 on page 5-16.

Values:

— 0 to 30

terminal identification for each of the 31 class numbers are in COMCLASS field of table TERMDEV. The operating company assigns the terminal identification.

— DUMPSAFE

sets the specified cmd_name, or commands for a specified mod_name, to DUMPSAFE. Refer to DUMPSAFE STATE Part 3 on page 15 for details.

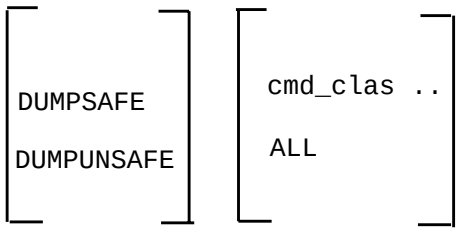
— DUMPUNSAFE

sets the specified cmd_name or mod_name to DUMPUNSAFE. Execution cannot occur during office image production.

- cmcl_lst

used when the enhanced command screening feature is turned on. Refer to Note 3. Specifies a list of command classes that you must assign to a cmd_name and/or mod_name. Sets DUMPSAFE state for the specified command classes.

Syntax



ALL
cmd_clas is normally used, value 0 to 30, to clear all assigned command classes. cmd_clas is used to make the associated command not restricted for all command classes.

Table 5-8 (Sheet 1 of 2)

Responses

`COMMAND DOES NOT HAVE A PRIVILEGE CLASS`
or
`COMMAND cmd_name IS NOT KNOWN TO CMDS TABLE`
(enhanced command screening only)
Meaning: The user enters PRIVCLAS cmd_name. Indicates that the specified command is not assigned a cmd_clas.
Action: There is no action required.

`COMMAND_PRIVILEGE MUST BE BETWEEN 0 AND 30.` **Meaning:** The user enters an out-of-range value for cmd_clas. **Action:** There is no action required.
`ILLEGAL PRIVILEGE CLASS` **Meaning:** A terminal is not assigned to the command class number that the user enters. **Action:** There is no action required.

`cmd_name IN |mod_name  |HAS|PRIVILEGE  CLASS|number 0 to 30`
`|symbol table|  |NO PRIVILEGE CLASS`
`AND IS |DUMPSAFE  |  |DUMPUNSAFE|`
Meaning: The user does not enter PRIVCLAS cmd_name mod_name. Displays the status of the specified command.
Action: There is no action required.

`COMMAND NAME  INCREMENT  DUMPSAFE  PRIVSET`
`cmd_name  mod_name  Y/N  cmd_clas`
`.  .  .  .  .`
`.  .  .  .  .`
`.  .  .  .  .`

Table 5-8 (Sheet 2 of 2)

Responses
Meaning: You enter the PRIVCLAS ALL command manually or as default. The list describes all current privileged commands/increments modules, and associated classes and DUMPSAFE states. **Action:** There is no action required.
`PRIVCLAS—ONLY A SINGLE COMMAND CLASS CAN BE ENTERED` **Meaning:** This response appears if the system has normal command screening, and the user enters PRIVCLAS with cmd_clas...parameters. This response does not appear if the system has enhanced command screening. Refer to Note 3. **Action:** There is no action required.
`PARAMETER MUST BE A CLASS NUMBER, DUMPSAFE OR DUMPUNSAFE` **Meaning:** Prompts the user to select the correct values during the entry of cmd_clas parameter. **Action:** There is no action required.
`PRIVCLAS—WRONG NUMBER OF PARAMETERS` **Meaning:** A syntax error occurs. Appears if the user enters more than one command when enhanced command screening is not present. **Action:** There is no action required.

Examples:

1. Queries the privilege class assigned to CLEAR command.

   PRIVCLAS CLEAR

   CLEAR HAS PRIVILEGE

   CLASS 6 AND IS DUMPUNSAFE.

2. Sets the command classes enhanced command screening of TYPE command to 0,2,3,4.

   PRIVCLAS TYPE 0 2 3 4

   There is no response if the user executes a command. Refer to Note 5 on page 5-17.

3. Clears all command classes assigned before, from TYPE and sets to DUMPSAFE state enhanced command screening.

   PRIVCLAS TYPE DUMPSAFE ALL

   A response does not occur when the user executes a command.

4. Sets STARTDEV command in LOGUTIL to DUMPUNSAFE and assigns command classes 0,3,4,15 enhanced command screening.

   PRIVCLAS LOGUTIL STARTDEV DUMPUNSAFE 0 3 4 15

5. Lists all commands assigned privilege classes. The CLEAR and STARTDEV commands appear in a list because the associated command classes are assigned. Refer to examples 1 and 4. The TYPE command does not appear in the list because this command is not restricted. Refer to example 3. The TYPE command is not restricted when associated cmd_lst parameter contains the value ALL, enhanced command screening. Refer to Note 5 on page 5-17.

   PRIVCLAS ALL

```
COMMAND NAME    INCREMENT   DUMPSAFE   PRIVSET
    CLEAR           LOGUTIL       N       6
    STARTDEV        LOGUTIL       N       0,3,4,15
        .               .                   .
        .               .                   .
        .               .                   .
```

Note 1: With the parameter cmd_clas of the PERMIT command that assigns the following:

- a privilege class to a user for access to commands
- a privilege class for access to one or more system data tables.

The operating company personnel must be careful during the definition of command classes in table TERMDEV with command PRIVCLAS. The operating company personnel must be careful during the definition of access to tables in table CUSTPROT. The personnel must make sure not to use the same class twice. You can use the same class one time for commands in TERMDEV and one time for tables in CUSTPROT. If personnel are not careful, a user can obtain access to a prohibited table or command.

Note 2: cmd_name and mod_name increment are used when the command name is not different, for example:

cmd_name mod_name

HOLD TTP

HOLD LTP.

Note 3: Normal command screening does not accept more than one command class for each command. This process is in effect when the ENHANCED_COMMAND_SCREENING field in data table OFCOPT is set to FALSE. Table CMDS is not present. Refer to Note 4.

Note 4: The enhanced command screening feature permits you to enter a list that contains a maximum of 31 command classes. You enter these classes for each command name. This feature is active when the correct software is present. You must also set the

ENHANCED_COMMAND_SCREENING field in data table OFCOPT to TRUE. When you use PRIVCLAS when this feature is active, the system enters the command names and associated command class(es) in data table CMDS. The ENHANCED_COMMAND_SCREENING field is first set at datafill time, and cannot change.

Note 5: The system acknowledges changes to command class assignments. These changes are not implemented immediately. The system stores the changes until a warm, reload, or cold restart occurs. The changes are implemented at the same time.

SETPRIV	adminpw

provides access to the priority MAP terminal feature when used with the proper password. Refer to Notes.

Where:

adminpw
is the password assigned to the ADMIN class of user

Table 5-9

Responses
No response: user has access to the PRIORITY command.
`COMMAND FAILS, ONLY ADMIN PASSWORD IS ACCEPTED` **Meaning:** You entered the wrong adminpw parameter. **Action:** There is no action required.

Note 1: This command can make the PRIORITY command available to the ADMIN user.

Note 2: The ADMIN user can access all classes of LOGUTIL commands.

Note 3: Normal command class assignments are restored at LOGOUT.

SHOW	USERS INCRS

displays a list of users and associated information, or a list of the current command modules, increments.

Where:

- USERS

  displays a list of all user names, assigned stacksizes, and resident device names that are not resident. Passwords do not appear.

- INCRS

  displays a list of current command modules, increments.

Table 5-10

Responses

`NAME  PRIO  STACK  NRDEV  LANGUAGE  PRIV  CLASSES`
`user_name  .  .  .  .  .  .`
`.  .  .  .  .  .  .`
`.  .  .  .  .  .  .`
Meaning: The user enters SHOW USERS. Lists user_names and parameters that the PERMIT command assigns to the names.
Action: There is no action required.

`INCR NAME`
`.`
`.`
Meaning: Response to SHOW INCRS.
Action: There is no action required.

`UNPERMIT`	`username  [password]`

deletes a user name from the list of users. Another user can delete a user name. Users cannot delete own user names.

Where:

- username

  a name of a maximum of eight characters that the operating company defines. Use SHOW USERS command to list all current usernames.

- password

  Required if the enhanced password control feature is on Refer to PERMIT Notes 1,2,3. Uses the DMS password for the username. The operating company defines passwords.

Table 5-11

Responses
`UNPERMIT:  username IS DELETED` **Meaning:** Normal response from system when enhanced password control feature is inactive. Refer to PERMIT Note 3. **Action:** There is no action required.
`UNPERMIT: ENTER PASSWORD` **Meaning:** Response from system in which UNPERMIT username is entered and enhanced password control feature is active. Refer to PERMIT Note 2. After you have entered the correct password, the response is: **Action:** There is no action required.

`UNPERMIT: username IS DELETED`
 	
`NO USER`
 	
Meaning: Invalid user_name parameter is entered. Use SHOW USERS for display of correct user_names.
 	
Action: There is no action required.

Report Routing MMI

Report routing MMI are operable after the user uses the LOGUTIL command to access the log system. This group consists of the following commands:

- ADDCLASS
- ADDREP
- BACKUP
- CLASS
- DELCLASS
- DELDEVICE

- DELREP
- LISTDEVS
- LISTREPS
- LISTROUTE
- LISTTIME
- REROUTE
- RESET
- RESETROUTE
- RESUME
- STARTDEV
- STOPDEV
- SUPPRESS
- THRESHOLD
- TIMERESET.

`ADDCLASS`	`io_dev repclass...`

Adds more output report classes to the classes for the specified primary IOD.

Where:

- io_dev
  is defined in Table 5-44.
- repclass
  is defined in Table 5-44.

Table 5-12

Responses
`n..  CLASSES ADDED` **Meaning:** The specified classes are added. **Action:** There is no action required.

Refer to Table 5-2, items 9, and 11 for other responses to this command.

ADDREP	io_dev repname...

Adds more reports to reports that the system routes to the specified primary IOD.

Where:

- io_dev

  is defined in Table 5-1
- repname

  is defiened in Table 5-1

Table 5-13

Responses
ADDED **Meaning:** The specified report is added. **Action:** There is no action required.
n.. REPORTS ADDED **Meaning:** The quantity of reports specified by repname is added. **Action:** There is no action required.

Refer to Table 5-45, items 4,8,10, and 11 for other responses to this command.

BACKUP	io_dev BY alt_dev

Assigns another IOD to back up a specified primary I/O device. If the primary device fails, the system routes all reports first sent to the primary device, to the specified backup device.

Where:

- io_dev

  is defined in Table 5-1, item 5.
- BY

indicates that the device name that follows the back-up device.

- alt_dev

  is the name of the device for back-up. Supersedes the device in ALT field of data table TERMDEV for a short time.

Table 5-14

Responses
Refer to Table 5-2, item 11 for another response to this command. There is no response if the user executes command.

`CLASS`	`repclass repname...`

Assigns report class numbers to specified output reports.

Where:

- repclass

  is defined in Table 5-1

- repname

  is defined in Table 5-1

Table 5-15

Responses
`n.. REPORTS RECLASSED` **Meaning:** The quantity of reports that repname specifies is classed again. **Action:** There is no action required.

Refer to Table 5-45, items 2,4,8 and 9 for other responses to this command.

`DELCLASS`	`io_dev repclass`

Deletes specified report classes for the specified IOD.

Where:

- io_dev

  is defined in Table 5-44
- repclass

  is defined in Table 5-44

Table 5-16

Responses
`n..CLASSES DELETED` **Meaning:** The quantity of report classes that repclass specifies are deleted. **Action:** There is no action required.

Refer to Table 5-45 items 9 and 11 for other responses to this command.

Deletes the specified IOD from the list of devices that receive log reports. Use STOPDEV command first.

Where:

io_dev
is defined in Table 5-44

Table 5-17

Responses
`DEVICE IS STARTED` **Meaning:** This response appears if the user does not enter STOPDEV before DELDEVICE. **Action:** There is no action required.

Refer to Table 5-2, item 11 for another response to this command.

A response does not occur if the user executes a command.

`DELREP`	`io_dev repname...`

Deletes specified report(s) output to the specified Input/Output device.

Where:

- io_dev

  is defined in Table 5-44
- repname

  is defined in Table 5-44

Table 5-18

Responses

`DELETED`
 	
Meaning: The specified report is deleted.
 	
Action: There is no action required.
 	
`n...REPORTS DELETED`
 	
Meaning: The quantity of reports that repname specifies is deleted.
 	
Action: There is no action required.

Refer to Table 5-45, items 4,8,10 and 11 for other responses to this command.

`LISTDEVS`	

Displays the status of each Input/Output device for the log system.

Table 5-19

Responses

`NO. DEVICE STATUS REROUTED ALTERNATE FORMAT OUTPUT LANGUAGE`
`. .... .......... ...... .... ... ... ....`
`- End of devices -`
 	
Meaning: Lists all IOD and associated backup devices. Displays the device that is in use and the current status.
 	
Action: There is no action required.
 	
Example:
 	
`NO. DEVICE STATUS REROUTED ALTERNATE FORMAT OUTPUT LANGUAGE`
`0 PRT1 Inactive No Nil SCC2 ASCII English`
`- End of devices -`

Where:

- NO.

  is the log device number. A maximum of 32 log devices, 0-31 is allowed.

- DEVICE

  is the device type, where device is one of:

  — the devices in the list in TABLE TERMDEV

  — the devices assigned for a short time in TABLE SFDEV

  — disk or tape.

- STATUS

  indicates one of the following:

  — Process starts: the log device fails to send logs to an associated file or device.

  — Log output: logs are output to the log device.

  — Inactive: the log device is inactive

- REROUTED

  indicates by YES or NO if the system routes the log output again from the primary device to the alternate device.

- ALTERNATE

  indicates the other devices available for log outputs.

- FORMAT

  indicates if the output is in standard (STD) log format or Switching Control Center No. 2 (SCC2) log format.

- OUTPUT

  indicates if the output is ASCII or EBCDIC.

- LANGUAGE

  indicates the MMI language in which logs are output on that device, where language is one of:

  — ENGLISH

  — GERMAN

  — FRENCH.

LISTREPS	SPECIAL repname ... CLASS repclass SYSLOG

Displays details of SPECIAL log reports or of all log reports in a specified log class. Refer to Notes 1 and 2.

Where:

- SPECIAL

indicates that a list of special log reports is required. Special log reports are reports that have special routing or thresholding and reports that are suppressed.

- repname

  is defined in Table 5-1

- CLASS

  indicates that a list of reports by log class is required

- repclass

  is defined in Table 5-1

- SYSLOG

  specifies the system log reports

Table 5-20

Responses
Details that appear are: • repname • repclass • report event type • report event identification • IODs to which the system routes the report • report suppressed and/or thresholded

Refer to Table 5-2, items 2,3,8,9,10 and item 4, LISTREPS SPECIAL only.

Note 1: The displays that result from LISTREPS include a SYSLOG field if SYSLOG ON is applied to the specified repname.

Note 2: If the user enters LISTREPS and parameters are not included, a list of all repnames, except SECRET appears.

LISTROUTE	CLASS [repclass] ... DEVICE [io_dev] ... REPORT [repname] ...

Displays the associations between specified report classes, IOD, and report names, by CLASS, DEVICE, or REPORT.

Where:

- CLASS

  lists all the output reports for specific report classes and the IOD to which the system routes these classes.

- repclass

  is defined in Table 5-44 Specifies the required report class(es). If the user does not enter repclass, information on all classes appears.

- DEVICE

  lists all the report classes (and temporary classes) for a specified IOD.

- io_dev

  is defined in Table 5-44. Specifies the required IOD. If the user does not enter io_dev, information on all devices appears.

- REPORT

  lists the routing for specific report names

- repname

  is defined in Table 5-44. Specifies the required report(s). If the user does not enter repname, information on all reports appears.

Table 5-21 (Sheet 1 of 2)

Responses
`INVALID OPTION` **Meaning:** A parameter other than CLASS, DEVICE, or REPORT is entered. **Action:** There is no action required.
`CLASS repclass --> io_dev alt_dev` **Meaning:** Response to LISTROUTE CLASS. Displays the primary and backup IOD to which the system routes the specified report class(es). **Action:** There is no action required.

Table 5-21 (Sheet 2 of 2)

Responses

`DEVICE io_dev PRINTS CLASSES: n..`
`ADD REPORTS;`
`DELETE REPORTS:`
 	
Meaning: Response to LISTROUTE DEVICE. Displays the report class numbers for the specified IOD. Displays report class numbers that ADDCLASS or DELCLASS adds and deletes for a short time.
 	
Action: There is no action required.

`REPORT repname IS CLASS: n..`
`ADDED:`
`DELETED:`
 	
Meaning: Response to LISTROUTE REPORT. Displays the report class number associated with the specified report name(s). Displays the quantity of reports that ADDREP or DELREP adds and deletes for a short time.
 	
Action: There is no action required.

Refer to Table 5-45, items 2,3,4,8,9,10 and 11 for other responses to this command.

`LITTIME`	

Displays a list of all log reports that are on a threshold reset schedule. Refer to Note 1. There are no parameters required.

Table 5-22 (Sheet 1 of 2)

Responses
`NOTHING ON RESET LIST` **Meaning:** Log reports are not present on the reset list. **Action:** There is no action required.

Table 5-22 (Sheet 2 of 2)

Responses
LOG NUM MINUTES LEFT aaa nnn nnnn nnnn . . . . aaa nnn nnnn nnnn - END **Meaning:** Displays the log name and report number of all reports that had a time value. TIMERESET applies a time value. Lists the number of minutes to set, and the number of minutes left to reset. **Action:** There is no action required.

Note: Reset threshold parameters are set to default values in data schema table OFCENG, for normal office operations. These values, as a rule, are not variable, but can change to suit operating company requirements. Consult Northern Telecom for details.

REROUTE	[lang] io_dev

The system routes all reports for the specified primary IOD again to the associated backup IOD.

Where:

- langvalue

  FRENCH or GERMAN. Used if the language of MMI is other than the default language ENGLISH. Refer to PERMIT.

- io_dev

  is defined in Table 5-44

Table 5-23 (Sheet 1 of 2)

Responses
SYSTEM ROUTES DEVICE io_dev AGAIN **Meaning:** Action is not taken. The backup device for the specified io_dev is in use. **Action:** There is no action required.

Table 5-23 (Sheet 2 of 2)

Responses
`SYSTEM CANNOT ROUTE DEVICE io_dev AGAIN` **Meaning:** Action is not taken. Backup device is not assigned for the specified io_dev, or the assigned backup device is out of service. **Action:** Use LISTDEVS to check the status of the specified io_dev and the backup. If necessary, use BACKUP to assign another IOD.
`NUMBER OF DEVICES THAT THE SYSTEM ROUTES AGAIN: n` **Meaning:** The user executes the BACKUP command. Displays the number of IOD that switch to associated backup devices. **Action:** There is no action required.

Refer to Table 5-45, item 11, for another response to this command.

`RESET`	

Resets to set all threshold values to zero that the THRESHOLD command applies. Resumes the generation of all reports that the SUPPRESS command suppresses.

There are no parameters required.

Table 5-24

Responses
`NUMBER OF LOG REPORTS RESET: n` **Meaning:** The system executes the RESET command. Displays the number of reports for which threshold values are set to zero again. **Action:** There is no action required.

`RESETROUTE`	

Restores the temporary routing of output reports on all output devices to the original routing. The data schema tables LOGCLASS and TERMDEV describe this process.

There are no parameters required.

Table 5-25

Responses
`NOTE THAT ALL TEMPORARY ROUTING IS LOST` **Meaning:** The system executes the RESETROUTE command. Warns that all IOD change back to original routing. **Action:** There is no action required.

Note: Temporary routing consists of routing changes applied with: ADDCLASS, ADDREP, DELCLASS, DELREP, DELDEVICE, REROUTE.

`RESUME`	`repname ...`

Resumes the generation of specified output reports SUPPRESS suppresses.

Where:

repname
is described in Table 5-1

Table 5-26

Responses
`n.. REPORTS RESUME` **Meaning:** The system executes the RESUME command. Displays the number of reports from which suppression is removed. **Action:** There is no action required.

Refer to Table 5-45, items 2,4 and 8 for other responses to this command.

`STARTDEV`	`ASICC` `EBCDIC`	`lang`	`io_dev...`

Activates the output of reports, in a specified format and language, to the specified IOD that uses the original routing.

Where:

- ASCII

  is one format in which an IOD and the Device Controllers exchange data

- EBCDIC

  is one format in which the Device Controllers record data on Magnetic Tape Unit

- lang

  value: FRENCH or GERMAN. Used if the language of MMI is other than the default language ENGLISH. Refer to PERMIT.

- io_dev

  is defined in Table 5-44

Table 5-27 (Sheet 1 of 2)

Responses
`CANNOT FIND THIS DEVICE.` **Meaning:** An IOD name that is not correct that the user enters as the io_dev parameter. Refer to Table A on page 80 for a description of io_dev. Enter LISTDEVS for a display of all current IOD. **Action:** There is no action required.
`CANNOT START LOG DEVICE io_dev.` **Meaning:** The system cannot start the log device because a problem with the io_dev. A message that precedes this response explains the problem. **Action:** There is no action required.
`io_dev STARTS.` **Meaning:** The specified device is active. **Action:** There is no action required.
`LOG DEVICE io_dev STARTS.` **Meaning:** STARTDEV is applied to the specified io_dev. **Action:** There is no action required.
`NUMBER OF DEVICES STARTED: nn` **Meaning:** The system executes the STARTDEV command. Displays the number of devices activated. **Action:** There is no action required.

Table 5-27 (Sheet 2 of 2)

Responses
PROCESS CAN TAKE A MAXIMUM OF 15 MIN (FOR TAPE REWIND etc.). **Meaning:** STARTDEV is delayed for the specified reason. **Action:** There is no action required.

STOPDEV	io_dev ...

Stops the output of reports on the specified device(s). The user continues to enter reports in the log buffers. This way, the user can browse the reports with the appropriate LOGUTIL commands.

Where:

io_dev
is defined in Table 5-44

Table 5-28

Responses
io_dev STOPS. **Meaning:** Action is not taken. The specified io_dev is inactive. **Action:** There is no action required.
LOG DEVICE io_dev STOPS. **Meaning:** The specified device is deactivated. **Action:** There is no action required.
NUMBER OF DEVICES THAT STOP: nn. **Meaning:** The system executes the STOPDEV command. Displays the number of devices deactivated from 1-32. **Action:** There is no action required.
CANNOT STOP LOG DEVICE **Meaning:** Action is not taken. The specified io_dev fails to respond to STOPDEV. **Action:** There is no action required.

Note: You must use STOPDEV before DELDEVICE.

SUPPRESS	repname

Suppresses the specified output report(s). Suppressed reports are not entered in the log buffers.

Where:

repname
is defined in Table 5-44

Table 5-29

Responses
n.. REPORTS SUPPRESSED **Meaning:** The system executes the SUPPRESS command. Displays the number of reports suppressed. **Action:** There is no action required.

Refer Table 5-45, items 2,4 and 10 for other responses to this command.

THRESHOLD	n repname...

Sets a threshold value for the specified report(s).

Where:

- n
  is a counter from 0 to 255. Controls the frequency of output to IOD.
- repname
  is defined in Table 5-44

Table 5-30 (Sheet 1 of 2)

Responses
n...REPORTS THRESHOLDED **Meaning:** Threshold value is applied to the specified report(s). Displays the number of reports to which the specified threshold is applied. **Action:** There is no action required.

Table 5-30 (Sheet 2 of 2)

Responses
`THRESHOLD MUST BE A NUMBER fi 0 and 255` **Meaning:** You entered an out-of-range value for the n parameter. **Action:** There is no action required.

Refer to Table 5-45, items 2 and 8 for other responses to this command.

Note: The THRESHOLD parameter does not apply to lognames INIT and TRAP.

`TIMERESET`	`time repname ...`

Sets a time value that the system resets the threshold counter for specified report(s), when the set time limit ends.

Where:

- time

  is a value from 0000 to 9999 min. If time = 0, the threshold counter is not subject to a time limit.

- repname

  is defined in Table 5-44

Table 5-31

Responses
`FIRST PAR. MUST BE NUMBER OF MINUTES` **Meaning:** A syntax error occurs when the user enters the parameters. **Action:** There is no action required.
`n..REPORT(S) TIMERESET` **Meaning:** TIMERESET is applied to the specified reports. Displays the number of reports affected. **Action:** There is no action required.

Search and Display (Browse) MMI

The browse MMI are operable after the user accesses the log system with the LOGUTIL command. This group consists of the following commands:

- BACK
- CLEAR
- FIRST
- FORMAT
- FOWARD
- LAST
- LISTLOGS
- LOGTRACE
- OPEN
- OPENSECRET
- RENUMBER
- START
- STOP
- TYPE

Note: The user must enter the OPEN or OPENSECRET command before using the other browse commands.

BACK	

Displays the next report in the current log buffer that is older than the present display.

There are no parameters required.

Table 5-32

Responses
Complete report appears on MAP, but printer output is in NORMAL or SHORT format as FORMAT selects. **Example:** Refer to Figure 4-1. If the present log report is CMC108 at event-time 1630, the result of BACK is to display report CMC112 event-time 1615. **Action:** There is no action required.

CLEAR	logname

Deletes all reports from a specified log subsystem buffer.

Where:

logname
is defined in Table 5-44, can be a logname the command LISTLOGS displays

Responses: Refer to Table 5-45, items 2,4,5,6,7,8 and 10 for other responses to this command.

FIRST	

Displays the oldest report in the current log subsystem.

Table 5-33

Responses
Complete report appears on MAP, but printer output is in NORMAL or SHORT format as FORMAT selects. **Example:** Refers to Figure 4-1. FIRST causes log report CMC101 event time 1555 to appear. **Action:** There is no action required.

FORMAT	NORMAL SHORT

Selects the format in which output reports are printed.

Where:

- NORMAL

  prints the reports in standard complete log report format. NORMAL format is default if the user does not enter a parameter.

- SHORT

  prints the header information of the log reports

Table 5-34

Responses
There is no response if syntax is correct. Syntax error: refer to Table 5-45, item 6.

FORWARD	

Displays the next report in the current log. The current log is more recent than the present display.

There are no parameters required.

Table 5-35

Responses
Complete report appears on MAP, but printer output is in NORMAL or SHORT format as FORMAT selects. **Example:** Refer to Figure 4-1. If the present log report is CMC112 at event-time 1615, the result of FORWARD is to display log report CMC108 event-time 1630.

LAST	

Displays the most current report in the current log subsystem.

Table 5-36

Responses
Complete report appears on MAP, but printer output is in NORMAL or SHORT format as FORMAT selects. Displays the same report as OPEN. This report does not appear if a more current log report occurs after OPEN is entered. **Example:** Refer to Figure 4-1. LAST causes report CMC112 event time 1647 to appear.

LOGTRACE	ON logname [repnum] OFF [logname [repnum] ... / ALL]

Lists all lognames except SECRET lognames, in the DMS-100 Family system.

There are no parameters required.

Responses: Displays a list of all lognames except SECRET. Refer to Table 5-45, item 7.

Turns ON or OFF the traceback feature for specified report(s).

Where:

- ON

  turns on the traceback feature
- OFF

  turns off the traceback feature
- logname

  is defined in Table 5-1
- repnum

is defined in Table 5-1

- ALL

  Default for OFF, causes the traceback of all lognames and repnum to terminate

Table 5-37

Responses
`n REPORT(S) LOGTRACE ON` **Meaning:** The traceback feature is turned ON for all of the specified reports. **Example:** >logtrace on cmc sa 18 REPORT(S) LOGTRACE ON > Traceback feature turned ON for all CMC and SA reports.
`n REPORT(S) LOGTRACE ON` **Meaning:** The traceback feature is turned ON for all of the specified reports. **Example:** >logtrace on cmc 102 sa 203 2 REPORT(S) LOGTRACE ON > Traceback feature turned ON for the CMC 102 and SA 203 reports.
`2 REPORT(S) LOGTRACE OFF` **Meaning:** The traceback feature is turned OFF for all of the specified reports. **Example:** >logtrace off cmc 102 sa 203 >Traceback feature turned OFF for the CMC 102 and SA 203 reports. Traceback feature turned ON for the CMC 102 and SA 203 reports.

`OPEN`	`logname` `SYSLOG`

Provides access for display purposes to the specified log subsystem buffers, or to the SYSLOG buffers. Refer to Note 1.

Where:

- logname

  is defined in Table 5-44

- SYSLOG

  applies OPEN to log reports that the system routes to the SYSLOG buffers.

Table 5-38

Responses
The most current report in the specified log buffer appears. **Meaning:** Response to OPEN logname. Displays the most current report, the current log in the specified log subsystem when the user enters the OPEN command. Refer to Table 5-2, items 4,5,6 and 7 for other responses to this command.
The most current entry in the SYSLOG buffer, before the last reload restart appears. **Meaning:** Response to OPEN SYSLOG. Refer to Table 5-2, items 5,6,7,8 and 10 for other responses to this command.

Note 1: After the user enters OPEN, other reports in the specified log sub system, or SYSLOG can appear. The user uses the FIRST, LAST, BACK, FORWARD or TYPE commands to display the reports.

Note 2: If SYSLOG contains a SECRET logname, the non secret log names appear. SECRET lognames are accessible to users authorized to use the OPENSECRET command.

Example:

Access reports in log subsystem CMC.

OPEN CMC

OPEN CMC was entered at 1647 hours. That report CMC112 was the most current report in that log subsystem buffer at that time. If you selected the short report format, refer to FORMAT command, the response is:

CMC112 MAR02 16:47:00 7465 INFO PORT_ERROR CMC 0...etc.

OPENSECRET	sec_log

Provides access to log subsystems in the SECRET category.

Where:

sec_log

is the name of a log subsystem in the SECRET category. Privileged users can access SECRET lognames. LISTLOGS cannot display SECRET lognames.

Table 5-39

Responses
`LOGUTIL:` Command only applies to secret logs and syslog **Meaning:** The logname that a user enters as the sec_log parameter is not a SECRET log. Refer to Figure 1-2, items 5, 6 and 7 for other responses to this command. **Action:** There is no action required.

Note 1: After the user enters OPENSECRET, the FIRST, LAST, BACK, FORWARD, or TYPE commands can select a particular SECRET log report.

Note 2: You can use all other LOGUTIL commands, except CLEAR and SUPPRESS on SECRET logs after OPENSECRET.

Note 3: If SECRET lognames are in SYSLOG, you cannot use CLEAR on SECRET or another logname.

`RENUMBER`	`sec_log`

Assigns a report number to all report types that do not have a report number.

Where:

- sec_log

  is the name of a log subsystem in the SECRET category. SECRET lognames are accessible to privileged users only. LISTLOGS cannot display SECRET lognames.

Table 5-40

Responses
There are no responses to this command.

START	polltime [repclass]	[ASCII / EBCDIC]

starts the output of log reports to the specified device. Even with logs that run to the terminal, the user can continue to enter CI commands.

Where:

- polltime

  is the time interval in milliseconds between scanning the log buffer

  — Range: 10 to 2550 ms

  — Default value: 100 ms or .1 s

- repclass

  is defined in Table 5-44. Refer to Page 5-57, Note 3.

- ASCII

is the character code for printer or VDU default

- EBCDIC

  is character code for magnetic recording devices

Table 5-41

Responses
Displays reports in selected log classes.
`CANNOT FIND THIS DEVICE.` **Meaning:** The user enters an IOD name that is not correct as the io_dev parameter. Refer to Table A on page 5-1 for a definition of io_dev. Enter LISTDEVS for a display of all current IOD. **Action:** There is no action required.
`CANNOT START LOG DEVICE io_dev.` **Meaning:** The system cannot start the log device because of a problem with the io_dev. A message that precedes this response describes the problem. **Action:** There is no action required.
`io_dev IS ALREADY STARTED.` **Meaning:** START is applied at this device to the specified repclass. **Action:** There is no action required.
`THIS PROCESS CAN TAKE A MAXIMUM 15 MIN FOR TAPE REWIND etc.` **Meaning:** START is delayed for the specified reason. **Action:** There is no action required.
`CANNOT TO CREATE LOG DEVICE PROCESS.` **Meaning:** The system encounters a problem. **Action:** Contact the maintenance support group.
`YOU CAN USE THIS TERMINAL TO ENTER CI COMMANDS. TO GET RID OF THE CI PROMPT TYPE, WHILE (true) (sleep 100 mins). TO GET BACK THE CI PROMPT USE <break> STOP.` **Meaning:** The CI prompt is interleaved with log reports so that the user can continue to enter CI commands. The user can suspend and restore the CI prompt with the SLEEP and <break> STOP commands, in that order. **Action:** There is no action required.

Note 1: The START command is used to view reports for maintenance purposes.

Note 2: The START command does not cancel previous routings that ADD CLASS, DELCLASS or tables LOGCLASS and LOGDEV establish.

Note 3: If the user does not enter a repclass, the system outputs all classes.

STOP	

stops prints of reports on the device from which the command was issued. No parameters are required.

Table 5-42

Responses
CANNOT GET DEVICE OF THIS USER. **Meaning:** The system cannot find the device to which the user issued the STOP command. **Action:** Contact the maintenance support group.
io_dev STOPS. **Meaning:** There is no action taken. STOP is applied to the specified io_dev. **Action:** There is no action required.
THIS DEVICE STOPS. **Meaning:** The system executes the command. **Action:** There is no action required.
CANNOT TO STOP LOG DEVICE io_dev. **Meaning:** The system finds a problem, check the SWER log reports. **Action:** There is no action required.

TYPE	

Displays the report again in the current log subsystem buffer, that LAST, FIRST, BACK or FORWARD first display. Refer to Note.

There are no parameters required.

Table 5-43

Responses
`NO OPEN LOG`
`NO CURRENT REPORT TRY, FIRST OR LAST`
Refer to Table 5-45, items 4, 6 and 7 for other responses to this command.

Note: Use the TYPE command to restore a display that clears or runs over because of complete use of LAST, FIRST, BACK and FORWARD.

Table 5-44 Common parameters

Item No.	Parameter Name	Description
1.	logname	Indicates the name of a log subsystem that resides in the LOGS system. Maximum of four characters. The user can use the LISTLOGS command to display a list of all the lognames except SECRET.
2.	repnum	Indicates the number of a specific log report in a log subsystem. Value 100 to 999
3.	repname	Consists of logname and repnum, and identifies a specified output report. All repnames appear in a list in the *Log Report Reference Manua*l 297-1001-840. The user enters the same names in the REPNAME field of data schema table LOGCLASS. Use LISTREPS to display a list of all repnames.
4.	repclass	Indicates the report class number from 0 to 31 that associates with a specified repname in table LOGCLASS to route an IOD.
5.	io_dev	The name of an IOD in the office designated in the DEV field of data schema table TERMDEV, is a primary IOD.

Table 5-45 Common command responses (Sheet 1 of 2)

Item No.	Text of Response and Meaning

1.	`NAME BACKUP CURRENT INUSE`
	` XXXX XXXX XXXX XXX`
	`  *  *  *  *`
	`  *  *  *  *`
	` END OF DEVICES`
	Meaning: Lists all IOD and associated backup devices and displays which device is in use, and the current status of the device.
	.**Action:** There is no action required.

2.	`LOG logname NOT FOUND` **Meaning:** The user enters a log report repname parameter that is not correct. Refer to Table 5-1 for a definition of repname. .**Action:** There is no action required.
3.	`REPORTS PRINTED` **Meaning:** Displays the number or reports that the system prints as a result of the LISTREPS or LISTROUTE command. .**Action:** There is no user action required.
4.	`LOGUTIL: COMMAND DOES NOT APPLY TO SECRET LOGS.` **Meaning:** Appears if parameter repname is that of a SECRET log. Use OPENSECRET command if you are authorized to access SECRET logs. .**Action:** There is no action required.
5.	`DONE` **Meaning:** The system executes the command. .**Action:** There is no action required.

6.	`NOT FOUND`
	or
	`EITHER INCORRECT OPTIONAL PARAMETER(S) OR TOO MANY PARAMETERS`
	Meaning: An invalid parameter is entered with the associated command.
	.**Action:** Verify command syntax and enter again.

7	`LOG EMPTY` **Meaning:** The specified logname does not contain log reports. .**Action:** There is no action required.

Table 5-45 Common command responses (Sheet 2 of 2)

Item No.	Text of Response and Meaning
8.	`PARAMETER parmname IS NOT A LOG NAME OR REPORT NUMBER` **Meaning:** A repname that is not present and/or repnum parameter is entered. Refer to Table 5-1. .**Action:** There is no action required.
9.	`INCORRECT CLASS NUMBER AT PAR #: n` **Meaning:** An out-of-range class number is used as the repclass parameter with the associated command. Refer to Table 5-1. .**Action:** There is no action required.
10.	`REPORT logname repnum NOT FOUND` **Meaning:** The log report specified with the associated command is not on the LISTLOGS display. The user can enter an out-of-range repnum, with negative results. Refer to Table 5-1. .**Action:** There is no action required.
11.	`DEVICE io_dev NOT FOUND` **Meaning:** The user enters an IOD name that is not correct. The user enters the IOD as the io_dev parameter. Refer to Table 5-1 for a description of io_dev. Enter LISTDEVS for a display of all current IOD. .**Action:** There is no action required.

List of terms

BCS
Batch Change Supplement

BMMI
Bilingual Man-Machine Interface

CCC
Central Control Complex

CI
Command Interpreter

CMC
Central Message Controller

CPU
Central Processing Unit

DC
Device Controller

DMS
Digital Multiplex System

ETAS
Emergency Technical Assistance Service

I/O
Input/Output

IOC
I/O Controller

IOD
I/O Device

MAP
Maintenance and Administration Position

MMI
Man-Machine Interface

MTC
Magnetic Tape Controller

NMC
Network Message Controller

NT
Northern Telecom

NTP
Northern Telecom Practices

NWC
Network Management Control

NWM
Network Management

PEC
Product Engineering Code

SA
Service Analysis

SCCS
Switching Control Center System

TAC
Technical Assistance Center

TC
Terminal Controller

DMS-100 Family

Input/Output System

Reference Manual

Electronic mail: cits@nortelnetworks.com

Publication number: 297-1001-129
Product release: BASE13 and up
Document release: Standard 06.06
Date: September 2000
Published in the United States of America

NORTEL NETWORKS™