Critical Release Notice

Publication number: 297-2061-312
Publication release: Standard 05.04

The content of this customer NTP supports the SN06 (DMS) and ISN06 (TDM) software releases.

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

Bookmark Color Legend

Black: Applies to new or modified content for the baseline NTP that is valid through the current release.

Red: Applies to new or modified content for NA017/ISN04 (TDM) that is valid through the current release.

Blue: Applies to new or modified content for NA018 (SN05 DMS)/ISN05 (TDM) that is valid through the current release.

Green: Applies to new or modified content for SN06 (DMS)/ISN06 (TDM) that is valid through the current release.

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

Publication History

March 2004

Standard release 05.04 for software release SN06 (DMS) and ISN06 (TDM).

Change of phone number from 1-800-684-2273 to 1-877-662-5669, Option 4 + 1.

297–2061–312

DMS–100 FAMILY

Customer Data Change Operating Company

Guide

NA012 Standard 05.03 September 1999

northern telecom

DMS–100 FAMILY

Customer Data Change Operating Company

Guide

Publication number: 297–2061–312
Product release: NA012
Document release: Standard 05.03
Date: September 1999

Publication history

September 1999

NA012 Standard 05.03

- made minor edit changes

NA012 Standard 05.02

- made minor edit changes

NA012 Standard 05.01

- Chapter 3 – changed the “User classes” to reflect the feature A59006761
- “About this document” – added *Customer Data Schema Reference Manual* to “References in this document”
- Chapter 1 – corrected the stksize parameter default value (7000) for the PERMIT command

August 1998

DMSCCM03 Standard 04.02

- made format changes

November 1994

DMSCCM03 Standard 04.01

- removed “List of Terms” and added “Index”
- removed “How CDC documentation is organized” from “About this document”
- removed “Where to find information” from “About this document”

July 1992

BCS32 Standard 03.03

- added tables available to CDC users in chapter 3
- added information in chapter 4 for table “Pending order file commands”
- added information to chapter 5

- split the Service Orders commands table into three tables

October 1991

BCS 32 Standard 03.02

- changed information on reference documents in “About this document”

March 1991

BCS32 Standard 03.01

- added Chapter 4
- added PENDING command on page 2-3
- added the section CDC103 log report on page 5-5
- added a table on Service Order commands

September 1990

BCS 31 Standard 02.01

- added QDNA, QIT, and QLT
- added DNAs, LTIDs, and CUGs
- added CDCCUGS, CDCDNASLTID Qwnership, DNA Qwnership, CUG Qwnership, and PH parameters Ownership
- added CDCDNAS and CDCCUGS
- added QLT, QIT, and QDNA

Revision bars in the table of contents identify the sections where technical infomation has been changed. Revisions bars in the outside margin of a page indicate text that has been added or revised.

Contents

About this document

When to use this document

How to check the version and issue of this document

The version and issue of the document are indicated by numbers, for example, 01.01.

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

The second two digits indicate the issue. The issue number increases each time the document is revised but rereleased in the *same* software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

To determine which version of this document applies to the software in your office and how documentation for your product is organized, check the release information in the *DMS-10 and DMS-100 Family Product Documentation Directory,* 297-8991-001.

This document is written for all DMS-100 Family offices. More than one version of this document may exist. To determine whether you have the latest version of this document and how documentation for your product is organized, check the release information in the *DMS-10 and DMS-100 Family Product Documentation Directory,* 297-8991-001.

References in this document

The following documents are referred to in this document:

- *Basic Translations Tools Guide*, 297–1001–360
- *Input/Output System Reference Manual*, 297–1001–129
- *Servord Reference Manual*

- *Translations Guide*

What precautionary messages mean

The types of precautionary messages used in Nortel Networks documents include attention boxes and danger, warning, and caution messages.

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

Examples of the precautionary messages follow.

ATTENTION Information needed to perform a task

ATTENTION

If the unused DS-3 ports are not deprovisioned before a DS-1/VT Mapper is installed, the DS-1 traffic will not be carried through the DS-1/VT Mapper, even though the DS-1/VT Mapper is properly provisioned.

DANGER Possibility of personal injury

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless fuses F1, F2, and F3 have been removed. The inverter contains high-voltage lines. Until the fuses are removed, the high-voltage lines are active, and you risk being electrocuted.

WARNING Possibility of equipment damage

WARNING

Damage to the backplane connector pins

Align the card before seating it, to avoid bending the backplane connector pins. Use light thumb pressure to align the card with the connectors. Next, use the levers on the card to seat the card into the connectors.

CAUTION Possibility of service interruption or degradation

CAUTION
Possible loss of service
Before continuing, confirm that you are removing the card from the inactive unit of the peripheral module. Subscriber service will be lost if you remove a card from the active unit.

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 that the information that follows is a command:

>BSY

Commands and fixed parameters

Commands and fixed parameters that are entered at a MAP terminal are shown in uppercase letters:

>BSY CTRL

Variables

Variables are shown in lowercase letters:

>BSY CTRL ctrl_no

The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string.

Responses

Responses correspond to the MAP display and are shown 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 used in this document:

1 Manually busy the CTRL on the inactive plane by typing

>BSY CTRL ctrl_no
and pressing 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.
```

Setting up a CDC user

This chapter describes the steps required to give a new Customer Data Change (CDC) user access to the CDC features:

- assigning a terminal to a CDC user
- setting up table access for a CDC user
- defining a new CDC user
- setting up a user profile
- defining a remote CDC userid

Assigning a terminal to a CDC user

To assign a terminal to a CDC user, datafill Table TERMDEV in the data schema section of the *Translations Guide*. This table specifies the assignment of each terminal device.

Table TERMDEV also associates command classes with terminal devices. To ensure data security, the DMS-100 controls commands available to a user by associating the userid and the terminal device. Command privileges are grouped into command classes and CDC users are assigned a command class consisting only of those commands needed to perform CDC operations. The command classes range from 0 to 30 and are determined for a userid when it is defined by the PERMIT command.

> ***Note:*** A user can only log in to the DMS if Table TERMDEV is datafilled for the terminal at which the user is working.

Setting up table access for a CDC user

A CDC user may access a table or subtable only if the privilege class assigned to the table or subtable matches the users command class. These privilege classes are defined by adding tuples to Tables CUSTPROT and SUBPROT.

Table CUSTPROT

Table CUSTPROT (customer protection table) is used for table screening. It associates privilege classes to tables. CDC users, based on the control

assigned to their privilege class, may be able to read, change, and add or delete tuples for each table in the DMS-100.

The following table shows how to datafill Table CUSTPROT.

Table 1-1
Datafilling table CUSTPROT

Field	Subfield	Explanation and action
TABNAME		This field defines the table name. Enter the table name.
READPROT		This field defines the command class of users allowed to read the table entered in field TABNAME. Enter a value of 0-30.
UPDTPROT		This field defines the command class of users that can read and update the table entered in field TABNAME. Enter a value of 0-30.
ALLPROT		This field defines the command class that can read, update, and add or delete tuples from the table entered in field TABNAME. Enter a value of 0-30.
VALACC		This field defines the valid access. If the DMS-100 has the Security Enhancement feature and log TABL101 is required, enter WRITE. IF log TABL100 and TABL101 are required, enter ALL. If the Security Enhancement feature is not provided or logs TABL100 and TABL101 are not required enter OFF.
DENACC		This field defines the denied access. If the DMS-100 has the Security Enhancement feature and log TABL103 is required, enter WRITE. IF log TABL102 and TABL103 are required, enter ALL. If the Security Enhancement feature is not provided or logs TABL102 and TABL103 are not required enter OFF.

Note: The Security Enhancement feature allows operating companies to monitor access to tables through the generation of logs.

Table SUBPROT

Table SUBPROT (subtable protection table) is datafilled to screen CDC user's access to subtables. Datafill in this table is only required when one or more of the following subtables requires a command class different from it's control table.

- ATTRIB (control table HNPACONT)
- FNPACODE (control table FNPACONT)

- FNPASTS (control table FNPACONT)
- HNPACODE (control table HNPACONT)
- RTEREF (control table FNPACONT)
- RTEREF (control table HNPACONT)

The following table shows how to datafill Table SUBPROT.

Table 1-2
Datafilling Table SUBPROT

Field	Subfield	Explanation and action
TABNAME		This field contains subfield TABNAME and SUBNAME.
	TABNAME	This field defines the control table name. Enter FNPACONT or HNPACONT.
	SUBNAME	This field defines the subtable name. Enter the subtable name.
READPROT		This field defines the command class of users that can read entered in field SUBNAME. Enter a value of 0-30.
UPDTPROT		This field defines the command class of users that can read and update the subtable entered in field SUBNAME. Enter a value of 0-30.
ALLPROT		This field defines the command class that can read, update, and add or delete tuples from the subtable entered in field SUBNAME. Enter a value of 0-30.

Read or change only tables for CDC users

The following table list tables that should be defined as read or change only for CDC users. CDC users should *not* be given permission to add or delete tuples from these tables.

Table 1-3
Read or change only tables for CDC users

Table name	Userid ability
Table XLANAME	Change only
Table HNPACONT	Change or read only
Table FNPACONT	Read only

—continued—

Table 1-3
Read or change only tables for CDC users (continued)

Table name	Userid ability
Subtable FNPASTS	Read only
Table LCASCRCN	Change only
Table CLSVSCRN	Change only
Table COSMAP	Change only
Table STDPRTCT	Change only
Table DIGCOL	Change only
Table TODHEAD	Change only
Table VFGENG	Change or read only

Note 1: Use the CI command LISTTABS to show the tables that are available to a CDC user.
Note 2: Autologin is a feature that allows a user who is permanently associated with a terminal, or who uses the terminal frequently, to log in quickly without entering the password. Autologin is applied to a terminal when the device name entered in the TERMDES field of Table TERMDEV is the same as the userid (using PERMIT). When the userid is entered, the terminal is automatically logged in.

—end—

Defining a new CDC user

A CDC user is defined through use of the PERMIT command. The PERMIT command defines a new userid and associates one or more command classes with the userid. CDC users are allowed to use only those commands that are valid for their command class(es).

PERMIT command

Use the PERMIT command to define CDC user attributes in a DMS-100. PERMIT can also be used to change attributes. The changed attributes are recognized immediately. A warm restart is not required.

PERMIT command parameters and variables

Command	Parameters and variables					
PERMIT	*userid*	*pass*	*priority*	*stksize*	ENGLISH	*cmdcls*
					FRENCH	ALL
					SPANISH	
					default	

Parameters and variables	Description
userid	Defines the DMS user's login identification.
pass	Specifies the password assigned to the userid at login time.
priority	Defines the level the users' process will run. The range is 1 to 4 with 4 being the highest and default value.
stksize	Identifies the size of the stack assigned to this user's process. The range is 1,500 to 10,000. The default value is 7,000.
ENGLISH	Sets the system's output messages and input commands to English.
FRENCH	Sets the system's output messages and input commands to French.
SPANISH	Sets the system's output messages and input commands to Spanish.
default	Sets the system's output messages and input commands to a language defined in Table OFCENG.
cmdcls	Specifies the classes available to the userid. The class values are the same as the values assigned to command s. The range is 0 to 30.
ALL	Makes a command available to the userid.

Example

The following example shows the PERMIT command being used to add a userid to the DMS-100.

Examples of the PERMIT command

PERMIT *FRED PASSW 3 3000 ENGLISH 1*
where

The *userid* is Fred.
The *pass* is PASSW.
The *priority* is 3.
The *stksize* is 5000.
The specified language is English.
The *cmdcls* is 1.

CAUTION
Setting a userid command class to ALL allows a user to access all commands in a central office. The operating company should assign a command class to any table it does not want a CDC user to have access.

Setting up a user profile

A profile is a store file on disk or Store File Device (SFDEV) with commands that provide the userid with a logon configuration. To create a user profile, a file or SFDEV is created and converted into a user profile by using the PROFILE LOGIN and PROFILE RESTART commands.

Store File Device

A store file on a disk or SFDEV for the CDC user must be defined before a user profile can be created. For more information on creating a store file, see *Basic Translations Tools Guide*, 297-1001-360.

Login and restart profiles

The login and restart profiles are read automatically by the CI when the userid logs into the CDC terminal and enters their first carriage return (CR). The user profile contains commands that provide the CDC user with normal configuration.

The following table shows the two profiles associated with each userid:

Table 1-4
User profiles

Profile	Explanation
Login Profile	Executed automatically when the user logs in, unless the NOPROFILE command is entered as the first command.
Restart Profile	Executed if a command gets trapped or if the user stops a CI process by entering: <break> HX.
Note: The use of the NOPROFILE command is subject to command screening.	

The following command changes an existing file into a profile file.

PROFILE LOGIN *filename*
PROFILE RESTART *filename*
LOGOUT
where

The *filename* is the name of the profile file.

Defining a remote CDC userid

A userid can also be set up for a user working from a remote location. A CI process called a disconnected user process, can be created to accept input from a file instead of a terminal. The LOGIN command is used to create a disconnected user process for a userid.

LOGIN command

The LOGIN command activates a known userid and creates a disconnected user process in the DMS-100. The remote user can then access commands defined by the PERMIT command when the userid was created.

LOGIN command parameters and variables

Command	Parameters and variables				
LOGIN com	*userid*	*passw*	*infile*	*outdev*	*outfilename*

Parameters and variables	Description
userid	Specifies a string of characters the system recognizes as a userid.
password	Specifies the password assigned to the userid. The password is ignored if the position is defined as an auto login position.
infile	Specifies the name of an alternate profile to be executed before the first CI command.
outdev	Specifies an alternate output device where system responses should be sent. Use the SEND PREVIOUS command to restore the output device.
outfilename	Specifies the file name to be assigned to the output if the outdev is a tape device or a storage device.

CAUTION

For security reasons, autologin should be assigned only to local terminals, not to dial-up or remote terminals. The operating company should ensure that none of the device names at non-local terminals match any valid userid. If a match exists, an unauthorized autologin can result.

The userid logs in according to the usual rules pertaining to the validity of the userid and password. Input is taken from a specified file, and output is directed to a specified device.

Examples

The following examples shows the LOGIN command being used to add a remote user to the DMS-100.

The first example shows how to gain access to autologin position FRED.

Examples of the LOGIN command

LOGIN *FRED*
where

The *userid* is Fred.

After gaining access to the autologin position FRED, the user accesses a position.

Examples of the LOGIN command

LOGIN *HAWAII HOTDAY MIAMI PRT LOG*
where

The *userid* is HAWAII.
The *password* is HOTDAY.
The *infile* is MIAMI.
The *outdev* is PRT.
The *outfilename* is LOG.

Ensuring data security

This chapter describes how to limit CDC user access to commands and data tables, and how to record CDC user activity.

Command screening

Command screening allows an operating company to prevent CDC users from having access to unauthorized commands. There are two forms of command screening:

- Regular Command Screening
- Enhanced Command Screening

Regular command screening

Regular command screening gives CDC users limited access to commands needed to perform CDC operations.

Command privileges are grouped into command classes. The command classes are associated by commands and datafill in tables. The commands and tables required to associate command classes are listed below.

Table 2-1
Controlling tables and commands

Table CMDS		associates command classes with command names
Table TERMDEV		associates command classes with terminal devices
Table CUSTPROT		associates privilege classes to tables for CDC users
Table SUBPROT		associates privilege classes to subtables for CDC users
User profiles		associated with each LOGON_ID. Two profiles types are login profile and restart profile.
	Login profile	executed automatically when the user logs in
Note: With regular command screening, a command can have only one command class.		
—continued—		

Table 2-1
Controlling tables and commands (continued)

	Restart profile	executed if a command is trapped, or if the user stops his CI process by entering: <break> HX.
PERMIT command		associates one or more command classes with each LOGON_ID
Note: With regular command screening, a command can have only one command class.		
—end—		

Enhanced command screening

Enhanced Command Screening allows commands to be assigned to more than one command class. CDC users will only have access to commands in their command class(es).

The Enhanced Command Screening feature should be used in conjunction with the CDC feature (NTX412) to provide data security.

CAUTION
If the office does not have the Enhanced Command Screening feature, commands omitted from Table CMDS are available to all users.

To ensure that CDC users cannot amend or bypass their control profile, the PROFILE command must be entered in the Table CMDS with a command class that can not be assigned to CDC users.

Enhanced Command Screening is activated through the ENHANCED_COMMAND_SCREENING office parameter in Table OFCOPT.

When the ENHANCED_COMMAND_SCREENING office parameter is set to Y (yes), commands can be assigned any subset of 31 command classes. Subcommands from the CI increment can be also screened.

When the ENHANCED_COMMAND_SCREENING field is set to N (no), regular command screening is active. Regular command screening allows the assignment of only one class number per command.

For more information on Command Screening, refer to *Input/Output System Reference Manual*, 297-1001-129.

Setting up CDC commands

CDC commands are set up using the CDCSETUP command. The CDCSETUP command allows CDC users access to only commands needed to perform CDC operations. This command can be included in the Login Profile so that when the user logs in to the DMS, the CDCSETUP command creates a special directory of commands.

CDCSETUP command

The following example shows how to execute the CDCSETUP command.

Examples of the CDCSETUP command

CDCSETUP*environment*
and pressing the Enter key.
where
The *environment* is optional. It can be TELCO or NONTELCO. The default is NONTELCO.

When the environment is TELCO, the user has access to the special directory and all other user directories. Therefore, the user has access to all other commands available in the office. When the environment is NONTELCO, the user has access to the commands listed in the special directory created by the CDCSETUP command.

A standard CDC profile can be created and shared by all CDC users.

The CDCSETUP command does not allow other CI commands and subcommands to be screened. If Enhanced Command Screening is used, command screening applies to the CDCSETUP command and all commands available in the CDC increment.

After executing the CDCSETUP command, all other directories are taken away, leaving the user in the CDC increment. The LEAVE command can be used to leave the CDC increment, only if the environment is TELCO.

```
CDC:
```

Commands for CDC users

The following table list commands should be included in a command class for CDC users.

Table 2-2
CDC user commands

Command	Description
DATE	shows the current switch date
TIME	shows the current switch time
LOGOUT	logs a userid out of DMS-100
PASSWORD	changes a login password (optional)
SERVORD	enters the userid into the Service Order system
LEAVE	leaves from an increment
QDN	queries a Directory Number
QLEN	queries a Line Equipment Number
DEFAULT	sets certain CDC parameters
RESET	resets CDC parameters
PTE	enters the userid into the Table Editor
QGRP	queries Groups
QDNA	queries Data Network Addresses
QIT	queries ISDN terminals
QLT	queries logical terminals
PENDING	accesses the userid to the PO subsystem

The PERMIT command is used to associate the command classes with a userid. The PERMIT command associates one or more command classes with each LOGON_ID.

Table TERMDEV must be datafilled to associate the command class with the terminal device for dial-up ports used by a CDC userid.

The userid must be datafilled in Table CDCLOGON.

Logging CDC user activity

The following table list the three log reports available for recording CDC user activity.

Table 2-3
Log reports that record CDC user activity

CDC101	Records all CDC Service Order commands. This report, which can be used for billing purposes, contains the entire command string entered by the CDC user.
CDC102	Records Table Editor activity when a CDC user adds, changes, or deletes a tuple from a table.
CDC103	Records when a pending service order is entered.

Activating CDC log reports

The CDC101, CDC102, and CDC103 logs are controlled by the CUSTOMER_DATA_CHANGE_LOGS office parameter.

The following example shows how to datafill office parameter CUSTOMER_DATA_CHANGE_LOGS.

Datafill procedure for CUSTOMER_DATA_CHANGE_LOGS

Table OFCVAR Parameter	Explanation and action
CUSTOMER_DATA_CHANGE_LOGS	This parameter control whether or not CDC 101, CDC 102, or CDC103 log reports are generated. Enter Y for yes, N for no.
Note: Commands that are not part of the SERVORD increment (for example, QDN is a CI command) are not subject to command logging.	

The CUSTOMER_DATA_CHANGE_LOGS office parameter can be changed at any time and the change will take effect immediately. Command logging applies to all CDC users.

Note: For Pending Order logs, see the “Pending order files” section.

Setting up permanent log report routing

CDC log reports can be routed from the log system buffers to an I/O device, where they are printed, displayed or stored. This subsystem is controlled by two data tables. To set up permanent routing for CDC log reports, datafill the following tables:

- LOGCLASS – (associates a unique log class with the CDC log reports)

- LOGDEV – (associates the log class given in table LOGCLASS with an output device)

Setting up temporary log report routing

LOGUTIL is a CI increment that allows the operating company to control the routing and retrieval of log reports. Since the log system has a limited amount of storage, only the most recent log reports are accessible through LOGUTIL.

LOGUTIL commands

LOGUTIL commands allow temporary routing changes to supersede permanent entries. Permanent routing entries are not changed when temporary routing changes are made.

The following shows how to execute the LOGUTIL command.

Examples of the LOGUTIL

LOGUTIL
where
LOGUTIL is the command to access LOGUTIL commands.

CLASS *logname n*
where
CLASS is the command to set the class of the log report.
The *logname* is the name of the log.
The *n* is the report class number (0 to 31).

START n
and pressing the Enter key.
where
The *n* is the report class number (0 to 31)

Setting up data ownership

This chapter describes how to do the following:

- order of table datafill
- define a new owner
- establish ownership of data, LENS, DNs, DNAs, LTIDs, CUGs, and line options
- change an existing user into a CDC user
- identify tuple ownership in data tables

Table datafill order

When datafilling CDC information, tables must be datafilled in the following order.

- Table OWNER
- Table DATAOWNR
- Table IBNLINES
- Table KSETINV
- Table CDCLENS
- Table CDCDNS
- Table CDCDNAS
- Table CDCCUGS
- Table CDCOPTS
- Table CDCLOGON

Note: Table IBNLINES and KSETINV should be datafilled through SERVORD.

Defining a new owner

CDC data can be changed only by the owner of that data. If a new CDC user is not associated with an existing entry in Table OWNER, then a tuple must be added to this table.

Table OWNER

Table OWNER defines the (OWNER_ID). It contains two fields, owner and public.

Each tuple in Table OWNER contains the owner's identification (OWNER_ID) and specifies whether or not other owners are allowed to view this owner's data through the field PUBLIC. Ownership of the appropriate data is then assigned to this new owner.

When a tuple is deleted from Table OWNER, the following warning is displayed:

Figure 3-1
Warning message when a tuple is deleted

```
****************** WARNING *****************
This owner may be referred by the following
tables:
CDCLOGON, DATAOWNR, CDCLENS, CDCDNS, DNOWN,
CDCDNAS & CDCCUGS
Please check and delete them, else these
tables will contain undefined data.
************ END OF WARNING ***************
```

NILOWNER

When a telephone line belongs to a Customer Group with no owner or unowned items exist, the switch inputs the name NILOWNER as the owner. Table Editor does not allow NILOWNER to be datafilled as an OWNER_ID in Table OWNER.

Field public

If field public is set to Y, other owners are allowed to view all the data assigned to the new owner.

The ADD command is used to add a new owner to Table OWNER.

Using the add command to add a OWNER_ID to Table OWNER

The following procedure shows how to use the ADD command to set up a new owner called FRED.

System prompt	User input
>	**table owner**
TABLE OWNER:	
>	**add**
OWNER:	
>	**fred**
PUBLIC:	
>	**y**

Ownership of data

CDC OWNER_IDs have access to tables through the Partitioned Table Editor. Ownership information for a table or subtable is defined in Table OWNTAB, which is datafilled as part of the LOAD BUILD process.

Access to a table or subtable is possible only if the privilege class assigned to the table or subtable matches the command class of the user. These access rights are defined by adding tuples to Tables CUSTPROT and SUBPROT.

After changes have been made to the data controlling datafill ownership, a CDC user must do one of the following before the changes will be evident.

- Logout and login
- Use the ’default owner’ command
- Use the ’reset owner’ command

Table DATAOWNR

Table DATAOWNR contains the data associated with an OWNER_ID that a CDC user has access. Any additional data required for the CDC user must be added to Table DATAOWNR.

The field OWNER in table DATAOWNR identifies the owner associated with the subsets of data.

Use the ADD command in table DATAOWNR to add data for each owner.

Adding a customer group to Table DATAOWNR

In order for a CDC user to access IBN lines, (such as business sets, display sets and data units) the customer group must be datafilled in Table DATAOWNR and owned by a CDC owner. Business sets, display sets and data units are multiple key sets. The DMS allows the Operating Company to assign directory numbers belonging to different customer groups to the same business set or data unit.

If a new OWNER_ID has been created for an existing customer group whose data ownership is already set up, the status of the new user will now be changed to CDC user status.

If a OWNER_ID of a customer group is changed in Table DATAOWNR, the OWNER_ID for all LENs belonging to that customer group are automatically changed in Table CDCLENS.

The following example shows the ADD command adding customer group POTSDATA to Table DATAOWNR for owner FRED.

System prompt	User input
>	**table DATAOWNR**
TABLE DATAOWNR:	
>	**add**
TABNAME:	
>	**custgrp**
CUSTNAME:	
>	**potsdata**
OWNER:	
>	**fred**

Adding a Virtual Facility group to Table DATAOWNR

In this example, the ADD command is used to add Virtual Facility Group POTSVFG to Table DATAOWNR for owner FRED.

System prompt	User input
>	**table dataownr**
TABLE DATAOWNR:	
>	**add**
TABNAME:	
>	**virtgrp**
PUBLIC:	
>	**potsvfg**
OWNER:	
>	**fred**

Virtual Facility group tables

Table VFGDATA and Table VFGENG handle ownership of data contained in Table VIRTGRPS. Table VFGDATA stores customer group data for the incoming and outgoing ends of the VFG. Either end can be an IBN VFG or a POTS VFG.

Table VFGENG stores information about the size of each VFG. Only operating company users are allowed access to Table VIRTGRPS.

VFGNAME is the key to Table VIRTGRPS. The VFGNAME field associates ownership of each tuple.

Adding a user owned by another user to Table DATAOWNR

An owner can be owned by another owner. CDC users are allowed access to only that data which is datafilled in Table DATAOWNR for the OWNER_ID that they belong.

In this example, the ADD command is used to add owner ADMIN, which is owned by owner CNCP.

System prompt	User input
>	**table dataownr**
TABLE DATAOWNR:	
>	**add**
TABNAME:	
>	**owner**
OWNER:	
>	**admin**
OWNER:	
>	**cncp**

Tables identifying ownership

The following tables store CDC ownership information:

- Table CDCLENS
- Table CDCDNS
- Table CDCDNAS
- Table CDCCUGS

Table CDCLENS

Table CDCLENS stores the ownership information for Line Equipment Numbers (LEN) and Logical Terminal Identifiers (LTID).

LENs must also be assigned in Tables IBNLINES and KSETINV. LTIDs must be defined in Table LTDEF. Any LEN added to Table IBNLINES or KSETINV and assigned the CDC option through service orders will automatically be datafilled in Table CDCLENS.

A LEN that is assigned in Table CDCLENS cannot be used in any other lines table, with the exception of Tables IBNLINES and KSETINV. For example, a LEN that appears in Table CDCLENS becomes invalid for use in Table LENLINES, because it is now reserved for MDC use only. When the LEN is deleted from Table CDCLENS, it again becomes valid for use in Table LENLINES.

LEN ownership

Tuples in Table CDCLENS contain field LEN and OWNER. The field OWNER is the same as field OWNER in Table OWNER. The LEN is assigned to customer group. The DMS rejects any attempt to datafill that LEN in Table IBNLINES under a different customer group.

A LEN can be added to Table CDCLENS only under one of the following circumstances:

- The LEN is assigned in Table IBNLINES, and the OWNER_ID of that customer group matches the OWNER_ID in the tuple to be added to Table CDCLENS.
- The LEN appears in Table LNINV, but does not appear in any lines tables.
- The LEN appears in the Table KSETINV.
- The CDC option is added through SERVORD to the LEN in Table IBNLINES for IBN lines or to the LEN in Table KSETINV for business sets, display sets, and data units.

Before a user can access a LEN or LTID, the OWNER_ID must be datafilled in Table CDCLENS. Ownership of a LEN, or an LTID is removed by deleting the LEN, or LTID from Table CDCLENS.

Note 1: When the LEN of an IBN line is in Table CDCLENS, the CDC option is automatically added to the line.

Note 2: To delete the CDC option from a 500/2500 set, the set's LEN must be deleted from Table CDCLENS.

Adding the CDC option to LENs

The following examples show the CDC option added through SERVORD with the CHF command.

Adding the CDC option to LEN in Prompt mode

```
>CHF
SONUMBER: NOW 91 12 7 PM
>
DN_OR_LEN:
>01 0 01 01
OPTION:
>CDC
OPTION:
>$
```

Adding the CDC option to LEN in No-prompt mode

```
>CHF $ 01 0 01 01 CDC $
```

Note 1: When the CDC option is assigned to a LEN in Table IBNLINES or Table KSETINV, the LEN automatically appears in Table CDCLENS.

Note 2: Before LEN 01 0 01 01 can be assigned to an owner, a tuple that associates its customer group with an owner must be datafilled Table DATAOWNR. Use the add command to do this. See page 3-3 for an example of adding a tuple to Table DATAOWNR.

LTID ownership

If the line is an ISDN line, field LEN in Table CDCLENS is replaced by field Logical Terminal Identifier (LTID). The field LTID consists of two subfields: LTGRP and LTNUM.

The LTID must appear in table LTDEF before it can be added to table CDCLENS. Tables LTDEF and KSETINV are automatically datafilled with LTIDs when the operating company sets up logical terminals with the SLT ADD command.

When the CDC option appears with an LTID in table KSETINV, the LTID is automatically added to table CDCLENS.

Removing an LTID from table CDCLENS will automatically remove the CDC option for this LTID from table KSETINV.

Using the add command to add an LTID

In this example, the add command is used to add an LTID to Table CDCLENS.

System prompt	User input
>	**table cdclens**
TABLE CDCLENS:	
>	**add**
LEN:	
>	**ISDN 2**
OWNER:	
>	**BNR**

Table CDCDNS

Table CDCDNS lists the directory numbers (DN) assigned to a customer group that has the CDC feature. One entry is required for each DN or block of DNs assigned to a customer group.

Table CDCDNS must also be datafilled for that OWNER_ID to have access to the DN for that LEN.

When a tuple is added or changed to Table CDCDNS, Tables IBNLINES and KSETINV are checked to determine if the LEN also appears in Table CDCLENS. If the LEN is found in Table CDCLENS, the OWNER_ID must be the same. Otherwise, the Data Modification Order (DMO) is rejected.

DN ownership

To assign directory numbers to an owner, Table CDCDNS must be datafilled. The information for Table CDCLENS is downloaded from SERVORD or can be added in table entry. The following examples show how to add DNs to Table CDCDNS through data entry.

Using the add command to assign a block of DNs

In the following example, the ADD command is used to assign a block of directory numbers to Table CDCDNS.

System prompt	User input
>	**table cdcdns**
TABLE CDCDNS:	
>	**add**
SNPA:	
>	**613**
NXX:	
>	**777**
PROMDIGS:	
>	**4112**
TODIGS:	
>	**4222**
OWNER:	
>	**BNR**

Table CDCDNAS

Table CDCDNAS stores the ownership information for Data Network Addresses (DNA) for ISDN lines.

Use the ADD command in Table CDCDNAS to add Data Network Addresses for an owner.

Using the add command to assign a Data Network Address

In this example, the ADD command is used to assign a Data Network Address to Table CDCDNAS.

System prompt	User input
>	**table cdcdnas**
TABLE CDCDNAS:	
>	**add**
DNA:	
>	**1000**
OWNER:	
>	**bnr**

Note: Access to DNAs also depends on ownership information in Tables CDCLENS, CDCPHPAR and CDCCUGS. Table OWNTAB must be datafilled before Table CDCDNAS.

Table CDCCUGS

Table CDCCUGS stores ownership information on Closed User Groups (CUGs) for ISDN packet data.

CUG ownership

Table CDCCUGS stores ownership information on Closed User Groups for ISDN packet data.

Each tuple stores the CUG Number (CUGNUM), the CUG Type (CUGTYPE), and the CUG Data Network Identification Code (CUGDNIC).

Use the ADD command in table CDCCUGS to add Closed User Groups for an owner.

Using the add command to add a Closed User Group

In this example, the ADD command is used to assign a Closed User Group to table CDCCUGS for the national area.

System prompt	User input
>	**table cdccugs**
TABLE CDCCUGS:	
>	**add**
CUGNUM:	
>	**34**
CUGTYP:	
>	**n**
OWNER:	
>	**bnr**

Using the add command to add a Closed User Group to an international area

In this example, the ADD command is used to assign a Closed User Group to table CDCCUGS for an international area.

System prompt	User input
>	**table cdccugs**
TABLE CDCCUGS:	
>	**add**
CUGNUM:	
>	**13456**
CUGTYP:	
>	**1**
CUGDNIC:	
>	**8745**
OWNER:	
>	**civic**

Ownership of Packet Handler parameters

Table CDCPHPAR

Table CDCPHPAR provides a list of parameters for the Packet Handler commands. The datafill indicates whether these parameters can be changed by CDC. At load time, this table is datafilled to default values ('N' in the CHANGE field), indicating that CDC ownership of PH parameters is not allowed.

Use the Change command in Table CDCPHPAR to set the CHANGE field to 'Y', allowing CDC users to access the specified PH command parameters.

Using the change command to allow CDC access to parameter NORMCHRG

In the following example, the change made to Table CDCPHPAR will allow the CDC user to access parameter NORMCHRG for direct calls (DC) within the Packet Handler command options.

System prompt	User input
>	**table cdcphpar**
TABLE CDCPHPAR:	
>	**pos**
PARMNAME:	
>	**dc**
OPTION:	
>	**normchg**
DC NORMCHG: N	
>	**change**
CHANGE: N	
>	**y**

Using the change command to allow CDC access to parameter MRECVTPT

In this example, the change made to Table CDCPHPAR will allow the CDC user to access parameter MRECVTPT for permanent virtual circuits (PVC) within the Packet Handler command options.

System prompt	User input
>	**table cdcphpar**
TABLE CDCPHPAR:	
>	**pos**
PARMNAME:	
>	**pvc**
OPTION:	
>	**mrecvtpt**
PVC MRECVTPTN: N	
>	**change**
CHANGE: N	
>	**y**

Ownership of options

A customer group and the options assigned to it must be datafilled in Table CDCOPTS for a CDC user to add those options to a line assigned to that customer group.

Table CDCOPTS

Use the ADD command to add options to a customer group in table CDCOPTS.

Options are assigned to customer groups, not owners.

If there are no entries for a customer group in table CDCOPTS, a CDC user associated with that customer group can not assign any options.

Using the add command to assign options

In this example, the ADD command is used to assign options LNR and PRK to customer group COMKODAK.

System prompt	User input
>	**table cdcopts**
TABLE CDCOPTS:	
>	**add**
CUSTGRP:	
>	**comkodak**
OPTIONS:	
>	**lnr**
OPTIONS:	
>	**prk**
OPTIONS:	
>	**$**

Using the add command to assign options

In this example, the ADD command is used to assign options AIOD and ITD to customer group CENTESN.

System prompt	User input
>	**table cdcopts**
TABLE CDCOPTS:	
>	**ADD**
CUSTGRP:	
>	**CENTESN**
OPTIONS:	
>	**AIOD**
OPTIONS:	
>	**ITD**
OPTIONS:	
>	**$**

Changing an existing user into a CDC user

Table CDCLOGON

The purpose of table CDCLOGON (Customer Data Change Logon) is as follows:

- associates the LOGON_ID with the OWNER_ID
- assigns the user class
- allows a pending order file

The table also enforces ownership of data in the office. If the addition of the user to table CDCLOGON does not occur, the user can access all the data in the office, such as customer groups and trunk groups.

User classes at the CI increment

The following userclass privileges support the CI increment:

- TELCO – can view and change all data
- GENERAL – can view and change data owned by the OWNER_ID and all data that is public
- OBSERVER – cannot change any data, but can view data owned by a OWNER_ID and public data
- NONUSER – cannot view or change any data

User classes at the LTP MAP level

The command screening at the Lines Test Position (LTP) maintenance and administration position (MAP) level provides the user classes and privileges as follows:

- TELCO – can view and change all data
- GENERAL – can view and change data owned by the OWNER_ID
- OBSERVER – cannot view or change any data
- NONUSER – cannot view or change any data

Using the add command to datafill table CDCLOGON for a new user

Use the ADD command to enter information for a new user to table CDCLOGON. The new user OWNER_ID is BNR and the new user can view and change all data owned by this OWNER_ID. There is no Pending Order File (POF).

System prompt	User input
>	**table cdclogon**
TABLE CDCLOGON:	
>	**add**
USERNAME:	
>	**<LOGON_ID>**
OWNER:	
>	**BNR**
CLASS:	
>	**GENERAL**
POF:	
>	**N**

The LOGON_ID must be the same LOGON_ID that was used when the PERMIT command was used to create a new user.

If the field POF is set to N, the commands do not prompt for the SONUMBER in SERVORD.

Partitioned table editor

A CDC user can access tables and subtables by means of the Partitioned Table Editor. To access a table or subtable, the privilege class assigned to the table or subtable must match the command class of the user.

To use the Partitioned Table Editor from the CDC: increment, enter:

```
PTE
```

The following table lists the data tables that can be accessed by CDC users. They are partitioned and CDC users can see only their datafill.

Note: Only the tables listed in Table 3-1 are partitioned. If a telephone operating company gives CDC users access to other tables, the CDC user can see all datafill in the table.

Table 3-1
Tables available to CDC users through PTE

Table	Form	Description
AUTHCDE	2244	defines the authorization code and its attributes. KEY: AUTHPART (Partition name) and AUTHCODE (Authorization Code). OWNERSHIP: Field AUTHPART
AUTHPART	2243	defines the partition in the authorization code database where the authorization codes are stored for a customer group or Call Forwarding Remote Access (CFRA) lines. KEY: PARTNM (Partition name) OWNER: Field PARTNM (Partition name) determines ownership.
CGNSCRN	2345	this table is used for the Virtual Access to Private Networks (VAPN) feature. this table screens VAPN automatic number identification (ANI). Key: FROMDIGS and TODIGS (the range of AIN). OWNERSHIP: Table DNOWN determines ownership.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
CLSVSCRC	2463	provides for screening NPA code, class of service, type of call, and digits dialed. KEY: STS (Serving Translation Scheme), SCRNCL (Screening Class), and TYPCALL (Type of Call) OWNERSHIP: The STS field and the SCRNCL field indicate tuple ownership 1 Table CLSVSCRC is a head table for Subtable CLSVSCR 2 This table should be Change Only for CDC users.
CODEBLK	2234	lists code restriction of dialed calls. Each unique set of code restrictions is defined as a Code Restriction Level (CRL) which can be a number from 1 to 15. KEY: CUSTOMER (Customer Group Name) and NUMBER (the called number – up to 18 digits) OWNERSHIP: The CUSTOMER field indicates tuple ownership.
COSDATA	2251	provides the actual mapping of NCOS for the mapping names in the COSMAP table. KEY: MAPNAME and COS field OWNERSHIP: The MAPNAME field indicates tuple ownership.
COSMAP	2250	Tables COSMAP and COSDATA provide the facility for mapping one set of NCOS into another. Table COSMAP defines the mapping name and certain defaults. KEY: MAPNAME (COS Mapping Name) OWNERSHIP: The MAPNAME field indicates tuple ownership. This table should be Change Only for CDC users.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
CUSTCONS	2237	lists data and attendant console options for customer groups with consoles. KEY: CUSTNAME (Customer Group Name) OWNERSHIP: The CUSTNAME field indicates tuple ownership.
CUSTHEAD	2236	lists the customer groups and the parameters and options associated with each. KEY: CUSTNAME (Customer Group Name) OWNERSHIP: The CUSTNAME field indicates tuple ownership.
CUSTSMDR	2239	lists the Station Message Detail Recording (SMDR) options assigned to each of the customer groups. KEY: CUSTNAME (Customer Group Name) OWNERSHIP: The CUSTNAME field indicates tuple ownership. Billing considerations may necessitate this table as being READ ONLY.
CUSTSTN	2238	lists the station options assigned to each of the customer groups. KEY: CUSTNAME (Customer Group Name) OWNERSHIP: The CUSTNAME field indicates tuple ownership.
DAYOWEEK	2262	defines the day-type for each day of the week (for each TOD system). KEY: TODNAME (Time-of-Day Name) and DAY OWNERSHIP: The TODNAME field indicates tuple ownership.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
DAYOYEAR	2263	defines the day-type for any special days of the year. It is used to override the DAYOWEEK table. KEY: TODNAME and MONTH and DAY OWNERSHIP: The TODNAME field indicates tuple ownership.
DIGCOL	2201	is required for IBN digit collection. KEY: DATNAME (Name of Digit Collection Table) and DIGIT (0-9, *, or #) OWNERSHIP: The DATNAME field indicates tuple ownership. This table should be Change Only for CDC users. Default should be: 'RPT'.
DIGMAN	2242	defines commands used in outpulsing and retranslation for simplified dialing. KEY: DMIKEY (Digit Manipulation Key) OWNERSHIP: The DMIKEY field indicates tuple ownership.
FNMAP	2223	lists the feature to which each of the attendant console keys (numbered 2 to 43) are assigned on each of the attendant consoles. (Key numbers 0 and 1 on all the consoles are for night service). KEY: CONSCLLI (Console Common Language Location Identifier) and ACKEY (2 - 43) Attendant Console Key. OWNERSHIP: The CONSCLLI field indicates field ownership.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
FNPACONT	2410	is used for routing six-digit translation. KEY: NPA (the three digit FNPA code) 1 Table FNPACONT is a head table for Subtable FNPASTS 2 All tuples are accessible to all users. 3 This table must be Read Only for all CDC users. Subtables RTEREF and FNPACODE of Table FNPACONT must be made unavailable to the CDC user through table SUBPROT.
FNPACONT. FNPASTS (subtable)	2412	is used for partitioning six-digit translation. KEY: STS (three-digit code) OWNERSHIP: The STS field indicates field ownership. 1 Subtable FNPASTS is head table for Subtables STSCODE and RTEREF 2 This table should be Read Only with the COMMON_FNPA field set to 'N' to ensure subtable RTEREF is created for each STS.
FNPACONT. FNPASTS STSCODE (subtable)	2413	is provided for each STS specified in the FNPASTS table. KEY: KEY (three-digit code)
FNPACONT. RTEREF (subtable)	2432	consists of route lists. KEY: RTE (Route Reference Index)
FTRGDEFS	2178	allows residential and business features to be packed into logical grouping that can be assigned to individual lines with a single Service Order prompt. KEY: FTRGRP (Feature Group Name) OWNERSHIP:

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
FTRGOPTS	2180	assigns line options to all feature groups defined in an office. KEY: FTRGRP (Feature Group Name) and OPTION (Feature Group Option) OWNERSHIP:
HNPACONT	2400	is used for POTS and private network translation. KEY: STS (Serving Translation Scheme) OWNERSHIP: The STS field indicates the field ownership. 1 Table HNPACONT is a head table with Subtables HNPACODE, RTEREF, and ATTRIB 2 This table should be Change Only or Read Only for CDC users.
HNPACONT. ATTRIB (subtable)	2402	is used for call screening and Equal Access. KEY: LATTIX (LATA Attribute Index)
HNPACONT. HNPACODE (subtable)	2401	lists the route, treatment, or table to which translation is to route for each of the codes dialed by the user. KEY: FROMDIGS and TODIGS (range of digits to be translated) For the CDC user, the head table tuple must be visible for a subtable to be accessible.
HNPACONT. RTEREF (subtable)	2430	specifies the list of routes associated with code datafilled in table HNPACODE. KEY: RTE (Route Reference Index)

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
IBNRTE, IBNRT2, IBNRT3, IBNRT4	2433	contains route lists, which may consist of up to eight routes that are identified by a route reference index number. KEY: RTE (Route Reference Index) OWNERSHIP: The RTE field indicates tuple ownership. 1 CDC users are restricted to 'T' or 'SK' in field CONDRTE. 2 For CDC users, IBNRTE/2/3/4 are correct inputs in field TABNAME when specifying 'T' type routes.
IBNTREAT	2215	is required for the routing of lines to customer definable treatments. KEY: CUSTGRP (Customer Group Name) and IBN treatment number. OWNERSHIP: The CUSTGRP field indicates tuple ownership.
IBNXLA	2228	stores data for digit translation of calls from IBN stations, attendant consoles, incoming IBN trunk groups, or Virtual Facility Groups. KEY: XLANAME (Translator Name) and DGLIDX (the dialed digits) OWNERSHIP: The XLANAME field indicates tuple ownership. For CDC users, IBNRTE is the only valid input in field TABNAME when specifying 'T' type routes.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
LCASCRCN	2460	lists the number of Local Calling Area Screening subtables and the serving area NPA to which each belongs. KEY: STS (Serving Translation Scheme) and LCANAME (Local Calling Area Name) OWNERSHIP: The STS field and the LCANAME field indicate tuple ownership. 1 Table LCASCR is a head table with Subtable LCASCR and CLSVSCR. 2 This table should be Change Only for CDC users.
LCASCRCN. LCASCR (subtable)	2461	determines, based on the digits dialed, whether a call is to be local or non-local termination. KEY: FROMDIGS (digits dialed)
LCASCRCN. CLSVSCR (subtable)	2464	is only required if the screening of the call is dependent upon the digits dialed. KEY: FROMDIGS (digits dialed)
LINEATTR	2208	provides POTS translation data and Private Network translation data. KEY: LAIDX (Line Attribute Index) OWNERSHIP: The LAIDX field indicates tuple ownership.
LSCFLAGS	2218	shows the relationship between Line Screening Code Flag numbers and Line Screening Codes (LSC). It is used for restricting terminations on TRUNKS and VFG. KEY: LSCNO (Line Screening Code flag Number) OWNERSHIP: The LSCNO field indicates tuple ownership.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
NCOS	2175	lists the NCOS numbers assigned to attendant consoles, IBN stations, incoming IBN trunk groups, authorization codes, and VFGs. KEY: CUSTGRP (Customer Group Name) NCOS number OWNERSHIP: The CUSTGRP field indicates table ownership.
PACMAN	2497	interprets the ESN call and sub-call types for incoming calls. KEY: PMI (Protocol Manipulation Index) OWNERSHIP: The PMI field indicates tuple ownership.
STDPRTCT	2465	lists the names assigned by the operating company to represent each of the Standard Pretranslator subtables (STDPRT). KEY: EXTPRTNM (Standard Pretranslator Name) OWNERSHIP: The EXTPRTNM field indicates tuple ownership. 1 Table STDPRTCT is a head table for subtable STDPRT. 2 This table should be Change Only for CDC users.
STDPRTCT. STDPRT (subtable)	2467	is the first table to be indexed for digit translation. KEY: FROMDIGS and TODIGS (range of digits to be translated)
SUBGRP	2222	stores information on each subgroup of a customer group. KEY: CUSTGRP (Customer Group Name) and Subgroup number. OWNERSHIP: The CUSTGRP field indicates tuple ownership.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
TIMEODAY	2264	defines the TOD result for a given TOD system and day-type. KEY: TODNAME and DAYTYPE and TIME OWNERSHIP: The TODNAME field indicates tuple ownership.
TODHEAD	2261	defines TOD system names and defaults. KEY: TODNAME (Time-Of-Day system Name) OWNERSHIP: The TODNAME field indicates tuple ownership.This table should be Change Only for CDC users.
VFGDATA	2220	contains the data for one end of a VFG (each tuple). Each end of the VFG can be an IBN VFG or POTS VFG and can be either incoming or outgoing. KEY: VFGNAME (Virtual Facility Group Name) and TYPDIR (Type and Direction of the VFG) Tables VFGENG and VFGDATA represent the data in Table VIRTGRPS. Table VFGENG represents the VFG connection data. Table VFGDATA represents the data for each end of the VFG. When a tuple is added or deleted in Table VIRTGRPS, the corresponding tuples are added or deleted in Tables VFGENG and VFGDATA. Table VFGENG is Change Only. Tuples cannot be added or deleted from this table. It is possible for one end of a VFG to be owned by one owner, the other end by another owner, and the connection of the two ends by a third owner. A CDC user must be associated with the OWNER_ID that owns the INCOMING side of the VFG in order to change the NCOS of the VFG using the CHG command in SERVORD. The same is true with regard to LSC or ALSC information on the OUTGOING side of the VFG.

—continued—

Table 3-1
Tables available to CDC users through PTE (continued)

Table	Form	Description
VFGENG	2249	gives the size information of each VFG. KEY: VFGNAME (Virtual Facility Group Name) OWNERSHIP: The VFGNAME field indicates tuple ownership. This table should be Change Only or Read Only for CDC users.
XLANAME	2202	defines translator names for IBN translation table (IBNXLA) and default results. translator name NXLA is assigned in the customer group or table NCOS when a customer group or NCOS number does not require a preliminary or feature translator. KEY: XLANAME (Translator Name) OWNERSHIP: The XLANAME field indicates tuple ownership.This table should be Change Only for CDC users.
		—end—

Service Order commands available to CDC users

Some Service Order input commands are available to CDC users. These commands are divided into three groups: Basic Service Commands, Hunt/CPU Group Commands, and Modifying Data Commands.

Basic Service Order commands

The following table list basic Service Order commands available to CDC users.

Table 3-2
Basic Service Order commands

Command	Descriptions of use
ADO	**Add** options to assigned Single Line and Multi-line Telephone Sets. Add DNH option to Single Line Sets only (see Adding Options).
DEO	**Delete** options from Single Line and Multi-line Telephone Sets. Delete DNH options from Single Line Sets only (see Deleting Options).
NEW	**Establish** service for unassigned Single Line and Multi-line Telephone Sets, with or without options. Pilots and members of DNH/DLH/MLH/BNN groups cannot be established with this command with the exception of Single Line Set DNH pilots and members (see Establishing Service).
OUT	**Remove** service from Single Line and Multi-line Telephone Set directory numbers and line equipment numbers with the exception of DNH/DLH/MLH/BNN group members (see Deleting Service and Hunt Groups).

Hunt/CPU Group commands

The following table list Hunt/CPU Group commands available to CDC users.

Table 3-3
Hunt/CPU Group commands

Command	Descriptions of use
ABNN	**Add** a bridged night number to a DNH/DLH/MLH group member without forming a BNN hunt group.
ADA	**Add** an authcode.
ADD	**Add** unassigned Single Line and Multi-line Telephone Set directory numbers to DNH/BNN groups. Add unassigned Single Line Set LENs and Multi-line Telephone Set keys to DLH/MLH groups (see Hunt Groups). Add assigned Single Line and Multi-line Telephone Set directory number to Call Pickup groups (see Call Pickup Groups).
	—continued—

Table 3-3
Hunt/CPU Group commands (continued)

Command	Descriptions of use
DBNN	**Delete** the BNN option from a DNH/DLH/MLH group member that is not in a BNN hunt group.
DEA	**Delete** an authcode.
DEL	**Delete** members of a DNH/DLH/MLH/BNN group. Takes directory number of DNH/BNN member out of service. Takes Single Line LEN of DLH/MLH member out of service. Removes key assignment of Multi-line DLH/MLH member; removes LEN from service if member is on Key 1. Pilot of hunt groups cannot be deleted with this command (see Hunt Groups). Delete members from a CPU group. Only removes CPU option; directory numbers remain in service (see Call Pickup Groups).
EST	**Establish** unassigned Single Line and Multi-line Telephone Set directory numbers as DNH/DLH/MLH/BNN pilots, with or without members. All potential members must be unassigned (see Hunt Groups). Establish CPU groups on assigned Single Line and/or Multi-line Telephone Sets (see Call Pickup Groups).
—end—	

Modifying Data command

The following table list Modifying Data commands available to CDC users.

Table 3-4
Hunt/CPU Group commands

Command	Descriptions of use
CDN	**Change** directory number of standard directory numbers or DNH group members on Single Line and Multi-line Telephone Sets. MDN members and hunt group pilots cannot be changed with this command (see Changing a Directory Number).
CHF	**Change** secondary feature data on features assigned to Single Line and Multi-line Telephone Sets(see Changing Feature Data).
CHG	**Change** the NCOS, customer group, subgroup or LCC of directory numbers on Single Line and Multi-line Telephone Sets. Change the ring option for directory numbers on multi-line sets (see Changing Customer Group, LCC, NCOS, Ring Option or Subgroup). Also used to change information on CLLIs (Common Language Location Identifiers), virtual facility groups, authorization codes, and time of day routing.
CICP	**Change** type of intercept on unassigned directory numbers (see Changing an Intercept Treatment).
CKLN	**Changing** the LEN on multi-line telephone sets (see Changing a Line Equipment Number).
CLN	**Change** the LEN on Single Line sets. This command cannot be used with multi-line telephone sets (see Changing a Line Equipment Number).
DSP	**Displays** LCC information assigned to a multi-line set.

Query commands

These commands help determine the status of DNs or LENs and the data associated with an assigned single line set or multiline telephone set. A listing of the members in a CPU, GIC, HNT, KSH, MADN, QBS, or SCU group can also be obtained.

These commands can be used from any software level, including command interpreter (CI), SERVORD, and PENDING.

Table 3-5
Query commands

Command	Query Call Member	Partitioned
QCM	**Query Call Member** Queries	
QDN	**Query Directory Numbers** Queries assigned single line and multiline telephone set directory numbers. Queries unassigned directory numbers.	Yes
QDNSU	**Query Unassigned Directory Numbers** Obtains a summary or detailed listing of unassigned directory numbers.	No
QDNWRK	**Query Assigned Directory Numbers** Obtains a summary or detailed listing of assigned directory numbers.	No
QGRP	**Query Groups** Queries a CPU, GIC, HNT, KSH, MADN, QBS or SCU group to obtain a list of member LENs.	Yes
QHA	Query Assigned Hardware Obtains a summary or detailed listing of assigned hardware.	No
QHASU	**Query Assigned Hardware Unassigned Software** Obtains a summary or detailed listing of hardware assigned/software unassigned line equipment numbers.	No
QHU	Query Unassigned Hardware Obtains a summary or detailed listing of unassigned LENs.	No

—continued—

Table 3-5
Query commands (continued)

Command	Query Call Member	Partitioned
QLE	**Query LENs** Queries assigned line equipment numbers of single line and multiline telephone sets. Queries unassigned line equipment numbers.	Yes
QLENWRK	**Query Assigned LENs** Obtains a summary or detailed listing of assigned line equipment numbers.	No
QLOAD	Queries LEN Assignments by LCC Obtains a summary or detailed listing of LEN assignments according the the LCC assigned to it.	No
QLT	Queries ISDN Logical Terminals Obtains a summary or detailed listing of ISDN logical terminals.	Yes
QMADN DISPLAY	Query MADN group members Obtains a summary or detailed listing of MADN group members.	No
QNCOS	**Query NCOS** Obtains a count of terminals by network class of service. Includes a short summary count and a detailed summary count.	No
	—end—	

Pending order files

This chapter describes the following:

- pending order file (POF) operation
- entering a service order into the POF
- setting up a POF user
- automatic activation of POF
- log reports for POF

Pending order file operation

POFs allow CDC users to enter service orders, due at a future time and date, over several days instead of entering all the data at the time it is needed. POFs are stored in the pending order (PO) subsystem. Operating companies, general, and observer classes of CDC users can enter the PO subsystem.

Note: Observer classes will only be permitted to view their partition.

Pending order file types

There are two types of POFs:

- pending service orders (PSOs)–created in the Service Order (SERVORD) environment. CDC users with POF capabilities will use SERVORD to create POFs.
- data modification orders (DMOs)–created in the Partition Table Editor (PTE) environment.

Pending order subsystem storage limits

The PO subsystem storage capacity is initially set to 4K of protected data store. 2K is allotted for pending orders. Increased amounts of memory may be allocated by technical support personnel in Table DSLIMIT.

Entering a service order into the pending order file

Entering a service order for future activation is similar to entering an order for immediate activation. The service order is entered from the SERVORD

subsystem. The main difference is that a unique identification number and a due date and time are entered in response to the SONUMBER prompt.

Pending service orders are identified by the entered SONUMBER. The SONUMBER contains the following variables.

- Valid Input Format **>abnnnnnc yy mm dd tt**
- Pending Order File Identifier **>abnnnnnc**
- Activation Date **>yy mm dd**

where:

a mandatory alphabetical character (A-Z)
b optional alphabetical character (A-Z)
nnnnn five mandatory numerical characters
c optional alphabetical character (A-Z)
yy year (0-99)
mm month (1-12)
dd day (1-31)
tt AM or PM

To enter a pending service order into the POF, follow these basic steps:

Creating a pending order file using the no-prompt mode

At your current location:

1 From SERVORD, type the service order input command, for example, ADO. Press the CR key or carriage return. The system will respond with the SONUMBER prompt and the current switch date and time. (The current date and time in the example are January 8, 1990, AM.)

Example of display:

```
SO:
>ADO (CR)
SONUMBER: NOW 90 1 8 AM
>
```

2 Instead of entering a carriage return to accept the default value of the current switch date and time, enter a valid response for the SONUMBER prompt. The identifier and due date may be entered on one line after the SONUMBER prompt in the no-prompt mode. After a carriage return, the system will respond with the next prompt for the input command entered, in this case, DN_OR_LEN.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222 90 2 16 AM
DN_OR_LEN:
>
```

3 Continue to enter a valid response to each prompt as it appears. Prompts appear after each valid response until the system has all the data needed to complete the service order.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222 90 2 16 AM
DN_OR_LEN:
>0 0 7 5
OPTION:
>3WC
OPTION:
>$
```

4 When all the prompts have been responded to, the system will display the data entered. Then a request to confirm the service order will appear.

Check the input data displayed for accuracy. Note that the due date for future activation is listed rather than the current switch date and time. (The due date and time here are February 16, 1990, AM.)

If all data is correct, enter a **Y** to confirm the service order (and enter it into the POF).

If a mistake has been made and data must be changed, enter an **E** to edit.

If you want to reject the service order completely, enter an **N**.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222 90 2 16 AM
DN_OR_LEN:
>0 0 7 5
OPTION:
>3WC
OPTION:
>$
COMMAND AS ENTERED:
ADO A22222 90 2 16 AM
HOST 00 0 07 05 (3WC) $
ENTER Y TO CONFIRM,
N TO REJECT
OR E TO EDIT
>Y
```

Creating a pending order file using the prompt mode

At your current location:

If the user enters a carriage return after the SONUMBER identifier is entered, individual prompts for date and time will appear. The following steps show an example of a service order entered in the prompt mode.

1 Enter a valid SONUMBER and carriage return. The system will respond with DUE.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>
```

2 The system will request the expected due date for this pending order. At least the year must be entered (valid input: currently 00-99). If only the year is entered, the system will respond with MONTH after a carriage return.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>90
MONTH:
>
```

3 At least the month must be entered here (valid input: 1-12). If only the month is entered, the system will respond with DAY after a carriage return.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>90
MONTH:
>2
DAY:
>
```

4 At least the day must be entered here (valid input: 1-31). If only the day is entered, the system will respond with TIME after a carriage return.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>90
MONTH:
>2
DAY:
>16
TIME:
>
```

5 Enter the time of day the order will need to be activated, either **AM** or **PM**, and depress the CR key. The system will respond with the next prompt for the input command entered, in this case, DN_OR_LEN.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>90
MONTH:
>2
DAY:
>16
TIME:
>AM
DN_OR_LEN
>
```

6 Continue to enter a valid response to each prompt as it appears. Prompts will appear after each valid response until the system has all the data needed to complete the service order.

Always enter a DN as a ten-digit national number at the DN_OR_LEN prompt. An additional office code added to the switch while an order is pending could cause a seven-digit DN to fail the duplicate NXX test when the pending order is invoked.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222
DUE:
>90
MONTH:
>2
DAY:
>16
TIME:
>AM
DN_OR_LEN
>0 0 7 5
OPTION:
>3WC
OPTION:
>$
```

7 When all the prompts have been responded to, the system will display the data as input. Then a request to confirm the service order will appear.

Check the input data displayed for accuracy. Note that the due date for future activation is listed rather than the current switch date and time. (The due date and time here are February 16, 1990, AM.)

If all data is correct, enter a **Y** to confirm the service order (and enter it into the POF).

If a mistake has been made and data needs to be changed, enter an **E** to edit.

If you want to reject the service order completely, enter an **N**.

Example of display:

```
SO:
>ADO
SONUMBER: NOW 90 1 8 AM
>A22222 90 2 16 AM
DN_OR_LEN:
>0 0 7 5
OPTION:
>3WC
OPTION:
>$
COMMAND AS ENTERED:
ADO A22222 90 2 16 AM
HOST 00 0 07 05 (3WC) $
ENTER Y TO CONFIRM,
N TO REJECT
OR E TO EDIT
>Y
```

Activating pending orders

Pending orders can be activated two way: manually and automatically.

Automatic activation of pending orders

PSOs created by CDC users can be activated automatically when the PSO is due. An AUTOEXEC process exists on the DMS switch. (At 3:30 every morning, this process wakes up and executes AUTO_SCHED in the SFDEV.)

An auto activate facility in the POF system is implemented by the AUTOEXEC process. The SO_POF (pending order command file) containing the ACTIVATE command and PSOF DUE option must be created by the operating company. This command file will be stored in the SFDEV. The following table shows an example of what the SO_POF command file should contain. The SO_POF file is read by the AUTO_SCHED file.

Note: The central office must have Feature NC0120, Pending Order File (POF) Enhancements, before POFs can automatically activated.

Figure 4-1
Example of SO_POF file

```
SERVORD
PENDING_$
ACT NP PSOF DUE
Y
LEAVE
```

Figure 4-2
Example of AUTO_SCHED file

```
LISTSF all
READ SO-POF
```

Manual activation of pending orders

To activate a pending service order, you must enter the PENDING subsystem from the SERVORD level. If you enter PENDING from the CI level, you cannot activate orders; you can only display or delete orders.

The following steps show how to activate pending orders by using the ACT command with various parameters.

Activating pending orders

At your current location:

1 To activate the current POF or the pending order just displayed, type

>ACT

and press the Enter key.

2 To activate a specific pending order by POFid, type

>ACT POF A22223A

and press the Enter key.

3 To activate all pending service orders due prior to and including a specific date (AM and PM orders), type

>ACT PSOF DATE MAR 2

and press the Enter key.

4 To activate all pending service orders due prior to a specific date and the AM orders only for the date specified, type

>ACT PSOF DATE MAR 2

and press the Enter key.

5 To activate all pending service orders that have reached their due dates prior to the current switch date and time, type

>ACT PSOF DUE

and press the Enter key.

6 To activate all pending service orders in the system regardless of due date, type

>ACT PSOF ALL

and press the Enter key.

Pending order subsystem commands

The following table shows the PO subsystem commands used with various parameters and describes the use of each entry. See *Basic Translations Tools Guide,* 297-1001-360, and *Servord Reference Manual* for examples and additional details.

Table 4-1
Pending order file commands

Command Parameters	Description of use
D	Display. Show the pending service order that was just displayed through the DIS command or the pending order associated with the SONUMBER just entered when prompted for `PENDING FILE NAME`.
DIS POF A12345	Display Pending Order File**.** Show the pending order associated with the SONUMBER (in this example, A12345).
DIS DATE FEB 2	Display Pending Order Files with the Date Command**.** List all SONUMBERS that are due up to and including the date specified. In this example, the specified date is February 2.
DIS DUE	Display Due Pending Order Files**.** List all SONUMBERS that are due prior to the current switch date and time.
DIS ALL	Display all Pending Order Files**.** List all SONUMBERS in the order of input.

—continued—

Table 4-1
Pending order file commands (continued)

Command Parameters	Description of use
ACT	Activate**.** Activate the pending order that was just displayed through the DIS command or the pending order associated with the SONUMBER just entered when prompted for `PENDING FILE NAME`.
ACT POF A12345	Activate Pending Order File**.** Activate only the pending order associated with the specified SONUMBER (for this example, A12345) with prompting.
ACT PSOFDATE FEB 3	Activate Pending Service Order File with the Date command**.** Activate chronologically all pending service orders (with prompting) scheduled for activation prior to and including the specified date, February 3.
ACT NP PSOF DUE	Activate all Pending Service Order Files due without prompts**.** Activate chronologically all pending service orders that are due prior to the current switch date and time, without prompting.
ACT NP PSOF ALL	Activate all Pending Service Order Files without prompts**.** Activate all pending service orders regardless of due date, without prompting.
DELETE	Delete**.** Delete the pending service order that was just displayed through the DIS command or the pending order associated with the SONUMBER entered when prompted for `PENDING FILE NAME`.
DELETE POF A12345	Delete Pending Order File**.** Delete the specified SONUMBER (in this case, A12345) with prompting.
DELETE PSOF DATE FEB 4	Delete Pending Service Order File with the date command**.** Delete chronologically all pending service orders (without prompting) that are due prior to and including the date specified. For this example the specified date is February 4.

—continued—

Table 4-1
Pending order file commands

Command Parameters	Description of use
DELETE NP PSOF DUE	Delete all Pending Service Order Files due without prompts**.** Delete chronologically all pending service orders that are due prior to the current switch date and time, without prompting.
DELETE NP PSOF ALL	Delete all Pending Service Order Files without prompts**.** Delete chronologically all pending service orders, with prompting.
	—end—

Setting up a pending order file user

For a user to have permission to create a POF, field POF in Table CDCLOGON must be datafilled Y. The following table shows the procedure for assigning POF to a user. For more detailed information on setting up a CDC user see the section “Setting up data ownership”.

Table 4-2
Datafill procedure for Table CDCLOGON

Field	Subfield	Explanation and action
USERNAME		Enter the user name assigned to the customer group.
OWNER		This field defines the owner. This field must be datafilled the same as field OWNER in Table OWNER. Table OWNER must be datafilled before Table CDCLOGON. Enter the 1-8 character name.
CLASS		This field defines the class assigned to the user. Enter GENERAL, NONUSER, OBSERVER, or TELCO.
POF		This field defines whether a user can create a pending order file. Enter Y or N.

Log reports for pending order file

Five log repots are available for recording pending audit logs (PEND).

- PEND100–reports on any past due or due within 12 hours PSOs. This report is generated at midnight and noon.
- PEND101–reports on any PSOs within prompting range. This report is generated at midnight and noon.

- PEND102–reports the PSOs that have been activated manually or by the AUTOEXEC process and their status. This log report is created during activation of the PSOF.
- PEND103–records the number of PSOs that have been successfully activated manually or by the AUTOEXEC process.
- PEND104–records the number of PSOs that have been unsuccessfully activated manually or by the AUTOEXEC process.

PEND100 log report

The PEND100 log report is generated by the PSO subsystem when any PSOs are past due or due within 12 hours.

The following procedure describes the command sequence required to verify that the PEND100 log report can be generated.

Verifying generation of PEND100 log report

At your current location:

1. Create two PSO files: one due within 12 hours and one due at least one hour earlier than the current time.
2. At midnight or noon (depending on when you created the PSO), check if PEND100 has been generated on the specified output device for logs.

PEND101 log report

The PEND101 log report is generated by the PSO subsystem when PSOs are within prompting range.

The following procedure describes the command sequence required to verify that the PEND101 log report can be generated.

Verifying generation of PEND101 log report

At your current location:

1. Create a PSO file due within prompting range.
2. At midnight or noon (depending on when you created the PSO), check if log report PEND101 has been generated on the specified output device for logs.

PEND102 log report

The PEND102 log report is generated by the PSO subsystem when PSOs are activated manually or by the AUTOEXEC process.

The following procedure describes the command sequence required to verify that the PEND102 log report can be generated.

Verifying generation of PEND102 log report

At your current location:

1 Create a PSO file.

2 An auto activate facility in the POF system will start the AUTOEXEC process on the DMS switch. The AUTOEXEC process will activate the PSO. When the PSO has been processed, check if log report PEND102 has been generated on the specified output device for logs.

OR

At your current location:

1 Create a PSO file.

2 Activate the PSO file. When the PSO has been processed, check if log report PEND102 has been generated on the specified output device for logs

PEND103 log report

The PEND103 log report is generated by the PSO subsystem when PSOs are successfully activated.

The following procedure describes the command sequence required to verify that the PEND103 log report can be generated.

Verifying generation of PEND103 log report

At your current location:

1 Create a PSO file.

2 When the PSO has been activated, check to see if log report PEND103 has been generated on the specified output device for logs.

OR

At your current location:

1 Create a PSO file.

2 Activate the PSO file. Check that log report PEND103 has been generated on the specified output device for logs.

PEND104 log report

The PEND104 log report is generated by the PO subsystem when PSOs are not successfully activated.

The following procedure describes the command sequence required to verify that the PEND104 log report can be generated.

Verifying generation of PEND104 log report

At your current location:

1 Create a PSO file.

2 When the service order system finishes processing the command, check that log report PEND104 has been generated on the specified output device for logs.

OR

At your current location:

1 Create a PSO file.

2 Activate the PSO file. Check that log report PEND104 has been generated on the specified output device for logs.

Verifying datafill for the CDC user

Before a new CDC user is allowed to log in and access data on the switch, the following data must be verified:

- Logging in – The user is allowed to log in.
- Command Screening – The user's commands are screened properly.
- Data ownership – The correct data has been entered for the user.
- Command logging – Log reports CDC101, CDC102, and CDC103 can be generated if requested.
  - — If the user has pending order file capabilities, PEND100, PEND101, PEND102, PEND103, and PEND104 can be generated if requested. See the section "Log reports for POF" for verification instructions.
- Monitoring – The user is being monitored. (Optional)
- Logging out – The user is allowed to log out.

Logging in

To verify that a new CDC user can log in to the DMS, log in as the CDC user with his LOGON_ID and password. If command screening was used, check that the terminal is in the `CDC:` increment.

Command screening

If the Enhanced Command Screening feature was used, verify that only the commands datafilled for the CDC user are allowed.

If the CDCSETUP command was used for command screening, verify that only the following commands are allowed:

- CHANGE
- DATE
- DEFAULT
- DOWN
- EDIT
- FILE

- HELP
- INPUT
- LEAVE
- LIST
- LOGOUT
- PASSWORD (optional)
- PENDING
- PTE
- QDN
- QDNA
- QGRP
- QIT
- QLT
- QLEN
- RESET
- SERVORD
- TIME
- UP
- <break>HX
- <break>HT

Data ownership

Use the DEFAULT command to check ownership of the following data:

- OWNER_ID
- Customer Groups
- Trunks Groups
- Virtual Facility Groups
- Authcode Partition Names
- Time-Of-Day System Names

Using the DEFAULT command to check data ownership

At your current position:

1 Check data ownership by typing

>DEFAULT OWNER

and pressing the Enter key.

Example of display:

```
OWNER:
```

where:

OWNER is the name of the data owner

> ***Note:*** An invalid input entry results in a display of all the owners that are associated with this user.

2 Repeat this operation by typing

>DEFAULT

and pressing the Enter key.

Example of display:

```
WHAT:
```

Then type

>CUST

and press the Enter key.

Example of display:

```
CUST:
>invalid input
```

3 Repeat this process for the following commands:

>DEFAULT CLLI
>DEFAULT VFG
>DEFAULT AUTH
>DEFAULT TDR

4 All data owned by a CDC user can be checked in this way. A user can set up a file containing these commands to check data ownership.

Ownership of DNs and LENs

To check ownership of directory numbers (DN) and line equipment numbers (LEN), use the following sequence:

Checking ownership of DNs and LENs

At your current position:

1 Activate the Service Order system by typing

>SERVORD

and pressing the Enter key.

2 Enter the Add Option (ADO) command by typing

>ADO

and pressing the Enter key.

Response:

The DMS prompts for the DN_OR_LEN field.

3 Enter a valid DN or LEN that is owned by this user, and verify that the DN or LEN was accepted.

4 Repeat the ADO command sequence, using a DN or LEN that is not owned by the CDC user. Check that the DMS does not accept this value.

5 Repeat this command sequence until the ownership of all DNs and LENs have been verified.

Access to tables

To list all of the tables to which the CDC user has access, use the CI command LISTTABS as follows:

1 The operating company establishes itself as the owner (OWNER_ID) by using the PERMIT command and assigning a privilege class.

2 Using the PERMIT command again, the operating company defines itself as a user (LOGON_ID) and then enters the command LISTTABS. This command shows whether ownership has been datafilled in Table OWNTAB.

Example:

```
CI:
>LISTTABS
TABLE   ACCESS  OWNERSHIP
------------------------------------------------------
TODHEAD READ WRITE     Y
DAYOWEEK    READ ONLY      Y
OHIP    CHANGE ONLY    N
REPLNAME    READ ONLY      N
DAYOYEAR    CHANGE ONLY    Y
```

Note: Table OWNTAB is datafilled as part of the LOAD BUILD process. It cannot be datafilled by the operating company.

Command logging

If CDC user activity is to be logged, then verify that the appropriate log reports can be generated.

CDC101 log report

The CDC101 log report is generated only when office parameter CUSTOMER_DATA_CHANGE_LOGS is set to Y in Table OFCVAR.

The following procedure describes the command sequence required to verify that the CDC101 log report can be generated.

Verifying generation of CDC101 log report

At your current position:

1 Access the Service Order system by typing

>SERVORD

and pressing the Enter key.

2 Enter any valid Service Order command by typing (for example)

>DSP CLLI clli_name NCOS

where:

CLLI is a valid Trunk Group CLLI name for this user

3 When the Service Order system finishes processing the command, check that log report CDC101 has been generated on the specified output device for logs.

CDC102 log report

The CDC102 log report is generated only when office parameter CUSTOMER_DATA_CHANGE_LOGS is set to Y.

The following procedure describes the command sequence required to verify that the CDC102 log report can be generated.

Verifying generation of CDC102 log report

At your current position:

1 Edit a table of the Partitioned Table Editor by typing

>PTE table

and pressing the Enter key.

where:

table is the name of a table to which the CDC user has access

2 Enter a valid PTE command to add, change, or delete a table, by typing (for example)

>CHANGE n

and pressing the Enter key.

where:

n is the field number of a table to be changed

3 When the Partitioned Table Editor finishes processing the command, check that log report CDC102 has been generated on the specified output device for logs.

CDC103 log report

The CDC103 log report is generated only when office parameter CUSTOMER_DATA_CHANGE_LOGS is set to Y.

The following procedure describes the command sequence required to verify that the CDC103 log report can be generated.

Verifying generation of CDC103 log report

At your current position:

1 Access the Pending Service Order system by typing

>SERVORD

and pressing the Enter key.

Then typing

>PENDING DC12121

and pressing the Enter key.

2 Enter a valid PTE command to add, change, or delete a table, by typing (for Example)

>DSP CLLI clli_name NCOS

and pressing the Enter key.

where:

DC12121 represents a unique POFID

3 When the Service Order system finishes processing the command, check that log report CDC103 has been generated on the specified output device for logs.

Monitoring

Existing DMS-100 features provide a means of monitoring a user by recording the commands entered by that user in a file.

The simplest way to record a CDC user is to use the RECORD command in the user profile.

Using the RECORD command in the user profile

At your current position:

Edit the user profile and add the following line by typing

>RECORD START ONTO SFDEV filename

and pressing the Enter key.

where:

filename is the name of the file that will contain the commands entered by the user.

Note 1: The RECORD command ensures that all commands entered by the user are recorded, and that the DMS responses to the user commands are recorded.

Note 2: Recording can only be stopped when the user logs out.

Note 3: To stop monitoring the user, edit the user profile by deleting the RECORD line.

Note 4: When the CDC user logs in, the RECORD file from the previous session is erased.

Logging out of the DMS

Logging out of the DMS

At your current position:

To log out of the DMS, type

>LOGOUT

and press the Enter key.

Note: If all of the previous checks have been successfully verified, the new user can be given his access rights, LOGON_ID, and password.

Returning a CDC user to normal user status

Use one of the following methods to returning a CDC user to NORMAL user status:

- Change the user class to TELCO in the CDCLOGON table.

or

- Delete the user from the CDCLOGON table.

Note: When a CDC user is restored to NORMAL user status, that user has access to all the data in the office.

Index

S

T

DMS–100 FAMILY

Customer Data Change Operating Company

Guide

Product Documentation–Dept 3423
Nortel Networks
P.O. Box 13010
RTP, NC 27709–3010
1-877-662-5669, Option 4 + 1

Publication number: 297–2061–312
Product release: NA012
Document release: Standard 05.03
Date: September 1999
Printed in the United States of America

NORTEL NETWORKS™

How the world shares ideas.