585-223-700
June, 1992

DEFINITY®
Manager IV
System Administration

TO ORDER COPIES OF THIS DOCUMENT

CALL: AT&T Customer Information Center
(800) 432-6600
In Canada: (800) 255-1242

WRITE: AT&T Customer Information Center
2855 North Franklin Road
P.O. Box 19901
Indianapolis, Indiana 46219

For more information about AT&T documents, see *Business Communications Systems Publications Catalog* (555-000-010)

TRADEMARK NOTICES

DEFINITY, Dimension, OPEN LOOK and Quorum are registered trademarks of AT&T.
INFORMIX is a registered trademark of Informix Software, Inc.
MS-DOS is a registered trademark of Microsoft Corporation.
UNIX is a registered trademark of UNIX System Laboratories, Inc., a subsidiary of AT&T.

NOTICE

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, AT&T can assume no responsibility for any errors. Changes or corrections to the information contained in this document may be incorporated into future reissues.

Prepared by
AT&T Technical Publications Department
Lincroft, NJ

Printed in USA

CONTENTS

1. MANAGER IV SYSTEM ADMINISTRATION

2. USER ADMINISTRATION

3. MONITORING SYSTEM ACTIVITY

4. TARGET ADMINISTRATION

5. HARDWARE ADMINISTRATION

6. DATABASE ADMINISTRATION

7. TROUBLESHOOTING AND USING THE LOGS

APPENDIX A: DELTA REPORTS

APPENDIX B: INTRODUCTION TO AUDITS

APPENDIX C: UNIVERSAL OUTWARD FEEDS

APPENDIX D. SUPPORTING DOCUMENTATION

APPENDIX E: PROC MODE APPLICATION

APPENDIX F. HIGH CAPACITY BACKUP AND RECOVERY FOR 3B2

APPENDIX G. HIGH CAPACITY BACKUP AND RECOVERY FOR 386 PC AT

INDEX

ABOUT THIS GUIDE

This manual is a guide to the system administration application of DEFINITY ® Manager IV. It also defines some of the System Administrator's responsibilities and how often system administration jobs should be performed.

The system administration application gives you the tools you need to accomplish daily maintenance and administrative tasks. You use it to perform backup and recovery procedures, maintain logs of system activity, administer users, and administer data communications ports.

This manual assumes a working knowledge of the UNIX® System V Operating System as well as hands-on experience with the AT&T 3B2-600 processor or the AT&T 6386E/33 Work Group Station. You must also have some understanding of switch operation.

AT&T offers a variety of courses on the UNIX operating system and system management. Besides training courses, Manager IV provides a line of documentation. Refer to Appendix D for a list of available Manager IV and related documentation.

CONVENTIONS USED IN THIS MANUAL

The following conventions are used to represent prompts, entries, and keys throughout this manual:

Commands

Commands are shown in bold type. All commands are from the **system administration** application, unless otherwise indicated. Utilities are available from any application, but in this manual utility commands are preceded with **system administration**.

The variable <target> is not specified in commands that require a target, since you are not required to enter a target if you have done this for a prior command.

Function Keys and Screen-Labeled Keys

Both function and screen-labeled keys are shown graphically, as in the following: **RETURN** or **ESC**. Character keys, such as **y** for yes, are printed in bold type but without the key outline.

Optional Entries

When a Manager IV maintenance command offers additional features that may be selected by the user, the options are printed in lowercase bold type and enclosed by brackets. For example, **bradm log_info [-s] -c** means that **-s** is an option.

Prompts

A prompt is the UNIX System or Manager IV symbol that indicates that you must enter data. The dollar sign **($)**, pound sign (**#**), and the right-angle bracket (>) are examples of screen prompts.

Screen Messages

Messages displayed by Manager IV are printed in `computer voice type.` Where possible, the entire screen is reproduced.

User Entries

Input that you must type or enter is printed **in bold type**.

Variable Entries

User-determined input, such as yes or no or the date, is a variable entry. Words or phrases to represent these one-word entries are enclosed in angle brackets: < >. For example, the entry **passwd <login_id>** means that you supply the appropriate login ID.

CONTENTS OF THE MANUAL

Chapter 1:
Manager IV System Administration

- Explains the System Administrator’s role and responsibilities.
- Explains how to use the system administration application and access the UNIX shell.
- Provides a table of all the objects and verbs in the system administration application.

Chapter 2:
Administering Users

- Defines the system administration class and user classes.
- Supplies procedures for adding, displaying, removing, and changing login data.

Chapter 3:
Monitoring System Activity

- Explains how to monitor service request activity.
- Explains the transaction log and how to read it.

Chapter 4:
Target Administration

- Supplies procedures for database administration including adding, displaying, and listing product and corporate descriptions.
- Explains agent and set assignments.

Chapter 5:
Hardware Administration

- Explains how to administer the host processor and product access ports.

Chapter 6:
Backup and Recovery Procedures

- Explains how to perform the **log_dump** procedure for backups.
- Supplies procedures for recovering files lost due to system failure or other reasons.

Chapter 7:
Troubleshooting and Using the Logs

- Explains how to use the Manager IV error logs to prevent and solve problems.

Appendices:

- Appendix A, "Reports," explains how to access and use delta reports.
- Appendix B, "Introduction to Audits," explains the auditing feature that checks synchronization between System 85 R2V2-R2V4 and Generic 2 switches and the Manager IV database.
- Appendix C, "Universal Outward Feeds," explains how to set up and

activate Universal Outward Feeds so external system management applications can access Manager IV data.

- Appendix D, "Manager IV Documentation," lists all available Manager IV and related documentation.
- Appendix E, "Proc Mode Application," explains how to use Maintenance (Proc Mode), the Manager IV application that allows you to maintain AT&T DEFINITY Generic 2, System 85 R2V2-R2V4, and DIMENSION FP8 Issues 1.16 and 3.8 switches by running maintenance-related tasks.

  PROC MODE WARNING:
  Before the connection to the specified switch is established, this warning message will be generated: "THE MANAGER IV DATABASE WILL NOT REFLECT CHANGES DONE WITH THIS TRANSACTION."

  This is a reminder that any administration done via Proc Mode will directly affect the switch but not the Manager IV database, which may result in "out-of-sync" condition. Therefore, if you modify the switch configuration in Proc Mode, you must either update the Manager IV database to keep it "in sync" with the switch, or report any switch updates to the System Administrator.
- Appendix F, "High Capacity Backup and Recovery for 3B2", describes how to back up and restore the entire Manager IV database and the transaction logs using the high capacity (8mm) tape.
- Appendix G, "High Capacity Backup and Recovery for 386 PC AT", describes how to back up and restore the entire Manager IV database and the transaction logs using the high capacity (8mm) tape.

Index: There are three separate listings in this chapter:

- Index, which contains alphabetical listings of references in the manual.
- Command Index, which lists all commands used in this manual.
- Procedure Index, which lists all procedures in this manual.

1. MANAGER IV SYSTEM ADMINISTRATION

A Manager IV System Administrator’s responsibilities involve daily, weekly, and as-needed tasks to ensure smooth system operation. Some maintenance procedures are performed automatically by Manager IV. If they cannot complete automatically, you must perform them manually.

SYSTEM ADMINISTRATOR´S RESPONSIBILITIES

As Manager IV System Administrator, your responsibilities include the following:

- Assist the Implementation and Installation Team
- Administer Users
- Monitor System Activity
- Administer Targets
- Administer Hardware
- Administer Database
- Administer Errors
- Call for Assistance

These responsibilities are explained in the following chapters.

Assist the Implementation and Installation Team

The implementation team is a group of AT&T and customer representatives who are assigned to coordinate all Manager IV -related activities. Among other activities, the implementation team schedules the Manager IV software installation and helps your site gather the data needed to initialize the database. The data is collected on forms provided in *Manager IV Planning and Implementation*. You will be involved in supplying some of the information for these forms, particularly those involving user requirements.

During installation, you are expected to have those completed forms available for the installer. You are also expected to participate in the installation as much as possible by being present during the entire process and performing the "Adding a Login" procedures in Chapter 2.

Administer Users

Administering users includes assigning permissions via user classes, adding users to the UNIX and Manager IV systems, and attending to the daily needs of those users once they are added. It is your responsibility to create a user profile for each user who is to be added to the system. Refer to the User Login ID Assignment Form in *Manager IV Planning and Implementation.* This form should contain information about which terminals, printers, and products the user may access and what privileges the user may have.

Refer to Chapter 2 for procedures on adding a user to the UNIX System and to Manager IV. Chapter 2 also defines the user classes, which determine the levels of permissions for a user.

Monitor System Activity

Keep track of system usage by reading the logs and monitoring service request activity.

The transaction log displays all user activity. You can monitor the activity of one, several, or all users. Call for a transaction report as needed; for example, if problems occurred during a specific time of day, you can request a transaction report that shows transactions for that time. Or if a specific user is having difficulties, activating the transaction log for that user will show you his or her activity at any level of detail: date, time, and target. If no problems are reported, check the transaction log each day.

Other Manager IV logs provide information about the system's current configuration and status, attempted product connections, service request activity, user errors, and failed processes. See Chapter 3 for information on the transaction log, service request log, and service requests. Chapter 7 contains explanations of the other logs.

Administer Targets

As System Administrator, you may sometimes be expected to perform procedures regularly handled by an AT&T service technician. The administration of corporate and product descriptions is among these services. Products and corporations are normally added during installation, but you will display and change corporate and product descriptions as your system configuration changes. See Chapter 4 for procedures about products and corporations.

Administer Hardware

You monitor the Manager IV host processor for mechanical failures or disruptions of electrical power. You also monitor product access ports that provide access to and from the host processor and the PBX. Use the **stopsm** and **startsm** commands to shut down and reboot Manager IV. Shut down Manager IV for hardware maintenance as needed. Check port connections daily with **port display**. When necessary for servicing, you will use **port disable** and **port enable**, or in case of emergency service, **port release**.

Chapter 5 contains information on hardware administration.

Administer Database

As System Administrator, you must perform regular software maintenance besides the daily backup of the transaction logs. Perform a full backup of the Manager IV database weekly with the **bradm full_dump** procedure. This copies the transaction logs and all stored data. If extensive changes are made to the database, you should do the full backup twice a week. After full backups, back up the switch with **tape run**. You are also expected to use this command as necessary to back up service requests.

Some of the scheduled software tasks are performed automatically with the cron utility. Cron checks the status of transaction log devices, switches log devices, and sends the results to the **smgr** login. You should check mail to this login daily. If cron is not operating, you must perform these two tasks manually. Cron normally checks the status of transaction log devices every 30 minutes. Use **ck_log** to accomplish this manually. To switch log devices, use **log_sw**.

Accurate and up-to-date backups enable you to retrieve data when necessary. You use **bradm recovery** to restore the CORE database after a system crash.

See Chapter 6 for information on backup and recovery procedures. Backup and Recovery Procedures for the 8mm tape on 3B2 and 386 PC AT are described in Appendices F and G, respectively.

Administer Errors

The System Administrator is expected to use the logs and reports to prevent problems when possible, and solve them with or without the help of AT&T’s service team.

You should check the transaction log (trxlog) and system log (syslog) daily; check them more frequently if trying to locate the source of a problem. You should monitor the System Administrator error log (sadmlog) and information log (infolog) at least daily, and monitor them more frequently if there is a high volume of activity. The data communications error log (dclog) should be run weekly, unless there is a problem, in which case you should check the data communications error log first.

See Chapter 7 for information on accessing and using all the logs.

Call for Assistance

If you cannot solve a problem, it is your responsibility to contact the AT&T Services Support Center. Always maintain a record of all completed Manager IV maintenance procedures, such as backups and recoveries, that have been performed manually. These records should be available to the AT&T technician.

Chapter 7 describes service support and warranty coverage.

For customer service and support, call the following toll-free number:

1-800-548-8861

SCHEDULE OF SYSTEM ADMINISTRATOR DUTIES

The following table summarizes the System Administrator tasks. The *Manager IV System Administration Checklist*, available from the AT&T Customer Information Center (CIC), is a quick reference card that contains the commands you need to perform each task.

Task	Performed
Back up database transaction logs	Daily. System will prompt if the logs become full more frequently. (See Chapter 6)
Back up UNIX files	Daily (See UNIX documentation.)
Assure port connections	Daily (See Chapter 5.)
Monitor service request status	Daily, in a.m. (See Chapter 3.)
Monitor service request results files	Daily (See Chapter 3.)
Back up the switch	As needed. System performs automatically on a daily basis; System Administrator should run as backup to service requests and after a full backup. (See Chapter 6.)
Review error logs	Daily. (See Chapter 7.)
Clean out log devices	Daily, if warranted by large number of transactions. (See Chapter 7.)
Back up Manager IV	Weekly, and before system shutdown (Bi-weekly if changes are extensive) (See Chapter 6.)
Analyze system usage	Regularly, recommended weekly.
Back up CORE database files	Weekly, if not done in conjunction with full backup. (See Chapter 6.)
Recover UNIX files	As necessary due to loss by users or system failure. (See UNIX documentation.)
Shut down Manager IV	As necessary to maintain hardware. (See Chapter 5.)
Administer logins	As necessary. (See Chapter 2.)
Administer product access ports	As necessary. (See Chapter 5.)
Restore system files and databases	After crash or partial loss. (See Chapter 6.)
Apply software updates	As necessary.
Assign SM agents	As necessary. (See Chapter 5.)

ACCESSING THE SYSTEM ADMINISTRATION APPLICATION

All procedures in this manual, unless otherwise indicated, are performed from the system administration application from the **smsa** login. The **smsa** login was assigned at installation along with a temporary password. The first time you use this login, you should choose a new password. When you log in to Manager IV, enter **system-administration**, or **sy** (the shortest abbreviation that Manager IV will accept for this application) at the "Enter application" prompt. The system then prompts you for an object and a verb. If you know the entire command path (including application, object, and verb), you can enter it all at once. For example: **system-administration port display**. Each procedure in this manual presents the full command path below the procedure heading. You enter the entire command or abbreviated form of that command.

Table 1-2 lists all the objects and verbs that are part of the system administration application. Note that you must enter a target before entering the verb, unless you have entered a target for a prior command. The target name is determined by what is installed at your site.

The final column of the table refers you to the chapter, appendix, or other manual that contains information about this command. Commands covered in *DEFINITY Manager IV Installation, Initialization, and Maintenance* are used by the service team during installation and initialization. It is extremely unlikely that you will need to use these commands during daily maintenance, but if you do, refer to that manual.

Table 1-2. System-Administration Path Directory

Object:	Verbs:	Refer to:
anlg-audit Checks for synchronization errors that may exist between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
application-database Retrieves the required Application data elements from the Manager IV product-image database to produce Universal Outward Feeds data transfer files.	**audit** **initialize**	Appendix C
button-audit Compares station attributes and corresponding button assignments for the specified range of equipment locations between the System 85 or Generic 2 switch and the Manager IV database.	**cleanup** **report** **restart** **run** **start** **status-display**	Appendix B
ccgp-audit Compares the call coverage group number and the points for the specified range of call coverage groups between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
cds-bulk-load-tape Initializes the Personnel Database of the AP Messaging Server from the Manager IV extension and name database.	**run**	*Manager IV Installation, Initialization, and Maintenance*
co-fx-did-aplt Adds trunk types, including CO, FX, DID, and APLT and their nontranslation characteristics to the Manager IV database.	**create**	*Manager IV Installation, Initialization, and Maintenance*
corporation Manages the description of the corporation associated with your switch(es).	**add** **change** **display** **list** **remove**	Chapter 4

(Continued)

Table 1-2. Continued

Object:	**Verbs:**	**Refer to:**
database Manages file name and product ID information in the database.	**list** **remove**	Chapter 4; *Manager IV Installation, Initialization, and Maintenance*
extn-user-information Enters data about the user associated with a particular extension.	**create**	*Manager IV Installation, Initialization, and Maintenance*
hardware Manages a carrier and its associated packs. Not available for DEFINITY Generic 2.	**add** **change** **display** **remove**	*Manager IV Installation, Initialization, and Maintenance*
initialization Supplies switch translation data and nonswitch data to the Manager IV database.	**delta** **restart** **setup** **start**	Appendix A; *Manager IV Installation, Initialization, and Maintenance*
login Adds, changes, displays, or removes Manager IV users.	**add** **change** **display** **remove**	Chapter 2
name-audit Compares the presence/nonpresence of a name for the specified range of extensions between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
network-file One of the commands in the initialization process for multiple-switch customers (Number Portability Network only).	**create** **remove**	*Manager IV Installation, Initialization, and Maintenance*
non-switch-data Manages nonswitch data incorporated into the Manager IV database.	**add** **retrieve**	*Manager IV Installation, Initialization, and Maintenance*
product Manages a supported product in the Manager IV CORE database.	**add** **change** **display** **list** **remove**	Chapters 4 and 5
set-attributes Manages nontranslation set attributes such as color, mount, and set adjuncts.	**create**	*Manager IV Installation, Initialization, and Maintenance*

(Continued)

Table 1-2. Continued

Object:	Verbs:	Refer to:
set-type-name Manages mnemonic set-type names for set type encodes (DEFINITY Generic 2).	**create**	*Manager IV Installation, Initialization, and Maintenance*
target-group Administers target group attributes and members for multi-node transactions such as user and auth-code.	**add** **change** **display** **remove**	Chapter 4
terminal-audit Compares the station equipment locations for all terminals between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
tie-trunk Adds trunk groups and their nontranslation characteristics to the Manager IV database.	**create**	*Manager IV Installation, Initialization, and Maintenance*
trk-audit Compares the trunk group number and the corresponding equipment locations for the specified range of trunk groups between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
trk-grp-audit Compares the trunk group number, dial access code, and trunk type for the specified range of trunk groups between the System 85 or Generic 2 switch and the Manager IV database.	**report** **restart** **run** **start** **status-display**	Appendix B
user-activity Provides information about Manager IV activity to be utilized by telecommunications management or System Administrator.	**report**	Appendix A

(Continued)

Table 1-2. Continued

Object:	Verbs:	Refer to:
user-information Administers data for authorization-code users not associated with extensions.	**create**	*Manager IV Installation, Initialization, and Maintenance*
wats-trunk Adds WATS trunk groups and their nontranslation characteristics to the Manager IV database.	**create**	*Manager IV Installation, Initialization, and Maintenance*
UTILITIES: **connection** Manages information about port connections.	**create** **display** **end**	*Manager IV Installation, Initialization, and Maintenance*
errors Displays error descriptions for error numbers found in a transaction.	**display**	Chapter 7
port Manages a product access port and its attributes. (This is the same as the system administration port command.)	**add** **change** **disable** **display** **enable** **release** **remove**	Chapter 5
results Manages information concerning the results of scheduled transactions.	**display** **remove**	Chapter 3
scheduled-entry Manages information concerning transactions currently scheduled.	**display** **list** **remove**	Chapter 3
shell Permits access to the UNIX shell.	**create**	Chapter 1

Procedure: Accessing The UNIX Shell

Command: system-administration shell create

The shell utility, available from all of the Manager IV applications or by entering **utilities** at the "Enter Application" prompt, gives you access to the UNIX shell. UNIX capabilities may be restricted to some users depending on the level of access permitted. As Manager IV System Administrator, you have access to the UNIX shell and all utilities. Use the following procedure to access the UNIX System prompt.

1. Enter **system-administration shell create**.

   The system displays the following:

   ```
   env, shell, list>
   ```

2. Enter **shell**.

   When you receive a prompt (usually a **$**), you can perform any UNIX System command.

   Notes:

   - If you enter **env**, you may set the value of a local environment variable.
   - If you enter **list**, you may view the values of all variables in your environment.

3. Return to Manager IV at any time by pressing **CTRL** **d** or entering **exit**.

For information on UNIX System commands, refer to your standard UNIX documentation.

2. USER ADMINISTRATION

Manager IV ensures system security through the use of user logins and passwords to prevent unauthorized use or misuse of the system. This chapter describes the administrative tasks and procedures to add users to the system, determine their access permissions, and monitor user activity.

USER CLASSES

In Manager IV, the capabilities of each user are defined by a user class — that is, a set of criteria that identifies which areas of Manager IV are accessible. Any user can be assigned one or more user classes that permit or restrict access to selected applications and commands. Assignments can be made in any combination—either to permit unrestricted display and update capabilities or to allow only display capabilities.

System Administration Classes

As System Administrator, you should use the login **smsa**, which was added to the system during installation. This login enables you to perform most of your regular administrative tasks. Occasionally you may have to log in as **root**, but it is recommended that you use **smsa**.

The **smsa** login is assigned the user class **all**. This user class allows access to all areas and commands of Manager IV.

Application User Classes

When you add a new user to the Manager IV database via **system-administration login add**, you define user privileges by the class of login you assign. You can allow one user access to all applications, limit another to transactions within only one application, or allow yet another user to display information but not change it. The access allowed to each user class is predefined in the system and may not be altered. However, one login can be associated with more than one user class.

To help ensure that administrative changes are not made inadvertently and that certain activities and information remain restricted, the following user classes are available within Manager IV.

Administrator Permissions

all	Access to all user classes.
aa	Access to Adjunct Administration commands.
sys-admin	Access to System Administration commands.
expert	Shell access only.
super-admin	Administration Supervisor.
reviewer	Review; display only.

TCM User Class Permissions

TCM users can be assigned to four classes.

These user classes include:

- tcm-1
- tcm-2
- precut
- fm-4

These user classes are discussed below.

tcm-1

The *tcm-1* user has access to all TCM administration and report-administration commands. However, this user is denied access to the product-administration and database-administration areas.

tcm-2

The *tcm-2* user has access to all TCM commands in all areas of the application. This user class is appropriate for the administrator who will be responsible for error recovery if there is an out-of-sync condition in the database. These users may also have access to other related Manager IV applications.

precut

The *precut* user requires access to dial tone transactions and reports and must be defined with a user type of "precut." The dial tone transactions omit some features and data checks available in regular TCM transactions. The Manager IV Database and Switch Reports require connection to the switch for longer periods of time than most Manager IV transactions.

fm-4

The *fm-4* user class gives TCM users access to Facilities Management (FM) authorization code transactions.

FM User Class Permissions

FM users can be assigned one of three classes.

fm-1

The **fm-1** user is permitted access to commands and areas appropriate to a new FM user. This user is allowed to perform, in the administration area, specific tasks related to AAR location codes; ARS 6-digit numbering plans, scheduling, and tolls; administration of the World Class Routing feature on a Generic 2.2 switch; Foreign and Home Numbering Plan (FNPA, HNPA) assignments; intercept programming; main/satellite configuration changes; Miscellaneous Trunk Restriction Group (MTRG) assignments; trunk group changes; and various phases of ACD/UCD administration. This user is also permitted access to all report-administration commands and all FM displays (except barrier-code). The user class prohibits access to the database-administration and product-administration areas.

fm-2

This class of user is allowed access to the same tasks as the **fm-1** user as well as database-administration, product-administration, report-administration commands, and all FM displays (except barrier code).

fm-3

For the **fm-3** user, all commands in all areas under the FM application are available.

Note: The **fm-4** class exists also, which gives TCM users access to the authorization code transactions in FM.

Maintenance and Multi-Node Transaction Permissions

maint-1 Access to maintenance procs for a given switch.

mnfe For multi-node transactions.

User Class Permissions for Services Personnel

precut Access to commands needed to provide dial tone to phones on new systems during the pre-cut phase of Manager IV installation.

bulk-init Access to those commands used in bulk initialization. Access to all utilities except the UNIX shell.

ADMINISTERING USER LOGINS

To assign logins and privileges to the users under your administration, you must configure a profile for each user to define the user's access options and limitations within Manager IV. These attributes include the following:

- The login ID for that user. It must be the same as the login ID used when adding the login to the UNIX System. See "Procedure: Adding a Login to UNIX" below.
- The type of terminal through which the user will usually be accessing the system.
- The printer(s) that will accept the user's print requests.
- The product type(s) that the user may administer. You should also note if the user will be allowed access to only a specific subset of those product types. If so, you must obtain the product ID of those specific products by using the **product display** or **product list** commands.
- The appropriate class(es) for that user.
- The shell that the user will access when executing **shell create** from the SMUE (**sh** for access to the UNIX shell or **rsh** for restricted access). More information is available in "Access to the Restricted UNIX Shell" later in this chapter.

All this login data should be planned in advance and written on the User Login ID Assignment Form in *Manager IV Planning and Implementation.* Use the information on the User Login ID Assignment Form whenever you perform the **login add/change/remove** procedures.

Also, if Manager IV is co-resident with other applications, refer to the *AT&T Co-Resident Applications Front End (CAFE) User's Guide* when you are administering users.

Making Screen Entries

To make entries on the **login add/change/remove** screens, type the information as you are prompted, one line at a time, and press **RETURN** to go to the next entry. To change your entries at any time, use the following keys for such actions as moving from one field to another, deleting your entry, or asking for help.

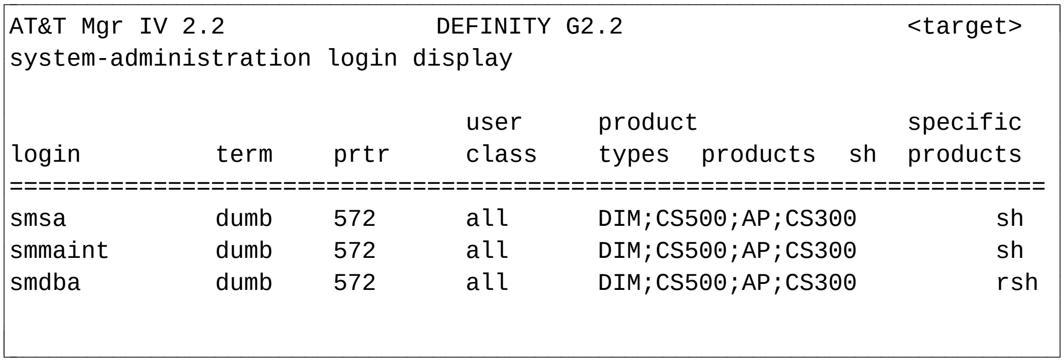
Type **?** at any time and press **RETURN** to see the following list:

```
type anything to enter a value,

type X to clear a value,

type ? to get this information,

type ?? to get item help,

type ^ to back up to the previous items,

type @ to delete the current line you are typing,

type RETURN to move to the next items,

type / followed by an item name to move to that item,

type . to end data entry,

type ! to stop the program.

Enter verb: <current verb>
Remember to end every input line with RETURN.
```

Procedure: Displaying System Logins

Command: system-administration login display

Before adding new users to your system, you might want to review the logins currently installed. The command **system-administration login display** displays user logins and their attributes with a screen similar to the sample below:



```
AT&T Mgr IV 2.2               DEFINITY G2.2                   <target>
system-administration login display

                                user     product              specific
login         term    prtr      class    types  products  sh  products
========================================================================
smsa          dumb    572       all      DIM;CS500;AP;CS300          sh
smmaint       dumb    572       all      DIM;CS500;AP;CS300          sh
smdba         dumb    572       all      DIM;CS500;AP;CS300          rsh
```

ADDING LOGINS

Adding a user login is a three-step process. First, you must add the login using the appropriate UNIX "adduser" command for your processor. This command performs several tasks such as updating the **/etc/passwd** file, creating a home directory, creating a user profile and assigning an initial password.

Second, you must assign the user access—direct or indirect—to Manager IV. Third, you must add the login to Manager IV using the **system-administration login add** command. Manager IV checks the **/etc/passwd** file to confirm the user's identity before it will accept the login.

These procedures are explained in the following chapters.

Procedure: Adding a Login to the UNIX Operating System [3B2 600]

The following procedure creates an entry in the **/etc/passwd** file and creates the user's home directory.

Shell Command: sysadm adduser

1. Log in to the UNIX System as **root**.
2. Enter **sysadm adduser**.

   Note:: You can also enter **sysadm** without the verb. This gives you a menu from which you can select **adduser** or another function.

3. Type in the first name, middle initial, and last name of the user you wish to add. It is not necessary to enclose the name in quotes.
4. Enter the user's login ID, preferably three initials or some other unique combination of letters or letters and numbers.
5. Enter the user's ID number, group ID number or group name, and user's login (home) directory name.

   — Press **RETURN** at each entry to accept the defaults, or enter a different number and different user directory according to your site's system.

   — When adding Manager IV users, you must enter **smgr** at the group ID number or group name prompt.

6. The screen displays all the entered information for you to review. Follow the prompts to install the login, make changes, delete the entry and begin again, or quit the process.
7. If you install the login, the screen displays the message "Login installed."
8. If you want to give the user a password, enter **y** at the next prompt and then enter the user's new password. This password should be at least six characters, one of which is non-alphabetic. The user should change this password as soon as he or she logs in.

Procedure: Adding a Login to the UNIX Operating System [6386 WGS]

Shell Command: adduser

1. Log in to the UNIX system as **root**.
2. Enter **adduser <login ID> <user-name> <user ID> <home directory>** where:
   - **<login ID>** is the user’s login ID, preferably three initials or some other unique combination of letters and numbers.
   - **<user-name>** is the name or title that you want to assign to the login ID, such as **John H. Doe**.
   - **<user-ID>** is the numerical ID that will be associated with the login ID.
   - **<home directory>** is the home directory where the user resides.
3. Designate a password for each added login. This password should be at least six characters, one of which is non-alphabetic.
4. Type the initial password, press **RETURN**, and re-enter the new password at the "Re-enter new password" prompt.

   If the two passwords do not match, then you will be prompted to re-enter the password and reconfirm it. If they match, then the new user login will be added to the system.
5. After adding the user, use the UNIX editor to change the user’s group ID to **smgr** in the /etc/passwd file, and change the user’s group ID for their home directory to **smgr**.
6. Tell the new user the login ID and temporary password to access the system, and advise the new user to change the temporary password to their own personal password as soon as he or she logs in.

Procedure: Designating User Access to Manager IV

There are two possible ways a user can access Manager IV:

- Logging in directly to Manager IV. Most users require direct Manager IV access.
- Initially logging in to the UNIX System and executing SMUE to enter Manager IV.

  Access to Manager IV via the UNIX shell affords greater flexibility, but should be given only to users whose functions warrant such access.

To set up direct Manager IV access for a user:

1. Enter **sysadm chgshell**, or enter **sysadm** and select **chgshell** from the User Management Menu.
2. Enter the login you wish to modify.
3. The following message appears:

   ```
   The current shell is /bin/sh
   Enter new shell command:
   ```
4. Enter **/<application>/smgr/usr/prog/SMUE**

   where <application> is the application software file system name previously designated for Manager IV.
   - To determine the Manager IV file system name, enter the following command:

     echo $SYSROOT

The system response will be similar to the following:

```
/mgr4/smgr
```

- At the Enter new shell command prompt, enter:

  ```
  /mgr4/smgr/usr/prog/SMUE
  ```

  or substitute the directory name that appears instead of "mgr4" in the system response to the "echo $SYSROOT" command above.

If you want a user to have initial access to the UNIX shell, do not perform the **chgshell** procedure. Instead, instruct the user to do one of the following:

- Log in to the UNIX System, type **. /etc/envlist**, press **RETURN** and type **$PROG/SMUE** each time they need to access Manager IV.
- Or, add the following line to their . profile: **PATH = $PATH:/***appl***/smgr/usr/prog** where *appl* is the application software file system name previously designated for Manager IV. Then, the user accesses Manager IV by typing **SMUE** at the UNIX prompt to access Manager IV.

Procedure: Adding a Login to Manager IV

Command: system-administration login add

Once you have added the user login to the **/etc/passwd** file, you can then add it to Manager IV. You must perform the **system-administration login add** command separately for each new user you want to add to the Manager IV database.

1. Log in to Manager IV as **smsa**.
2. At the "Enter application:" prompt, enter **system-administration login add**.
3. Enter the following user login information. Where applicable, use the same information already used when adding the login to the UNIX System **/etc/passwd** file. The system prompts you for all of the following:
4. `User ID>`

   Enter a login ID for the user. This must be the same as the login ID assigned when adding a login to the UNIX System **/etc/passwd** file. The system does not check the validity of the ID until the procedure has finished. You will have to start again if the ID does not match the one already added.
5. `Terminal Type>`

   Enter one of the following valid terminal types:

AT386	AT&T 6386 Work Group Station
513	AT&T 513 Business Communications (BCT) Terminal
615	AT&T 615 BCT Terminal
4410	AT&T Teletype 4410
4425	AT&T Teletype 4425
vt100	DEC® VT100
630	Multi-Tasking Graphics (MTG) terminal

730	Multi-Tasking Graphics (MTG) terminal
sys75	AT&T 615 BCT Terminal with sys75 emulation.

Note: The user may temporarily override this assignment by specifying another terminal when logging in.

6. `Default Printer>`

   This prompt asks for the printer to which output will be directed. Enter the name of one of the printers already at your site and already identified to the system. A user may temporarily override this assignment when logging in.

7. `User Class>`

   Enter one or more of the valid user classes. If more than one class is assigned to a user, separate user classes with a semicolon (;).

   For information on user classes, refer to "User Classes" earlier in this chapter.

   To assign all user classes, enter **all**.

   Valid codes for this field are:

TCM users:	**tcm-1**, **tcm-2**, **precut**, **fm-4**
FM users:	**fm-1**, **fm-2**, **fm-3**, **fm-4**
Maintenance	**maint-1**
Shell access only:	**expert**
Multi-node transactions:	**mnfe**
Adjunct Administration:	**aa**
System Administration:	**sys-admin**
Administration Supervisor:	**super-admin**
Display only:	**reviewer**
Database Initialization:	**init**. The user with this class can access the following system administration objects: **product**, **corporation**, **initialization**, **nonswitch-data**, and **hardware**. This class can access all utilities except **database** and **shell**. (If AT&T Services performs the initialization, this type does not appear as an option to the customer.)
Bulk Initialization:	**bulk-init**. The user with this class can access the following system administration objects: **set-attributes**, **user-information**, **wats-trunk**, **tie-trunk**, **co-fx-did-aplt**, **tie-trunk**, **extn-user-information** and **set-type-name**. This class can access all utilities except **database** and **shell**.

8. `Which product types may the user access?>`

   This field identifies the code(s) that identifies which product types the user may access. If more than one product may be accessed, separate each product code with a semicolon.

   If no product access is allowed, or to restrict a user to a particular target, leave this field blank, or enter **NONE** .

CODE	PRODUCT
D2000	DIMENSION products
SYS85	System 85 products
DEFINITY G2	DEFINITY Generic 2 products
NP	Number Portability Network
TARGRP	Target Group Network
ADJUNCT	Any adjunct product including Information Systems Network products, Centralized System Management, Adjunct Processors, Audio Information Exchange, Local Storage Unit, Central Message Detail Recorder, Manager IV
ALL	Assigns all of the above product types.
NONE	No product types allowed. ||

Note:: With **NP** or **TARGRP**, the user must choose at least one of these product codes: **D2000**, **SYS85**, or **DEFINITY G2**.

9. `What additional specific products may the user access?>`

   Enter a list of products that the user can access in addition to the ones defined in the table above. If no other product can be accessed, enter **NONE** or leave blank and press **RETURN**. |

   If the user can access more than one target, separate the targets with a semicolon.

   If the user can access all products, enter **ALL**.

10. `What shell type may user access?>`

    If the user may access the UNIX shell from within Manager IV, enter **sh**.

    If the user is permitted to access only the restricted UNIX shell, enter **rsh**. Refer to "Access to the Restricted UNIX Shell," below.

11. `Done?>`

    Enter **y** (yes) or **n** (no).

    where: **y** closes the session and adds this login to the Manager IV database.

    n returns the cursor to the first prompt where changes may be made to any field by tabbing to that field and entering new information or deleting the entry.

12. Review your entry with **system administration login display**.

Access to the Restricted UNIX Shell

When you set a user's shell type to **rsh** during the **login add** procedure, you give that user restricted access to the UNIX shell. For instance, the user could be permitted to read and send mail but not execute any other UNIX commands.

For restricted access, set the user's environment variable to RSHPATH instead of PATH. Refer to the **sh** command in the *UNIX® System V User's Reference Manual* for information on **sh** and **rsh** and setting up a directory of commands (**/usr/bin**) to be invoked by **rsh**.

Removing a Login

Removing a user login is a two-step process. For users who no longer need to access Manager IV, but who must access other applications, you must remove their Manager IV login. If a user leaves the company, you must also remove login information from **/etc/passwd**.

Procedure: Removing a Manager IV Login

Command: system-administration login remove

Remove this login if an employee no longer requires access to Manager IV. Service requests associated with the user should either be run, removed, or rescheduled and assigned to a current Manager IV user.

1. Enter **system-administration login remove**.
2. The screen displays the following:

   ```
   User’s login id to be removed>
   ```

   Enter the login ID you are removing.

Procedure: Removing a Login from the UNIX Operating System [3B2 600]

If a user leaves the company, you must also remove that user’s login information (mail file, home directory, and user id) from the **/etc/passwd** file.

1. Log into the UNIX system as **root**.
2. Enter **sysadm deluser** and enter the appropriate user information as prompted.

Procedure: Removing a Login from the UNIX Operating System [6386]

If a user leaves the company, you must also remove that user’s login information (mail file, home directory, and user id) from the **/etc/passwd** file.

1. Log in to the UNIX system as **root**.
2. Enter **deluser** and enter the appropriate user information as prompted.

Procedure: Changing a Login

Command: system-administration login change

To change a login, enter **system-administration login change**. The prompts will be similar to the ones in "Adding a Login." You can change any of the information assigned to the user: Press **RETURN** to skip to the field that must be changed and type over the current information, or use the keys described in "Making Screen Entries" to change data.

Changing a Password

Passwords are known only to the user and are established and maintained by that user, but may be changed at any time by the owner of the password or by the System Administrator with super-user capabilities. To change or remove an entry in the password file, refer to the appropriate AT&T UNIX System V Release 3 System Administrator’s Guide for your processor.

Maintenance Passwords

When a service technician at a remote site requires access to Manager IV, the technician typically uses the **smmaint** login ID. If the technician requires the **root** password, change this password temporarily for the service technician's use. Once the technician has completed all remote maintenance, change the password back, or assign a new password to ensure system security.

ADMINISTERING GLOBAL MODELING

For the user to take advantage of global modeling, the System Administrator must first create a global modeling directory.

Procedure: Administering Global Modeling

1. Create a directory (**gscrap**) for the global models in a selected filesystem.
2. To define this directory, enter the variable, **gscrap** to the **/etc/profile** (**gscrap = directory path**).
3. Export the **gscrap** variable.

See: Chapter 2, "Using Manager IV" in *Getting Started with DEFINITY® Manager IV*. This chapter contains the procedure for using Global Models.

3. MONITORING SYSTEM ACTIVITY

The System Administrator can monitor system usage by following service request activity and by reading the logs. Manager IV produces many logs that record system activity and store error messages. The transaction logs, which are described in this chapter, detail the activities of Manager IV users. See Chapter 7 for information on the other logs.

THE TRANSACTION LOG

The transaction log is the best method for keeping track of system use and the type of transactions being used. Transaction logs detail the activities of Manager IV users. You can review these logs for information about the state of your system during a specific period, for a specific user, or target. You can also use these logs to determine which tasks were being executed when problems were reported by users. The transaction log is retrieved via a command invoked from the UNIX shell. Procedures for using this log follow.

Displaying All Logged-In System Users

Command: system-administration login display

Before requesting a transaction report, you may wish to see who is logged on to the system. Display a list of all users and their attributes with the Manager IV command **system-administration login display**. This command may take a few seconds. Do not press **RETURN** more than once or the display could scroll off your screen.

You can also use the command **who** at the UNIX shell prompt to see a list of all users currently logged on to the processor. The display includes the user's login, terminal line designation, and the date and time the user logged in.

Procedure: Activating Transaction Logs

Shell Command: trxstart <loginid>

1. Access the UNIX shell prompt.
2. Enter **trxstart <loginid>**.

   The login ID after **trxstart** may be a specific user's login ID, a list of several users login IDs, or **all** to activate transaction logging for all users.
3. The log begins to record transactions performed by the specified user(s).

Note: If you attempt to activate the transaction logs after another user has already activated them, you will receive the message "Can't touch."

Procedure: Deactivating Transaction Logs

Shell Command: trxstop <loginid>

You can turn off the logs for an individual login, a list of several user's login IDs, or all (which stops recording transactions for *all* logins) by entering **trxstop <loginid>**.

Procedure: Displaying Transaction Logs

Shell Command: trxrep <loginid>

Once the transaction logs have been activated, you can display information about users' activities by calling for a transaction report.

1. Access the UNIX shell.
2. Enter **trxrep [[-d] [-s] [-e] [-t]] <loginid(s)>**.

   The options are defined as follows:

   -d <MMdd> Shows transactions for a specific date. The default is today's date.

   -s hh[:mm[:ss]] Displays transactions that started after a specified time. Minute and second entries are optional.

   -e hh[:mm[:ss]] Shows transactions that ended before a specified time. Minute and second entries are optional.

   -t <target> Displays transactions only for the target named.

   The **<loginid(s)>** can include a specific user or a specific set of users. Instead of a specific login ID, you can enter **all** to display transactions for all users.

Transaction logs contain:

— The user's login ID

— The target's ID

— The start time when the transaction began

— The run time of the transaction in seconds

— The exit status of the transaction

— The command path used to initiate the transaction.

For example, suppose you enter **$ trxrep -s11:15 -e11:20 smsa** to see transactions performed between 11:15 and 11:20 by the **smsa** login.

System response:

```
smsa       85v5         11:15:13        1         SUCCESS
/tcm/admin/service-request/create    yjw123

smsa       85v5         11:17:09        12        SERV-REQ
/tcm/admin/extension/add    yjw123

smsa       85v5         11:18:55        1         SUCCESS
/tcm/admin/service-request/end    yjw123
```

MANAGING SERVICE REQUEST ACTIVITIES

Manager IV allows you to group a set of transactions and schedule them to be downloaded to the target switch at a specified time through the use of Service Requests. Scheduled Service Requests help Manager IV to operate more efficiently by promoting optimal use of switch and personnel time and resources.

The application user enters the changes, which are immediately made in the Manager IV database, but not made in the switch until the scheduled download time. Users of Manager IV during regular working hours can schedule changes for execution during off-hours such as weekends or evenings.

One of the most important jobs you have as System Administrator is to monitor the success and failure of service requests. All failed service requests must either be resubmitted or backed out of the database. You can use system administration commands to accomplish the following:

- View transactions that have been scheduled for execution. You have the option of displaying information about all entries or selecting specific information.
- Display the results of scheduled executions.
- Correct any failed transactions before they disrupt the system integrity.

The following procedures should be run daily. Refer to the document *Getting Started with Manager IV* for a full explanation of the service request subsystem.

Procedure: Listing All Scheduled Entries

Command: system-administration scheduled-entry list

Enter **system-administration scheduled-entry list** to find out the next execution time, entry type, product ID, and task number associated with each scheduled entry. The output is sorted in ascending order of Scheduled Time.

The fields are the following:

— **Next Execution** - The date and time of the next scheduled execution.

— **Entry Type** - The type of the scheduled entry, such as a service request.

— **Product ID** - The name of the target for which a task has been scheduled.

— **Task Number** - A unique user-specified task number of up to 12 characters.

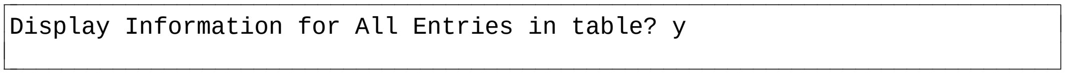
```
AT&T Mgr IV 2.2              DEFINITY G2.2                 <target>
system-administration scheduled-entry list

  Next Execution      Entry Type       Product ID     Task Number
------------------   ---------------   -------------- ---------------
12/31/87 Tue 12:00   Service Request   (023)834-2221   wmmserv1
12/31/87 Tue 12:00   Service Request   (023)834-2221   wmmserv2
```

Procedure: Displaying Selected Scheduled Entries

Command: system-administration scheduled-entry display

1. Enter **system-administration scheduled-entry display** to display a customized set of selected fields.

   System response:



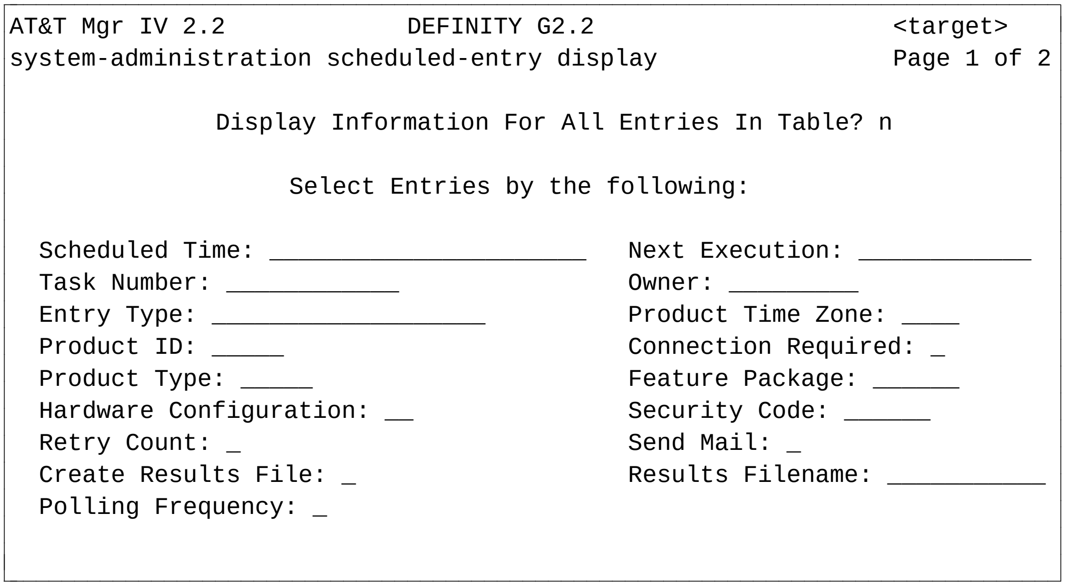
```
Display Information for All Entries in table? y
```

2. Select information for the display:

   — Enter **n** if you wish to enter selection criteria for entries to display; go to step 3.

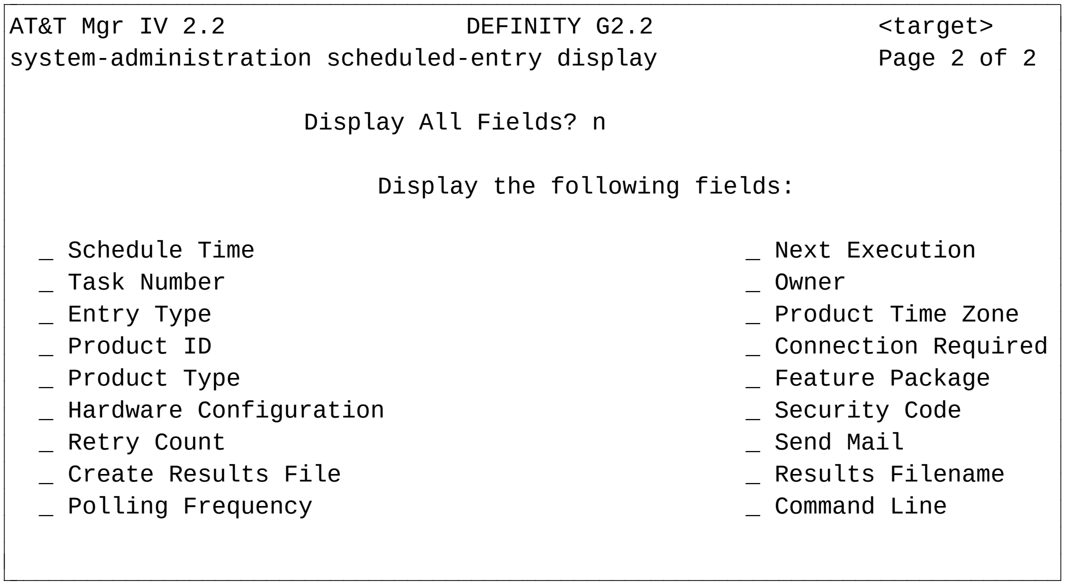
   — Press **RETURN** to choose the default selection of **y** to display *all* scheduled entry information.

3. Specify selection criteria for the scheduled entries to display. For example, you can display scheduled entries for a specific Task Number or Product ID by entering the task number or product ID in the appropriate field.



```
AT&T Mgr IV 2.2             DEFINITY G2.2                       <target>
system-administration scheduled-entry display                   Page 1 of 2

              Display Information For All Entries In Table? n

                   Select Entries by the following:

  Scheduled Time: ______________________     Next Execution: ____________
  Task Number: ____________                  Owner: _________
  Entry Type: ___________________            Product Time Zone: ____
  Product ID: _____                          Connection Required: _
  Product Type: _____                        Feature Package: ______
  Hardware Configuration: __                 Security Code: ______
  Retry Count: _                             Send Mail: _
  Create Results File: _                     Results Filename: ___________
  Polling Frequency: _
```

4. Press **RETURN** to go to page 2. The second page of the input screen allows you to restrict the output of the command to display only selected fields.



```
AT&T Mgr IV 2.2                DEFINITY G2.2               <target>
system-administration scheduled-entry display              Page 2 of 2

                    Display All Fields? n

                         Display the following fields:

  _ Schedule Time                                 _ Next Execution
  _ Task Number                                   _ Owner
  _ Entry Type                                    _ Product Time Zone
  _ Product ID                                    _ Connection Required
  _ Product Type                                  _ Feature Package
  _ Hardware Configuration                        _ Security Code
  _ Retry Count                                   _ Send Mail
  _ Create Results File                           _ Results Filename
  _ Polling Frequency                             _ Command Line
```

5. Select the scheduled entry fields that you want displayed by entering an **x** in front of the options.

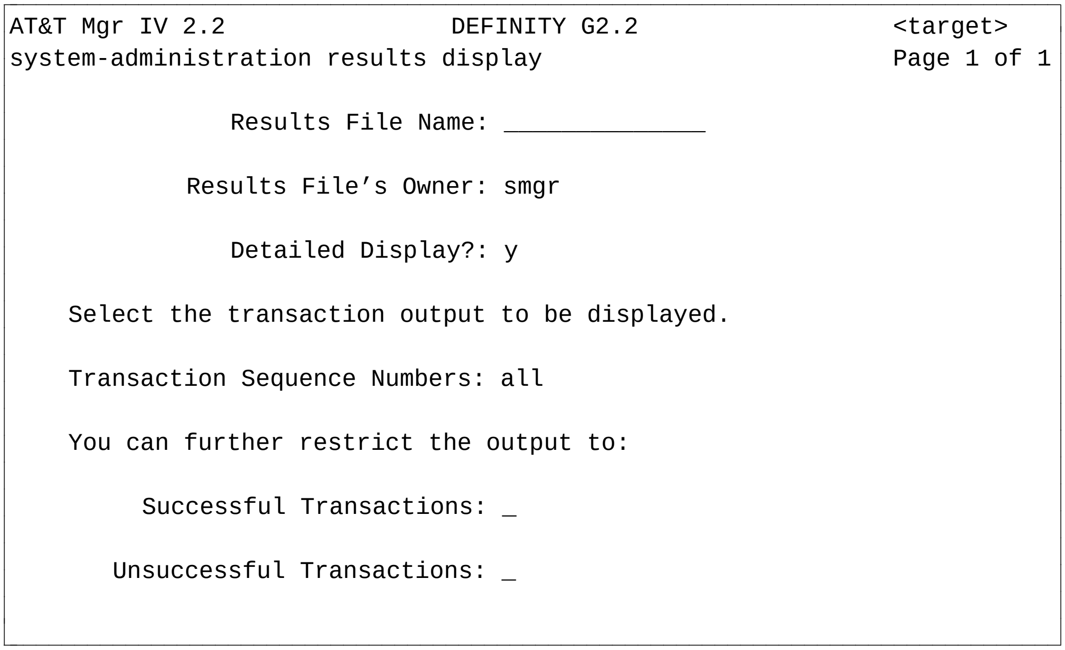
6. Press **ESC** **e** to execute **scheduled-entry display**. Scheduled entries by selected options are displayed.

Procedure: Displaying Results Files

Command: system-administration results display

Results files contain the data normally returned to the screen during product download when a service request is executed. The following procedure enables you to display the contents of a results file:

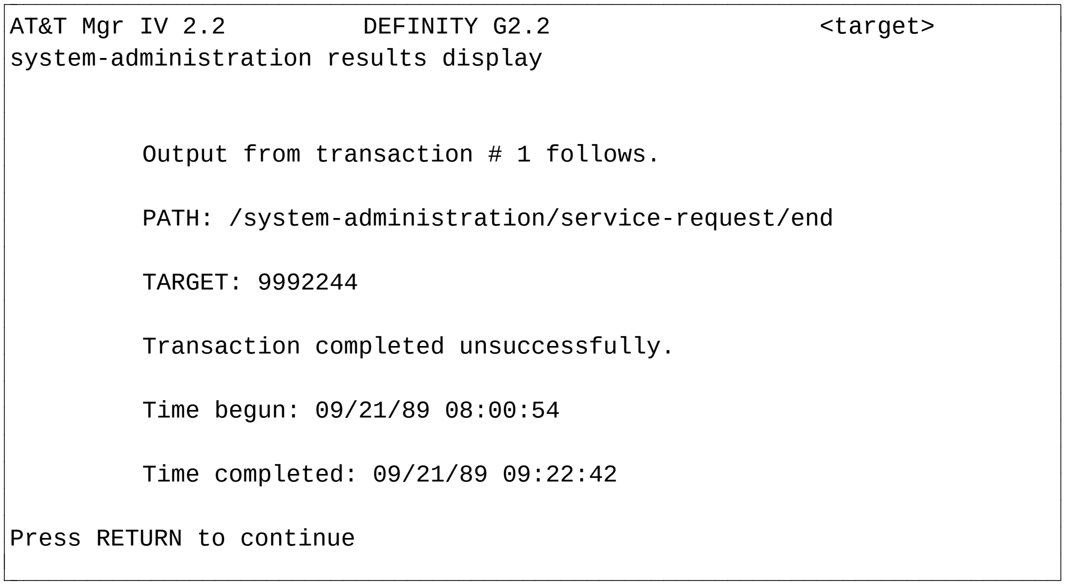
1. Enter **system-administration results display**. The following screen appears:



```
AT&T Mgr IV 2.2               DEFINITY G2.2                   <target>
system-administration results display                         Page 1 of 1

               Results File Name: ______________

            Results File’s Owner: smgr

               Detailed Display?: y

    Select the transaction output to be displayed.

    Transaction Sequence Numbers: all

    You can further restrict the output to:

         Successful Transactions: _

       Unsuccessful Transactions: _
```

2. Fill in the fields as follows:

   - Enter the name of the results file you wish to view.
   - Enter the name of the owner of the results file. This field defaults to your login ID.
   - Answer **y** (yes) or **n** (no) depending on how much detail you want in your display.
     - If you enter **n**, you will see a screen that summarizes the results for the entire SR, like the one shown below.



```
AT&T Mgr IV 2.2         DEFINITY G2.2                  <target>
system-administration results display


         Output from transaction # 1 follows.

         PATH: /system-administration/service-request/end

         TARGET: 9992244

         Transaction completed unsuccessfully.

         Time begun: 09/21/89 08:00:54

         Time completed: 09/21/89 09:22:42

Press RETURN to continue
```

This summary screen shows the transaction number, target and time the transaction attempted to download. It is the only screen that appears if you select **n** at the Detailed Display prompt.

— Press **y** if you want to see a detailed display. Then enter the display criteria:

- Enter the appropriate transaction numbers. You can enter **all** to view the contents of an entire results file, or one or more specific transaction numbers.
- Enter **y** to display successful transactions; enter **n** to restrict the output in the next prompt to unsuccessful transactions only.
- Enter **y** to display unsuccessful transactions; enter **n** if you want to restrict the output to successful transactions only.
- Execute the command.

3. The output from the requested transactions will appear as a series of screens. These screens appear just as if you had executed an immediate transaction or if you had run the SR using the command **service-request run**. All messages that would have appeared on the screen are logged instead in the results file.

   Press (**RETURN**) to page through the screens.

Procedure: Removing a Results File

Command: system-administration results remove

Enter **system-administration results remove <filename>** to remove a results file from your home directory.

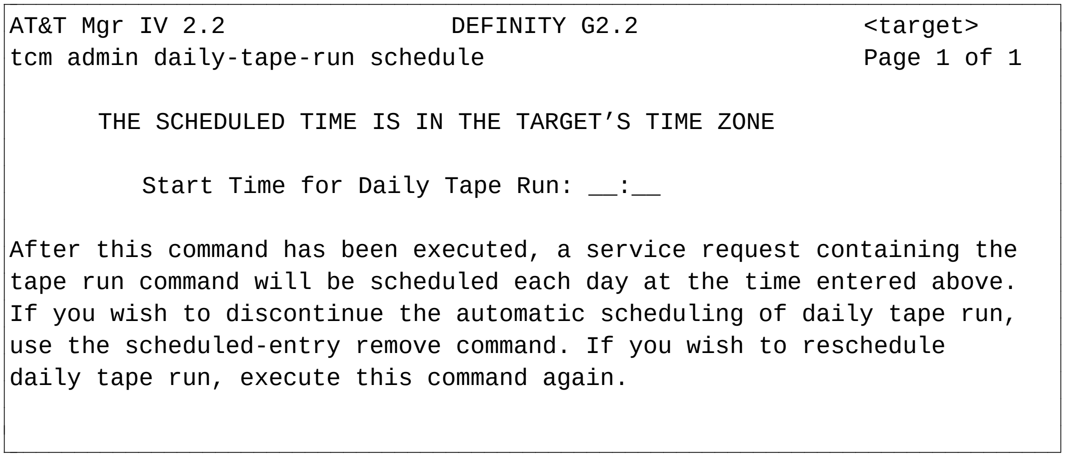
Procedure: Backing Up PBX Downloads

Command: tcm admin daily-tape-run schedule or fm admin daily-tape-run schedule

The command **admin daily-tape-run schedule** enables you to schedule a tape backup of switch translations to run each day at the same time. The command does not allow you to schedule more than one tape run per day for a switch.

Schedule the tape run during periods of low usage because the process may take over an hour to complete and the switch is unavailable for downloading until the process is complete. From the TCM or FM application, perform the following:

1. Enter **admin daily-tape-run schedule**.
2. System response:



```
AT&T Mgr IV 2.2               DEFINITY G2.2               <target>
tcm admin daily-tape-run schedule                         Page 1 of 1

      THE SCHEDULED TIME IS IN THE TARGET’S TIME ZONE

         Start Time for Daily Tape Run: __:__

After this command has been executed, a service request containing the
tape run command will be scheduled each day at the time entered above.
If you wish to discontinue the automatic scheduling of daily tape run,
use the scheduled-entry remove command. If you wish to reschedule
daily tape run, execute this command again.
```

3. Enter the time for the scheduled run and press **EXECUTE**.

Whenever you perform a full backup with **bradm full_dump**, execute the command **tape run** at the switch as well. This is done in addition to the regularly scheduled tape run.

Service Request Log

The service request log contains an entry describing the status and history of every executed service request. You can access the service request log from the UNIX shell; service request log messages appear in the file $LOG/srlogDATE. For example, messages for October 17 appear in the directory **$LOG** in the file srlog1017.

To view the log, identify the date for which you would like information, then cat it to your screen:

cat $LOG/srlogDATE

All information stored in the log for that date will be displayed on your screen.

The following sample shows two messages as they might appear on a terminal screen or console printout. The first message is generated when the service request is started. The second message is generated when the service request has completed successfully. The fields of information in a service request log message are defined below the sample message.

```
>>
TI:    19:16:09
SR:    tape0927ae
ST:    START
MO:    SCHEDULED
MA:    9992255
LO:    jvg


==
TI:    19:21:31
SR:    tape0927ae
ST:    START
MO:    INTERACTIVE
MA:    9992255
LO:    jvg
CO:    Executing service request:remove to remove all transactions
```

TI is the time of day the entry was logged. Format is **hh:mm:ss** where:

hh is the hour of the day (0-23);
mm is the minutes of the hour (0-59);
ss is seconds of the minute (0-59);

SR is the number of the service request.

ST is the status of the service request where:

START indicates the service request was started;
SUCCESS indicates the service request was successfully completed;
FAIL indicates the service request did not complete successfully.

MO is the operating mode in which the service request was executed where:

INTERACTIVE is used if the service request was run interactively;
SCHEDULED is used if the service request was downloaded at a later time.

MA is the target or product ID of the switch receiving the service request.

LO is the login of the user who entered the service request.

CO is a comment describing the action performed on the service request.

To preserve the Service Request log messages, Manager IV accumulates new entries on daily backup tapes taken from the system. Normally, they are saved for two weeks unless you authorize a different period. When the backup tapes are again used to record new entries after the off-line cycle, the old entries are erased. There is no way to study the old entries unless you save the daily console printout for review.

Pending Flag Cleanup

A pending flag appears in Manager IV’s product-image database files to indicate the presence of any pending-queue entries associated with the change of a specific product-image database record. The flag is set to **p** to indicate that a transaction that will affect the product-image database is pending download to the switch.

However, the value of the PENDF flag is sometimes set to **p** even though there are no pending queue entries associated with the product-image database record. This error can be detected and corrected with the Pending Flag Cleanup (**pfclean**) tool. Refer to the section "Directory of Tools" in *Manager IV Installation, Initialization, and Maintenance* for information on **pfclean**. If you cannot correct this error, contact the TSC.

INCREASING THE HIGH-WATER MARK

A low- and high-water mark are associated with each Manager IV daemon process to maximize system performance. A daemon's low-water mark specifies the minimum number of instances of the daemon that will be running at any given time. A daemon's high-water mark specifies the maximum number of instances of the daemon that will be running at any given time.

Low- and high-water marks are set for each Manager IV daemon during the system's installation based on typical user needs. However, these parameters may be manually adjusted to meet your specific performance requirements. Generally, the only adjustment needed is the increase of a daemon's high-water mark.

If you receive a message in the System Administrator error log (explained in Chapter 7) indicating a need to change the high-water mark, contact the TSC.

Procedure: Increasing the High-Water Mark

Shell Command: upctl

This procedure changes the high-water mark for the Manager IV daemon.

1. Access the UNIX shell.
2. Enter **upctl**.
3. At the Transaction prompt, enter **map**. The system responds by listing all Manager IV daemons and their associated parameters.

   System response:

```
NAME        KEY         QBYTES    LWNUM    HWNUM    NUM    IDLECNT

ueutil      840001      8192      2        10       1       1
canclsr     870001      8192      1        10       1       1
customer    900001      8192      2        10       2       2
fmtrk5      930001      8192      2        10       2       2

DUMP SUCCESSFUL

Transaction>
```

4. At the "Transaction" prompt, enter **change**.
5. At the "Name" prompt, enter the name of the daemon you will be changing:

```
Name> fmtrk5
```

   Depending on your terminal type, the parameters associated with the daemon will be displayed either vertically or horizontally. If the parameters are displayed vertically, press **RETURN** twice to skip the Qbytes and Lwnum parameters, then enter the new high-water mark.

   If the parameters are displayed horizontally, press **TAB** twice to skip the Qbytes and Lwnum parameters, then enter the new high-water mark.

6. Enter the new high-water mark.

Note: Raise the number by one only and resume normal system operation. If the number still is not high enough, more error messages will appear.

System response:

```
Qbytes (8192) >
Lwnum  (2)  >
Hwnum  (10) >  11
Key for fmtrk5 successfully changed key is 93000

Transaction >
```

At the "Transaction" prompt, enter **map** again to check the status of your transaction.

The system responds with the new numbers and the message `DUMP SUCCESSFUL.`

Enter **!** to exit the **upctl** program.

CAUTION: Do not attempt to change any daemon parameters other than the low- and high-water marks, or attempt to run any commands other than **change** and **map.**

4. TARGET ADMINISTRATION

To successfully access and manage a product, a description of that product — including product/corporation-specific data and product location —must reside in the database. The System Administrator manages this descriptive information using procedures that add, change, display, list, and remove corporate and product descriptions.

All products and corporations should have been entered into the system during installation by an AT&T service technician. However, there may be times when you must add a new product to the database or update the description of an existing product. If that is necessary, you will find the procedure here for adding a product or adding cut-through access to a product.

PRODUCT AND CORPORATE DESCRIPTIONS

This section contains procedures that you are expected to use, but does not include information on all the commands available for the **product** and **corporation** objects. For more information about **product** and **corporation**, refer to *Manager IV Installation, Initialization, and Maintenance* .

Procedure: Listing Corporations

Command: system-administration corporation list

The command **system-administration corporation list** lists the corporations that Manager IV supports in your system. They will be displayed in this format:

```
AT&T Mgr IV 2.2                  DEFINITY G2.2             <target>
system-administration corporation list

CORPORATION ID: appcorp
        DCS ID: dcsnet1

CORPORATION ID: blxcorp
        DCS ID: blxdcs
        ETN ID: blxetn
         NP ID: blxnp
```

Note that Distributed Communications Service (DCS), Electronic Tandem Network (ETN), and Number Portability (NP) IDs are listed when applicable. DCS, ETN and NP IDs are listed separately.

Procedure: Listing Products

Command: system-administration product list

Use the command **product list** to list and verify information about each product. This command lists the Product ID, Product Type, Time Zone the product is located in, the ETN ID, the DCS ID, and the Number Portability Network ID.

This is a sample of the information displayed using the **product list** command:

```
AT&T Mgr IV 2.2                  DEFINITY G2.2              <target>
system-administration product list

Product ID
 (Target)    Product    Type   Time Zone   ETN ID   DCS ID    NP ID
---------    --------   ----   ---------   ------   ------    ----
Miami        SYS85      R2L3       EST       et1     dcs1
Orlando      SYS85      R2L3       EST       et1     dcs1
Ojus         SYS85      R2L3       EST
```

Procedure: Displaying Manager IV Database File Names

Command: system-administration database list

Use this display after the initialization process to verify that the product IDs have been keyed correctly and to note the assigned product ID (PBXID) numbers. Product IDs are required whenever you load, save, or remove files from the Manager IV database.

Enter **database list**. The filename, product ID, and DOSS number will be displayed. If the column under STAT says yes, the number of records and the number of bytes are displayed for the file and its subfile.

A database file display follows:

```
AT&T Mgr IV 2.2                  DEFINITY G2.2              <target>
system-administration database list
FILENAME      PBXID    NREC   NBYTE   STAT  LDN            DOSNO

smb           1        0      0       no    (022)834-3569 00228343569
rnx           2        0      0       no    (022)834-3303 00228343303
crac          2        0      0       no    (022)834-3303 00228343303
fnpa          4        0      0       no    (021)834-3304 00218343304
```

Procedure: Adding a Corporate Description

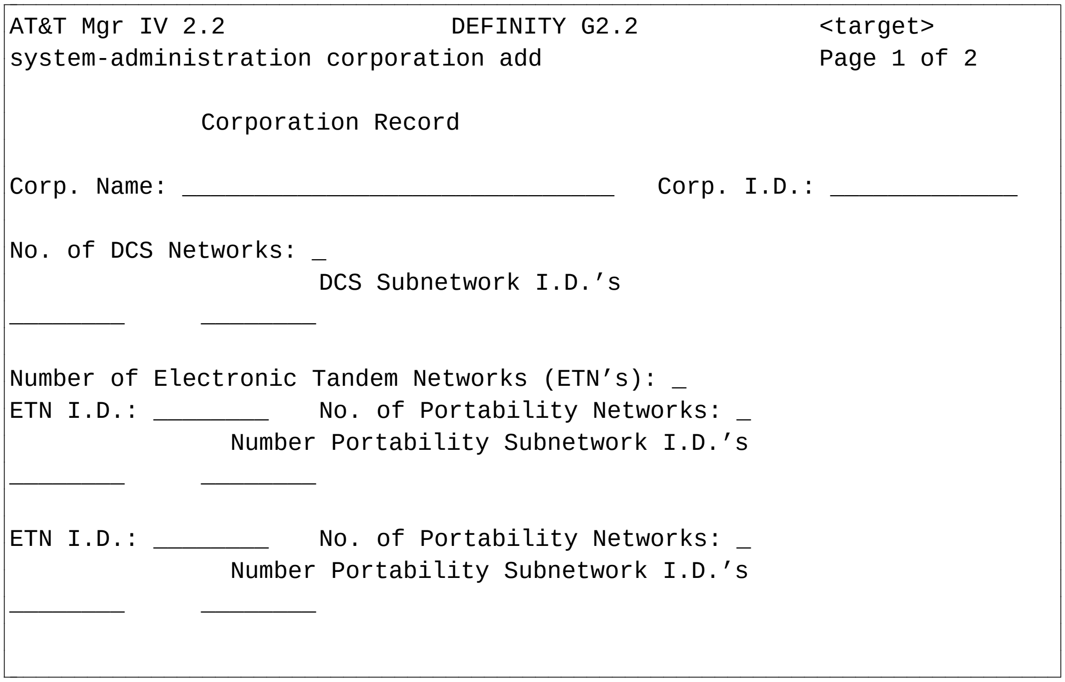
Command: system-administration corporation add

This procedure defines the corporation(s) associated with your switch(es). Corporations must be defined before products can be defined.

Only the user class **init** has access to the **corporation add** command. If you need help with this procedure, contact the National Customer Service Center.

Refer to the previous display procedures — **product list, database list,** and **corporation list** — when entering information about corporations and products. If information you need isn't found on the display screens, check the data collection forms filled out prior to installation.

1. Enter **system-administration corporation add** to access the following screen:



```
AT&T Mgr IV 2.2               DEFINITY G2.2            <target>
system-administration corporation add                  Page 1 of 2

             Corporation Record

Corp. Name: ______________________________   Corp. I.D.: _____________

No. of DCS Networks: _
                     DCS Subnetwork I.D.'s
________     ________

Number of Electronic Tandem Networks (ETN's): _
ETN I.D.: ________   No. of Portability Networks: _
               Number Portability Subnetwork I.D.'s
________     ________

ETN I.D.: ________   No. of Portability Networks: _
               Number Portability Subnetwork I.D.'s
________     ________
```

Define a corporation name and ID in the Manager IV database and identify any associated Electronic Tandem Networks (ETNs), Distributed Communication System (DCS) subnetworks, and Number Portability subnetworks.

The corporation data should be available on the Corporation Information data collection form that was completed by the customer prior to installation. (The form is found in *DEFINITY Manager IV Planning and Implementation*.)

The System prompts for the following fields.

Corp. Name
Enter the full name of the corporation. Maximum length is 30 characters.

Corp. I.D.
This ID is a shortened key that is valid for identifying the corporation at the target level. The ID can not contain blank spaces and may be a maximum length of 13 characters.

No. of DCS Networks
Enter number of DCS networks to be managed through Manager IV. Valid entries are **0-9**.

DCS Subnetwork I.D.'s
This ID is a unique identifier for the DCS Network. The ID may be a maximum length of 8 characters.

Number of Electronic Tandem Networks (ETN's)
Enter the number of ETN networks present for this corporation. Valid entries are **0-5**.

ETN I.D.
This ID is a unique identifier for the ETN Network. The ID may be a maximum length of 8 characters.

No. of Portability Networks
Enter number of NP networks for this corporation. Valid entries are **0-9**.

Number Portability Subnetwork I.D.'s
This ID is a unique identifier for the NP networks. The ID may be a maximum length of 8 characters.

2. Execute the corporation add transaction. Press **ESC** **e** or **EXECUTE**.

Procedure: Adding a Supported Product

Command: system-administration product add

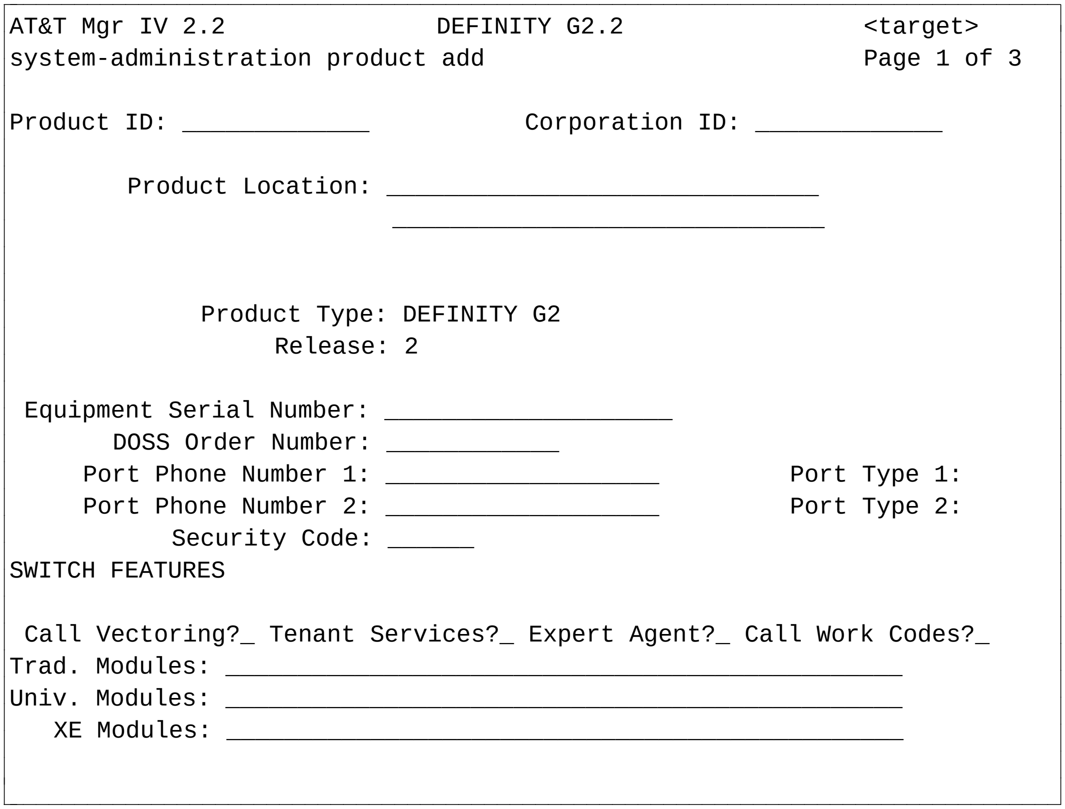
Use this procedure to define each supported product in the Manager IV CORE database.

Corporate information must be defined before a product can be added. See "Procedure: Adding a Corporate Description" above to define corporate information.

Product data should be available on the Product Definition Data Collection Form completed by the customer prior to installation. The form is found in *Manager IV Planning and Implementation*.

For information regarding the addition of cut-through accessed products, see "Procedure: Adding Cut-Through Access to a Product" in this section.

1. Enter **system-administration product add** to access the first page of the **product add** screen:



```
AT&T Mgr IV 2.2               DEFINITY G2.2                <target>
system-administration product add                          Page 1 of 3

Product ID: _____________           Corporation ID: _____________

        Product Location: ______________________________
                          ______________________________


             Product Type: DEFINITY G2
                  Release: 2

 Equipment Serial Number: ____________________
       DOSS Order Number: ____________
     Port Phone Number 1: ___________________        Port Type 1:
     Port Phone Number 2: ___________________        Port Type 2:
           Security Code: ______
SWITCH FEATURES

 Call Vectoring?_ Tenant Services?_ Expert Agent?_ Call Work Codes?_
Trad. Modules: _______________________________________________
Univ. Modules: _______________________________________________
   XE Modules: _______________________________________________
```

2. Enter the product information from the Product Definition data collection form(s). The type of product being defined determines the required fields and valid entries. The charts below list the required fields and valid entries by product. Use the charts as a guide when entering the information.

`Product ID:`

The Product ID is a unique identifier for the managed product. Each Product ID cannot contain blank spaces and has a maximum length of 13 characters.

`Corporation ID:`

The corporation ID is assigned through the **corporation add** transaction. Maximum length is 13 characters.

`Product Location:`

The Product Location is the address of the product. Maximum length is two lines of up to 60 characters.

`Product Type:`

This is the code that identifies the type of product being added.

CODE	**PRODUCT**
ADJUNCT	All products for which Manager IV provides cut-through access
SYS85	System 85 products
D2000	DIMENSION products
DEFINITY G2	DEFINITY Generic 2 products

- **System 85:**

Release:	[System generated] A single digit: (**2**).
Version:	A single digit: (**2,3,** or **4**).
Issue:	Issue number: *default* (**1.0**)

- **DIMENSION 2000:**

Bus Type:	Enter **1** for single bus; **2** for dual bus
Feature Package:	[System generated] A single digit: (**8**)
Issue:	Issue number: **1.16** or **3.8**
Hardware Configuration:	Switch memory size. Maximum length is 2 characters. The first letter represents memory size and a trailing D represents a dual processor. Sample entries are: **B** or **CD**.

Valid entries are:

- **B**
- **C** (not valid for FP8 Issue 3.8)
- **D** (not valid for FP8 Issue 1.16)
- **F**
- **D** (dual processor).

- **DEFINITY Generic 2:**

  Release: A single digit: (**1** for G2.1; **2** for G2.2).

Provide identification for the product, the network, the present applications, and the administrators' logins. This information should be on the Product Definition Data Collection Form. Use the field descriptions below as a guide when entering information.

`Equipment Serial Number:` Enter the serial number in the form:

<NNNN-YY-XXXXXXXXX-Z>

where: NNNN = Product Code - 4 digits identifying the product type

YY = Manufacturer's Code - 2 digits identifying the manufacturer

XXXXXXXXX = Serial Number - 9 characters unique to the product

Z = Check digit - 1 character (numeric or dash [-])

`DOSS Order Number`: Enter the DOSS Order number in the following format: <XXXXXXXXXNN>

where: XXXXXXXXX = DOSS Sales Order Number

NN = DOSS Segment Number

`Port Phone Number 1`: Enter the product port number as dialed from the product access port or "dedicated". This field is required.

The number may contain any combination of digits, dash (—), equal (=), asterisk (*), or pound sign (#).

— pause
= wait for secondary dial tone
***** touch tone asterisk
touch tone pound sign
0-9 dialed digit

`Port Type 1:` [DEFINITY Generic 2] This field appears only in Generic 2. Enter **r** for RMATS, **p** for PPG or **n** for none.

`Port Phone Number 2:` [System 85 and DEFINITY Generic 2] This field is optional and cannot be designated as dedicated. This field has the same format as the "Port Phone No. 1" and is used to specify the second dial-up port.

`Port Type 2:` [DEFINITY Generic 2] This field appears only in Generic 2. Enter **r** for RMATS, **p** for PPG or **n** for none.

`Security Code:` Security codes are stored in the switch.

[DIMENSION 2000] Enter the four-digit security code.
[System 85 and DEFINITY Generic 2] Enter the six-digit security code.

Note:: If unrestricted switch alarm dial-out is required on System 85, only "Port Phone No. 1" should be specified. The number used should be the switch port without the dial-out capability. This ensures that the dial-out port is never busy for servicing Manager IV when a switch alarm occurs.

Switch Features

[D2000 and SYS85 only] `Asgnd Modules:`

Enter the assigned module numbers. Valid entries are a single digit separated by commas (,) or a range of numbers separated by dashes (—), i. e. 2, 3, 4-7.

[System 85R2V4 or DEFINITY G2] `Call Vectoring`

A system generated field informing you whether Call Vectoring is present.

[System 85 R2V4 or DEFINITY G2] `Tenant Services`

A system generated field informing you whether tenant services is present.

[System 85 R2V4 or DEFINITY G2] `Trad. Univ., or XE Modules:`

System generated fields providing specific information on the type of modules present.

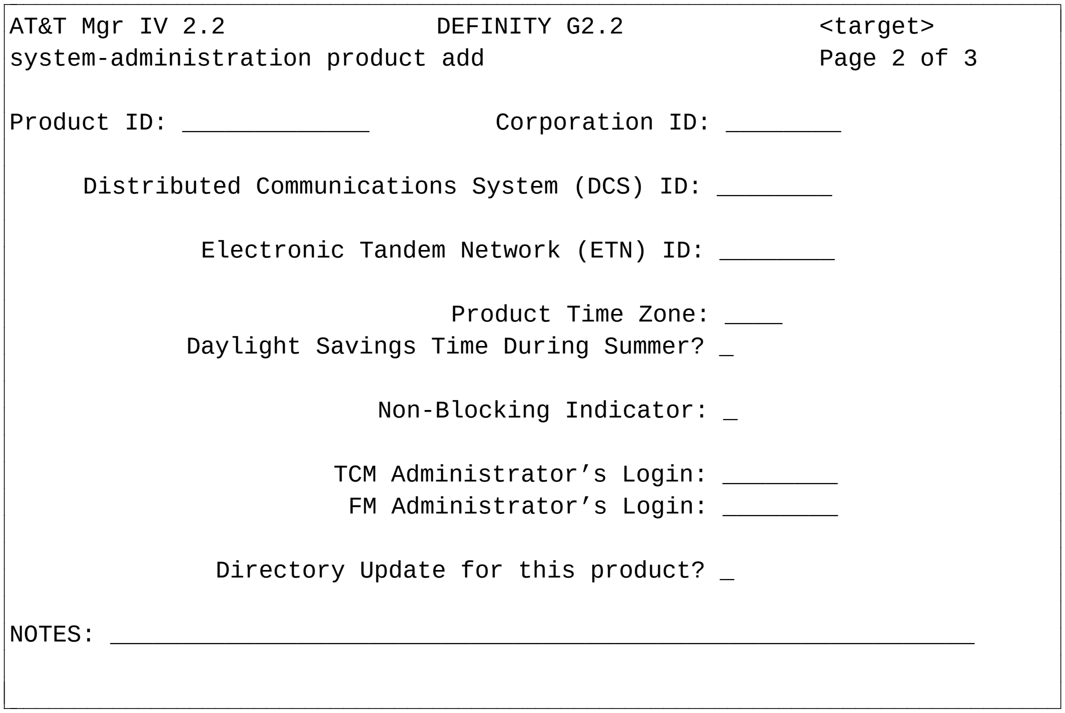
[DEFINITY G2.2] `Expert Agent?`

A system generated field informing you whether Expert Agent Selection is present.

[DEFINITY G2.2] `Call Work Codes?`

A system generated field informing you whether Call Work Codes is present.

Page 2 of the **product add** screen displays:



```
AT&T Mgr IV 2.2              DEFINITY G2.2             <target>
system-administration product add                      Page 2 of 3

Product ID: _____________        Corporation ID: ________

     Distributed Communications System (DCS) ID: ________

             Electronic Tandem Network (ETN) ID: ________

                               Product Time Zone: ____
            Daylight Savings Time During Summer? _

                          Non-Blocking Indicator: _

                       TCM Administrator’s Login: ________
                        FM Administrator’s Login: ________

               Directory Update for this product? _

NOTES: ____________________________________________________________
```

3. `DCS ID`:

   Enter the DCS ID associated with the switch. This ID must be assigned to the entered corporation ID. Maximum length is eight characters.

4. `ETN ID:`

   Enter the ETN ID associated with the switch. This ID must be assigned to the entered corporation ID.

5. `Number Portability ID`:

   This prompt appears if ETN ID is supplied. The Number Portability ID must be assigned to the entered corporation ID.

6. `Product Time Zone`:

   Enter the correct time zone associated with the switch. Valid entries are as follows:

Valid Entry	**Time Zone**
AST	Alaskan Standard Time
CST	Central Standard Time
EST	Eastern Standard Time
HST	Hawaiian Standard Time
MST	Mountain Standard Time
PST	Pacific Standard Time
TST	Atlantic Standard Time

7. `Daylight Savings Time During Summer?`

   Enter **y** (yes) or **n** (no).

8. `Non-Blocking Indicator`:

   Enter **e** if the switch is essentially nonblocking.
   Enter **n** if the switch is nonblocking.

9. `Administrator’s Logins`

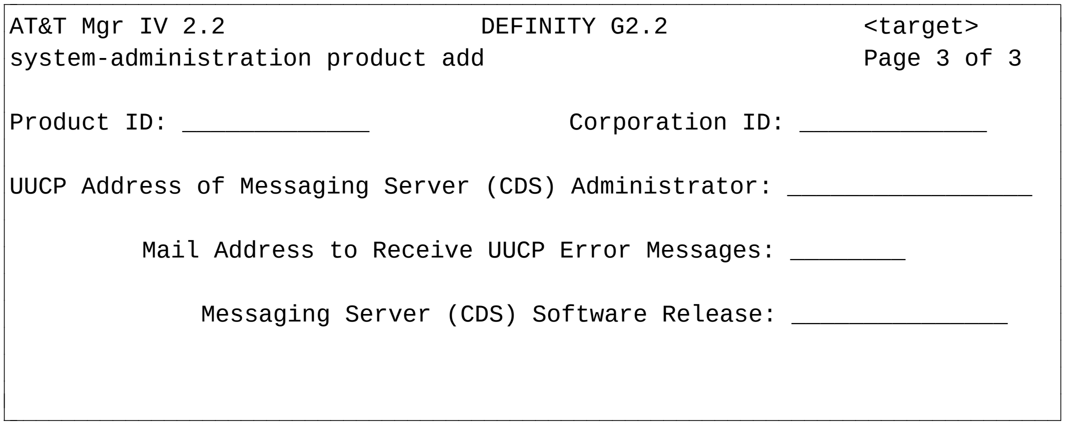
   Enter the primary TCM and FM Administrators’ logins.

10. `Directory Update for this product?`

    If this product utilizes the 3B2 Messaging Server or CDS Directory Synchronization feature, enter **y**; if not, enter **n** and execute the **product add** transaction.

11. If the Directory Synchronization Feature of Manager IV is used to update an existing Personnel Database for the Messaging Server, page 3 of the **product add** screen appears.

12. `Notes`: Enter any pertinent comments about this product in this field. It is a free-format field of up to 72 characters.



```
AT&T Mgr IV 2.2                    DEFINITY G2.2            <target>
system-administration product add                           Page 3 of 3

Product ID: _____________               Corporation ID: _____________

UUCP Address of Messaging Server (CDS) Administrator: _________________

         Mail Address to Receive UUCP Error Messages: ________

             Messaging Server (CDS) Software Release: _______________
```

Enter the following information:

`UUCP Address of CDS Administrator`

Enter the remote mailing address of the Messaging Server. The address is the processor name and the login of the CDS administrator, separated by an exclamation point (!).

When using Messaging Server or CDS in a number portability environment, assign the UUCP address to only one of the nodes in the number portability network. For each of the other nodes, enter the target name of the first node preceded by a tilde (~) in this field. For example, enter ~ **node1.**

`Mail Address to Receive UUCP Error Messages`

Enter the login ID of the Manager IV System Administrator.

`CDS Software Release`

Enter the release number of the CDS software.

13. Execute the **product add** transaction by pressing **ESC** **e** or **EXECUTE**.

Procedure: Adding Cut-Through Access to a Product

Command: system-administration product add

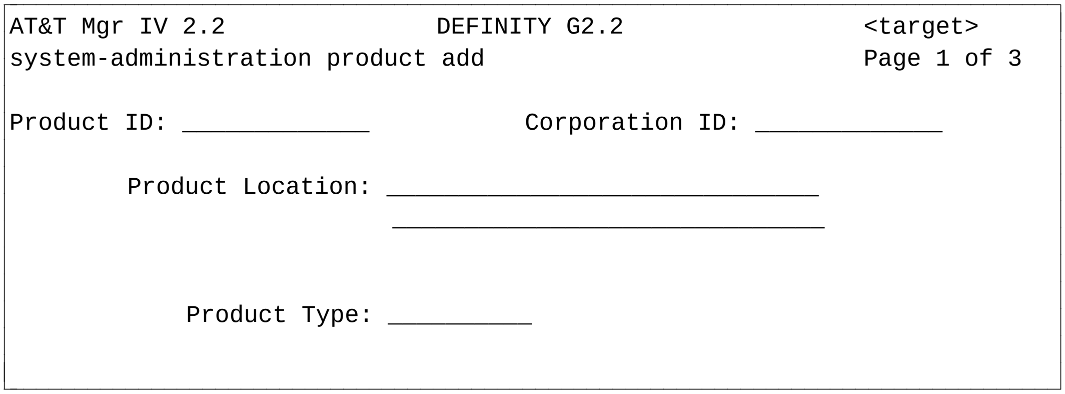
Use this procedure to identify each product for which the application provides cut-through access and enter this information into the Manager IV CORE database. Product data is available on the Product Definition Data Collection Form completed prior to installation. (The form is found in *Manager IV Planning and Implementation*.)

Corporate information must be defined before the product can be added. See "Procedure: Adding a Corporate Description" to define corporate information.

The command used in this procedure is the same command as the one used to add supported products. For more information, see "Procedure: Adding a Supported Product" in this section.

1. Enter **system-administration product add** to access the product add screen.

   System Response:



```
AT&T Mgr IV 2.2               DEFINITY G2.2                    <target>
system-administration product add                              Page 1 of 3

Product ID: _____________          Corporation ID: _____________

        Product Location: ______________________________
                           ______________________________


            Product Type: __________

```

2. Enter the product information from the Product Definition data collection form(s).
3. `Product ID:`

   The product ID is a unique identifier for the product. The Product ID cannot contain spaces and has a maximum length of 13 characters.
4. `Corporation ID`:

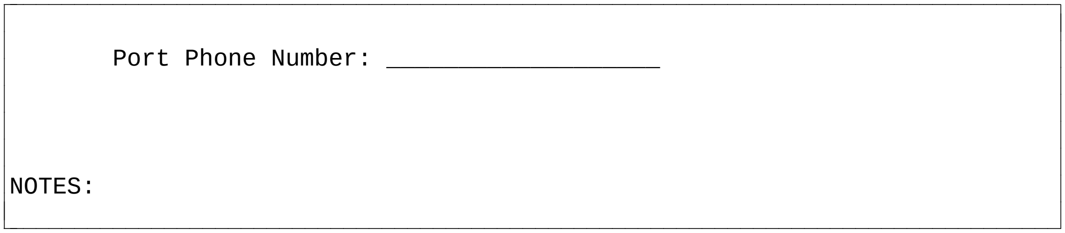
   The corporation ID is assigned through the **corporation add** transaction. Maximum length is 13 characters.
5. `Product Location:`

   This is the address of the product. Maximum length is two lines of 60 characters.

6. `Product Type`:

   Enter **ADJUNCT** for all products for which Manager IV will provide cut-through access including System 75, Adjunct Processors, Audio Information Exchange (AUDIX), Information Systems Network, Centralized System Management, Local Storage Units, Centralized Message Detail Recorder, DEFINITY Generic 1, and Manager IV.

   Once you identify the product type, the following field appears:



```
      Port Phone Number: ___________________



NOTES:
```

7. `Port Phone Number:`

   Enter the product port number as dialed from the product access port.

   The number may contain any combination of digits, dash (—), equal (=), asterisk (*), or pound sign (#).

   - pause
   = wait for secondary dial tone
   ***** touch tone asterisk
   # touch tone pound sign
   0-9 dialed digit

8. Execute this command by pressing **ESC** **e** or **EXECUTE**.

TARGET GROUP TRANSACTIONS

A target group is a set of PBXs belonging to the same corporation. A single switch may belong to more than one target group. Through the use of this new identifier, users will be able to update several PBXs at one time for certain multi-node transactions.

Only the System Administrator can add (**target-group add**), change (**target-group change**), or remove (**target-group remove**) target groups. Any user can display a target group by performing **target-group display**.

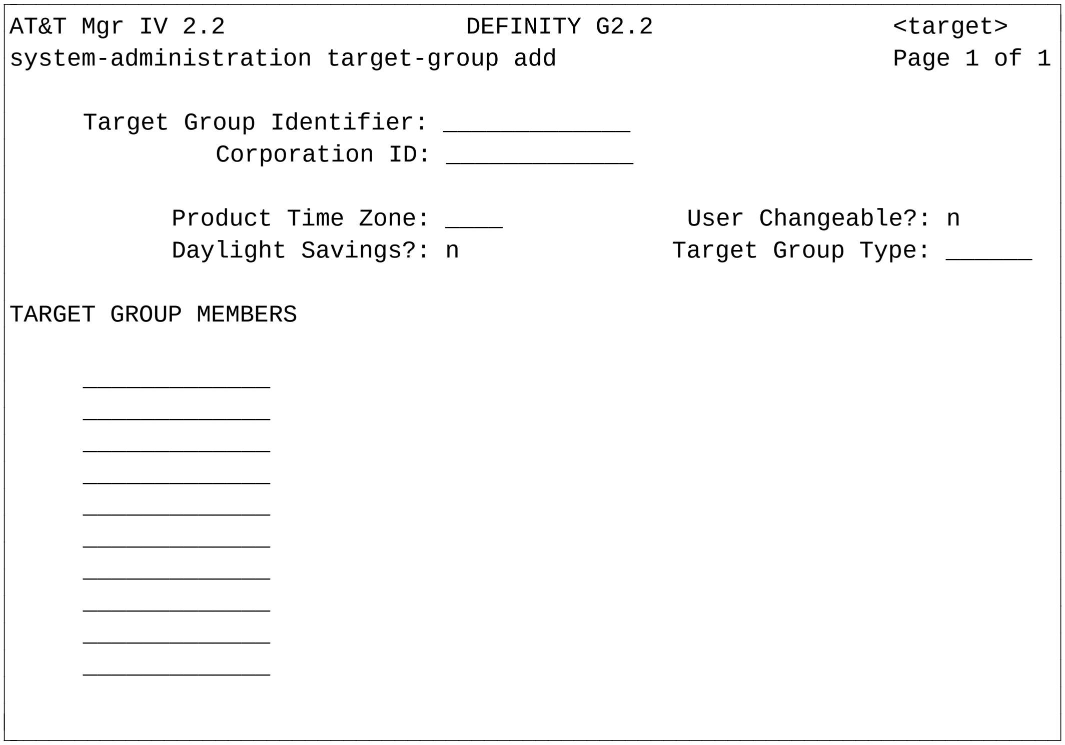
If desired, target groups can be edited at run time — that is, before the command is executed, the user can select a subset of the targets in the target group for the current transaction.

Before the **target-group** transaction will work, corporations must already be added. At least one product must already be added for that corporation.

Procedure: Adding a Target Group

Command: system-administration target-group add

1. Enter the command **system-administration target-group add** and enter data in the fields as follows:



```
AT&T Mgr IV 2.2                DEFINITY G2.2                <target>
system-administration target-group add                      Page 1 of 1

     Target Group Identifier: _____________
              Corporation ID: _____________

           Product Time Zone: ____            User Changeable?: n
           Daylight Savings?: n              Target Group Type: ______

TARGET GROUP MEMBERS

     _____________
     _____________
     _____________
     _____________
     _____________
     _____________
     _____________
     _____________
     _____________
     _____________
```

2. `Target Group Identifier:`

   Enter the unique identifying name for a target group, up to 13 characters.

3. `Corporation ID:`

   Enter the unique identifier of the corporation that owns this target group. Use **system-administration corporation list** to obtain this information.

4. `Product Time Zone:`

   Enter the time zone used for scheduled tasks for this target group. Choices are as follows:

EST	Eastern Standard Time
CST	Central Standard Time
MST	Mountain Standard Time
PST	Pacific Standard Time
AST	Alaskan Standard Time
HST	Hawaiian Standard Time
TST	Atlantic Standard Time

5. `User Changeable?`

   If the user should be allowed to change the set of targets at run time, enter **y**.

6. `Daylight Savings?`

   Enter **y** if Daylight Savings Time is appropriate for this time zone.

7. `Target Group Type:`

   Enter an optional description of this type of group.

8. `Target Group Members`

   Enter the code(s) for the targets you are adding to this target group. Use **system-administration product list** to obtain this information.

9. Execute the command.

The target-group identifier works with the following transactions:

- auth-code (auth-code)
- Number-portability commands (number-groups, extension move)
- portability-routing
- user (database only)

Changing, Displaying, or Removing a Target Group

If you use the commands **system-administration target-group change, display,** or **remove**, the screen will contain fields for "Target Group Identifier" and "Corporation ID." Enter the appropriate data in these two fields. Execute the command after you receive the message `End of Form.`

5. HARDWARE ADMINISTRATION

Your responsibilities as System Administrator include administration of the processor and product access ports. Manager IV resides on an AT&T 3B2-600 processor or an AT&T 6386E/33 Work Group Station (WGS). Refer to the appropriate AT&T System Administrator's Guide for your processor for details about general operating policy and processor maintenance. This chapter also includes information on system management agents and how to recognize when Manager IV exceeds a limited database capacity.

SHUTTING DOWN AND REBOOTING MANAGER IV

The **startsm** and **stopsm** commands enable you to shut down Manager IV without affecting any other applications on your processor. Certain procedures, such as the full backup of the Manager IV database (see Chapter 6), require that you enter **stopsm** to bring down the system.

The following procedures explain how to set up your system in order to use **stopsm** and **startsm**.

Procedure: Setting up startsm and stopsm

To start Manager IV automatically at machine boot time, do the following:

1. Log in as **root**.
2. At the UNIX prompt, change directories to the appropriate **etc/rc[2] [3].d** directory.
3. Create a file called "S91startsm" with the following lines:

```
. /etc/envlist
LOGNAME=root
HOME=/
export HOME LOGNAME
$SYSROOT/etc/startsm
```

To stop Manager IV automatically at machine shutdown time, do the following:

1. Log in as **root**.
2. Change directories to **/etc/rc0.d** directory.
3. Create a file called "K03stopsm" with the following lines:

```
. /etc/envlist
LOGNAME=root
HOME=/
export HOME LOGNAME
$SYSROOT/etc/stopsm
```

Procedure: Shutting Down and Rebooting Manager IV

UNIX Command: # stopsm and **startsm**

1. Log in as **root**.
2. Enter **. /etc/envlist**
3. At the UNIX prompt, enter **cd $SYSROOT/etc**
4. Enter **stopsm** to shut down Manager IV.

   This command brings down the Manager IV applications without shutting down any other applications on your processor.
5. Enter **startsm** to reboot Manager IV.

ADMINISTERING PRODUCT ACCESS PORTS

Although enabling and disabling ports is usually the responsibility of the installation team, occasionally the System Administrator will have to perform these tasks. You can define, display, and monitor the product access ports that are configured to support Manager IV and its products. If you have questions about how ports are set up on the processor, check your UNIX system documentation to ensure that the proper number and type of ports have been assigned for your Manager IV software.

Check configurations of the ports in the **/dev** directory and the **/etc/inittab** file.

The following utilities administer product access ports.

Use:	**To:**
connection display	List all users currently connected to products.
port add	Define port attributes. Used after a peripheral or modem is plugged into a product access port, so the port can properly communicate with Manager IV and defined products.
port change	Change descriptive comments for a port.
port disable	Disable a defined port for servicing.
port display	Display the names of currently configured ports.
port enable	Enable a defined port for servicing.
port release	Release a port currently in use. Use for emergency purposes to terminate a connection.
port remove	Remove a port.

Procedure: Displaying Product Access Port Attributes

Command: system-administration port display

With the command **port display**, you can display the current attributes of each enabled and disabled product access port configured for Manager IV. Information displayed via **port display** reflects the actual port status file, not changes being made by a currently active **port add**, **port change**, or **port remove** command.

Port names are site-dependent and were assigned during system configuration. (Port names on the 3B2 and the 6386 WGS consist of *tty* followed by a number.) The **port display** command will give you the following response:

```
AT&T Mgr IV 2.2             DEFINITY G2.2             <target>
system-administration port display

 Port: /dev/tty12    ACU: none
 State: enabled      Product ID: none         Port Type: autodial
 Dialer: 2224        Protocol: async          Speeds: 300, 1200
 Comments: This is a modem compatible with 2224

 Port: /dev/tty13    ACU: none
 State: enabled      Product ID: none         Port Type: autodial
 Dialer: 2224        Protocol: async         Speeds: 300, 1200
 Comments: This is how a 2224 should be configured.
```

Procedure: Displaying Users Connected to Products

Command: system-administration connection display

Use the command **connection display** to list all users currently connected to products including the product ID they are connected to, the identity of the port in use for that connection, and the date and time the connection was last accessed. When the "user" is a service request, "Extract" is shown in the user column.

Enter **connection display** to receive the following output:

```
AT&T Mgr IV 2.2             DEFINITY G2.2               <target>
system-administration connection display


                            Mgr IV Connections
User  Product ID       Dataport     PBX Port  Last Access
----  ------------     ---------    --------  -----------
smsa    lt             /dev/tty42      0     Mon Oct 23 09:17:45 1989

                            Non-Mgr IV Connections
User  Product ID       Dataport     PID       Last Access
----  -------------    ----------   --------  -------------
```

Procedure: Adding a Port

Command: system-administration port add

This procedure adds a new product access port to the configuration and defines its attributes.

When adding product access ports, first check the configuration of the ports in the **/dev** directory and in **/etc/inittab**, as described in the "Verifying the Product Access Ports" procedure in *Manager IV Installation, Initialization, and Maintenance*. To reallocate a product access port, the port must be removed and added with a new configuration.

The port data should be available on the Manager IV Port Configuration Form that has been completed by the Implementation Team. The form can be found in *Manager IV Planning and Implementation*.

1. Enter **system-administration port add**.

   The system will prompt you for the following information.

2. `Port Name >`

   Enter the name of the port you want to add. Port names are site-dependent and are assigned during the configuration of the system.

3. `Conn Type >`

   Enter the connection type you want to assign to this port. Enter **auto** for dial-out lines using modems with integral autodialers.

4. `Speed >`

   Enter all the line speeds that this port will support. Enter one speed per prompt. End the list by entering **!** on a line by itself.

   Supported transmission speed(s) are as follows:

SPEED	DESCRIPTION
300	300 baud transmission rate.
1200	1200 baud transmission rate.
2400	2400 baud transmission rate.

   Recommendations:

   - For AT&T 2224CEO asynchronous modems, enter both 300 and 1200.
   - 300 is recommended for DIMENSION 600 and DIMENSION 2000.
   - 1200 is recommended for System 85, Generic 2, and cut-through access.
   - 2400 is recommended for dial-up remote access.

5. `Enable Port? >`

   Enter **y** or **n**

   where: **y** means to enable the port now

   n means to leave the port disabled until a later time. (See "Procedure: Enabling a Port" below to enable a port at a later date.)

6. `Comment ([ ]) >`

   [Optional] One line of text for future reference. To view the comment field for each record, use **port display**.

7. After entering all needed data, execute the command by pressing **RETURN**.

To test product access ports, refer to *Manager IV Installation, Initialization, and Maintenance*, "Enabling and Testing Ports."

Procedure: Enabling a Port

Command: system-administration port enable

Use this procedure to enable a product access port if you did not enable it during the "Adding a Port" procedure, or if the port has been disabled for servicing.

Execute **system-administration corporation add** and **system-administration product add** to define corporations and products before using this procedure.

Product access ports must have been configured through **system-administration port add**.

1. Enter **system-administration port enable**.

   The system will prompt you for the following information:

2. `Port Name >`

   Enter the name assigned previously to the port. Port names are site-dependent and are assigned during the configuration of the system.

   Use the command **system-administration port display** to display the name of each port in the form **/dev/tty** followed by a number.

   System response: `Product port <xx> enabled.`

Procedure: Disabling a Port

Command: system-administration port disable

Use the **system-administration port disable** command to disable the product access port. To disable a port, you must enter the same information in all fields as you entered in **system-administration port enable**.

1. Enter **system-administration port disable**.

   The system will prompt you for the following information:

2. `Port Name >`

   Enter the /dev filename for this port.

   Use the command **system-administration port display** to display the name of each port in the form **/dev/tty** followed by a number.

   System Response: `Product port <xx> disabled.`

SYSTEM MANAGEMENT AGENTS [SYSTEM 85 AND GENERIC 2]

The System 85 R2V3-R2V4 and Generic 2 switches allow you to restrict an agent's access to a group of procs. An agent could be Manager IV, a Maintenance and Administration Access Panel (MAAP), or something similar that communicates with the managed switch product.

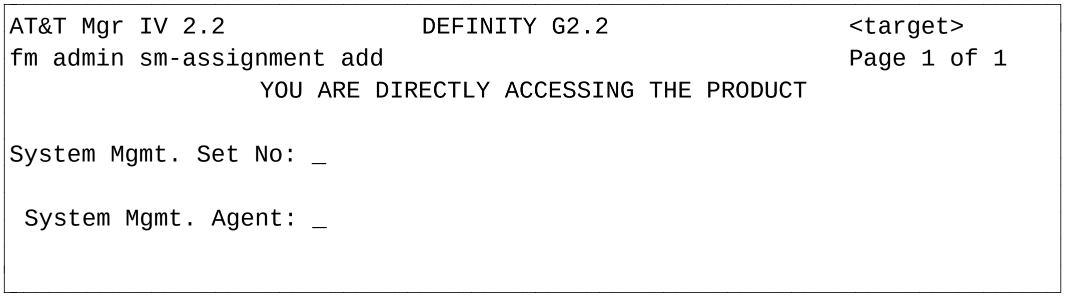
The group of procs is referred to as a set; you can assign up to 50 procs at one time. By restricting agent's access to certain procs, you reduce the possibility of error and help maintain synchronization between Manager IV and the switch. For further information about proc administration, refer to the *AT&T System 85 Feature Translations Service Manual* or the appropriate feature translations manual for your product.

Procedure: Assigning an Agent

Command: fm sm-assignment add or tcm sm-assignment add

1. From the FM or TCM application, enter **admin sm-assignment add**.

   System response:



```
AT&T Mgr IV 2.2             DEFINITY G2.2                 <target>
fm admin sm-assignment add                                Page 1 of 1
                 YOU ARE DIRECTLY ACCESSING THE PRODUCT

System Mgmt. Set No: _

 System Mgmt. Agent: _
```

   Remember to set the system clock prior to execution of the **sm-assignment** command;otherwise, the **sm-history display** command will not reflect the correct date and time for the changes administered.

2. Enter the set number.

   Your system management set number is a value between 0 and 9. (This is the same number found in field 1 of proc 277w1.)

3. Enter the agent at the prompts.

   The encode for the system management agent is a value between 0 and 255. (This is the same number found in field 2 of proc 277w1.)

Enter **admin sm-assignment change** to redefine what system will be used to execute transactions for a group of procs. If you use this command, you are first asked to enter the data in the Set No. field. Then the current agent assigned to a given set is displayed, and you can change only the agent field for the given set number.

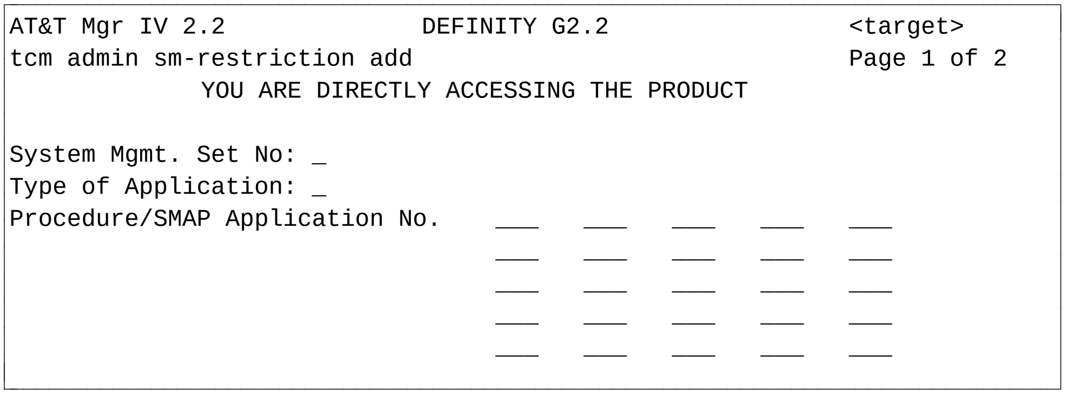
Use **admin sm-assignment remove** to remove the association between a system management agent and a system management set.

Procedure: Assigning System Management Application Procs (SMAP)

Command: fm sm-restriction add or tcm sm-restriction add

Follow this procedure to define the group or set of procs that a system management agent can administer.

1. Enter **admin sm-restriction add** to display the following screen:



```
AT&T Mgr IV 2.2             DEFINITY G2.2                 <target>
tcm admin sm-restriction add                              Page 1 of 2
             YOU ARE DIRECTLY ACCESSING THE PRODUCT

System Mgmt. Set No: _
Type of Application: _
Procedure/SMAP Application No.    ___   ___   ___   ___   ___
                                  ___   ___   ___   ___   ___
                                  ___   ___   ___   ___   ___
                                  ___   ___   ___   ___   ___
                                  ___   ___   ___   ___   ___
```

2. Enter the System Management Set No.. This is a value between 0 and 9. (Same number found in field 1 of proc 277w2.)
3. Enter the type of the restricted application: 0 for proc, 1 for SMAP administration, or 2 for SMAP data collection. This is the same number found in field 2 of proc 277w2.
4. Enter the Procedure/SMAP Application No., which is a value between 0 and 499. This is the same number found in field 3 of proc 277w2.

Use the command **sm-administration restriction change** to change a group of procs that a system management agent can administer. You can change up to seven procs at one time.

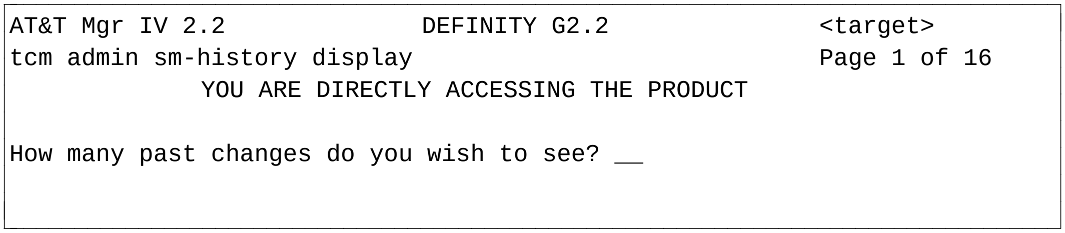
Procedure: Displaying Changes to System Management Restrictions

Command: tcm admin sm-history display or fm admin sm-history display

Use the command **admin sm-history display** to check what changes were made to system management restrictions and agent assignments.

1. Enter **admin sm-history display**.

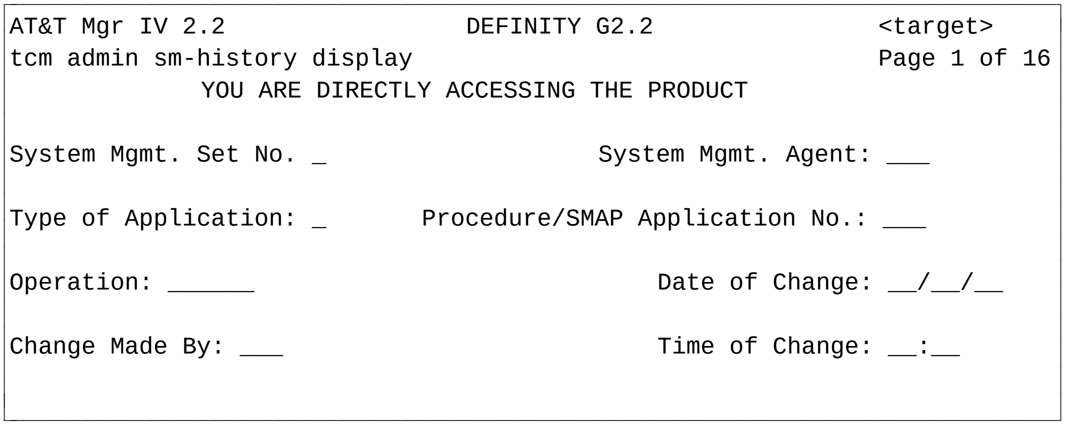
   System response:



```
AT&T Mgr IV 2.2             DEFINITY G2.2               <target>
tcm admin sm-history display                            Page 1 of 16
             YOU ARE DIRECTLY ACCESSING THE PRODUCT

How many past changes do you wish to see? __
```

2. You may search through up to 16 changes. Enter a number indicating how far back you want to look.

   The results screen will look like the following:



```
AT&T Mgr IV 2.2                 DEFINITY G2.2               <target>
tcm admin sm-history display                                Page 1 of 16
             YOU ARE DIRECTLY ACCESSING THE PRODUCT

System Mgmt. Set No. _                   System Mgmt. Agent: ___

Type of Application: _       Procedure/SMAP Application No.: ___

Operation: ______                            Date of Change: __/__/__

Change Made By: ___                          Time of Change: __:__
```

SIZE-SENSITIVE PRICING

Rather than purchasing a full capacity license, your company may have purchased Manager IV with a limited database capacity.

This capacity is fixed at time of installation. Manager IV then performs periodic checks of your system to ensure that you do not reach your capacity without warning. As your system approaches its capacity, a warning message is sent upon all login attempts stating the remaining capacity. The following message is displayed upon each login when you reach 80% of your licensed capacity:

```
The DEFINITY (TM) Manager IV software is currently at 80% of the
___,000 port capacity that your company has licensed to use.  The
software license (and right to use fee) depends on the number of
ports that are to be supported.  (Ports are defined as the total
number of DEFINITY Generic 2, System 85 and DIMENSION FP8 stations
and trunks.)

The software will not support additional ports beyond the licensed
amount.  If additional growth is expected beyond the licensed
capacity, please contact your AT&T Account Executive.

Please allow at least one week for the implementation of a larger
software license.  Additional hardware (and a new configuration) may
be required if the processor was not originally configured to
support the larger capacity.
```

A similar message is also displayed when you reach 90% and 95% of your licensed capacity.

In addition to the displayed message, a warning is issued to the System Administrator Log:

```
D: You have exceeded 80% of your purchased Manager IV capacity. If
you exceed 100%, all Manager IV product access will cease.
A: Purchase a higher capacity. Contact your AT&T Account Executive.
```

Similar messages are sent to the System Administrator Log when you reach 90% and 95% of your purchased capacity.

If the total port capacity falls below 80% of your purchased capacity, the following message is issued to the System Administrator Log:

```
D: You have gone below 80% of your purchased Manager IV capacity.
A: No action necessary.
```

Exceeding the Licensed Capacity

When you exceed 100% capacity, the following message is displayed at every login:

```
The DEFINITY(TM) Manager IV software currently exceeds the port
capacity that your company has licensed to use.  After <mm/dd/yy>,
additional DEFINITY Generic 2, System 85 or DIMENSION FP8 stations
or trunks cannot be added through Manager IV.  (Ports are defined as
the total number of DEFINITY Generic 2, System 85 and DIMENSION FP8
stations and trunks.)

Please order a larger Manager IV software license from your AT&T
Account Executive.

Please allow at least one week for the implementation of a larger
software license.  Additional hardware (and a new configuration) may
be required if the processor was not originally configured to
support the larger capacity.
```

In addition to the displayed message at login, the following warning is sent to the System Administrator Log:

```
D: You have exceeded your purchased Manager IV capacity.  Your grace
period extends until <end date>.  When the grace period has expired,
all Manager IV product access will cease.
A: Purchase a higher capacity.  Contact your AT&T Account Executive.
```

Once you have reached 100% of the capacity allowed by your license, Manager IV will allow a 30-day "grace" period during which you may continue to operate Manager IV without hindrance. After the 30-day grace period has passed, all product connections are blocked.   The following message is displayed:

```
The DEFINITY (TM) Manager IV software currently exceeds the port
capacity that your company has licensed to use. Additional DEFINITY
Generic 2, System 85, or DIMENSION FP8 stations or trunks cannot be
administered through Manager IV.  (Ports are defined as the total
number of administered ports for DEFINITY Generic 2, System 85, and
DIMENSION FP8 stations and trunks.)

Please order a larger Manager IV software license from your AT&T
Account Executive.

Please allow at least one week for the implementation of a larger
software license.  Additional hardware (and a new configuration) may
be required if the processor was not originally configured to
support the larger capacity.
```

All product access capabilities are disabled. **It is imperative that you contact your AT&T representative at this point** since a capacity upgrade must be performed to restore service.

If you have purchased Manager IV at its full capacity, no restrictions are placed against the number of ports allowed. You can enable as many ports as available within your configuration.

6. DATABASE ADMINISTRATION

Manager IV is highly user-interactive and certain "housekeeping," (or backup) operations must be performed to ensure that the system functions properly. Some of the backup procedures are conducted regularly; others are performed as needed.

Recovery procedures are performed in the event of a problem. One of your most important roles as System Administrator is to recover any files, file systems, or databases that are lost due to hardware failure, power down, or user error. Recovery means restoring the system to a state as close as possible to its state prior to corruption.

BACKING UP MANAGER IV DATABASES

Software maintenance conducted regularly by the Manager IV System Administrator includes administering the transaction logs and backing up databases to tape. The following table provides details on these two activities.

Table 6-1. Schedule of Software Maintenance

MAINTENANCE FUNCTION	FREQUENCY	RUNNING MODE	PURPOSE
Backing up the database transaction logs: **log_dump**	Daily, or as logs become full (done manually upon demand). The system console displays a message requesting the **log_dump**.	Multi-user	Copies only the current unmounted log area, which was the previous active log area, containing latest entries. **Notes:** ● If not done: - No further Manager IV transactions can be executed due to lack of available disk slice space. - Inability to fully recover changes made to CORE database.
Backing up the Manager IV database: **full_dump**	Weekly (done manually during off-peak hours).	Any UNIX system state with Manager IV shut down.	Copies the transaction logs and all stored data.

Bradm: Manager IV´s Backup and Recovery Tool

Administration of your host processor is done using the Manager IV backup and recovery administration program, **bradm**.

Log in as **root** to perform all backup and recovery procedures.

The following list describes each of the **bradm** commands that are available to you.

bradm ? Used to display the command list and a short description of each command.

bradm crash Run automatically by **startsm** if Manager IV was booted after an abnormal shutdown. It checks to make sure that databases and log devices are in sync. A warning message is displayed if there is no log device to clean.
Running mode: Manager IV shut down.

bradm full_dump Dumps the logs and CORE database to tape.
Running mode: Manager IV shut down.

bradm help <command> Displays additional instructions on how to use a command.

bradm log_dump Used to back up a full log device onto tape. A warning message is displayed if there is no full log device to back up (one or more log entries qualifies the log as full), or if there is no tape mounted to record the backup.
Running mode: multi-user with Manager IV up.

bradm log_sw Used to switch (swap) log devices on demand. The active log device is switched off and the standby log device is switched on and becomes the active log device. This command is usually run automatically by the system and will not be activated if a standby log device has not been mounted.
Running mode: multi-user with Manager IV up.

bradm menu Used to display the command list and a short description of each command.

bradm log_info Used to display status information about the logs.

Scheduling Backups

The bradm tool provides a means for backing up and restoring the CORE database and journals. In addition to this, you should regularly back up your users’ areas. This can be done by using one of the available UNIX System options. It is recommended that the UNIX command **cpio** be used for ease of backup and recovery. It is also recommended that you back up your application at least once after installation and also after any software updates. Your users’ areas should be backed up at least once a week and kept for four weeks before you recycle your tapes.

Backups require that you mount scratch tapes on the system to capture data for storage off-line. Generally, you should have at least 60 scratch tapes for 3B2 and 6386 WGS backups.

A full backup (**full_dump**) of the entire Manager IV system should be done once a week. This ensures that at least once a week you capture all the changes that have been made to the system.

In addition to weekly full backups, it is recommended that you perform a log dump each day or as necessary to back up the database incremental changes.

Procedure: Backing up the Manager IV Database

Command: # bradm full_dump

The **bradm full_dump** command enables you to save and protect all stored data and back up any existing transaction logs. You must shut down Manager IV before performing this procedure.

1. Log in as **root** and enter your system password.
2. Enter **. /etc/envlist**
3. Shut down Manager IV by typing **stopsm**
4. Enter **bradm full_dump**

   Include the underscore between the two words.

   — **Bradm** checks the log devices. If the journal is empty, you will receive the message:

   ```
   No log device to dump at this time
   ```

5. The system prompts you for the name of the tape drive and device you are using. Type in the responses at the prompt.
6. When you have mounted the appropriate tape (scratch or recycled), enter **go**.

   The **full_dump** procedure is easy to follow. The system prompts you for responses as you proceed. The output that follows is an example of what you can expect when you perform this procedure. Parts of the output may differ depending on what processor you use:

   ```
   Creating a LOG tape ...

   Skipping label check
   NEW fsname = LOG_1, NEW volname = 1 -- DEL if wrong !!

   Rel 1, 969 feet, 6250 BPI
   You will need 1 reels.
       The same size and density is expected for all reels)
   From: /dev/rlog1, to: /dev/rmt/c1t2d0s0? (DEL if wrong)

   Writing REEL 1 of 1, VOL = 1
       END: 48825 blocks.
   Volcopy tape created successfully

   Unmount the tape from the drive and affix the following label:

       BACKUP   :   LOG
       LOG #    :   1
       DATE     :   <MM/DD/YY>
       TIME     :   <HH/MM/SS>
       MACHINE  :   <machine_name>

       Type "go" to continue.
       [go] =>
   Created tape LOG successfully
   ```

7. The procedure continues for log tapes and CORE tapes until you receive the following message:

```
CORE BACKUP FINISHED SUCCESSFULLY

FULL DUMP PROCEDURE COMPLETED

Manager IV can now be started.
```

8. To restart Manager IV, enter **startsm**

You can also use the UNIX system utility **sysadm** to back up the Manager IV application filesystem and any other resident application filesystems.

Performing a Tape Run

Once you have done a full backup, it is recommended that you also do a **tape run** from TCM or FM **admin** at the switch. This will preserve the information at the switch, allowing you to synchronize the data in the switch and the Manager IV database should the two become unsynchronized at any time. Do this in addition to the regularly scheduled tape run, which you set with **admin daily-tape-run schedule**. Refer to Chapter 3, "Backing up PBX Downloads," for details on **admin daily-tape-run schedule**.

Cron Service Procedures

Cron is a UNIX operating system utility that performs scheduled tasks automatically at specified times. These include checking the status of the transaction logs and switching the log devices. If cron is not operating, these tasks must be completed manually.

The results of all cron activity are mailed to appropriate users such as smsa, smgr, uucp, adm, and root. The Manager IV System Administrator should monitor all mail to these users and make note of any problems requiring administrative action.

The following table identifies the database maintenance service procedures performed automatically by cron. Procedures for manual execution follow the table.

Table 6-2. Cron Service Procedures

SERVICE TASK	FREQUENCY	RUNNING MODE	PURPOSE
Check status of transaction log devices.	Every 30 minutes (done automatically during workday).	● normally: cron-controlled ● manually: multi-user	● Determines if only the active log area is available. ● Generates **log_dump** request at system front console. **Notes:** ● If cron fails to run, both log areas become full. No Manager IV transactions can be executed due to lack of available disk slice space. ● An unusually high number of log entries can fill active log area before **ck_log** does its inspection of remaining disk slice space.
Switch log devices.	Daily (done automatically during off-peak hours).	● normally: cron-controlled ● manually: multi-user	Switches log areas on disk. **Note:** If Manager IV is down when cron is scheduled to run **log_sw**, the transaction log areas are not switched.

Procedure: Switching Log Devices

Command: # bradm log_sw

The **log_sw** command is automatically performed every day by cron during off-peak hours (or as needed by database software). If the processor is down when cron is scheduled to run **log_sw**, this command will not be executed. It can be performed manually in multi-user mode.

Use the command **log_sw** to change the active log area to standby status for copying to tape and to activate the standby log area for recording.

Once you enter the command **log_sw**, you will receive a message that reads "log_sw completed successfully." The active and standby log areas have been switched and the standby log area should be backed up to tape as soon as possible.

It is possible to not fill the active log area during the course of a workday. This would occur when very few changes are made to the database. Depending upon the number of changes, a single active log area may not become filled for several days, weeks, or months. Thus, a single, unfilled log area may contain changes entered over a long time period. If an unexpected disk loss occurs, perhaps because of a head crash, all of those entries will be lost. Because it is more difficult to remember all of the changes entered over several weeks than it is to remember a single day's entries, the log areas are forcibly switched every day. This sets aside the partially filled log area for later backup and directs all new journal entries to a fresh log area.

Procedure: Backing up the Database Transaction Logs

Command: # bradm log_dump

The **log_dump** procedure allows you to copy the database transaction logs to tape if the logs become full.

All changes to the CORE database are recorded in the transaction log as journal entries. Two separate journal areas operate alternately. One area serves as the active device to record new changes, while the other area remains in the standby mode. When the active log (journal area) becomes full, the logs are switched and the standby area becomes the new active device, while the full journal area is placed in the "full" mode. The **log_dump** backs up the contents of the filled device. Logs are sequentially numbered for identification. After the log area is backed up, the log area is "scratched" (reset to 0) so that it can become the standby area.

A **log_dump** must be performed in multi-user mode.

1. Log in at the system console as **root**
2. Enter **. etc/envlist**
3. Enter **bradm log_dump**
4. The system prompts you for the name of the tape drive and device name you are using. Type in the responses at the prompt.

5. When you have mounted the appropriate tape (scratch or recycled), enter:

   go

   The **log_dump** procedure is easy to follow. The system prompts you for responses as you proceed. The output that follows is an example of what you can expect when you perform this procedure. Parts of the output may differ depending on which processor you use:

```
Creating a LOG tape ...

Skipping label check
NEW fsname = LOG_1, NEW volname = 3 -- DEL if wrong !!

Rel 3, 969 feet, 6250 BPI
You will need 1 reels.
    The same size and density is expected for all reels)
From: /dev/rlog1, to: /dev/rmt/c1t2d0s0? (DEL if wrong)

Writing REEL 1 of 1, VOL = 3
    END: 48825 blocks.
Volcopy tape created successfully

Unmount the tape from the drive and affix the following label:

    BACKUP   :   LOG
    LOG #    :   3
    DATE     :   <MM/DD/YY>
    TIME     :   <HH/MM/SS>
    MACHINE  :   <machine_name>

    Type "go" to continue.
    [go] =>
Created tape LOG successfully
```

Procedure: Displaying Database Journaling Status

Command: # bradm log_info

This procedure reports on the status of the database journaling process.

1. Enter **bradm log_info [-s] [-l [log1][log2]] -c**

   The options are defined as follows:

   — **-s** prints current mounted log device information.

   — **-l [log1]** prints the long listing of log 1.

   — **-c** prints status information.

RECOVERING MANAGER IV DATABASES

The Manager IV CORE database and log devices are partitioned throughout the processor disks.

Journaling, or the storage of system information on backup tapes, is a critical part of the recovery process. If you fail to do backups -- full backups (**full_dump**) weekly and incremental backups (**log_dump**) as necessary, your system cannot be restored adequately.

In addition to the information on the backup tapes you make, Manager IV provides a method for restoring information about completed transactions in the transaction log. As a user successfully enters data for a transaction, the information that changes the Manager IV database is stored in the active transaction log. To add additional insurance that this information is protected against loss, the transaction log is located on a disk separate from the disk where the Manager IV CORE database resides. Thus, if the CORE database (which stores switch information) is corrupted, the transaction log is protected.

When the system is rebooted after a crash, the information in the log is automatically dumped to tape by the **bradm crash** recovery procedure. Then, during the boot procedure, **bradm crash** compares the information in the log to the information in the Manager IV database. Any completed transactions logged in the transaction log that do not appear in the Manager IV database are added to the database, thus adjusting any discrepancy between what is in the Manager IV database and what has been sent (or scheduled to be sent) to the switch. Any transactions that are not complete in the transaction log are erased. These transactions must be entered again.

Using the Bradm Command

As with backups, you will be using the Manager IV Backup and Recovery tool, **bradm**, to restore file systems in the event of a system crash. The **bradm** commands that are used for recovery processes are **bradm crash, bradm help, bradm menu, bradm recovery,** and **bradm log_info**. See the section "Bradm, Manager IV's Backup and Recovery Tool" in this chapter for more information on the **bradm** tool.

Use the **bradm recovery** command to restore all Manager IV database files from available backup tapes. When recovering the CORE database, you must begin with the latest full backup tapes, and supplement that information with information from additional log tapes. In all cases, follow the system prompts. You will be asked to mount backup tapes until all selected file systems or databases have been recovered.

Procedure: Restoring The CORE Database

Command: # bradm recovery

Major recovery of the Manager IV database is done through the **bradm recovery** command. Bradm will prompt you through the recovery process. If you need help with this procedure, contact the Technical Service Center (TSC).

Shut down the system to single-user mode. Refer to the shutdown procedure for your Manager IV host processor. When you receive the single-user prompt, follow these steps.

1. Enter the command **mount** to verify that the *root* file system is mounted.

   CAUTION: If *root* is not mounted, do not continue.

2. Enter **. /etc/envlist**

3. Enter **bradm recovery**.

   The following message appears:

   ```
   START RECOVERY PROCEDURE

   Checking the LOG devices ...
   ```

4. The system prompts you for the name of the tape drive and device name you are using. Type in the responses at the prompt.

5. When you have mounted the appropriate tape (scratch, or recycled), enter **go**

   The following output is an example of what you can expect when you perform this procedure:

   ```
   Creating a coredb00 tape ...

   Skipping label check
   NEW fsname = CORE0, NEW volname = 1 -- DEL if wrong !!

   Reel 1, 969 feet, 6250 BPI
   You will need 1 reels.
   (    The same size and density is expected for all reels)
   From: /dev/coredb00, to: /dev/rmt/c1t2d0s0? (DEL if wrong)

   Writing REEL 1 of 1, VOL = 1
       END: 92480 blocks.
   Volcopy tape created successfully

   Unmount the tape from the drive and affix the following label:

       BACKUP   :   V5DB01
       LOG #    :   1
       DATE     :   <MM/DD/YY>
       TIME     :   <HH/MM/SS>
       MACHINE  :   <machine_name>

       Type "go" to continue.
       [go] => go
   Created tape V4db0 successfully

   Do you want to restore only the log(s) or the core database too
    [log|core] =>
   ```

6. Enter **core** at this prompt to restore the CORE database.

   The procedure continues similarly as it recovers the CORE database. When you receive the message `Do you wish to restore any LOG tape(s),` type **y** to start the update of the CORE database. Mount the tape that you want to recover.

7. Continue until there are no more log tapes to recover. You receive this message:

   ```
   CORE RECOVERY COMPLETED SUCCESSFULLY
   ```

8. Manager IV can now be started.

   To restart Manager IV, enter **startsm**

7. TROUBLESHOOTING AND USING THE LOGS

It is part of your job as Manager IV System Administrator to perform maintenance work that will prevent and even solve some of the trouble conditions that can occur during daily Manager IV operations. Report any error activity that you cannot handle to the AT&T Technical Service Center (TSC) for diagnosis and solution: 1-800-548-8861.

Check the logs regularly to become familiar with the information they contain. This will give you enough information to know the probable causes of any given problem. For instance, if some users do not clean up their service requests, a monitor of the logs will show this, and resulting problems can be forestalled.

The following logs are available:

- Dispatcher Log, which contains information about scheduled tasks.
- Information Log, which contains general information about the system's current configuration and status.
- Product Connection Log, which contains information about all product connections attempted.
- Service Request Log, which contains an entry for each executed service request, including status and history. (See Chapter 3 for information on this log.)
- Transaction Log, which shows the transactions executed by specific users. (See Chapter 3 for information on this log.)

Two additional logs store only error messages:

- System Administrator's Log, which contains information about errors or malfunctions that are due to user problems.
- System Error Log, which reports failed processes.

The Data Communications Log is a program that provides a summary of other logs. When you run the **dclog** report (explained later in this chapter), it gives you a summary of the other logs with entries listed chronologically.

UNDERSTANDING MANAGER IV ERROR CONDITIONS

Within Manager IV, there are four possible sources of error messages:

- Manager IV users
- Manager IV application software
- UNIX operating system software
- Host processor and peripheral hardware (for example, ports).

When any of these four elements of Manager IV is unable to complete an assigned task, that particular source issues a message indicating the nature of the problem. The message is displayed immediately or stored in a file for later retrieval. The same message may be repeated periodically if its source cannot detect that the problem has been corrected.

User-related errors are the ones you will encounter most frequently. Messages for these are caused by the processor's refusal to recognize improperly entered data. Manager IV rejects user-entry errors as they occur. The application user receives a message describing the error or Manager IV's inability to process the entered data. The application user must resolve the error by entering the data correctly.

User-related errors also occur when data is entered correctly (that is, the value entered is an acceptable value), but its logic is wrong. For example, if a TCM application user enters Class Of Service (COS) data correctly, Manager IV will not reject the entry. But if the wrong features and restrictions have been entered, an error may occur when the user tries to assign features to the voice terminal with that class of service. For information about correcting errors that result from entering incorrect data, refer to the appropriate Manager IV application operations guide.

Application Software Errors

Manager IV application software is capable of creating its own messages independent of the UNIX operating system. Manager IV application software error messages appear in the Manager IV System Administrator's Log (*sadm*) report, which contains two types of error messages: Manager IV administrative errors and Manager IV application software errors.

UNIX System Errors

All UNIX system error messages that affect Manager IV operation are written to a Manager IV system error file, the system error log *(sys)*. In each case, the affected Manager IV process is programmed either to ignore the UNIX system message and continue, or to respond to the UNIX system message by creating a Manager IV error message before terminating.

Hardware Errors

Hardware error messages specify either a mechanical or electronic failure and are directed toward hardware operations and maintenance personnel. Hardware failures may prevent the UNIX operating system from executing shell commands.

Severity Levels

An error's level of impact is determined by the number of system resources it affects. Since some errors are more significant than others, errors are usually assigned severity levels. Errors resulting from improperly entered data (user-related errors) are caught immediately by the application software and so are not assigned any severity level.

Manager IV system software errors fall within three severity categories: high, medium, and low. The categories are determined by the number of processes affected and by the amount of time it takes to fix a problem.

For example, a hardware error that affects all system resources must be fixed immediately, thereby rating a high severity level. A medium severity level error requires action within three to four hours after its receipt. At the low priority level are advance warnings of potential errors such as file space limitations. Low level errors require action within 24 hours. You can avoid these errors if you act as soon as you receive a warning.

If you can correct a problem without assistance, do so. If you are unable to correct the problem, contact the AT&T TSC at 1-800-548-8861. Describe the symptoms and the exact error messages received to the services center technician.

Table 7-1 illustrates how error messages are directed within Manager IV by indicating both the recipient of each type of message and the reason it was sent.

Table 7-1. Error Message Paths and Purposes

MESSAGE SOURCE:	SENDS MESSAGES TO:	TO CORRECT:
Manager IV application users	Manager IV System Administrator	Abnormal system responses and performance degradation
Manager IV System Administrator	Processor Operations	Hardware-related Manager IV errors and to perform routine maintenance
	National Customer Service Center	Software abnormalities
Manager IV application software	Manager IV user	Improper entries
	Manager IV System Administrator	Software performance through resource allocation
	Services center	Software abnormalities
UNIX Operating System Software	Manager IV System Administrator	Minor operating system errors
	Services center	Major operating system errors
Host processor and peripheral hardware	Processor Operations	Minor system failures and to perform routine maintenance
	Services center	Major system failures

Note:: The managed switch also can generate errors in response to operation abnormalities. Errors that originate at a source within the managed switch are not addressed in this discussion. For further information about troubleshooting the causes of switch errors, refer to the appropriate hardware documentation.

Error Message Distribution

Knowing which logs to consult will help you determine the source of the error. For example, if an error occurs in the Manager IV system hardware, logged-on Manager IV application users receive messages indicating a failure to execute requests or to download changes as scheduled. Descriptive error messages are designed to help Manager IV application users catch their own mistakes. When the user re-enters the data correctly, the error messages do not appear. If the hardware has failed, all user attempts to clear the problem through repeated entry will be ineffective. The same error messages will reappear with each new entry, and you will need more information to define the source of the problem.

The following table guides your troubleshooting efforts by directing you to the logs that contain pertinent messages. Consult each of the listed logs for details about the system error.

Table 7-2. Error Message Distribution

	A TROUBLESHOOTING-ORIENTED MESSAGE IS SENT TO:					
IF THE ERROR OCCURS IN:	Application User Terminal	UNIX System Error Log	System Administrator Log	Product Connection Log	Dispatcher Log	Information Log
Manager IV Application User Entries	**X**					
Manager IV Application Software			**X**	**X**	**X**	**X**
UNIX Operating System Software		**X**		**X**		
Manager IV Host Processor & Peripheral Hardware		**X**		**X**		

ACCESSING MANAGER IV LOGS

All logs are kept in a directory called $LOG. You can **cd** to the **$LOG** directory and list its contents if necessary to see what logs are available. The following abbreviations are used for the different system logs:

con	Product Connection Log
info	Information Log
dlog	Dispatcher Log
sadm	System Administrator’s Log
srlog	Service Request Log
sys	System Error Log
trxlog	Transaction Log

To view most of the logs,identify the log and the date for which you would like information, and then cat it to your screen.

cat $LOG/lognameDATE

For example, to read the information log (*info*) for October 12 enter **cat $LOG/info1012**

All information stored in that log for that date will be displayed to your screen. In addition, the command **dclog <MMDD>** will extract service request and communications-related data from all logs and reformat and display it.

The product connection log is retrieved by using the **logc** command (discussed later in this chapter) from the UNIX shell. See Chapter 3 for information about enabling the transaction log facility.

MONITORING THE ERROR LOGS

Monitor the following logs daily or hourly, depending on the volume:

- System Administrator Log (sadmlog)
- Information Log (infolog)
- Service request Log (srlog).

Note:: The Data Communications Log (dclog) program should be run weekly, unless there is a problem, in which case you should check it first.

A hard copy of the day's output at the Manager IV system console contains all the day's log messages. An important part of your responsibility is to recognize messages that signal potential problems and to act promptly to delay or avert the disruption of Manager IV operation.

Advance warning of every abnormality is not always possible, however. Your increasing familiarity with the logs will enable you to distinguish messages that indicate problems from those that do not.

To preserve the error log messages, Manager IV accumulates new entries on daily backup tapes taken from the system. Normally, they are saved for two weeks unless you authorize a different period. When the backup tapes are again used to record new entries after the off-line cycle, the old entries are erased. There is no way to study the old entries unless you save the daily console printout for review.

Defining the Problem

Understanding the error messages in the logs can help you locate problems that occur only intermittently. The difficulty is not in finding a solution to the problem but rather in duplicating the problem repeatedly to study it and discover why it happens. To duplicate the problem, you must be able either to recreate the unique combination of processor activities that existed at the precise moment the error occurred, or produce a snapshot of the activities of the system such as the Manager IV error logs provide. Only the failing processes need to be studied since it is a unique combination of failing processes that causes an intermittent problem.

Procedure: Troubleshooting an Intermittent Problem

The following procedure describes how the log messages can be a valuable resource when you are troubleshooting an intermittent problem.

1. Obtain all surviving hard copies of the daily error log reports that record other instances of the same intermittent problem.
2. Locate in these logs the messages that appeared just before the failure.
3. Compare the sequence of those messages in each of the logs. If the same sequence of messages occurs in more than one log, you have discovered the process failure pattern of the intermittent problem.
4. Find the first error message in the pattern. This is the leading failure. The source of the leading failure is likely to be the source of the intermittent problem.

Manager IV Log Message Formats

In the pages that follow, you will see the different types of log messages that Manager IV produces. Each description explains the contents of the log message, how to access the desired log file for a particular date, and how to interpret the messages.

System Error Log

The System Error Log reports in detail about system process failures. This log is particularly important to your AT&T service representative, who refers to a message directory to interpret the numbers in the system error log. System Error Log messages appear in the file **$LOG/sys<date>**. You can **cd** to the $LOG directory and enter **cat sys1109** to display all entries directed to the log on November 9.

Figure 7-1 gives a sample of output from the System Error Log. Definitions of the fields follow.

```
09:35:11 jvg:h:-1:2:updb:22240:scatch  Wrong security code (9992244)
```

SRLOG REFERENCE	**DESCRIPTION**
`09:35:11`	Time of day the transaction is executed (A 24-hour clock is used).
`jvg`	Login of the user who ran the transaction
`h`	Severity level (high, medium, or low)
`-1`	Manager IV error number
`2`	UNIX System error number
`updb`	Process name
`22240`	Process identification number
`scatch`	Subroutine name
`Wrong security code (9992244)`	Message describing the error

Figure 7-1. System Error Log Output

System Administrator Log

The System Administrator Log contains information about errors or malfunctions due to user problems. Figure 7-2 gives a sample of output from the System Administrator Log. Definitions of the fields follow.

```
---user = lak : pgm = scm : sev = high:smerr = 193: Fri Nov 9 13:05:29 1989
D: Can not add record frl.
A: Try to load manually.
```

SADMLOG REFERENCE	DESCRIPTION
`user=lak`	Login of the user or process that ran the transaction that generated this message
`pgm=scm`	Name of the Manager IV application software program in which the error was noted
`sev=high`	Severity level (High, medium, or low)
`smerr=193`	Manager IV Error number
`Fri Nov 9 13:05:29 1989`	Day, date, and time the message was generated
`D: Can not add record frl`	Message describing problem
`A: Try to load manually`	Action that must be taken to resolve the error

Figure 7-2. System Administrator Log Output

Viewing the System Administrator Log

System Administrator Log messages appear in the file **$LOG/sadm<date>.** Enter **cat sadm1109** to display all entries directed to the log on November 9.

Product Connection Log

The Product Connection Log contains information about the attempts Manager IV has made to connect to a product. Log entries are made for all product connections, successful and unsuccessful. It is particularly useful if you are experiencing problems connecting to products and you are trying to isolate the problem. Log data is stored for one calendar month. However, if the connection failed because of an abnormal condition such as a UNIX system call failure, an error message appears in the System Error Log. Use the information contained in both logs to assist troubleshooting efforts. Report any error activity that you cannot handle to the AT&T TSC at 1-800-548-8861 for diagnosis and solution.

Product Connection Log messages appear in the file $LOG/con<month>-<date> where the range for "month" is 1-12 and the range for date is 1-31. For example, messages for December 17 appear in the directory defined by $LOG in the file con12-17.

You can select certain options and parameters to be displayed. If you do not specify options the full log will be displayed.

Procedure: Displaying the Product Connection Log

UNIX Command: # logc <option>=<parameter>

1. At the UNIX shell prompt, enter the command **logc <option>=<parameter>**.

   Possible display options and their associated parameters are:

   port=<port name> to specify the outgoing data port requested

   product=<ID> to specify the product ID

   user=<login ID> to specify the user login ID requesting the connection

   start=<date/time> to specify the starting date and time of the connection

   duration=<minutes> to specify the duration (in minutes) of the connection

   message=<err mess> to enter a specific message

The fields of information in a product connection log are defined in the following example. All fields appear in every message.

```
port      pbxport   product    user      start            duration      attempt

/dev/tty14  0       9992255    fpm   08/25/89 15:58:28      00:23          1
Message: successful connection

/dev/tty14  0       949-5009   rap   08/25/89 16:04:42      00:08          2
Message: Echo not received from modem 2224
```

PRODUCT CONNECTION LOG REFERENCE	**DESCRIPTION**
`/dev/tty14`	Identifies the port through which the connection was attempted
`0`	Identifies the PBX port through which the connection was attempted
`9992255`	Product ID (target) number of the switch. (This is not necessarily the telephone number of the switch.)
`fpm`	User's login ID or a special ID for scheduled tasks
`08/25/89`	Date of Manager IV's attempt to connect to the switch
`15:58:28`	Time (in 24-hour notation) at which the connection attempt was initiated
`00:23`	Duration of port connection (in minutes and seconds)
`1`	Number of times read or write operations for this connection had to be retried due to errors
`Message: successful connection`	Short message describing the nature of the connection

Figure 7-3. Product Connection Log Output

Should you receive a significant number of port connection failures, you may want to test the port's access capabilities. Refer to *Manager IV Installation, Initialization, and Maintenance* for information on testing ports.

Dispatcher Log

The Dispatcher Log contains information about scheduled tasks. Check this log for possible entries when Manager IV users report problems executing service requests. For example, if a change entered on August 10 was scheduled to download to the switch on September 3, Manager IV will send the results of the service request to the user in September 3's mail. If these results are never received or are received before September 3, the service request may not have downloaded according to schedule. The dispatcher process or scheduler may be at fault. If so, it will be readily apparent from the list of dispatcher transactions that the service request has been improperly administered either because it has been omitted from the list or because it has been executed at the improper time.

Dispatcher Log Messages appear in the file $LOG/dispDATE. For example, messages for September 3 appear in the directory defined by $LOG in the file disp0903.

The following figure shows an example of a Dispatcher Log entry with the fields of information defined below.

```
sched(13722) 14:53:39 - Started. Shell Request, ldn testinit, taskno 14513.6
```

DISPATCHER LOG REFERENCE	**DESCRIPTION**
`sched(13722)`	Process name (process ID)
`14:53:39`	Time of day when dispatcher function was initiated. A 24-hour clock is used. Tasks are scheduled for execution at a user-specified time. If the user specifies "offhours" as the scheduled time, the dispatcher will schedule the task to run after 5:00 p.m. on the specified day.
`Started`	Message
`Shell Request`	Task type
`ldn testinit`	Target
`taskno 14513.6`	Unique target task number (up to 13 characters) identifying the task

Figure 7-4. Dispatcher Log Output

Information Log

The Information Log contains general information about the system’s current configuration and status.

Information Log messages appear in the file $LOG/infoDATE. For example, messages for July 27th appear in the directory defined by $LOG in the file info0727.

An example of Information Log output follows:

```
00:30:39 smgr:l:91:2:ueutil:4161:scatch Process received normal system shutdown signal(15)
```

INFOLOG REFERENCE	DESCRIPTION
`00:30:39`	Time of day transaction was executed. A 24-hour clock is used.
`smgr`	User’s login ID
`l`	Severity level (high, medium, or low)
`91`	Manager IV error number
`2`	UNIX System error number
`ueutil`	Process name
`4161`	Process identification
`scatch`	Subroutine name
`Process received normal system shutdown signal (15)`	Brief description of the activity. Not every Manager IV process is recorded in this log. For example, the normal creation and deletion of clone daemons will not appear. Only the activities of major Manager IV system software processes such as the extractor, controller, and scheduler are recorded.

Figure 7-5. Information Log Output

Data Communication Log Report (dclog)

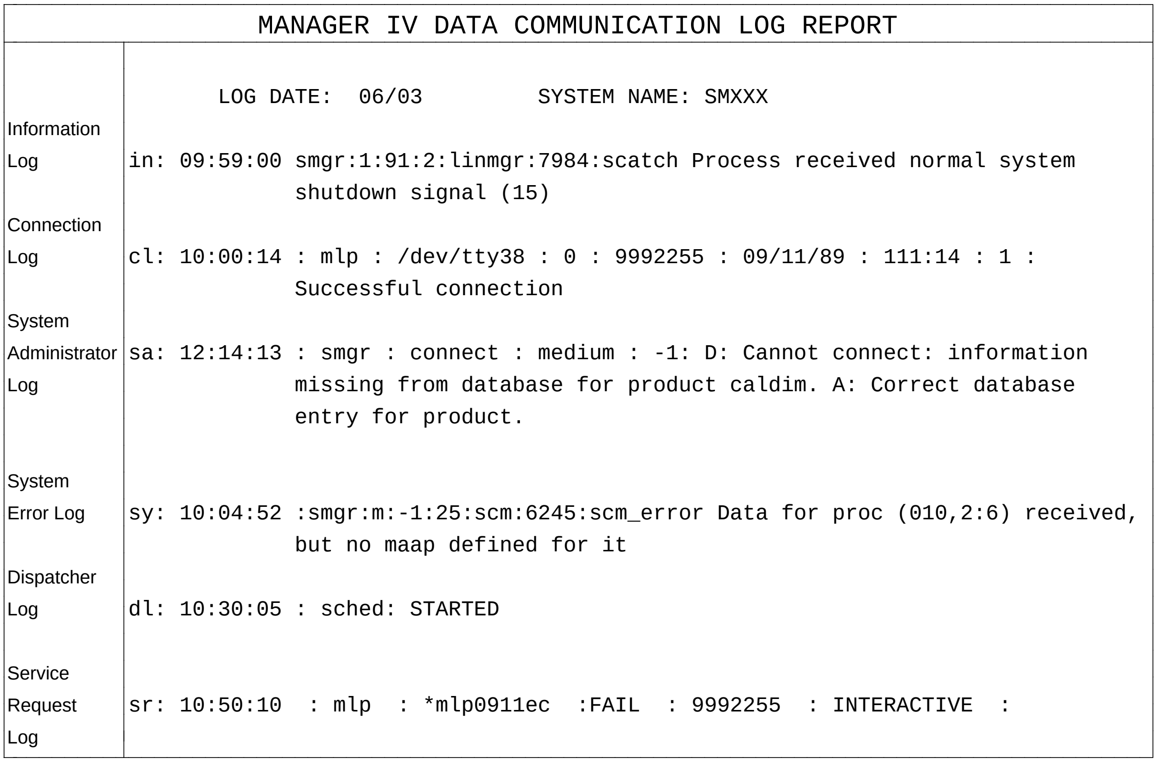
Information describing the communications problems is spread among many log files. The Data Communications Log Report (dclog) is a tool that combines all product access logged messages into one organized, easy-to-read report. Dclog makes it easier to identify and diagnose data communications problems. The Data Communication Log Report will only deal with data communications problems for System 85, Generic 2, and DIMENSION product administration.

Dclog is run from the UNIX shell. The report can be stored as a file, displayed on the screen, or printed.

This log compiles and organizes information from the following:

- System Error Log
- System Administrator Log
- Service Request Log
- Information Log
- Product Connection Log
- Dispatcher Log

All entries in the report are put into a standard format for easier readability. An identifier precedes each entry. Figure 7-6 illustrates the dclog report output; captions identifying the different report references appear in the left column.



```
                    MANAGER IV DATA COMMUNICATION LOG REPORT


                    LOG DATE:  06/03         SYSTEM NAME: SMXXX
Information
Log            in: 09:59:00 smgr:1:91:2:linmgr:7984:scatch Process received normal system
                            shutdown signal (15)
Connection
Log            cl: 10:00:14 : mlp : /dev/tty38 : 0 : 9992255 : 09/11/89 : 111:14 : 1 :
                            Successful connection
System
Administrator  sa: 12:14:13 : smgr : connect : medium : -1: D: Cannot connect: information
Log                         missing from database for product caldim. A: Correct database
                            entry for product.


System
Error Log      sy: 10:04:52 :smgr:m:-1:25:scm:6245:scm_error Data for proc (010,2:6) received,
                            but no maap defined for it
Dispatcher
Log            dl: 10:30:05 : sched: STARTED

Service
Request        sr: 10:50:10  : mlp  : *mlp0911ec  :FAIL  : 9992255  : INTERACTIVE  :
Log
```

Figure 7-6. Dclog Report Output

Data Communication Log Format

Figure 7-7 provides a key to the information in each dclog entry shown above in figure 7-6.

```
     CL : time : user : port : pbx port : product : date
              : connect duration in MM:SS : connect attempt number
     SY & IN : time , user : severity : Manager IV error number
            : unix error number : process name : process id : subroutine name
     SA : time : user : process name : severity : Manager IV error number
     DL : time : process name
     SR : time : user : sr number : status : product : mode
```

Figure 7-7: Dclog Report Key

Procedure: Producing dclog Reports

UNIX Command: # dclog <MMDD>

To produce the dclog report,

1. Enter **dclog <MMDD>**

   where MM is the month and DD is the day.

2. The report is displayed on the terminal. To write the report into a file, redirect the output by entering the following:
   dclog <MMDD> > <filename>

   where *filename* is the name you give this file.

Interpreting the Results

The report sorts messages chronologically. You can diagnose problems by checking the messages from different logs that relate to any failure. Check the messages that appeared just before the failure and compare the sequence of those messages in each log. If the same sequence of messages occurs in more than one log, you have probably discovered the problem. Find the first error message in the pattern to identify the leading failure. The source of the leading failure is likely to be the source of the intermittent problem.

Use the information that follows to help you interpret the information from the logs as you see it in dclog.

Procedure: Displaying Error Messages

Command: system-administration errors display

Follow this procedure to display error descriptions for error numbers encountered in any transaction using the command **errors display**.

1. Enter **system-administration errors display**.

   The prompt `ERROR NUMBER:>` will appear.

2. Enter the error number to be described.

   The application user error message associated with the error number you enter is displayed.

SERVICE AND MAINTENANCE SUPPORT

As System Administrator, it is your job to execute Manager IV service procedures in an attempt to resolve all Manager IV abnormalities at the user level. If you are unable to clear the abnormal condition, you should contact the TSC at 1-800-548-8861. A service technician will work on-site or at a remote console to diagnose the problem.

You must record all information related to a Manager IV abnormality (for example, the command path in which the user encountered difficulty) and report that information to AT&T when requesting assistance. You must also maintain a log of completed Manager IV file backups and recoveries. These handwritten journals should be available for reference if the Manager IV host processor is down for service.

Silent Knight Auto Dialer

One way error conditions reach the attention of the TSC is via the error message reporting mechanism, the Silent Knight Auto Dialer. The Silent Knight is optional hardware, attached to your Manager IV system, that dials the TSC to report alarms.

The Silent Knight responds in the following ways to three different types of error conditions:

- It reports pre-alarm messages that warn of impending alarms. Copies of the pre-alarm messages are sent to the System Administrator's Log. Some pre-alarm messages notify you of problems that you can correct yourself, such as too many entries scheduled for the same time. If you are not available to respond to the pre-alarm message, the services center will directly access the processor, notify you of the problem, and correct it, assuming that your site has the type of coverage that provides this service.
- It reports alarms generated when there is a hardware problem or when system activity causes the core database to run low on space. Excessive system load causes severe performance problems. Alarm messages are sent every 30 minutes to the service support center. When an alarm is received, the service technician logs into the system and examines all the errors that have been logged. The records of these error messages remain in the various system log files. The amount of time it takes the service technician to respond depends upon the type of coverage your site carries. The service technician will work at a remote console, or if necessary, at your site to resolve the problem.
- If a message is not pre-alarm or alarm status, the error is written to the System Administrator's Log file and not reported to the TSC. You are expected to resolve this problem. If the error disables Manager IV operations, it will become an alarm and be reported by the Silent Knight Auto Dialer.

Calling the Help Line

If you do not have the Silent Knight Auto Dialer, you must keep careful watch on the error logs and respond to problems as they arise. If an error condition threatens to disrupt system activity or is beyond your experience, it is your responsibility to call the TSC for help.

You can also call the following toll-free number if you need assistance with *any* problem that is not reported as an alarm:

1-800-548-8861

This is a help line provided for Manager IV customers. If the person answering the phone cannot answer your question, he or she will report it to a higher level.

Reporting Trouble

When you call the help line with a question or problem, a Tier 1 technician will take your call and try to answer your question. The Tier 1 technician also determines what warranty or maintenance agreement exists on your Manager IV system and advises you of any applicable charges. (See "Warranty Coverage," following.)

If the problem requires access to the Manager IV system, the Tier 1 technician escalates the problem to Tier 3, an engineer at the TSC (Technical Service Center). Any problems that cannot be solved at that level are escalated still further, to Tier 4 field support.

WARRANTY COVERAGE

All Manager IV software includes a fixed-term warranty. This guarantees that an experienced software maintenance technician will provide standard maintenance services within the terms and conditions detailed under the standard warranty service discussed below. When you contact the services center about a problem, the services center representative will have immediate access to a description of the service agreement you have with AT&T.

Manager IV software is warrantied for 90 days from the date of initialization. The standard warranty provides "business day" service coverage of the product. Any costs to resynchronize the Manager IV database with the switch database will be borne by the customer. (See "Maintenance Option 1," below.)

Manager IV operating deficiencies that are determined to be a result of unauthorized changes made by the customer to the Manager IV software are excluded from coverage agreements specified in the standard Manager IV warranty. All work performed by AT&T services personnel to isolate or repair such troubles will be billed to the customer on a time and materials basis.

Problems caused by malfunctions of the host processor or its operating system should be handled according to existing contractual agreements for those products.

Upon expiration of your standard Manager IV warranty, you may contract for continued coverage under one of several maintenance service options. Post-warranty coverage information is contained in the mechanized trouble report managed by the Business Maintenance Information System (BMIS) at AT&T.

Maintenance Option 1. Business Day Service

Under the terms of "business day" service, AT&T responds within four coverage period hours of the trouble report for failures that materially affect the operation of the products or the system (major system failures) as determined by AT&T. AT&T responds within 24 hours of the trouble report for minor failures as determined by AT&T, provided that AT&T shall perform such work only during the hours of 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding any standard AT&T holidays.

Maintenance Option 2. Around-The-Clock Service

Under the terms of "around-the-clock" service, AT&T responds within four coverage period hours of the trouble report for failures that materially affect the operation of the products or the system (major system failures) as determined by AT&T. AT&T responds within 24 hours of the trouble report for minor failures as determined by AT&T, and this coverage is provided for a 7-day, 24-hour-per-day period.

Maintenance Option 3. Dedicated Service

Under the terms of "dedicated" service, AT&T personnel are dedicated to a specified customer location to perform maintenance, moves, changes, and rearrangements of AT&T-provided equipment at the customer’s discretion. Depending upon the terms of this agreement, there is (optionally) one-, two-, or three-shift coverage for (optionally) five, six, or seven days per week.

Maintenance Option 4. Per-Occurrence Service

Under the terms of "per-occurrence service," there is no contractual customer agreement.   Any service provided is on a time-and-materials basis.

For more details on your Manager IV warranty and the different software service coverage programs, consult a Manager IV customer representative at AT&T.

APPENDIX A: REPORTS

USER-ACTIVITY REPORT

The User-Activity Report is designed to provide information about Manager IV activity to be utilized by telecommunications management or System Administrator. This report can be accessed or executed from the system-administration area by a user who has the system administration privileges.

PATH: system-administration user-activity report

PURPOSE: This report will provide a concise Daily, Weekly, Monthly, or Daily Detailed Summary of Manager IV user activity which includes the number of transactions per user and transaction type.

DESCRIPTION: For every transaction attempted by a user, a transaction log is created in the **$LOG** directory containing this information: login ID, target, clock time, cpu time, status, and transaction path.

Daily report will collect information from the **$LOG/trxlog***mmdd* logs. Daily report data will be logged in the **$LOG/mgr/daily/drept***mmdd* files.

Daily Summary report data will be logged in the **$LOG/mgr/dsum/dsum***mmdd* files.

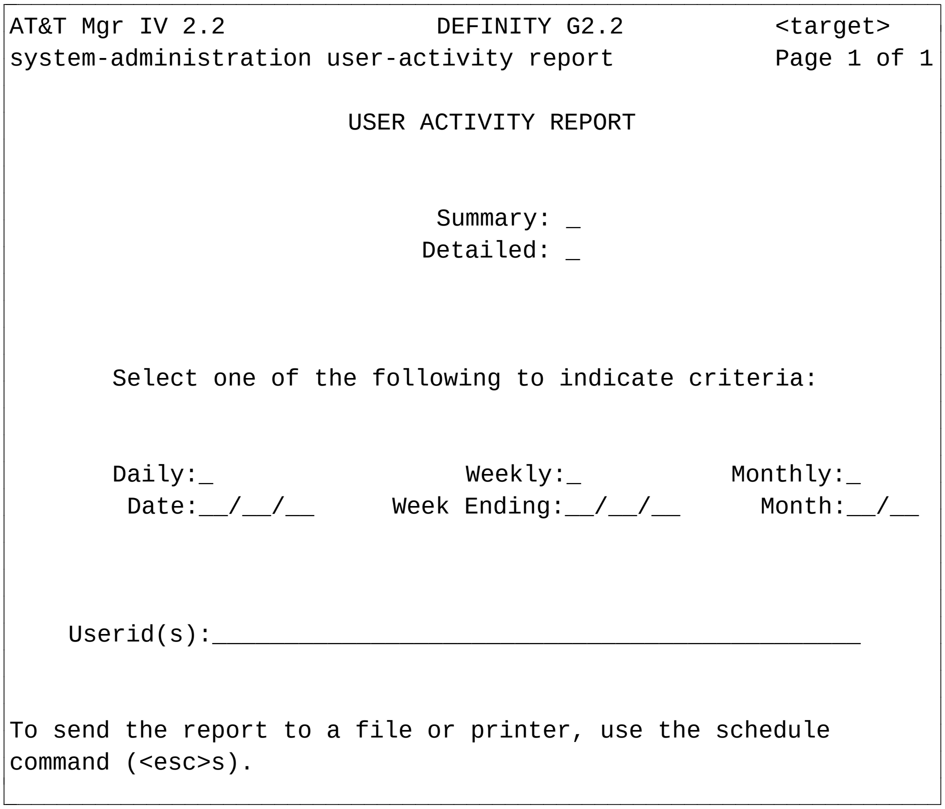
Monthly report will collect information from the **$LOG/drept***mmyy* logs. Monthly report data will be stored in the **$LOG/mgr/month/mrept***mmyy* files as they have been defined in the database and the switch.

SELECTION OPTIONS:

- Summary:
  - — You may select Daily, Weekly, or Monthly. For each of the selected report criteria, you must enter the timeframe: for Daily, enter a date from the last 60 days in the format "mmddyy"; for Weekly, enter the week ending date from last 60 days in the format "mmddyy"; for Monthly, enter the number of the month and the year from the last 15 months in the format "mmyy".
  - — Userid(s):
    a. You may enter a specific user ID, a list of users' IDs, or "all" for all users' IDs. A maximum of 5 entries are allowed for a List option.
- Detailed:
  - — You can select Daily only, excluding the current date. Weekly and Monthly Detailed reports are not available.
  - — Userid(s):
    a. You may enter a specific user ID, a list of users' IDs, or "all" for all users' IDs. A maximum of 5 entries are allowed for a List option.

SORT ORDER: Output is arranged by the USER-ID. For the DATE, WEEK ending, or MONTH specified, the total transactions completed per USER are provided. If the Detailed Summary has been selected, the transaction types are provided in the alphabetic order as well.

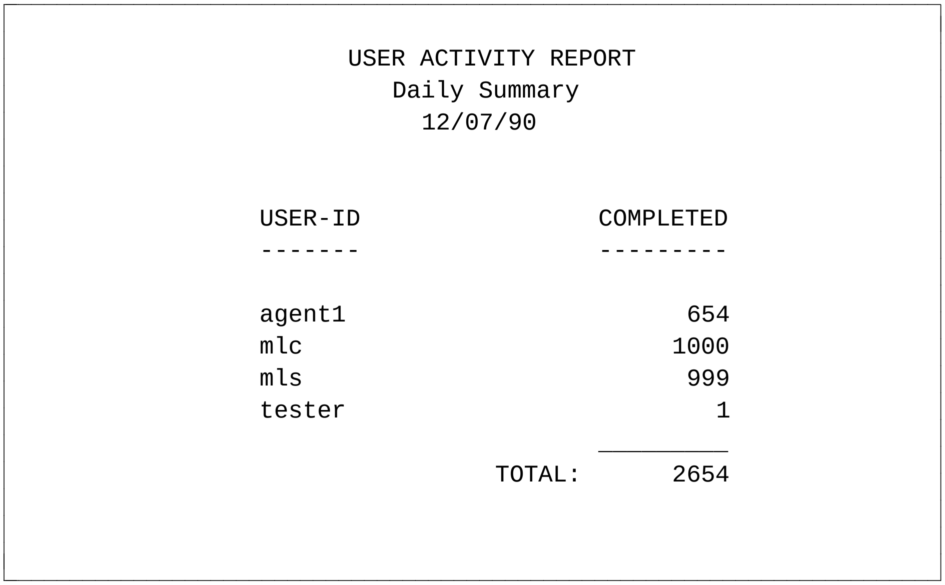
SAMPLE INPUT:



```
AT&T Mgr IV 2.2             DEFINITY G2.2          <target>
system-administration user-activity report          Page 1 of 1

                       USER ACTIVITY REPORT


                             Summary: _
                            Detailed: _



       Select one of the following to indicate criteria:


       Daily:_                 Weekly:_          Monthly:_
        Date:__/__/__     Week Ending:__/__/__     Month:__/__



    Userid(s):_____________________________________________


To send the report to a file or printer, use the schedule
command (<esc>s).
```

SAMPLE OUTPUTS:

Output is arranged by user IDs. COMPLETED TRANSACTIONS are the total transactions completed per USER for the DATE specified.



```
                       USER ACTIVITY REPORT
                          Daily Summary
                            12/07/90


                 USER-ID                COMPLETED
                 -------                ---------

                 agent1                       654
                 mlc                         1000
                 mls                          999
                 tester                         1
                                        _________
                                TOTAL:       2654
```

Output is arranged by Routing Designator. COMPLETED TRANSACTIONS are the total transactions completed per USER for the WEEK ending specified.

```
                       USER ACTIVITY REPORT
                          Weekly Summary
                         ending: 12/15/90


                 USER-ID                COMPLETED
                 -------                ---------

                 agent2                      888
                 agent3                      777
                 mlc                       10000
                 mls                       15000
                                        _________
                                 TOTAL:     26665
```

```
                       USER ACTIVITY REPORT
                            Detailed
                            12/14/90


      USER-ID               TYPE                 COMPLETED
      -------               ----                 ---------

      mlc      abbreviated-dial-lists remove         1234
               bearer-capability-cos display         1002
               carrier add                            123
                                                 ---------
                                      User Total:    2359

      mls      aar-non-portability change            1005
               primary-code-rst-level report         2046

                                                 ---------
                                      User Total:    3051
```

COMPLETED TRANSACTIONS are the total transactions completed per USER for the MONTH specified.

```
      USER ACTIVITY REPORT
        Monthly Summary
        December, 1991


USER-ID                 COMPLETED
-------                 ---------

agent1                        987
agent2                       7899
agent3                      21000
mlc                         11000
mls                         18000
                        _________
                TOTAL:      58886
```

DELTA REPORTS

The Delta Reports feature provides a convenient means of accessing station and user information from the Manager IV database. It also tracks various updating activities performed on the database. Both original information and changes (including additions and deletions to the database) can be reported.

When the database is initialized, a master file is created based on the nonswitch data information loaded from the TRACS Tape. When a report option is executed, the present database is compared to the master file, and any differences can be reported depending on the option chosen.

ACCESSING REPORTS

There are eight options available in the main menu, including six terminal installation report options. The main menu is accessed via the command **system-administration initialization delta**. Reports display the customer name, DOSS order number, and related nonswitch data, which is sorted by Set I.D. The terminal installation reports are as following:

Master Terminal Installation Report. Displays the original master file, which was created during initialization, or updated through Delta Reports.

Changed Terminal ONLY (fields) Installation Report. Displays terminal information that has been changed in the database since the master file was created. Changed information is flagged with "C" and is paired with the original information, which is flagged with "U." Changed fields are flagged with an asterisk (*).

Add Terminal Installation Report. Displays terminal information added to the database since the master file was created. The action field contains an "A."

Remove Terminal Installation Report. Displays terminal information removed from the database since the master file was created. The action field contains an "R."

Changed Terminal Installation Report. Encompasses the Add, Remove, and Changed Terminal ONLY reports. The action field may contain "R", "A", or "U" and "C."

Terminal Installation Summary Report. Displays statistics of the master file and of any changes made to the database subsequent to the creation of the master file. Statistics are grouped as follows:

File:

— number of records in the Master Terminal Installation File

— number of records in the New Master Terminal Installation File

— total number of terminal installation changes (changes, adds, removes)

Terminal:

— number of terminals added

— number of terminals removed

— total number of changed fields

Field:

— number of changed ELLs

— number of changed locations

— number of changed set types

— number of changed equipment

Note:: Each one of these counters is incremented once for each terminal when a change has been detected. The "total number of changed fields," however, gives a count of *all* changed fields. Therefore, totaling the field counters will not give the same result as the "total number of changed fields."

Other Options

Saved Changed Data. Creates a new master file by combining the changes from the Changed Terminal Installation Report.

Exit Delta Reports. Returns to the SMUE command line.

Notes::

- Only one delta report can be accessed by anyone at any given time.
- It is recommended that Delta Reports be scheduled since these reports run a long time.

Procedure: Accessing the Master Terminal Report

Command: system-administration initialization delta

Use this procedure to view the original station and user information placed into the Manager IV database during initialization.

Make sure that the Manager IV database has been initialized with TRACS Tape data.

This procedure can be used to access any report. However, during the initialization phase, there should be no changes, adds, or deletes applied to the database.

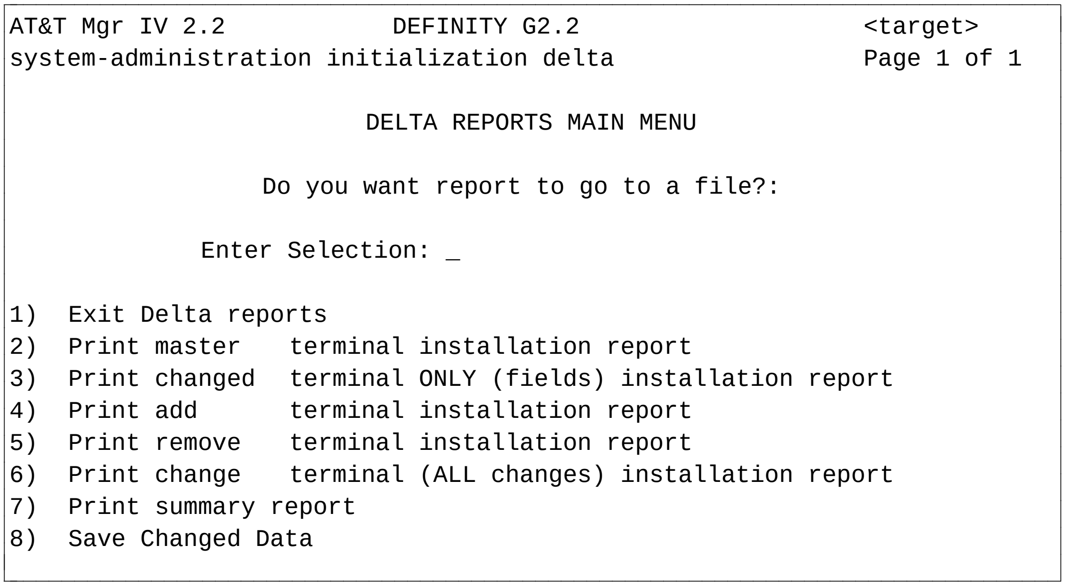
Since the Master Terminal Installation Report can be quite large, it is recommended that this report be viewed on the terminal display. If it is deemed necessary to save the file, move it from the **$WORK/delta** directory to another directory, or print it out. This will eliminate the possibility of running out of space in the **$WORK/delta** directory.

1. Access the **initialization delta** menu.

   The system will prompt you for the following information:

Application >	Enter **system-administration initialization**
Enter target >	Enter the target name
Enter verb >	Enter **delta**

   System Response:



```
AT&T Mgr IV 2.2            DEFINITY G2.2                  <target>
system-administration initialization delta                Page 1 of 1

                        DELTA REPORTS MAIN MENU

                 Do you want report to go to a file?:

             Enter Selection: _

1)  Exit Delta reports
2)  Print master   terminal installation report
3)  Print changed  terminal ONLY (fields) installation report
4)  Print add      terminal installation report
5)  Print remove   terminal installation report
6)  Print change   terminal (ALL changes) installation report
7)  Print summary report
8)  Save Changed Data
```

2. If the report is to be saved to file, enter **y** when prompted; otherwise the report will be displayed on the terminal.

3. To view the master terminal installation report, enter **2** as the selection.

Sample Output:

```
AT&T Mgr IV 2.2           DEFINITY G2.2                <target>
system-administration initialization delta


                   MASTER TERMINAL INSTALLATION REPORT

Customer Name: __________________________DOSS Order Number: ________
Sorted by Set I.D.

  SET                                        SET         SET
  I.D.   SEG  LOC     FLOOR    ROOM       TYPE        COLOR
 ------- ---  ---     -----    ------     ------      -------
 2000    00   _______ _____    ______     510bt       _______
    USER: ___________________________    ELL: 00/0/2/00/0 JACK NO:_____
    AUX EQP: (mount:wall  adjuncts:[speaker _ hdset 1])

 2002    00   _______ _____    ______     7406d       _______
    USER: ___________________________    ELL: 00/0/0/00/0 JACK NO:_____
    AUX EQP: (mount:wall  adjuncts:[speaker _ hdset 1])

 2003    00   topflr_ _____    ______     met10       _______
    USER: ___________________________    ELL: 00/0/0/00/0 JACK NO:_____
    AUX EQP: (mount:desk  adjuncts:[speaker _ hdset 1])
         .                         .                         .
         .                         .                         .
         .                         .                         .
         .                         .                         .
         .                         .                         .
         .                         .                         .
         .                         .                         .

 2004    00   topflr_ _____    ______     7403d       _______
    USER: ___________________________    ELL: 00/1/1/03/2 JACK NO:_____
    AUX EQP: (mount:wall  adjuncts:[speaker 1 hdset _])
```

4. If the report has been sent to file, the following message is displayed:

```
The Master terminal
installation report is in $WORK/delta/<ptarget>.
```

5. Press **RETURN** to go back to the verb level.

Procedure: Accessing the Changed Terminal Only Report

Command: system-administration initialization delta

Use this procedure to view changes made to the nonswitch data records since the original master file was created. This shows changes to fields only; it does not show added or removed records.

1. Access the **initialization delta** menu with the command **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.
2. If the report is to be saved to file, enter **y** when prompted, otherwise the report will be displayed on the terminal.
3. To view the changed terminal ONLY installation report, enter **3** as the selection.

   Sample Output:

```
AT&T Mgr IV 2.2                  DEFINITY G2.2                <target>
system-administration initialization delta



                      CHANGED TERMINAL ONLY REPORTS

Customer Name: __________________________DOSS Order Number: ________
Sorted by Set I.D.

     SET                                        SET         SET
ACT  I.D.    SEG  LOC      FLOOR    ROOM        TYPE        COLOR
--- ------- ---  ---      -----    ------      ------      -------
U   2000    01   main___ 2nd__     12____      7403d       RED____
    USER: ___________________________     ELL: 00/0/2/00/0 JACK NO:1____
    AUX EQP: (mount:wall   adjuncts:[speaker _ hdset 1])

C   2000   *00  *_______ 2nd__    *______     *7406d      *_______
    USER: ___________________________     ELL:*00/0/0/00/0 JACK NO:*____
    AUX EQP: (mount:*desk adjuncts:[speaker _ hdset 1])

U   2001    00   topflr_ 1st__     3T212_      7403d       GREEN__
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:7____
    AUX EQP: (mount:desk   adjuncts:[speaker 1 hdset 1])

C   2001    00  *garage_ 1st__     ______     *met108      *______
    USER: ___________________________     ELL:*00/0/0/03/2 JACK NO:_____
    AUX EQP: (mount:desk   adjuncts:[speaker 1 hdset 1])

U   2002    00   topflr_ 3rd__     ______      7403d       _______
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:_____
    AUX EQP: (mount:wall   adjuncts:[speaker 1 hdset _])

C   2002   *01   topflr_ 3rd__    *3D156_     *7406d       _______
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:_____
    AUX EQP: (mount:*desk adjuncts:[speaker *_ hdset _])
```

4. If the report has been sent to file, the following message is displayed:

```
delta report retrieval completed.   The changed terminal only
installation report is in $WORK/delta/<otarget>.
```

5. If no changes have been made to the master file, the following message is displayed:

```
Delta report retrieval completed.

The master file and database have not been changed.
```

6. Press **RETURN** to go back to the verb level.

Procedure: Accessing the Add Terminal Report

Command: system-administration initialization delta

Use this procedure to view additions made to the nonswitch data records since the original master file was created.

1. Access the **initialization delta** menu with the command **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.

2. If the report is to be saved to file, enter **y** when prompted; otherwise the report will be displayed on the terminal.

3. To view the add terminal installation report, enter **4** as the selection.

   Sample Output:

```
AT&T Mgr IV 2.2            DEFINITY G2.2            <target>
system-administration initialization delta
                    ADD TERMINAL INSTALLATION REPORT

Customer Name: __________________________DOSS Order Number: ________
Sorted by Set I.D.

     SET                                        SET         SET
ACT  I.D.   SEG  LOC     FLOOR    ROOM       TYPE        COLOR
--- ------- ---  ---     -----    ------     ------      -------
A   2000    01   main___ 2nd__    12____     7403d       RED____
    USER: ___________________________     ELL: 00/0/2/00/0 JACK NO:1____
    AUX EQP: (mount:wall   adjuncts:[speaker _ hdset 1])

A   2001    00   topflr_ 3rd__    3T212_     7403d       GREEN__
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:7____
    AUX EQP: (mount:desk   adjuncts:[speaker 1 hdset _])

A   2002    00   garage_ 1st__    ______     7406d       _______
    USER: ___________________________     ELL: 00/1/1/02/2 JACK NO:_____
    AUX EQP: (mount:desk   adjuncts:[speaker 1 hdset _])

A   2003    00   LZ_____ 2nd__    3D256_     7406d       _______
    USER: ___________________________     ELL: 00/1/1/03/1 JACK NO:_____
    AUX EQP: (mount:desk adjuncts:[speaker   _ hdset _])
```

4. If the report has been sent to file, the following message is displayed:

```
delta report retrieval completed.   The add terminal
installation report is in $WORK/delta/<atarget>.
```

5. If no changes have been made to the master file, the following message is displayed:

```
Delta report retrieval completed.
The master file and database have not been changed.
```

6. Press **RETURN** to go back to the verb level.

Procedure: Accessing the Remove Terminal Report

Command: system-administration initialization delta

Use this procedure to see which nonswitch data records have been removed from the database since the original master file was created.

1. Access the **initialization delta** menu with **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.
2. If the report is to be saved to file, enter **y** when prompted; otherwise the report will be displayed on the terminal.
3. To view the remove terminal installation report, enter **5** as the selection.

   Sample Output:

```
AT&T Mgr IV 2.2            DEFINITY G2.2           <target>
system-administration initialization delta

                   REMOVE TERMINAL INSTALLATION REPORT

Customer Name: __________________________DOSS Order Number: ________
Sorted by Set I.D.

     SET                                      SET         SET
ACT  I.D.   SEG  LOC     FLOOR    ROOM       TYPE        COLOR
--- ------- ---  ---     -----    ------     ------      -------
R   2003    01   main___ 2nd__    12____     7403d       RED____
    USER: ___________________________     ELL: 00/0/2/00/0 JACK NO:1____
    AUX EQP: (mount:desk  adjuncts:[speaker _ hdset 1])

R   2004    00   topflr_ 3rd__    3T212_     7403d       GREEN__
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:7____
    AUX EQP: (mount:wall  adjuncts:[speaker 1 hdset _])

R   2005    00   garage_ 1st__    ______     7406d       _______
    USER: ___________________________     ELL: 00/1/1/02/2 JACK NO:_____
    AUX EQP: (mount:desk  adjuncts:[speaker 1 hdset _])

R   2006    00   LZ_____ 2nd__    3D256_     7406d       _______
    USER: ___________________________     ELL: 00/1/1/03/1 JACK NO:_____
    AUX EQP: (mount:desk adjuncts:[speaker   _ hdset 1])
```

4. If the report has been sent to file, the following message is displayed:

```
delta report retrieval completed.  The remove terminal
installation report is in $WORK/delta/<rtarget>.
```

5. If no changes have been made to the master file, the following message is displayed:

```
Delta report retrieval completed.
The master file and database have not been changed.
```

6. Press **RETURN** to go back to the verb level.

Procedure: Accessing the Change Terminal Report

Command: system-administration initialization delta

Use this procedure to view all nonswitch data record changes (adds, removes, and changes) performed on the database since the original master file was created.

1. Access the **initialization delta** menu with the command **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.
2. If the report is to be saved to file, enter **y** when prompted; otherwise the report will be displayed on the terminal.
3. To view the change terminal installation report, enter **6** as the selection.

   Sample Output:

```
AT&T Mgr IV 2.2           DEFINITY G2.2            <target>
system-administration initialization delta


                  CHANGED TERMINAL INSTALLATION REPORT

Customer Name: __________________________DOSS Order Number: ________
Sorted by Set I.D.

     SET                                     SET         SET
ACT  I.D.   SEG  LOC     FLOOR    ROOM       TYPE        COLOR
--- ------- ---  ---     -----    ------     ------      -------
R   2000    01   main___ 2nd__    12____     7403d       RED____
    USER: ___________________________     ELL: 00/0/2/00/0 JACK NO:1____
    AUX EQP: (mount:desk  adjuncts:[speaker 1 hdset _])

R   2001    00   topflr_ 2nd__    3T212_     7403d       GREEN__
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:7____
    AUX EQP: (mount:wall  adjuncts:[speaker 1 hdset _])

U   2003    01   _______ 3rd__    11____     met10       RED____
    USER: ___________________________     ELL: 00/0/2/00/0 JACK NO:1____
    AUX EQP: (mount:desk  adjuncts:[speaker 1 hdset _])

C   2003   *00  *garage_ 3rd__   *______    *7406d      *_______
    USER: ___________________________     ELL:*00/0/0/00/0 JACK NO:*____
    AUX EQP: (mount:desk  adjuncts:[speaker 1 hdset _])

A   2002    00   topflr_ 4th__    3D456_     7403d       GREEN__
    USER: ___________________________     ELL: 00/1/1/03/2 JACK NO:7____
    AUX EQP: (mount:wall adjuncts:[speaker  1 hdset _])

R   2005    00   _______ 4th__    1A419_     7403d       RED____
    USER: ___________________________     ELL: 00/1/1/01/2 JACK NO:7____
    AUX EQP: (mount:desk adjuncts:[speaker  _ hdset 1])

A   2006    00   garage_ 3rd__    ______     7406d       _______
    USER: ___________________________     ELL: 00/1/1/02/2 JACK NO:_____
    AUX EQP: (mount:desk adjuncts:[speaker  _ hdset 1])
```

4. If the report has been sent to file, the following message is displayed:

```
delta report retrieval completed.  The change terminal
installation report is in $WORK/delta/<ctarget>.
```

5. If no changes have been made to the master file, the following message is displayed:

```
Delta report retrieval completed.

The master file and database have not been changed.
```

6. Press **RETURN** to go back to the verb level.

Procedure: Accessing the Summary Report

Command: system-administration initialization delta

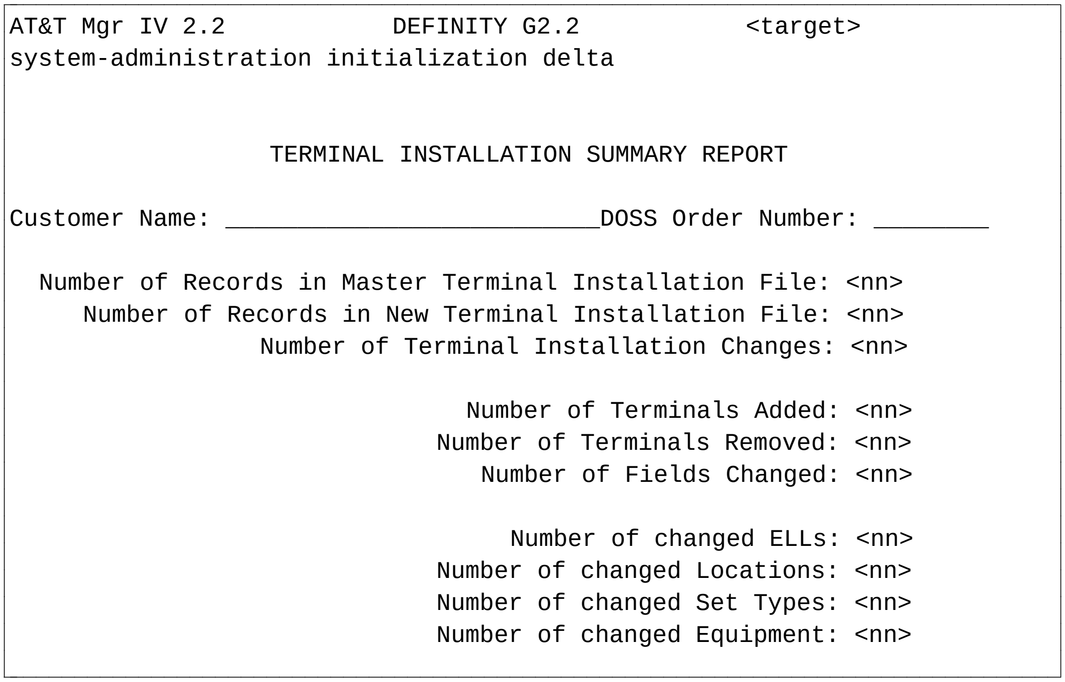
Use this procedure to view statistical information concerning the master file and the changes applied to it since its creation.

1. Access the **initialization delta** menu with the command **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.

2. If the report is to be saved to file, enter **y** when prompted; otherwise the report will be displayed on the terminal.

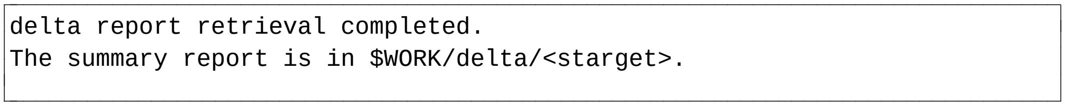
3. To view the summary report, enter **7** as the selection.

   Sample Output:



```
AT&T Mgr IV 2.2            DEFINITY G2.2            <target>
system-administration initialization delta


                  TERMINAL INSTALLATION SUMMARY REPORT

Customer Name: __________________________DOSS Order Number: ________

  Number of Records in Master Terminal Installation File: <nn>
     Number of Records in New Terminal Installation File: <nn>
                 Number of Terminal Installation Changes: <nn>

                                Number of Terminals Added: <nn>
                              Number of Terminals Removed: <nn>
                                 Number of Fields Changed: <nn>

                                   Number of changed ELLs: <nn>
                              Number of changed Locations: <nn>
                              Number of changed Set Types: <nn>
                              Number of changed Equipment: <nn>
```

4. If the report has been sent to file, the following message is displayed:



```
delta report retrieval completed.
The summary report is in $WORK/delta/<starget>.
```

5. Press **RETURN** to go back to the verb level.

Procedure: Create New Master Terminal Report

Command: system-administration initialization delta

Use this procedure to create a new master file. This option should be executed when a substantial amount of update activity has taken place.

1. Access the **initialization delta** menu with the command **system-administration delta**. See "Procedure: Accessing the Master Terminal Report" for an illustration of the Delta Reports Main Menu.
2. Enter **8** as the selection to invoke the "Save Changed Data" option.

   System Response:

   ```
   You are about to create a new Master Terminal Installation
   Report with all changes from the Changed Terminal Installation
   Report.  Do you want to proceed? (y/n)
   ```

3. Enter **y** to proceed. If **n** is entered, no changes will take place, and the main menu will be displayed.

   System Response:

   ```
   The existing Master Terminal Report will be overwritten.
   Are you sure you want to do this? (y/n)
   ```

4. Enter **y** to continue. After the master file is updated, the system will respond with a success message.

APPENDIX B: INTRODUCTION TO AUDITS

There are seven audits that check the synchronization between System 85 R2V2/R2V4 (or DEFINITY Generic 2) switches and the associated product database in Manager IV. Audits upload critical proc information from the switch and compare it to the Manager IV database.

Audits should be executed by an individual with a working knowledge of the UNIX operating system, while the discrepancies identified in the audit reports should be corrected by a person who understands System 85 or Generic 2.

All audits are performed under the system-administration hierarchy; it is in this area that you choose the audit you want to run. Once you have entered the appropriate target, the switch release will be checked to see if the audit/object applies to System 85 or Generic 2.

CAUTION: Since these transactions can be time-consuming, you should perform all audits during off hours by scheduling them with **ESC** **s** . Additionally, you can run only one audit at a time. *Do not* schedule audits simultaneously; this will cause the results files to be overwritten.

INTERPRETING RESULT FILES

After completing a **run** or a **start**, a result file is sent to your $HOME/smgr directory with a message indicating whether it was successful or not. Examples from the result files for each audit are included in this chapter.

The result file name is given when the audit run or start step is complete. Use **results display** to view the file.

Generally, the report files and auout files, which are found in $WORK/dbdata, are translated as follows:

- auout1 <pbxid> - database only report
- auout2 <pbxid> - switch only report
- auout3 <pbxid> - database and switch discrepancy report
- auout4 <pbxid> - pending service request report

The information from the **status-display** can be found in $WORK/dbdata/austat<pbxid>.

- type 1 discrepancy - database only
- type 2 discrepancy - switch only
- type 3 discrepancy - database and switch discrepancy
- type 4 discrepancy - pending service request on type 1 and type 3 records

TROUBLESHOOTING

There are two types of results files that are used for troubleshooting audit transactions:

- The first type of result file appears in your $HOME/smgr directory as "results <audit abbreviation> <pbxid>." This file will contain a message indicating whether the audit transaction was successful or unsuccessful.

- The second type of result file appears in your $WORK/dbdata directory as "vresults <audit abbreviation> <pbxid>." This result file traces the procs that were displayed from the switch.

Following are some common errors you may encounter while running audit transactions and some troubleshooting suggestions.

Product Busy/No Answer

If you did a **start** for any of the audits, and the "results <> #" file indicated that the switch was immediately busy or did not answer, execute the **start** again if no data has been retrieved from the switch.

CAUTION: Do not use the **restart** command if you receive a product busy/no answer message and no data was retrieved, because it will fail when trying to **restart**. The **restart** command is used only in the instances when a partial amount of the data has been retrieved from the switch and you wish to continue retrieving data from the point at which the **start** command stopped.

Correct Discrepancies

Use the report files to aid in correcting any discrepancies. It is recommended that you send the reports to the printer. The commands listed in the reports are only recommendations regarding how to correct the discrepancy; the final choice is up to you or your administrator. You can either add or remove changes to the database or switch (via the Manager IV database-admin and prod-admin transactions) to synchronize the database and the switch.

ANALOG AUDIT

The **anlg-audit** checks for synchronization errors that might exist between the System 85 switch and the Manager IV database. It accomplishes this by comparing the analog extension to the corresponding equipment location for a specified range of extensions.

Analog Audit: Command List

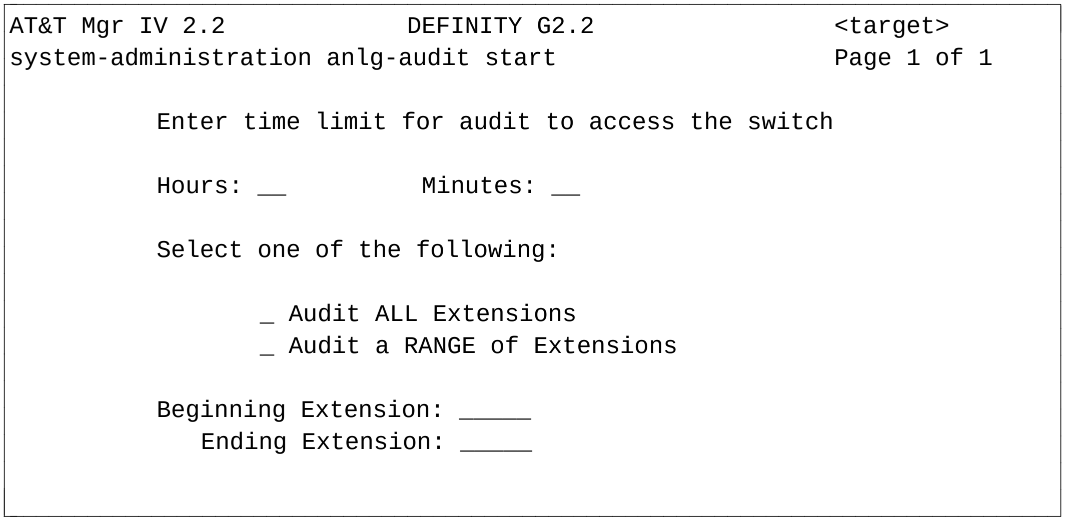
One complete cycle for an analog audit would be in the following order:

- **anlg-audit start**
- **anlg-audit restart** (only if all the data is not retrieved)
- **anlg-audit run**
- **anlg-audit status-display**
- **anlg-audit report**

Procedure: Starting an Analog Audit

Command: system-administration anlg-audit start

1. Enter **anlg-audit start** to retrieve the extension and equipment location data from the switch.



```
AT&T Mgr IV 2.2            DEFINITY G2.2                <target>
system-administration anlg-audit start                  Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __         Minutes: __

          Select one of the following:

                 _ Audit ALL Extensions
                 _ Audit a RANGE of Extensions

          Beginning Extension: _____
             Ending Extension: _____
```

2. Enter the number of hours, the number of minutes, or both for the audit to run. Valid entries are from **0** - **23** for hours; **0** - **59** for minutes.
3. Choose to audit ALL or a RANGE of extensions. If you choose the latter, you must enter a valid Beginning Extension number and a valid Ending Extension number. Valid entries are from **3** - **5** digits for both fields.
4. Press **ESC** **e** to execute the audit immediately or **ESC** **s** to schedule the audit for an off-peak time.
5. If the **anlg-audit start** command completed successfully for the range specified, use **anlg-audit run** to execute the comparison between the switch and the database. However, if the **anlg-audit start**

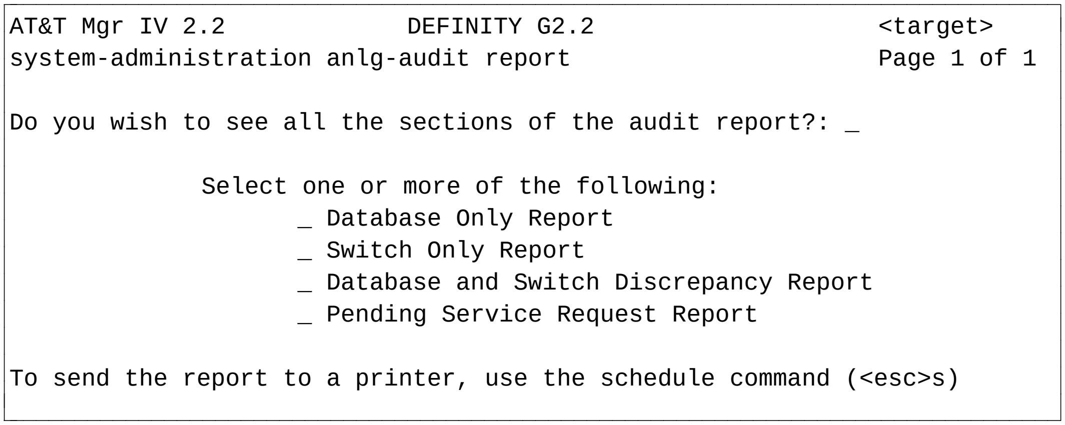
command did not complete the entire range of extensions specified within the time allocated, you have two options to retrieve the remainder of the data from the switch:

- Use **anlg-audit run** to execute a comparison of the extensions completed at this time; then use **anlg-audit start** to process the remainder of the extensions to be audited.
- You can also use the **anlg-audit restart** command to continue retrieving the data from the switch. The audit will automatically restart at the extension at which it left off, and you can perform an **anlg-audit run** when the restart is successful.

6. Use the **anlg-audit status-display** command to display the status of the audit and whether it was successful. If the audit was successful, a statistics summary is displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors occur, they will be displayed below the statistics. All errors should be investigated, and depending on the error, you may need to rerun the audit. Each error will generate a specific error message.

   Note: The **anlg-audit status-display** command can be invoked at any time during a start, restart, or run. If you attempt to use the status-display command before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to be displayed. (Maybe need to start or run audit?)"

7. Enter **anlg-audit report** to check for any discrepancies or errors after successfully completing the **anlg-audit run** command. This command will print both the auout and austat report files from $WORK/dbdata.



```
AT&T Mgr IV 2.2            DEFINITY G2.2                    <target>
system-administration anlg-audit report                     Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:
                    _ Database Only Report
                    _ Switch Only Report
                    _ Database and Switch Discrepancy Report
                    _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

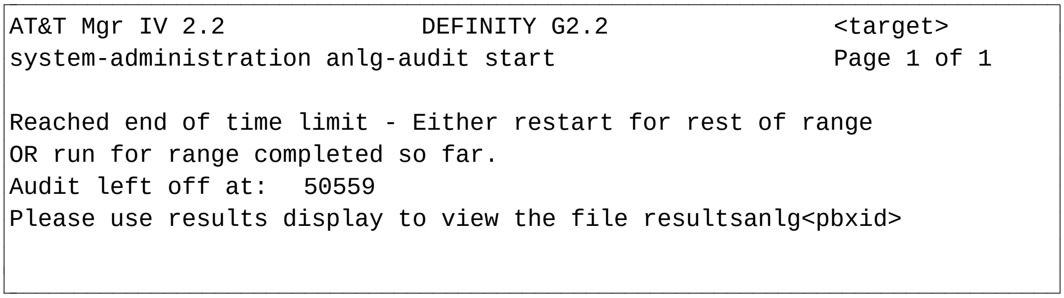
   If you enter **n** to the question "Do you wish to see all the sections of the audit report?" select one or more of the subsequent choices.

8. Press **ESC** **e** to execute the audit report or **ESC** **s** to send the report to a printer. It is recommended you send the report to a printer, so that you have a hard copy for checking discrepancies or errors identified by the audit report.

   CAUTION: After completion of the report, copy or move the four auout files and austat file out of the $WORK/dbdata directory into a separate directory (refer to "Interpreting Result Files," earlier in this chapter, for file-naming conventions). This will prevent these files from being overwritten when the audit is started again or another audit is started. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Analog Results Files

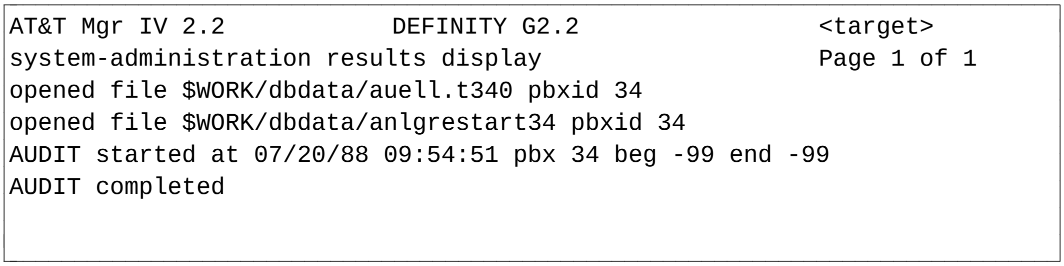
After running **anlg-audit start**, the following screen appears when the time limit has been reached before all the data has been retrieved:



```
AT&T Mgr IV 2.2              DEFINITY G2.2                <target>
system-administration anlg-audit start                    Page 1 of 1

Reached end of time limit - Either restart for rest of range
OR run for range completed so far.
Audit left off at:  50559
Please use results display to view the file resultsanlg<pbxid>
```

Analog Audit: Start Successful

The following is an example of the results file from a **start** if it was successful:



```
AT&T Mgr IV 2.2             DEFINITY G2.2                <target>
system-administration results display                    Page 1 of 1
opened file $WORK/dbdata/auell.t340 pbxid 34
opened file $WORK/dbdata/anlgrestart34 pbxid 34
AUDIT started at 07/20/88 09:54:51 pbx 34 beg -99 end -99
AUDIT completed
```

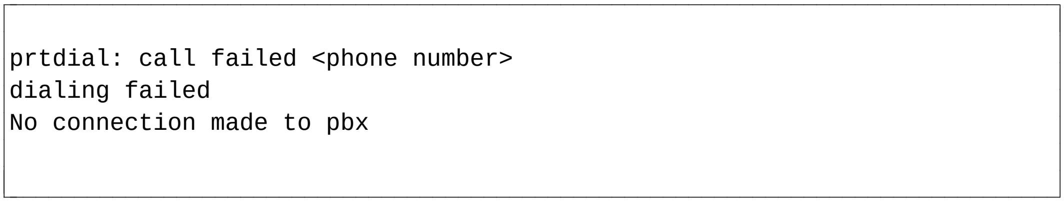
Analog Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the **start** is unsuccessful, the original transaction screen will show the following message:

```
           * * * * CONNECTION FAILED * * * *
      Please use results display to view the file resultsanlg#
```

The following is an example of the results file if a **start** was unsuccessful. This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.



```
prtdial: call failed <phone number>
dialing failed
No connection made to pbx
```

Analog Audit: Run

After running **analog-audit run**, the following screen appears:

```
AT&T Mgr IV 2.2            DEFINITY G2.2           <target>
system-administration anlg-audit run
Please use results display to view the file
resultsanlg<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Analog Audit: Run Successful

The following is an example of the results file if the **run** step was successful:

```
AT&T Mgr IV 2.2
system-administration results display
Analog audit was successful.
```

Analog Audit: austat

The **austat** file contains statistics indicating the total number of records audited and the number of discrepancies reported in the other files. Use the **status-display** command to view the results.

This austat report file has a pbxid number appended onto the file name. For example, a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid> file:

```
austat34
auell  total number or recs = 6
       type 1 discrepancy : 0
       type 2 discrepancy : 1
       type 3 discrepancy : 0
       type 4 discrepancy : 0
```

Analog Audit: auouta

There are four auouta files. All these report files have a pbxid number appended onto the file name. For example, a pbxid of 2 would generate auout12a, auout22a, auout32a, and auout42a.

- Auout1a contains records that are in the database and not in the product.
- Auout2a contains records that are in the product, but not in the database.
- Auout3a contains records where the database and product records do not match.
- Auout4a contains type 1 and type 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2a<pbxid>file:

AUOUT2a

```
Product Reports:
Object                     Verb         Label          Data
------------------------------------------------------------------------
electronic-sets            add          Set I.D.          33007
                                        ELL             0211031
```

BUTTON AUDIT

The **button-audit** compares the station attributes and the corresponding button assignments for the specified range of equipment locations between System 85 and the Manager IV database. This audit differs from the other audits in that as soon as the start command retrieves the data from the switch, it does a comparison immediately.

Note: The time to run a button audit is directly related to the number of buttons.

Button Audit: Command List

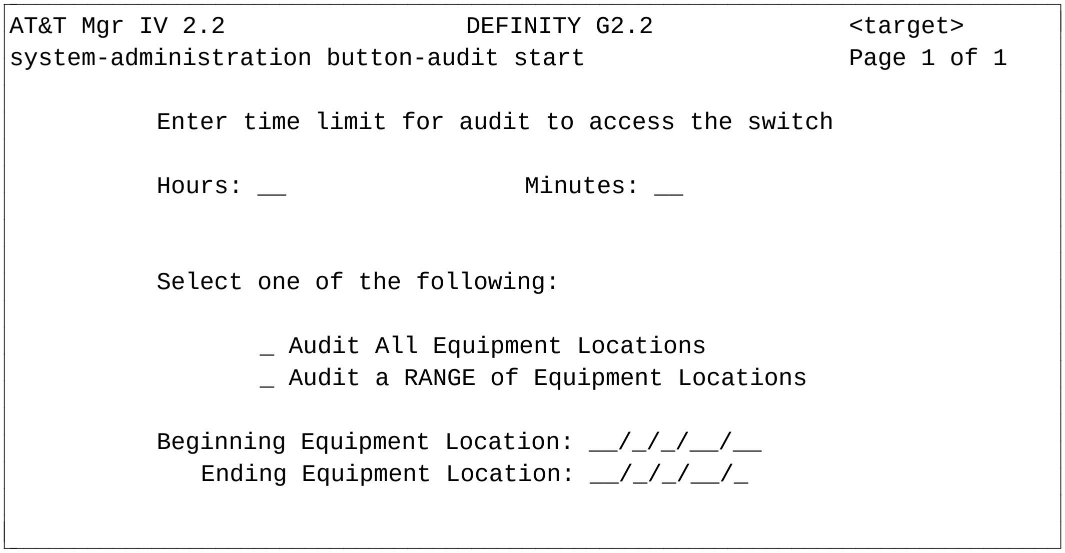
One complete cycle for a button audit would be in the following order:

- **button-audit start**
- **button-audit restart** (only if all the data is not retrieved)
- **button-audit status-display**
- **button-audit report**
- **button-audit cleanup**

Procedure: Starting a Button Audit

Command: system-administration button-audit start

1. Enter **button-audit start** to retrieve the set and button data from the switch and compare the information to the database.



```
AT&T Mgr IV 2.2                DEFINITY G2.2             <target>
system-administration button-audit start                 Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __                 Minutes: __


          Select one of the following:

                 _ Audit All Equipment Locations
                 _ Audit a RANGE of Equipment Locations

          Beginning Equipment Location: __/_/_/__/__
             Ending Equipment Location: __/_/_/__/_
```

2. Enter the number of hours, the number of minutes, or both for the audit to run. Valid entries are from **4 - 23** for hours; **0-59** for minutes.

3. Choose to audit ALL or a RANGE of equipment locations. If you choose the latter, the following are valid entries for the Beginning and Ending Equipment Location - Format fields:

    1. Enter module number (**00** - **30**).
    2. Enter cabinet number (**0** - **7** for System 85 or Generic 2 Traditional Module; **0** for Generic 2 Universal or XE Module).
    3. Enter carrier number (**0** - **3** for System 85 or Generic 2 Traditional Module; **c - e** for Generic 2 Universal or XE Module).
    4. Enter slot number (**0** - **3**, **5 - 8**, **13 - 16**, **18 - 21** for System 85 or Generic 2 Traditional Module; **1 - 20** for Generic 2 Universal or XE Module).
    5. Enter circuit (**0** - **7** for System 85 or Generic 2 Traditional Module; **0 - 23** for Generic 2 Universal or XE Module).

4. Press **ESC** **e** to execute the audit immediately, or press **ESC** **s** to schedule the audit for an off-peak time.

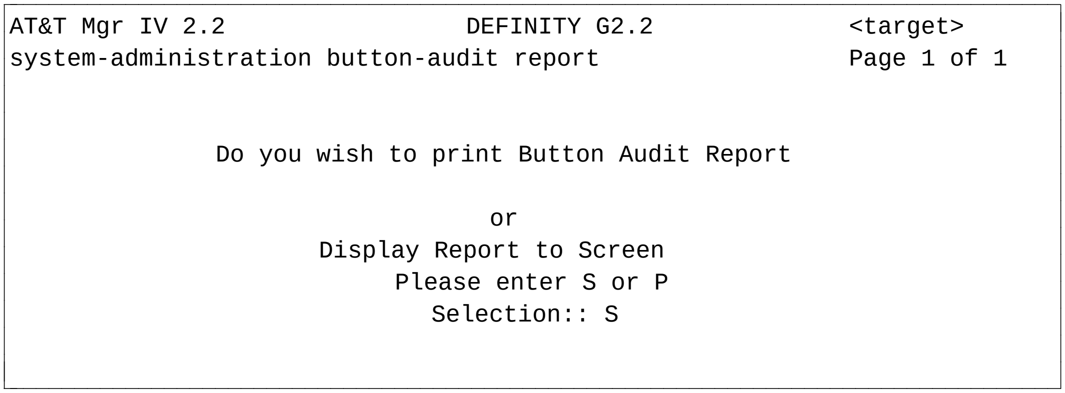
5. If the **button-audit start** command completed successfully for the range specified, proceed directly to step 6. However, if the **button-audit start** command did not complete the entire range of equipment locations you specified within the allocated time, you then have two options to retrieve the remainder of the data from the switch:

    - Use the **button-audit restart** command to continue from the last completed ELL.
    - Use the **button-audit start** command, specifying the equipment location at which the **button-audit start** command stopped or a different range of ELLs.

6. Use the **button-audit status-display** command to display the status of the audit and whether it was successful or not. If the audit was successful then a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors did occur they will be displayed below the statistics. The error should be investigated and depending on the error, you may need to rerun the audit. Each error will generate a specific error message.

    Note: The **button-audit status-display** command can be invoked at any time during a start or restart.

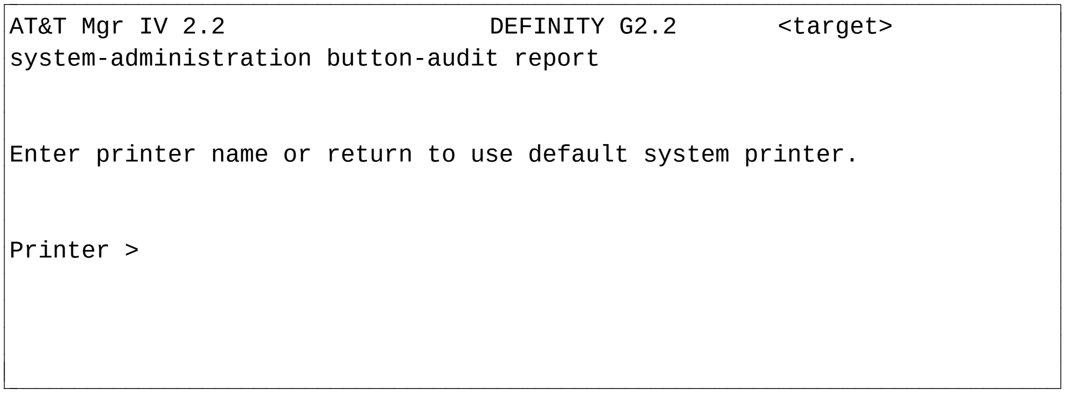
7. Use the **button-audit report** to check for any discrepancies or errors while using the **button-audit start/restart** command. This command will print files from the current run.



```
AT&T Mgr IV 2.2                DEFINITY G2.2              <target>
system-administration button-audit report                 Page 1 of 1



              Do you wish to print Button Audit Report

                                 or
                     Display Report to Screen
                          Please enter S or P
                            Selection:: S
```

8. Enter **P** to print a button-audit report or enter **S** if you want to view a button audit report on the screen.

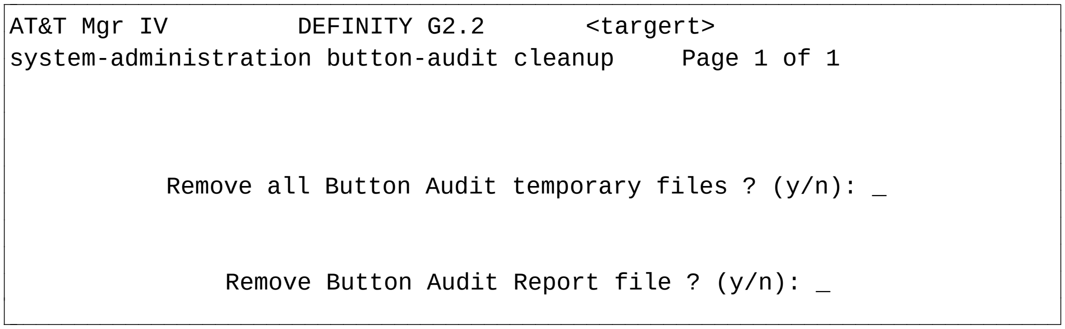
9. If you select the printer option, the following screen will appear.



```
AT&T Mgr IV 2.2                  DEFINITY G2.2       <target>
system-administration button-audit report


Enter printer name or return to use default system printer.


Printer >
```

10. Press **Return** to use the default system printer, or enter the name of your printer at the "Printer >" prompt.

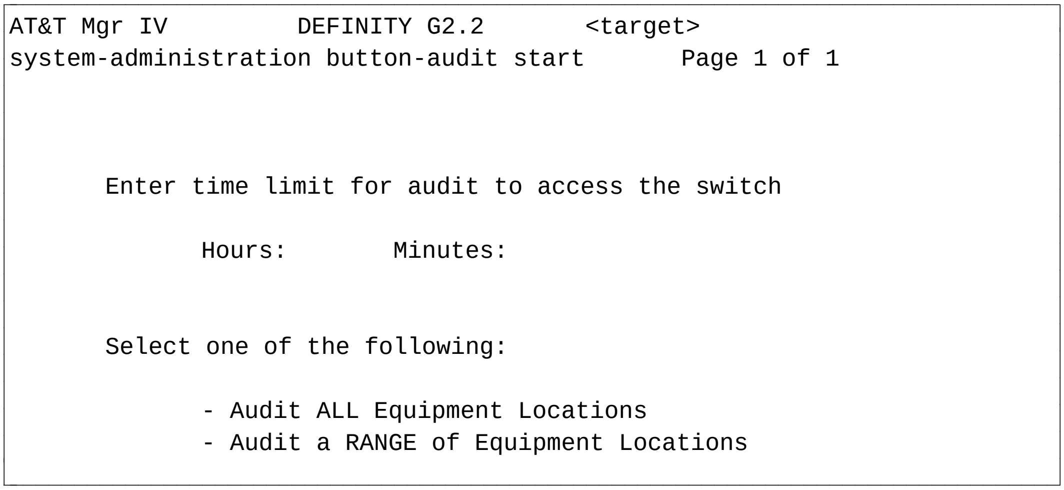
11. Use **button-audit cleanup** to remove the temporary files from the $WORK/dbdata directory after all the desired sets have been audited. Once cleanup has been run, you must use **button-audit start** to begin another button audit because the previous restart will no longer be valid.



```
AT&T Mgr IV         DEFINITY G2.2       <targert>
system-administration button-audit cleanup     Page 1 of 1



           Remove all Button Audit temporary files ? (y/n): _


               Remove Button Audit Report file ? (y/n): _
```

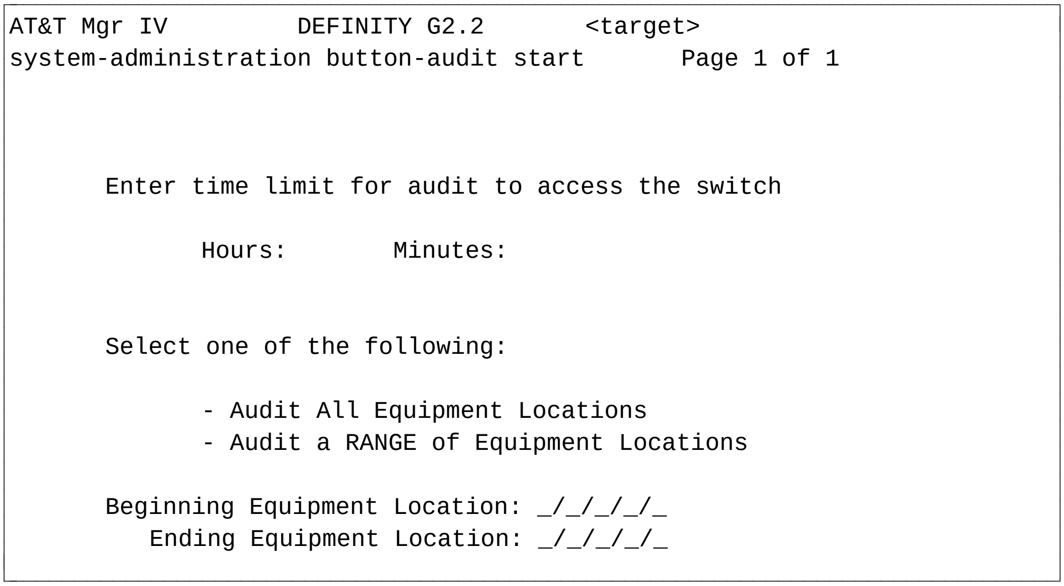
Interpreting Button Results Files

The following screen is used to start a button audit. An audit must be started with at least a four hour minimum. If the audit ends because of a time limit, or if some error condition occurs, you must use **button-audit restart** to start the audit again from the last ELL processed. This screen should be used only when beginning a new button audit, since it removes all previous button audits for the selected target.



```
AT&T Mgr IV         DEFINITY G2.2       <target>
system-administration button-audit start      Page 1 of 1



       Enter time limit for audit to access the switch

              Hours:       Minutes:


       Select one of the following:

              - Audit ALL Equipment Locations
              - Audit a RANGE of Equipment Locations
```

If an audit is selected with a Range of ELLs, then two additional fields will be added. These fields will have the starting and ending ELLs, and the resulting screen appears.



```
AT&T Mgr IV         DEFINITY G2.2       <target>
system-administration button-audit start      Page 1 of 1



       Enter time limit for audit to access the switch

              Hours:       Minutes:


       Select one of the following:

              - Audit All Equipment Locations
              - Audit a RANGE of Equipment Locations

       Beginning Equipment Location: _/_/_/_/_
          Ending Equipment Location: _/_/_/_/_
```

This next screen is used to restart an audit after it has ended because of a time limit or error condition. The restart will pick up at the last processed ELL and continue until the audit is finished or the time limit is reached.

```
AT&T Mgr IV         DEFINITY G2.2       <target>
system-administration button-audit restart     Page 1 of 1



             Enter time limit for audit to access the switch

              Hours: _            Minutes: _
```

This is an example of a field discrepancy for CALL buttons that would be included in the report.

```
Set ID:      8825   Set Mod: 0   Button: 05   Button Type: CALL
ELL: 01/0/3/07/1

                           Switch Database
                           ====== ========
           Extension:       8825    8825
     Line Appearance:        03      03
           Line Type:         1       1
          Alert Type:         1       1
         Originating:         0       1  <----
     A/D Alert encode:        1       1
     Ringing Transfer:        0       0
     SAC Group Member:        1       1

Last Service Request: Unknown
```

The following is an example of buttons found in the switch but not in the database.

```

       ELL: 00/0/2/06/0    Set Mod: 0   Button: 03

       1.0.0.2.6.0.0.3.3138.1.1.1.1.0.1.1.        052 00 01
```

The following is an example of buttons found in the database but not in the switch.

```

Setid: 8030  Button Type: CALL

ELL: 01/0/3/15/2    set Mod: 0   Button: 01


Last Service Request: Unknown
```

Button Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

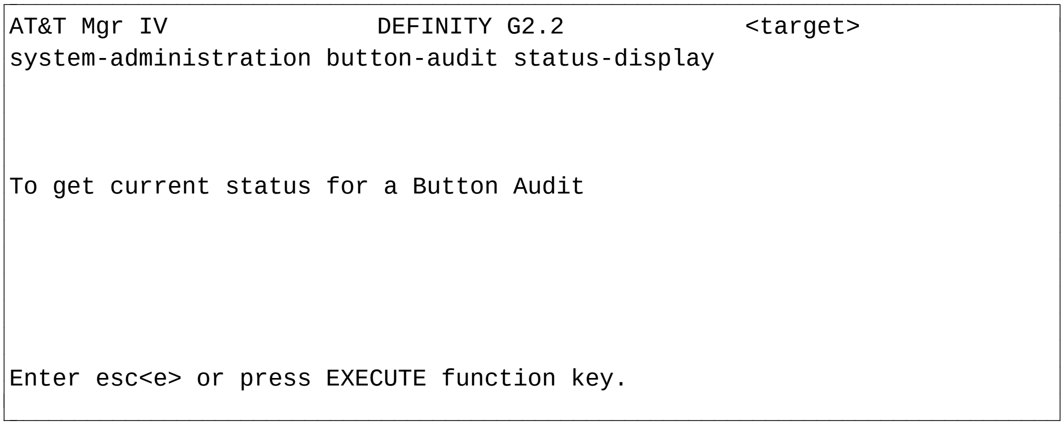
```
              * * * * CONNECTION FAILED * * * *
      Please use results display to view the file resultssmb#
```

The following is an example of the results file if a **start** was unsuccessful. This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.

```
prtdial: call failed <phone number>
dialog failed
No connection made to pbx.
```

Button Audit: Status Display

The following is an example of the **button-audit status-display** screen. This screen is used to display the status messages from a run of the button audit. It can be used at any time when a button audit is running or ended.



```
AT&T Mgr IV               DEFINITY G2.2            <target>
system-administration button-audit status-display



To get current status for a Button Audit





Enter esc<e> or press EXECUTE function key.
```

CALL COVERAGE GROUP AUDIT (CCGP)

The ccgp-audit compares the call coverage group number and the points, whether extension or Automatic Call Distribution (ACD) group, for the specified range of call coverage groups between the System 85 switch and the Manager IV database.

Call Coverage Group Audit: Command List

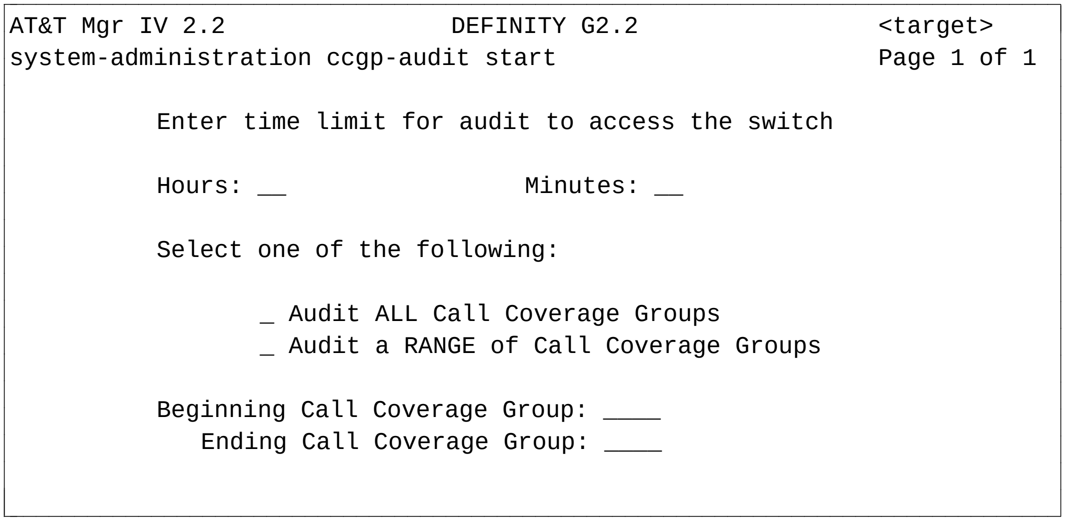
One complete cycle for a call coverage audit would be the following:

- **ccgp-audit start**
- **ccgp-audit restart** (only if all the data is not retrieved)
- **ccgp-audit run**
- **ccgp-audit status-display**
- **ccgp-audit report**

Procedure: Starting a Call Coverage Group Audit

Command: system-administration ccgp-audit start

1. Enter **ccgp-audit start** to retrieve the call coverage group number, ccg path, and ccg point data from the switch.



```
AT&T Mgr IV 2.2               DEFINITY G2.2                 <target>
system-administration ccgp-audit start                      Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __                 Minutes: __

          Select one of the following:

                 _ Audit ALL Call Coverage Groups
                 _ Audit a RANGE of Call Coverage Groups

          Beginning Call Coverage Group: ____
             Ending Call Coverage Group: ____
```

2. Enter the number of hours, the number of minutes, or both for the audit run. Valid entries are from **0** - **23** for hours; **0** - **59** for minutes.
3. Choose to audit ALL or a RANGE of Call Coverage Groups. If you choose the latter, enter a Beginning and Ending Call Coverage Group number. Valid entries are from **1** - **1999** if single coverage or **2000** - **4094** (even numbers only) if dual coverage.
4. Press **ESC** **e** to execute the audit immediately or **ESC** **s** to schedule the audit for an off-peak time.

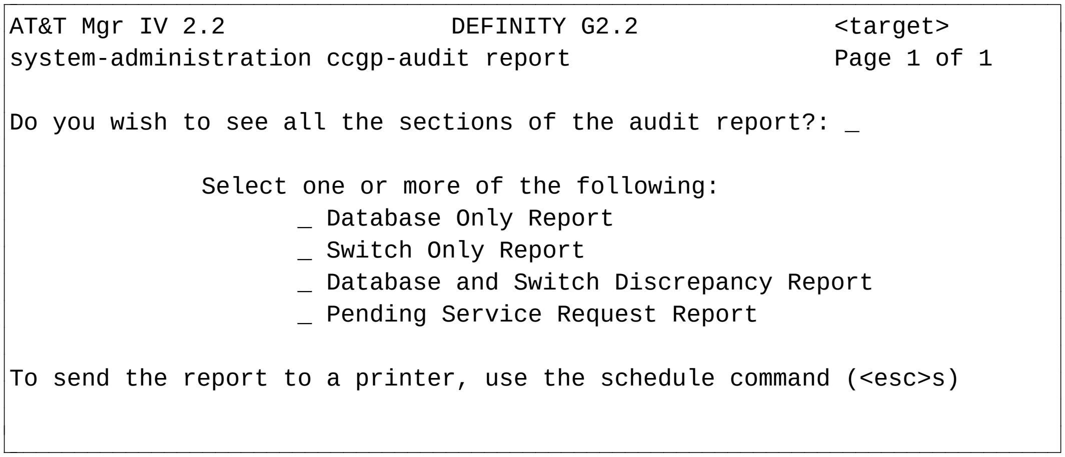
5. If the **ccgp-audit start** command completed successfully for the range specified, use **ccgp-audit run** to execute the comparison between the switch and the database. However, if **ccgp-audit start** did not complete the entire range of call coverage groups that you specified within the allocated time, you have two options to retrieve the remainder of the data from the switch:

    - Use **ccgp-audit run** to execute a comparison of the range of call coverage groups completed at this time; then use **ccgp-audit start** to process the remainder of the call coverage groups to be audited.
    - Use **ccgp-audit restart** to continue retrieving the data from the switch. The audit will automatically restart at the call coverage group at which it left off, and you can perform a **ccgp-audit run** when the restart is successful.

6. Use **ccgp-audit status-display** to display the status of the audit and whether it was successful or not. If the audit was successful, a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors occur, they will be displayed below the statistics; all errors should be investigated, and depending on the error, you may need to rerun the audit. Each error will generate a specific error message.

    Note: The **ccgp-audit status-display** command can be invoked at any time during a start, restart or run. If you attempt to use the **status-display** command before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to display. (Maybe need to start or run audit?)"

7. Enter **ccgp-audit report** to check for any discrepancies or errors after successfully completing the **ccgp-audit run** command. This command will print both auout and austat report files.



```
AT&T Mgr IV 2.2               DEFINITY G2.2              <target>
system-administration ccgp-audit report                  Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:
                   _ Database Only Report
                   _ Switch Only Report
                   _ Database and Switch Discrepancy Report
                   _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

If you enter **n** to the question "Do you wish to see all the sections of the audit report?" you must select one or more of the subsequent choices.

8. Press **ESC** **e** to execute the audit report, or press **ESC** **s** to send the report to a printer.

    CAUTION: At this time, you should copy or move the four auout files and austat file from the $WORK/dbdata directory to a separate directory (refer to "Interpreting Result Files" earlier in this chapter for file-naming conventions). This will prevent these files from being overwritten when this audit is started again or another audit is started. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Call Coverage Group (ccgp) Results Files

After running **ccgp-audit start**, the following screen appears:

```
AT&T Mgr IV 2.2               DEFINITY G2.2             <target>
system-administration anlg-audit start
Please use results display to view the file resultsccgp<pbxid>
```

Ccgp-Audit: Start Successful

The following is an example of the results file from a **start** if it was successful:

```
AT&T Mgr IV 2.2                 DEFINITY G2.2             <target>
system-administration results display
started from 1 at 07/06/88 15:57:38
completed
```

Ccgp-Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

```
       * * * * CONNECTION FAILED * * * *
Please use results display to view the file resultsccgp#
```

The following is an example of the results file if a **start** was unsuccessful: This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.

```
prtdial: call failed <phone number>
dialing failed
No connection made to pbx.
```

Ccgp-Audit: Run

After running **ccgp-audit run**, the following screen appears:

```
AT&T Mgr IV 2.2               DEFINITY G2.2            <target>
system-administration ccgp-audit run
Please use results display to view the file
resultsccgp<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Ccgp-Audit: Run Successful

The following is an example of the results file if the **run** step was successful:

```
AT&T Mgr IV 2.2                DEFINITY G2.2           <target>
system-administration results display
The ccgp audit was successful.
```

Ccgp-Audit Report: austat

The **austat** file contains statistics indicating the total number of records audited and the number of discrepancies reported in the other files. Use the **status-display** command to view the results.

This report file has a pbxid number appended onto the file name. For example, a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid> file:

```
ccgp   total number of recs = 16
       type 1 discrepancy : 0
       type 2 discrepancy : 2
       type 3 discrepancy : 0
       type 4 discrepancy : 0
```

Ccgp-Audit Report: auoutc

There are four auoutc files. All these report files have a pbxid number appended onto the file name. For example, a pbxid of 2 would generate auout12c, auout22c, auout32c and auout42c.

- Auout1c contains records that are in the database, not in the product.
- Auout2c contains records that are in the product, not in the database.
- Auout3c contains records where the database and product records do not match.
- Auout4c contains type 1 and 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2c<pbxid> file:

```
Product Reports:
Object               Verb           Label                      Data
------------------------------------------------------------------------
call-coverage-path   add         CCG_Path_Point                  41
                                 Call Coverage Group No.          4
                                 Extension No                 10027


Object               Verb           Label                      Data
------------------------------------------------------------------------
call-coverage-path   add         CCG_Path_Point                  42
                                 Call Coverage Group No.          4
                                 Extension No                 10031
```

NAME AUDIT

The name audit compares the presence/non-presence of a name for the specified range of extensions between the System 85 switch and the Manager IV database.

Name Audit: Command List

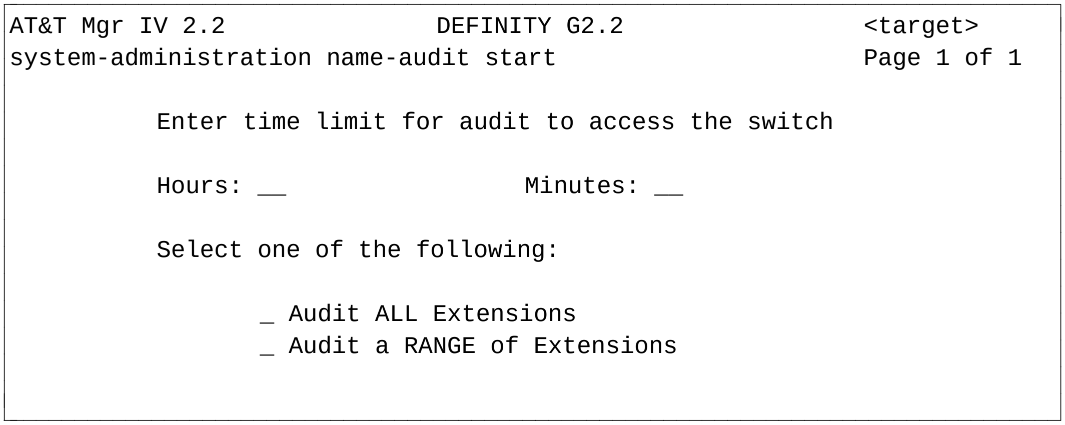
One complete cycle for a name audit would be in the following order:

- **name-audit start**
- **name-audit restart** (only if all the data is not retrieved)
- **name-audit run**
- **name-audit status-display**
- **name-audit report**

Procedure: Starting a Name Audit

Command: system-administration name-audit start

1. Enter **name-audit start** to start checking the extension data for the presence/non-presence of a name from the switch.



```
AT&T Mgr IV 2.2              DEFINITY G2.2                 <target>
system-administration name-audit start                     Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __                 Minutes: __

          Select one of the following:

                 _ Audit ALL Extensions
                 _ Audit a RANGE of Extensions
```

2. Enter either the number of hours, the number of minutes, or both for the audit to run. Valid entries are from **0** - **23** for hours; **0** - **59** for minutes.
3. Choose to audit ALL or a RANGE of extensions. If you choose the latter, enter a Beginning Extension number and an Ending Extension number. Valid entries are from **3** - **5** digits.
4. Press **ESC** **e** to execute the audit immediately, or press **ESC** **s** to schedule the audit for an off-peak time.
5. If **name-audit start** completed successfully for the range specified, use **name-audit run** to execute the comparison between the switch and the database.

   Note: The **name-audit run** command does not ask for a range of extensions; instead, it uses the list of extensions extracted from the switch to compare the information to the database. Additionally, it checks only for the presence of a name; it does not make comparisons of the actual name.

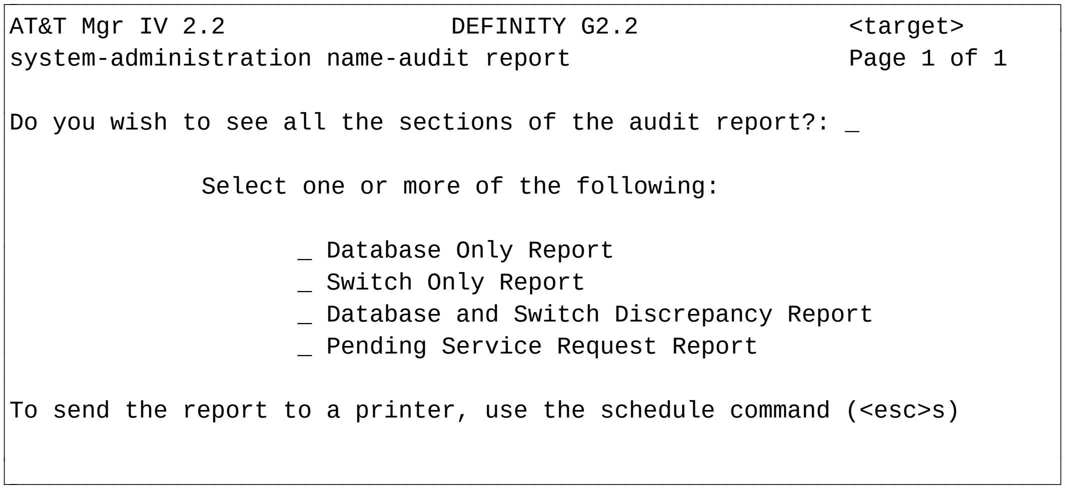
However, if **name-audit start** did not complete the entire range of extensions that you specified within the allocated time, you have two options to retrieve the remainder of the data from the switch:

- Use **name-audit run** to execute a comparison of the extensions completed at this time; then use the **name-audit start** command to process the remainder of the extensions to be audited.
- Use **name-audit restart** to continue retrieving the data from the switch. The audit will automatically restart at the extension at which it left off, and you can perform a **name-audit run** when the restart is successful.

6. Use the **name-audit status-display** command to display the status of the audit and whether it was successful or not. If the audit was successful, a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any major errors occurred, you may decide that the audit needs to be rerun. An error will generate a specific error message and will be given when the **name-audit status-display** command is executed following the statistics.

   Note: The **name-audit status-display** command can be invoked at any time during a start, restart, or run. If you attempt to use the **status-display** command before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to be displayed. (Maybe need to start or run audit?)"

7. Use **name-audit report** to check for any discrepancies or errors while using the **name-audit run** command. This command will print both auout and austat report files.



```
AT&T Mgr IV 2.2               DEFINITY G2.2              <target>
system-administration name-audit report                  Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:

                   _ Database Only Report
                   _ Switch Only Report
                   _ Database and Switch Discrepancy Report
                   _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

   If you enter **n** to the question "Do you wish to see all the sections of the audit report?" select one or more of the subsequent choices.

8. Press ESC **e** to execute the audit report, or press ESC **s** to send the report to a printer.

   CAUTION: Copy or move the four auout files and austat file from the $WORK/dbdata directory to a separate directory (refer to "Interpreting Result Files" earlier in this chapter for file-naming conventions). This will prevent these files from being overwritten when this audit is started again or another audit is started. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Name Results Files

The following screen appears only if the time limit has been reached; otherwise you will see the message "Please use results display to view the file resultsname<pbxid>."

After running **name-audit start**, the following screen appears:

```
AT&T Mgr IV 2.2               DEFINITY G2.2            <target>
system-administration name-audit start
Reached end of time limit - Either restart for rest of range
OR run for range completed so far.
Audit left off at:  50559
Please use results display to view the file resultsname<pbxid>.
```

Name Audit: Start Successful

The following is an example of the results file from a **start** if it was successful:

```
AT&T Mgr IV 2.2              DEFINITY G2.2             <target>
system-administration results display
opened file $WORK/dbdata/auname.t340 pbxid 34
opened file $WORK/dbdata/namerestart34 pbxid 34
AUDIT started at 07/20/88 09:54:51 pbx 34 beg -99 end -99
AUDIT completed
```

Name Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

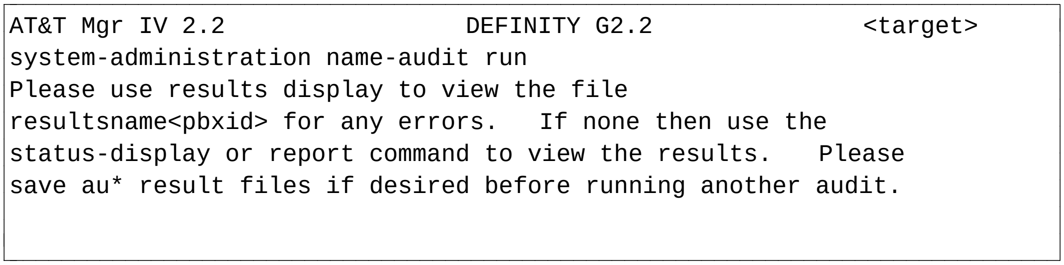
```
              * * * * CONNECTION FAILED * * * *
      Please use results display to view the file resultsname#
```

The following is an example of the results file if the **start** was unsuccessful. This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.

```
prtdial : call failed <phone number>
dialing failed
No connection made to pbx.
```

Name Audit: Run

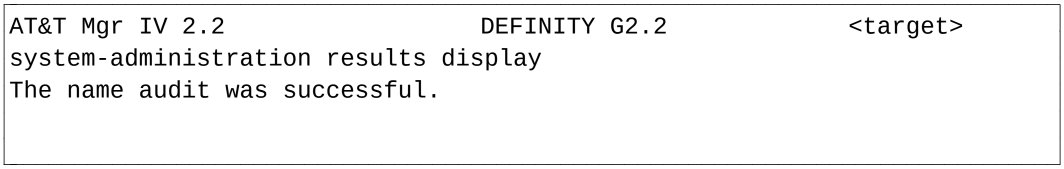
After running **name-audit run** the following screen appears:



```
AT&T Mgr IV 2.2                 DEFINITY G2.2              <target>
system-administration name-audit run
Please use results display to view the file
resultsname<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Name Audit: Run Successful

The following is an example of the results file if the **run** was successful:



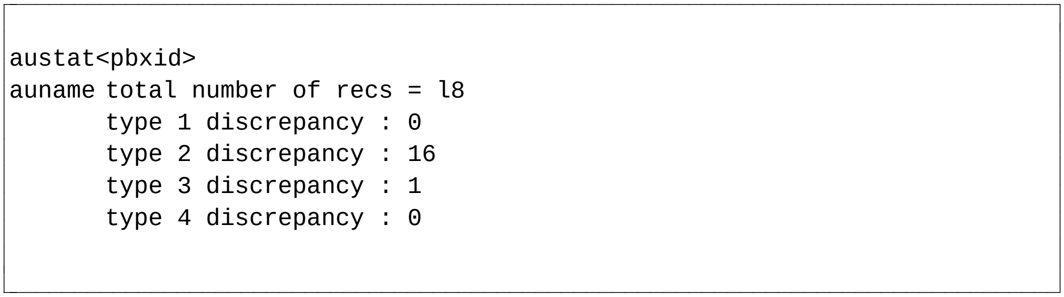
```
AT&T Mgr IV 2.2                  DEFINITY G2.2            <target>
system-administration results display
The name audit was successful.
```

Name Audit: austat

The **austat** file contains statistics indicating the total number of records audited and the number of discrepancies reported in the other files. Use the **status-display** command to view the results.

This report file has a pbxid number appended onto the file name. For example, a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid>file:



```
austat<pbxid>
auname total number of recs = l8
       type 1 discrepancy : 0
       type 2 discrepancy : 16
       type 3 discrepancy : 1
       type 4 discrepancy : 0
```

Name Audit: auoutn

There are four auoutn files. All these report files have a pbxid number appended onto the file name. For example, pbxid of 2 would generate auout12n, auout22n, auout32n and auout42n.

- Auout1n contains records that are in the database, not in the product.
- Auout2n contains records that are in the product, not in the database.
- Auout3n contains records where the database and product records do not match.
- Auout4n contains type 1 and 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2n<pbxid>file:

AUOUT2N

```


Product Reports:
Object              Verb            Label                      Data
-------------------------------------------------------------------------
extension           add          Extension No                10000
                                 Name Display                    y


Object              Verb            Label                      Data
-------------------------------------------------------------------------
extension           add          Extension No                10001
                                 Name Display                    n


Object              Verb            Label                      Data
-------------------------------------------------------------------------
extension           add          Extension No                10002
                                 Name Display                    y


```

AUOUT3N

```
Database Reports:
Object              Verb            Label                      Data
-------------------------------------------------------------------------
extension           change       Extension No                10124
                                 Name Display                    n
Product Reports:
Object              Verb            Label                      Data
-------------------------------------------------------------------------
extension           change       Extension No                10124
                                 Name Display                    y
```

TERMINAL AUDIT

The terminal audit compares the station equipment locations for all terminals between the System 85 switch and the Manager IV database. Primarily, this audit will report discrepancies in the database, but not in the switch.

Terminal Audit: Command List

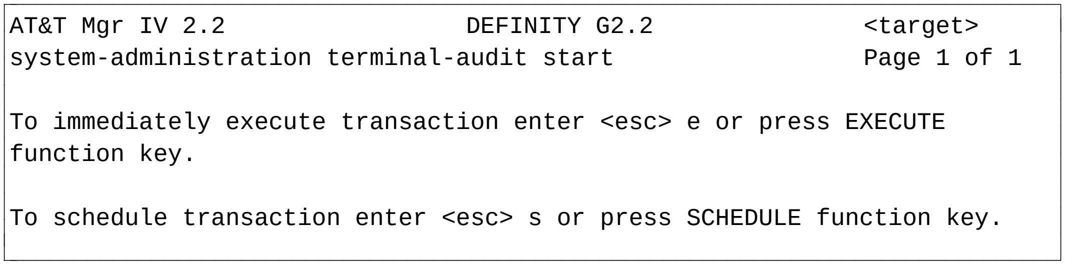
One complete cycle for a terminal audit would be the following:

- **terminal-audit start**
- **terminal-audit restart** (only if all the data is not retrieved)
- **terminal-audit run**
- **terminal-audit status-display**
- **terminal-audit report**

Procedure: Starting a Terminal Audit

Command: system-administration terminal-audit start

1. Enter **terminal audit start** to retrieve the equipment locations for *all* terminals from the switch.



```
AT&T Mgr IV 2.2                 DEFINITY G2.2                <target>
system-administration terminal-audit start                   Page 1 of 1

To immediately execute transaction enter <esc> e or press EXECUTE
function key.

To schedule transaction enter <esc> s or press SCHEDULE function key.
```

Note: This audit only takes about 1 to 2 hours to complete; therefore, no time limit is requested.

2. Press **ESC** **e** to execute the audit immediately, or press **ESC** **s** to schedule the audit for an off-peak time.
3. After the start command has executed successfully, use the **terminal-audit run** command to execute the comparison between the switch and the database.

Note: However, if the start command did not complete retrieving the data from the switch and an error message appears in the results file, you have the following options to retrieve the remainder of the data:

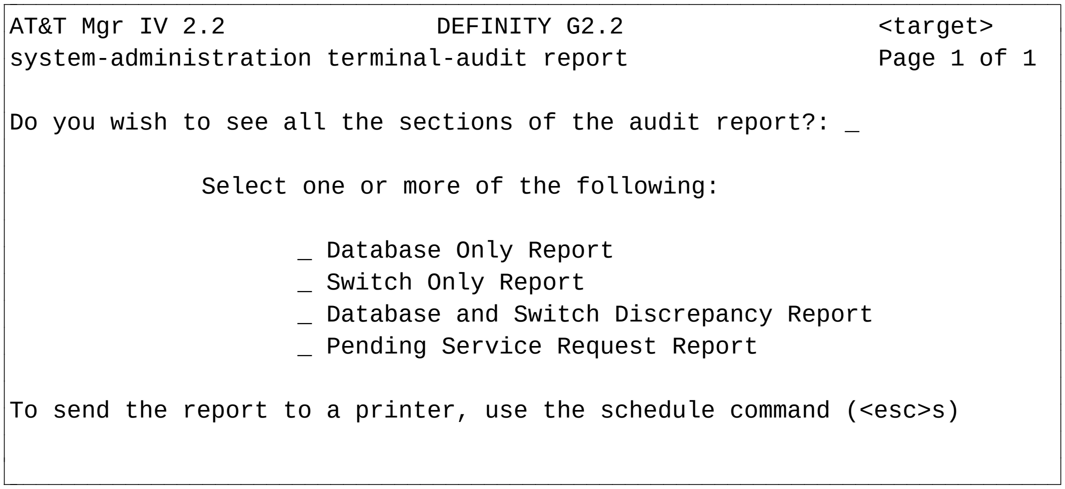
- Use the **terminal-audit restart** command to continue retrieving the data from the switch.
- Start from the beginning using the **terminal-audit start** command.

For example, if a line drop occurred, this could truncate the retrieving of all the data from the switch. An unsuccessful message would appear in the results file.

4. Use the **terminal-audit status-display** command to display the status of the audit and whether it was successful or not. If the audit was successful a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors occurred, you may decide that the audit needs to be rerun. Each error will generate a specific error message when the **terminal-audit status-display** command is executed.

   Note: The **terminal-audit status-display** command can be invoked at any time during a start, restart, or run. If you attempt to use the **status-display** command before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to be displayed. (Maybe need to start or run audit?)"

5. Use **terminal-audit report** to check for any discrepancies or errors after successfully using the **terminal-audit run** command. This command will print both auout and austat report files.



```
AT&T Mgr IV 2.2              DEFINITY G2.2                 <target>
system-administration terminal-audit report                Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:

                   _ Database Only Report
                   _ Switch Only Report
                   _ Database and Switch Discrepancy Report
                   _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

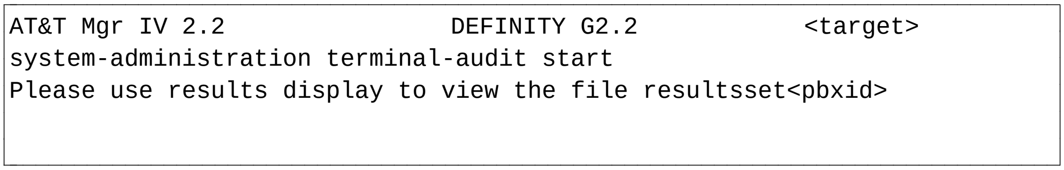
If you enter **n** to the question "Do you wish to see all the sections of the audit report?" select one or more of the subsequent choices.

6. Press **ESC** **e** to execute the audit report or press **ESC** **s** to send the report to a printer.

   CAUTION: After completion of the report, copy or move the four auout files and austat file from the $WORK/dbdata directory to a separate directory (refer to "Interpreting Result Files" earlier in this chapter for file-naming conventions). This will prevent these files from being overwritten when this audit is started again or another audit is started. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Terminal Results Files

After running **terminal-audit start**, the following screen appears:



```
AT&T Mgr IV 2.2               DEFINITY G2.2           <target>
system-administration terminal-audit start
Please use results display to view the file resultsset<pbxid>
```

Terminal Audit: Start Successful

The following is an example of the results file from a **start** if it was successful:

```
AT&T Mgr IV 2.2               DEFINITY G2.2            <target>
system-administration results display
AUDIT started at 07/20/88 14:03:56
Completed all sets.
AUDIT completed.
```

Terminal Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

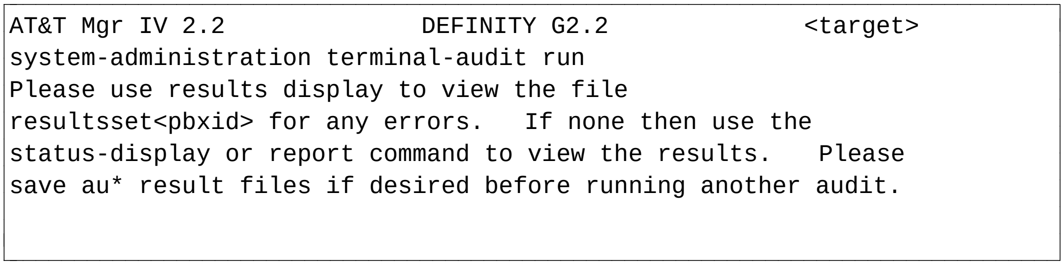
```
          * * * *CONNECTION FAILED * * * *
Please use results display to view the file resultsset#
```

The following is an example of the results file if the **start** was unsuccessful. This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.

```
prtdial: call failed <phone number>
dialing failed
No connection made to pbx.
```

Terminal Audit: Run

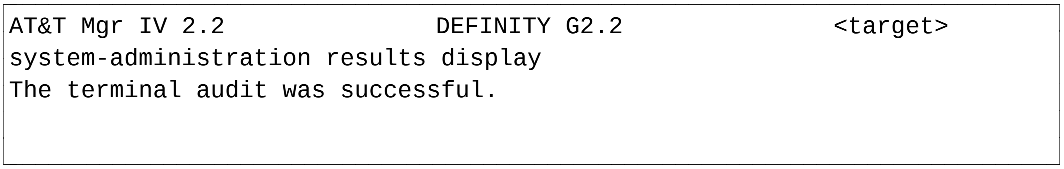
After running **terminal-audit run**, the following screen appears:



```
AT&T Mgr IV 2.2              DEFINITY G2.2              <target>
system-administration terminal-audit run
Please use results display to view the file
resultsset<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Terminal Audit: Run Successful

The following is an example of the results file if the **run** was successful.



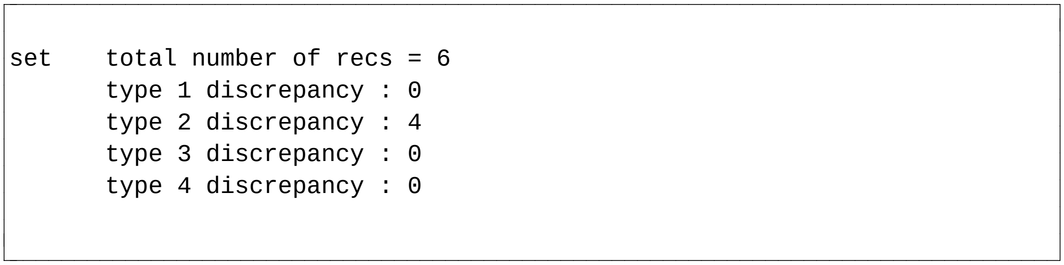
```
AT&T Mgr IV 2.2               DEFINITY G2.2               <target>
system-administration results display
The terminal audit was successful.
```

Terminal Audit Report: austat

The status display and austat file contain statistics indicating the total number of records audited and the number of discrepancies reported in the other files.

This file has a pbxid number appended onto the file name. For example a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid> file:



```
set    total number of recs = 6
       type 1 discrepancy : 0
       type 2 discrepancy : 4
       type 3 discrepancy : 0
       type 4 discrepancy : 0
```

Terminal Audit: auouts

There are four auouts files. All these report files have a pbxid number appended onto the file name. For example, pbxid of 2 would be auout12s, auout22s, auout32s and auout42s.

- Auout1s contains records that are in the database and not in the product.
- Auout2s contains records that are in the product, but not in the database.
- Auout3s contains records where the database and product records do not match.
- Auout4s contains type 1 and type 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2s<pbxid>file:

AUOUT2s

```
Product Reports:
Object                     Verb         Label                Data
----------------------------------------------------------------------
sets/trk/ucd-grp           add       ELL                 0031030
Object                     Verb         Label                Data
----------------------------------------------------------------------
sets/trk/ucd-grp           add       ELL                 0031032
Object                     Verb         Label                Data
----------------------------------------------------------------------
sets/trk/ucd-grp           add       ELL                 0211001
Object                     Verb         Label                Data
----------------------------------------------------------------------
sets/trk/ucd-grp           add       ELL                 0211003
```

TRUNK AUDIT

The **trk-audit** compares the trunk group number and the corresponding equipment locations for the specified range of trunk groups between the System 85 switch and the Manager IV database.

Trunk Audit: Command List

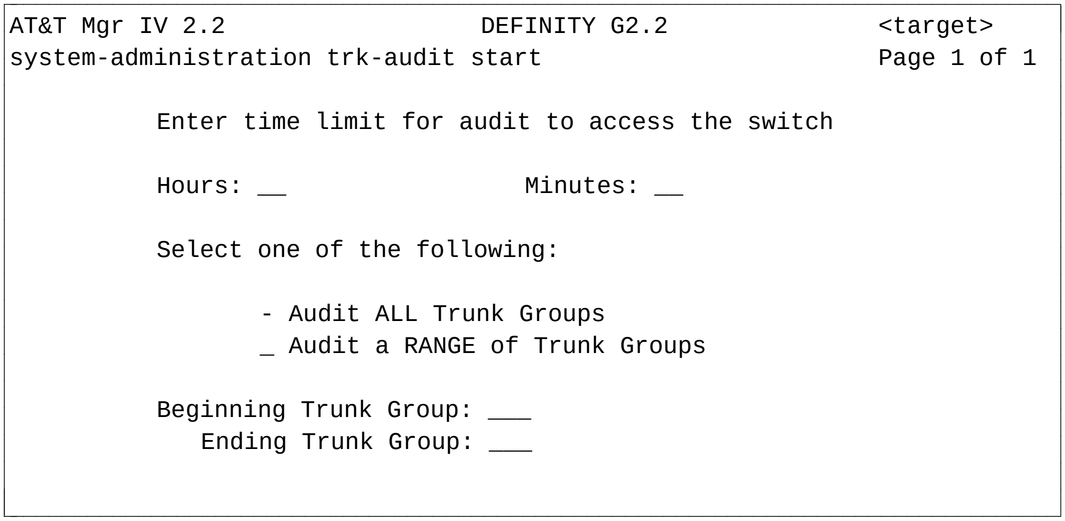
One complete cycle for a trunk audit would be in the following order:

- **trk-audit start**
- **trk-audit restart** (only if all the data is not retrieved)
- **trk-audit run**
- **trk-audit status-display**
- **trk-audit report**

Procedure: Starting a Trunk Audit

Command: system-administration trk-audit start

1. Enter **trk-audit start** to retrieve equipment locations for the specified trunk groups from the switch.



```
AT&T Mgr IV 2.2                 DEFINITY G2.2               <target>
system-administration trk-audit start                       Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __                 Minutes: __

          Select one of the following:

                 - Audit ALL Trunk Groups
                 _ Audit a RANGE of Trunk Groups

          Beginning Trunk Group: ___
             Ending Trunk Group: ___
```

2. Enter either the number of hours, number of minutes, or both for the audit to run. Valid entries are from **0** - **23** for hours; **0** - **59** for minutes.
3. Choose either to Audit All or a Range of Trunk Groups. If you choose the latter, enter a Beginning and Ending Trunk Group number. Valid entries are from **18** - **999** for both fields.
4. Press **ESC** **e** to execute the audit immediately or press **ESC** **s** to schedule the audit for an off-peak time.

5. If the **trk-audit start** command completed successfully for the range of trunks specified, then use the **trk-audit run** command to execute the comparison between the switch and the database. However, if the **trk-audit start** command did not complete the entire range of trunks specified within the allocated time, you then have two options to retrieve the remainder of the data from the switch:

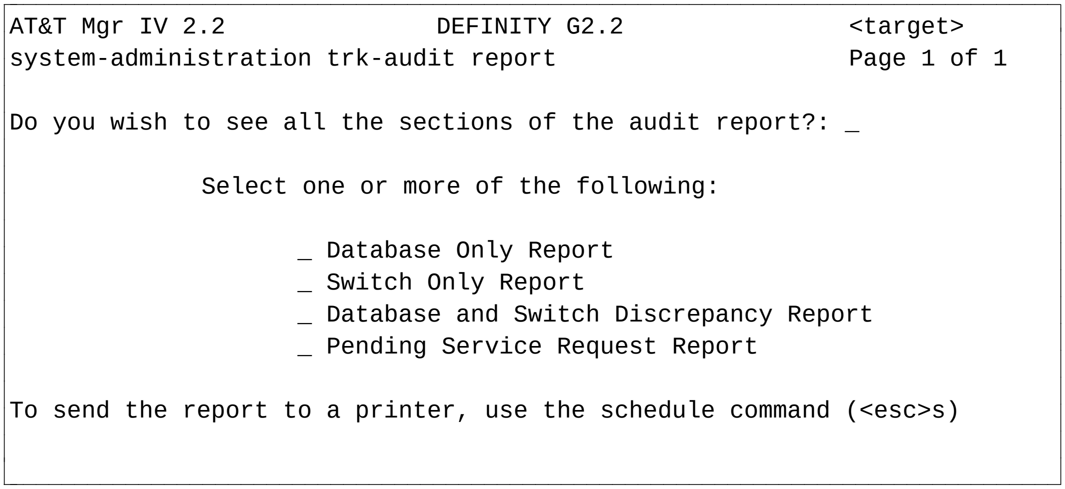
   - Use the **trk-audit run** command to execute a comparison of the trunks completed at this time, then use the **trk-audit start** command to process the remainder of the trunks to be audited.

   - You can also use the **trk-audit restart** command to continue retrieving the data from the switch. The audit will automatically restart at the trunk group at which it left off, and you can perform a **trk audit run** when the restart is successful.

6. Use the **trk-audit status-display** command to display the status of the audit and whether it was successful or not. If the audit was successful then a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors did occur, you may decide that the audit needs to be rerun. Each error will generate a specific error message and will be given when the **trk-audit status-display** command is executed.

   Note: The **trk-audit status-display** command can be invoked at any time during a start, restart or run. If you attempt to use the **status-display** command before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to be displayed. (Maybe need to start or run audit?)"

7. Use **trk-audit report** to check for any discrepancies or errors after successfully using the **trk-audit run** command. This command will print both auout and austat report files.



```
AT&T Mgr IV 2.2              DEFINITY G2.2              <target>
system-administration trk-audit report                  Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:

                    _ Database Only Report
                    _ Switch Only Report
                    _ Database and Switch Discrepancy Report
                    _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

   If you enter **n** to the question "Do you wish to see all the sections of the audit report?" select one or more of the subsequent choices.

8. Press **ESC** **e** to execute the audit report or press **ESC** **s** to send the report to a printer.

   CAUTION: Copy or move the four auout files and austat file from the $WORK/dbdata directory and to a separate directory (refer to "Interpreting Result Files" earlier in this chapter for file-naming conventions). This will prevent these files from being overwritten when this audit or another audit is started again. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Trunk Results Files

After running **trk-audit start**, the following screen appears:

```
AT&T Mgr IV 2.2               DEFINITY G2.2                <target>
system-administration trk-audit start
Please use results display to view the file resultstrk<pbxid>
```

Trunk Audit: Start Successful

The following is an example of the results file from a **start** if it was successful:

```
AT&T Mgr IV 2.2                 DEFINITY G2.2              <target>
system-administration results display
opened file $WORK/dbdata/autrk.t340 pbxid 34
opened file $WORK/dbdata/trkrestart34 pbxid 34
AUDIT started at 07/20/88 14:41:15 pbx 34 beg 18 end 999
AUDIT completed
```

Trunk Audits: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

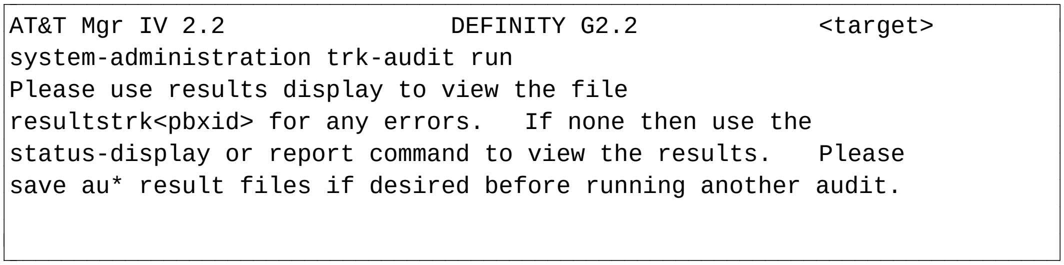
```
         * * * * CONNECTION FAILED * * * *
Please use results display to view the file resultstrk#
```

The following is an example of the results file if a **start** was unsuccessful. This message might differ slightly than what is presented below if the start failed for some reason other than busy.

```
prtdial: call failed <phone number>
dialing failed
No connection made to pbx.
```

Trunk Audit: Run

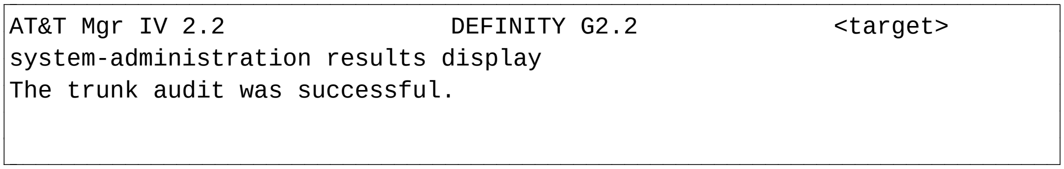
After running **trk-audit run** the following screen appears:



```
AT&T Mgr IV 2.2                DEFINITY G2.2            <target>
system-administration trk-audit run
Please use results display to view the file
resultstrk<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Trunk Audit: Run Successful

The following is an example of the results file if the **run** step was successful:



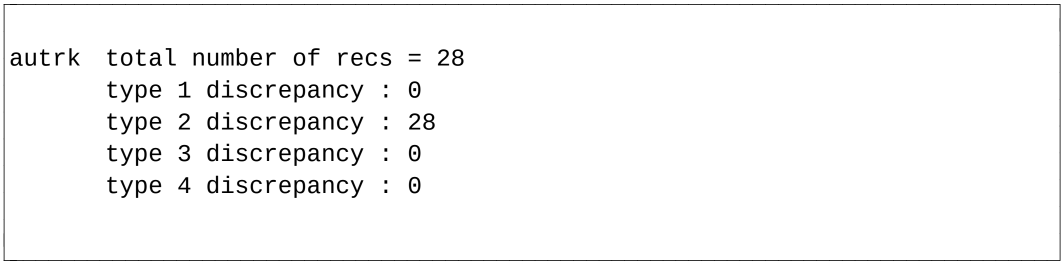
```
AT&T Mgr IV 2.2                DEFINITY G2.2             <target>
system-administration results display
The trunk audit was successful.
```

Trunk Audit: austat

The **austat** file contains statistics indicating the total number of records audited and the number of discrepancies reported in the other files. Use the **status-display** command to view the results.

This report file has a pbxid number appended onto the file name. For example, a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid>file:



```
autrk  total number of recs = 28
       type 1 discrepancy : 0
       type 2 discrepancy : 28
       type 3 discrepancy : 0
       type 4 discrepancy : 0
```

Trunk Audit: auoutt

There are four auoutt files. All these report files have a pbxid number appended onto the file name. For example, a pbxid of 2 would generate auout12t, auout22t, auout32t and auout42t.

- Auout1t contains records that are in the database, not in the product.
- Auout2t contains records that are in the product, not in the database.
- Auout3t contains records where the database and product records do not match.
- Auout4t contains type 1 and 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2t<pbxid>file:

```
Object           Verb           Label                       Data
--------------------------------------------------------------------------
trk              add         ELL                        0002021
                             Trunk Group #                   25

Object        Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0002022
                             Trunk Group #                   26

Object           Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0002050
                             Trunk Group #                   32

Object           Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0002051
                             Trunk Group #                   32

Object           Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0002080
                             Trunk Group #                   38

Object           Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0003050
                             Trunk Group #                  150

Object           Verb           Label                      Data
--------------------------------------------------------------------------
trk              add         ELL                        0003051
                             Trunk Group #                  150
Object              Verb         Label                     Data
-------------------------------------------------------------------------
sets/trk/ucd-grp    add       ELL                       0211003
```

TRUNK GROUP AUDIT

The **trk-grp-audit** compares the trunk group number, dial access code, and trunk type for the specified range of trunk groups between the System 85 switch and the Manager IV database.

Trunk Group Audit: Command List

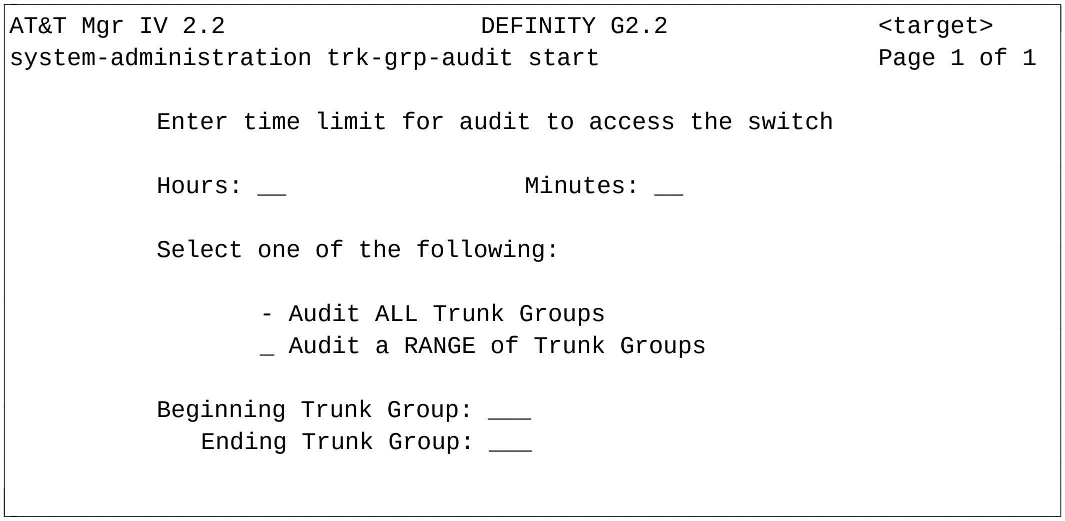
One complete cycle for a trunk group audit would be in the following order:

- **trk-grp-audit start**
- **trk-grp-audit restart** (only if all the data is not retrieved)
- **trk-grp-audit run**
- **trk-grp-audit status-display**
- **trk-grp-audit report**

Procedure: Starting a Trunk Group Audit

Command: system-administration trk-grp-audit start

1. Enter **trk-grp-audit start** to retrieve the trunk data from the switch for the specified trunk groups. The data includes:
   - trunk group number
   - dial access code
   - trunk type



```
AT&T Mgr IV 2.2                  DEFINITY G2.2              <target>
system-administration trk-grp-audit start                   Page 1 of 1

          Enter time limit for audit to access the switch

          Hours: __                 Minutes: __

          Select one of the following:

                 - Audit ALL Trunk Groups
                 _ Audit a RANGE of Trunk Groups

          Beginning Trunk Group: ___
             Ending Trunk Group: ___
```

2. Enter the number of hours, number of minutes, or both for the audit to run. Valid entries are from **0** - **23** for hours; **0** - **59** for minutes.
3. Choose either to audit all or a range of trunk groups. If you choose the latter, enter a Beginning and Ending Trunk Group number. Valid entries are from **18** - **999** for both fields.

4. Press **ESC** **e** to execute the audit immediately or press **ESC** **s** to schedule the audit for an off-peak time.

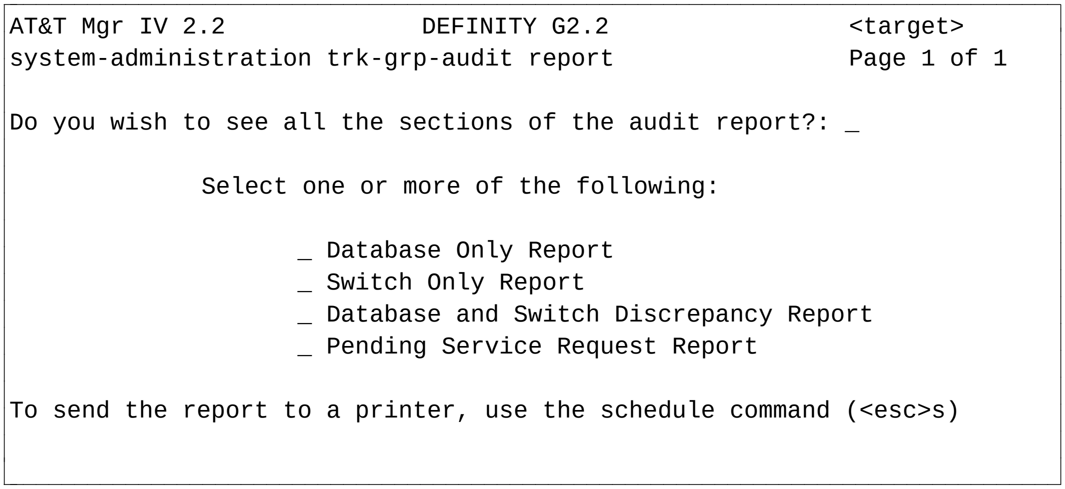
5. If the **trk-grp-audit start** command completed successfully for the range of trunk groups specified, use the **trk-grp-audit run** command to execute the comparison between the switch and the database. However, if the **trk-grp-audit start** command did not complete the entire range of trunk groups specified within the allocated time, you have two options to retrieve the remainder of the data from the switch:

   - Use the **trk-grp-audit run** command to execute a comparison of trunks completed at this time; then use the **trk-grp-audit start** command to process the remainder of trunks to be audited.
   - Use the **trk-grp-audit restart** command to continue retrieving the data from the switch. The audit will automatically restart at the trunk group at which it left off, and you can perform a **trk-grp-audit run** when the restart is successful.

6. Use the **trk-grp-audit status-display** command to display the status of the audit and whether it was successful or not. If the audit was successful, a statistics summary will be displayed indicating the number of records audited and the number of discrepancies, if any. If any switch errors occurred, you may decide that the audit needs to be rerun. Each error will generate a specific error message and will be given when the **trk-grp-audit status-display** command is executed.

   Note: The **trk-grp-audit status-display** command can be invoked at any time during a start, restart or run. If you attempt to use the **status-display command** before the audit is completed, you will see the message, "Audit is still running - Please try again later." However, if you never performed a start or have performed a start but not a run, the following message appears: "Audit is not running - no $WORK/dbdata/austat<#> file to be displayed. (Maybe need to start or run audit?)"

7. Use **trk-grp-audit report** to check for any discrepancies or errors after successfully using the **trk-grp-audit run** command. This command will print both auout and austat report files.



```
AT&T Mgr IV 2.2             DEFINITY G2.2                <target>
system-administration trk-grp-audit report               Page 1 of 1

Do you wish to see all the sections of the audit report?: _

             Select one or more of the following:

                    _ Database Only Report
                    _ Switch Only Report
                    _ Database and Switch Discrepancy Report
                    _ Pending Service Request Report

To send the report to a printer, use the schedule command (<esc>s)
```

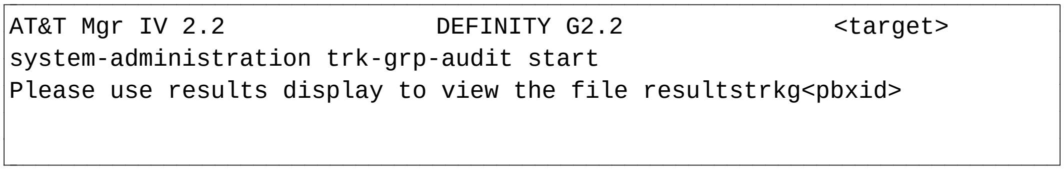
If you enter **n** to the question "Do you wish to see all the sections of the audit report?" select one or more of the subsequent choices.

8. Press **ESC** **e** to execute the audit report or press **ESC** **s** to send the report to a printer.

   CAUTION: Copy or move the four auout files and austat file from the $WORK/dbdata directory to a separate directory (refer to "Interpreting Result Files" earlier in this chapter for file-naming conventions). This will prevent the files from being overwritten when this audit or another audit is started again. Once the files have been moved, use the **cat** or **pr** command to view the files.

Interpreting Trunk Group Audit Results Files

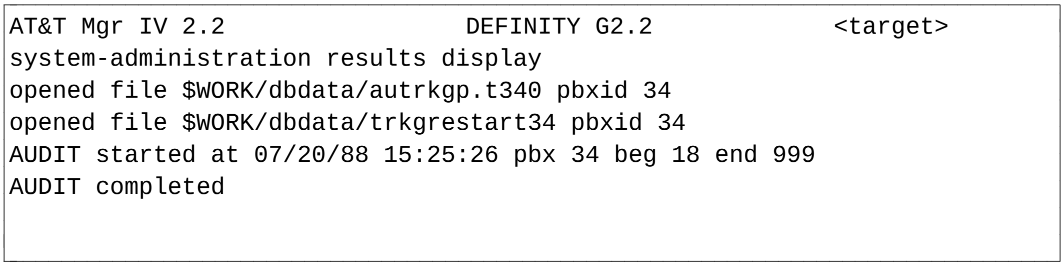
After running **trk-grp start**, the following screen appears:



```
AT&T Mgr IV 2.2               DEFINITY G2.2              <target>
system-administration trk-grp-audit start
Please use results display to view the file resultstrkg<pbxid>
```

Trunk Group Audit: Start Successful

The following is an example of the results file if a **start** was successful:



```
AT&T Mgr IV 2.2                 DEFINITY G2.2            <target>
system-administration results display
opened file $WORK/dbdata/autrkgp.t340 pbxid 34
opened file $WORK/dbdata/trkgrestart34 pbxid 34
AUDIT started at 07/20/88 15:25:26 pbx 34 beg 18 end 999
AUDIT completed
```

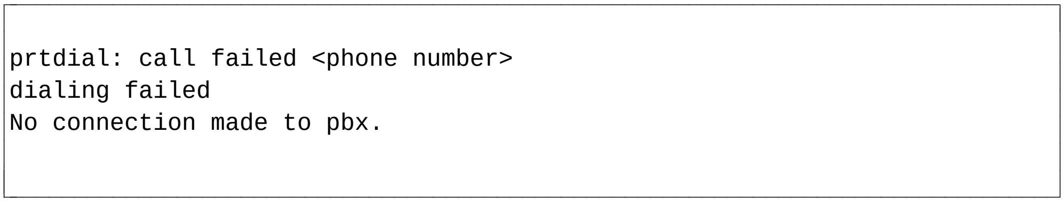
Trunk Group Audit: Start Unsuccessful

It may take several minutes to determine that the **start** was unsuccessful, because if the product is in use, the audit program will make several attempts to redial the product.

Note: If the start is unsuccessful, the original transaction screen will show the following message:

```
            * * * *CONNECTION FAILED* * * *
Please use results display to view the file resultstrkg#
```

The following is an example of the results file if a **start** was unsuccessful. This message might differ slightly than what is presented below if the **start** failed for some reason other than busy.



```
prtdial: call failed <phone number>
dialing failed
No connection made to pbx.
```

Trunk Group Audit: Run

After running **trk-grp-audit run**, the following screen appears:

```
AT&T Mgr IV 2.2              DEFINITY G2.2            <target>
system-administration trk-grp-audit run
Please use results display to view the file
resultstrkg<pbxid> for any errors.   If none then use the
status-display or report command to view the results.   Please
save au* result files if desired before running another audit.
```

Trunk Group Audit: Run Successful

The following is an example of the results file if the **run** step was successful:

```
AT&T Mgr IV 2.2             DEFINITY G2.2              <target>
system-administration results display
The trunk group audit was successful.
```

Trunk Group Report: austat

The **austat** file contains statistics indicating the total number of records audited and the number of discrepancies reported in the other files. Use the **status-display** command to view the results.

This file has a pbxid number appended onto the file name. For example, a pbxid of 2 would generate an austat2 file.

The following is an example of the $WORK/dbdata/austat<pbxid> file:

```
autrkgp      total number of recs = 66
       type 1 discrepancy : 0
       type 2 discrepancy : 66
       type 3 discrepancy : 0
       type 4 discrepancy : 0
```

Trunk Group Report: auoutg

There are four auoutg files. All these report files have a pbxid number appended onto the file name. For example, a pbxid of 2 would generate auout12g, auout22g, auout32g and auout42g.

- Auout1g contains records that are in the database, not in the product.
- Auout2g contains records that are in the product, not in the database.
- Auout3g contains records where the database and product records do not match.
- Auout4g contains type 1 and 3 records that have a pending service request.

The following is an example of the $WORK/dbdata/auout2g<pbxid> file:

```
Product Reports:
Object          Verb           Label                      Data
------------------------------------------------------------------------
trk-grp         add         Trunk Group #                 100
                            Trunk Type                     20


Object          Verb           Label                      Data
------------------------------------------------------------------------
trk-grp      add         Trunk Group #                 104
                            Trunk Type                     12


Object          Verb           Label                      Data
------------------------------------------------------------------------
trk-grp         add         Trunk Group #                 114
                            Trunk Type                     15


Object          Verb           Label                      Data
------------------------------------------------------------------------
trk-grp         add         Trunk Group #                 116
                            Trunk Type                     25
```

Trunk Group Report:Auoutg - continued

```
Object          Verb           Label                       Data
------------------------------------------------------------------------
trk-grp         add         Trunk Group #                  117
                            Trunk Type                      35


Object          Verb           Label                       Data
------------------------------------------------------------------------
trk-grp          add         Trunk Group #                  120
                             Trunk Type                      46


Object          Verb           Label                       Data
------------------------------------------------------------------------
trk-grp          add         Trunk Group #                  121
                             Trunk Type                      32


Object       Verb           Label                       Data
------------------------------------------------------------------------
trk-grp          add         Trunk Group #                  122
                             Trunk Type                      46


Object           Verb           Label                       Data
------------------------------------------------------------------------
trk-grp           add         Trunk Group #                  140
                              Trunk Type                      37


Object           Verb           Label                       Data
------------------------------------------------------------------------
trk-grp           add         Trunk Group #                  150
                              Dial_access_code              #150
                              Trunk Type                      75
```

APPENDIX C: UNIVERSAL OUTWARD FEEDS

Universal Outward Feeds allow Manager IV to output selected switch and non-switch data in a standard format for use by other system management applications.

A file that resides on the Manager IV processor describes the Manager IV data of interest to each application. The specified data is output for transactions performed in administration and service request modes after the data is successfully downloaded to the switch. For switch data, the recorded information reflects the current switch image.

The updates are recorded in data transfer files that may be retrieved for processing by other applications through UNIX uucp requests.

HOW DATA IS TRANSFERRED

Data transfer files containing the specified data elements are created on a per-target basis for each external application. Each data transfer file consists of a "file header" followed by one or more "records."

- The *file header* identifies the data source (Manager IV), the machine name, the target, and the external application for which the data was produced.
- A *record* describes the data that was updated when one of the specified data files has been updated as a result of a successful download to the switch. Each record consists of a record header, the data elements output as name-value pairs, and a record trailer.

  The record header includes a record sequence number, the name of the CORE product-image database file that was updated, the operation that was performed on the record (add, change, or remove), and the date and time the data was successfully downloaded to the switch. The record sequence number is reset to "0" at the beginning of each data transfer file.

For an "add" transaction, the name-value pairs that are output reflect the new data. For a "change" transaction, both before and after images of the data are output. A "remove" transaction causes a "before" image of the data to be output.

The transfer data for each target are written to one or more files each day, depending on the amount of data to be transferred and the ulimit of the Manager IV processor. These transfer files are named **tg<pbx id>.<month><day>.<sequence number>**, where:

- **<pbx id>** is the one- to four-digit PBX ID that uniquely identifies the target to Manager IV
- **<month>** is a two-digit value between 01 and 12 identifying the month the data transfer file is created
- **<day>** is a two-digit value between 01 and 31 identifying the day the data transfer file is created
- **<sequence number>** is a two-digit value between 00 and 99. This file sequence number is reset to 00 for each target and application at the beginning of each day.

A master file listing the names of the data transfer files is created each day. This master file is named **<application>.<month>.<day>** where:

- **<application>** is the name of the external application, maximum nine characters, which is assigned to the application when its data element specification file is installed
- **<month>** is a two-digit value between 01 and 12 identifying the month the master file is installed
- **<day>** is a two-digit value between 01 and 31 identifying the day the master file is installed.

The data transfer files and master files for each application are maintained in a separate shipping directory.

Each shipping directory is a subdirectory of /usr/spool/uucppublic/smgr and is named according to the application identifier.

Manager IV automatically removes each data transfer file and master file after 10 days.

Specification of External Applications

The Manager IV System Administrator must supply specification files describing the data to be output by Universal Outward Feeds. There are two types of specification files:

- A *data element specification file* identifies the Manager IV product-image database files and fields that are of interest to another system management application. A separate data element specification file is required for each external application using Universal Outward Feeds. Multiple data element specification files may be installed, depending upon your system management needs.

  Manager IV includes a data element specification file for AT&T Cost Allocator (CA) to simplify Universal Outward Feeds setup.

- The *active target specification file* identifies the targets using Universal Outward Feeds for each external application.

Once these files are supplied, the System Administrator must install the data element specification file(s), install the active target specification file, and then enable Universal Outward Feeds.

You can edit data element specification files if information requirements for a particular application should change. However, the revised data element specification file is not active until you re-enable Universal Outward Feeds.

You can request a report listing the installed active target and data element specification files, and you can also disable Universal Outward Feeds at any time.

All of these tasks are performed using the **xiadm** command and the Universal Outward Feeds Administration menu, which are explained in "Administering Universal Outward Feeds" later in this appendix.

Format of Specification Files

The formats for data element specification files and the active target specification file are defined below.

White space (i.e. carriage returns, line feeds, spaces, and tabs) is allowed anywhere within these files and does not affect the interpretation of the data.

You can also include comments by using the pound sign (#), which causes the rest of the input line to be ignored.

Data Element Specification Files

You must supply a data element specification file for each external application using Universal Outward Feeds. A data element specification file consists of one or more select statements. Each select statement consists of the following:

- the keyword "select"
- a list of one or more field names (e.g., "namdb"), separated by commas

  The list of fields for each file may optionally be enclosed in curly brackets and must include the file’s primary key. (The primary key of a file is the field in the file whose value must be unique for each record.)

  If all the fields in a given file are of interest to the application, you can substitute the keyword "all_fields" for a list of the actual field names.

- the keyword "from"
- a Manager IV database file name (e.g. "extn")

A sample file appears below:

```
# Sample Data Element Specification File

# Select Extension File (extn) Fields

select  {
         extn,  #  Extension Number (primary key)
         namdb, #  User Name
         lwcds, #  Leave Word Calling Destination
         ap     #  AP Number
} from extn

# Select All Fields from the Set File (set)

select all_fields from set
```

The Active Target Specification File

The active target specification file identifies the targets of interest to each system management application. This file consists of one or more activate statements. Each "activate" statement consists of the following:

- the keyword "activate"
- an application identifier (maximum nine alphanumeric characters)
- the keyword "for"
- one or more target names, separated by commas

  The list of target names for each application may optionally be enclosed in curly brackets. If all targets are of interest to a given application, the keyword "all" may be substituted for the list of target names.

Each activate statement may also be followed by an attribute clause that specifies the maximum data transfer file size in 512-byte blocks. An attribute clause consists of the following:

- the keywords "with file_limit"
- the maximum data transfer file size in 512-byte blocks

  Consult the System Administrator for each application to ensure that the size of the transfer file you specify does not exceed the ulimit of that application’s machine. If no maximum data transfer file size is specified, a default of 1024 512-byte blocks is used.

The following is a sample active target specification file for applications "CA" and "MCM" using Universal Outward Feeds:

```
#  Sample Active Target Specification File

#  Activate Application CA

activate CA for {
         nj-generic2, #  New Jersey located DEFINITY Generic 2
         nj-system85, #  New Jersey located System 85
         co-generic2  #  Colorado located DEFINITY Generic 2
}

#  Activate Application MCM for all targets with a maximum data transfer
#  file size of 2048 512-byte blocks.

activate MCM for all with file_limit 2048
```

ADMINISTERING UNIVERSAL OUTWARD FEEDS

The **xiadm** command allows you to administer the Universal Outward Feed specification files to accomplish the following tasks:

- Install a new data element specification file
- Display or retrieve an installed data element specification file
- Edit an installed data element specification file
- Install a new active target specification file
- Display or retrieve the installed active target specification file
- Edit the installed active target specification file
- Enable Universal Outward Feeds using the installed specification files
- Disable Universal Outward Feeds
- Provide a report detailing all installed specification files

Only the Manager IV System Administrator and maintenance logins (smsa and smmaint, respectively) are permitted to install or remove specification files or enable or disable Universal Outward Feeds. All users may display or retrieve specification files.

The Universal Outward Feeds Administration Menu

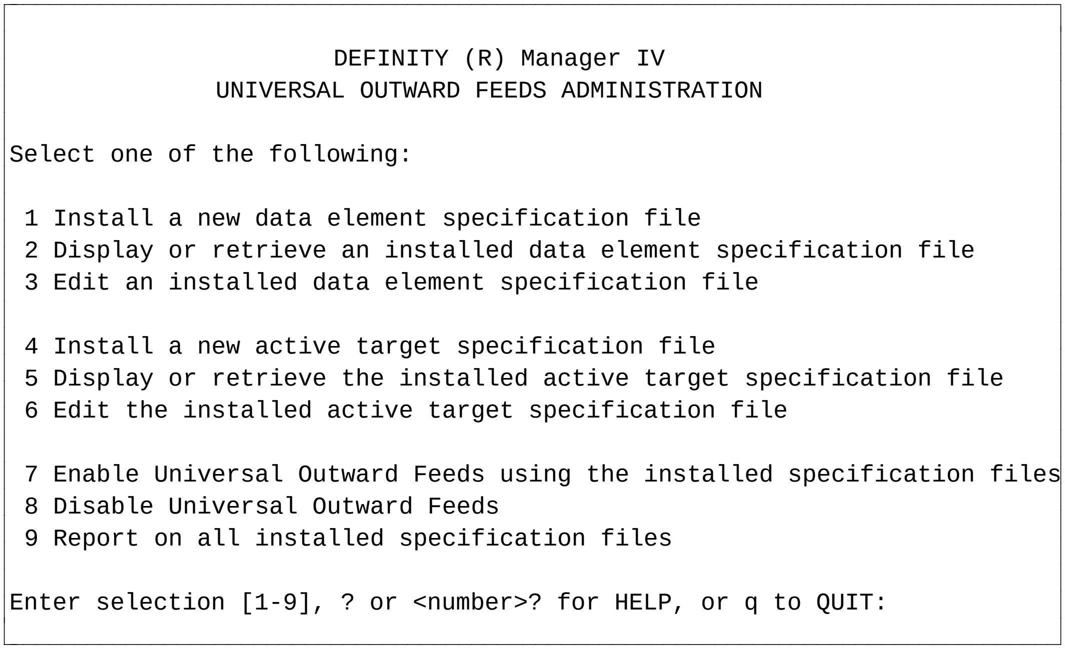
The **xiadm** command can be accessed two ways: either by typing **xiadm** and selecting a task from the Universal Outward Feeds Administration menu, or by typing the entire command line (for example, **xiadm newelements**) at the UNIX system prompt.

The command line interface provides the same capabilities as the menu interface but restricts you to performing a single task. The Universal Outward Feeds Administration menu returns you to the main menu after you complete each task.

The following procedure introduces you to the Universal Outward Feeds Administration menu.

1. Type **xiadm** at the UNIX system prompt.

   The Universal Outward Feeds Administration menu appears:



```
                        DEFINITY (R) Manager IV
                UNIVERSAL OUTWARD FEEDS ADMINISTRATION

Select one of the following:

 1 Install a new data element specification file
 2 Display or retrieve an installed data element specification file
 3 Edit an installed data element specification file

 4 Install a new active target specification file
 5 Display or retrieve the installed active target specification file
 6 Edit the installed active target specification file

 7 Enable Universal Outward Feeds using the installed specification files
 8 Disable Universal Outward Feeds
 9 Report on all installed specification files

Enter selection [1-9], ? or <number>? for HELP, or q to QUIT:
```

Manager IV prompts you to select the task from menu items numbered 1 through 9 above.

- You can administer data element specification files using options 1-3 of the **xiadm** menu.
- You can administer the active target specification file using options 4-6.
- Options 7 and 8 allow you to enable and disable Universal Outward Feeds, respectively.
- Option 9 provides a report on all installed specification files.

2. Enter the number of the task you want to perform. For example, type **3** to edit an installed data element specification file.

3. Use on-line help if you need more information.
   - Enter a question mark (**?**) at the main menu to display a general help message for the **xiadm** command.
   - Enter a menu item number followed by a question mark to display a help message for that menu item. For example, type **3?** for information about editing an installed data element specification file.

4. The system prompts you for the data needed to complete the task. After performing each task, the system returns you to the main menu.

To bypass the Universal Outward Feeds Administration menu, type **xiadm** followed by the appropriate command for the function you want to perform at the UNIX system prompt. For example, enter **xiadm chgelements** to change (edit) an installed data element specification file.

Table C-1 provides complete **xiadm** commands.

Table C-1: xiadm Command Summary

Menu Option	Command	Explanation
1	**xiadm newelements [file]**	Installs a new data element specification file. If a file name is not provided, you are prompted to enter one.
2	**xiadm getelements [id [file]]**	Retrieves an existing data element specification file. If an id is not provided, you are prompted to enter one. If a file name is provided, the output is written to the file; otherwise, the output is written to the screen.
3	**xiadm chgelements [id [editor]]**	Edits an existing data element specification file. If an editor is not provided, the vi editor is invoked.
4	**xiadm newtargets [file]**	Installs a new active target specification file. If a file name is not provided, you are prompted to enter one.
5	**xiadm gettargets [file]**	Retrieves the current active target specification file. If a file name is provided, the output is written to the screen.
6	**xiadm chgtargets [editor]**	Edits the active target specification file. If an editor is not provided, the vi editor is invoked.
7	**xiadm enable**	Enables/re-enables Universal Outward Feeds using the installed specification files.
8	**xiadm disable**	Disables Universal Outward Feeds without affecting the installed specification files.
9	**xiadm report [file]**	Provides a report detailing all specification files. If a file name is provided, the output is written to the file; otherwise, the output is written to the screen.

The following sections explain each of the tasks and commands in the Universal Outward Feeds Administration menu.

Procedure: Installing a New Data Element Specification File

Command: $ xiadm newelements

This option allows you to install a new data element file or overwrite an existing data element file. Before running this command, you must create an ASCII file containing the data element specification. (See "Specification of External Applications" earlier in this appendix.)

1. Enter **xiadm newelements** at the UNIX system prompt, or type **xiadm** and select **1** at the Universal Outward Feeds Administration menu.

   You are prompted for the application identifier for the new data specification file.

2. Enter a one- to nine-character alphanumeric application identifier.

   - If you enter an application identifier for a new data element specification file, go to step 3.
   - If you enter an application identifier for an existing data element specification file, a warning message displays and you must verify that the file is to be overwritten with the new specification.

     The message displayed depends on whether you entered a customer-defined or predefined application identifier.

     — If you enter an application identifier for a customer-defined data element specification file, the **xiadm** command displays this warning message:

     ```
     WARNING: A data element specification file is already installed for this
              application identifier.

     Do you wish to overwrite the installed data element specification file for
     this application identifier? (default n) [y, n]:
     ```

     — If you enter an application identifier for a pre-defined data element specification file such as CA (for Cost Allocator), the following warning message appears:

     ```
     WARNING: A data element specification file is already installed for this
              application identifier.

              Because this application requires the transfer of specific data
              elements, overwriting the data element specification file for
              this application may cause unpredictable results.

     Do you wish to overwrite the installed data element specification file for
     this application identifier? (default n) [y, n]:
     ```

   Enter **y** at the warning message to overwrite the installed data element specification file.

3. System response:

   ```
   Enter the name of the file that contains the new data element specification,
   or q to QUIT:
   ```

4. Enter the name of the file containing the new data element specification, or type **q** to quit.

   The system validates the contents of the designated file against the Manager IV product-image database. If no errors are present, the file is installed; otherwise, you are informed of any errors and instructed to correct them before attempting to install the file again.

5. [In menu mode only] If you exit the Universal Outward Feeds Administration menu after installing or updating one or more specification files but do not re-enable Universal Outward Feeds (see "Procedure: Enabling Universal Outward Feeds" in this appendix), the system prompts you to determine whether the latest specification files should be used:

   System response:

   ```
   Do you wish to re-enable Universal Outward Feeds using the new specification
   file(s) before exiting? (default y) [y, n]:
   ```

   - If you answer **y**, Universal Outward Feeds is enabled or re-enabled with the new specifications.
   - If you answer **n**, the old specification remains active until Universal Outward Feeds is enabled or re-enabled.

Procedure: Displaying an Installed Data Element Specification File

Command: $ xiadm getelements

This procedure explains how to display an installed data element specification file one page at a time, or write an installed data element specification file to an ASCII file.

1. Type **xiadm getelements** at the UNIX system prompt, or type **xiadm** and select **2** from the Universal Outward Feeds Administration menu.
2. An alphabetized list of application identifiers such as the following appears:

   ```
    Select one of the following application identifiers:

            1  CA
            2  MCM

    Enter selection [1-2], or q to QUIT:
   ```

   This list includes all pre-defined and customer-defined application identifiers.
3. Enter the number of the application identifier you wish to display or retrieve, or type **q** to quit.

   System response:

   ```
   Enter output file name, or press RETURN to view the file directly:
   ```

   - If you enter an output file name, the data element specification file for the selected application identifier is copied to the named file.
   - Or press **RETURN** to display the data element specification file a page at a time on your screen.

Procedure: Editing an Installed Data Element Specification File

Command: $ xiadm chgelements

Use the following procedure to edit an installed data element specification file. A specification file with one or more errors may not be installed.

1. Type **xiadm chgelements**, or type **xiadm** and select **3** from the Universal Outward Feeds Administration menu.
2. An alphabetized list of application identifiers such as the following appears:

   ```
    Select one of the following application identifiers:

             1  CA
             2  MCM

    Enter selection [1-2], or q to QUIT:
   ```

   This list includes all pre-defined and customer-defined application identifiers.

3. Enter the number of the application identifier you wish to edit.

   - If you select a pre-defined application identifier, you see the following warning message, and you are required to verify that the file should be edited:

   ```
   WARNING: Because this application requires the transfer of specific
            data elements, editing the data element specification file for
            this application may cause unpredictable results.

   Do you wish to continue? (default n) [y, n]:
   ```

   - Press **RETURN** to stop the procedure, or type **y** to continue.

4. If you selected a customer-defined application identifier, or entered **y** after the warning message in step 3 above, the system prompts you to select an editor.

   ```
   Select editor (default vi) [ed, vi]:
   ```

   Select the default "vi" editor, or type **ed.**

   - Check the value of your **$editor** environment variable to determine your default editor. If this variable is not set to either "ed" or "vi," "vi" is the default.

5. Once you select an editor, the selected data element specification file is copied to a temporary file and the editor is invoked. When you have finished editing the temporary file, the system evaluates its contents.

   - If no errors are present, the new specification file is installed.
   - If errors are present, the system informs you of the error and asks you to either re-edit the file or discard the edited file.

6. [In menu mode only] If you exit the Universal Outward Feeds Administration menu after installing or updating one or more specification files but do not re-enable Universal Outward Feeds (See "Procedure: Enabling Universal Outward Feeds" in this appendix), the system prompts you to determine whether the latest specification files should be used:

   System response:

   ```
   Do you wish to re-enable Universal Outward Feeds using the new specification
   file(s) before editing? (default y) [y, n]:
   ```

   - If you answer **y**, Universal Outward Feeds is enabled or re-enabled with the new specification.
   - If you answer **n**, the old specification remains active until Universal Outward Feeds is re-enabled.

Procedure: Installing a New Active Target Specification File

Command: $ xiadm newtargets

Selecting this option allows you to install a new active target specification file or overwrite the existing active target specification file.

Before running this command, you must install the data element specification file for each application, and create an ASCII file containing the active target specification. See "Specification of External Applications" earlier in this appendix.

Only the System Administrator can install an active target specification file. An active target specification file with errors may not be installed.

1. Type **xiadm newtargets**, or type **xiadm** and select **4** from the Universal Outward Feeds Administration menu.

   - If an active target specification file is already installed, the system asks you to verify that the existing active target specification file is to be overwritten.

     ```
     WARNING:  An active target specification file is already installed.

     Do you wish to overwrite the installed active target specification
     file? (default n) [y, n]:
     ```

     — Press **RETURN** for "no," or type **y** to overwrite the installed file.

   - If an active target specification file is not installed, the system prompts you for the name of the file containing the new active target specification.

     — Enter the name of the file, or type **q** to quit.

2. The system then validates the contents of the designated file.

   - If no errors are present, the file is installed.
   - If errors are present, you will be informed of the error and instructed to correct it before attempting to install the file again.

3. [In menu mode only] If you exit the Universal Outward Feeds Administration menu after installing or updating one or more specification files but do not re-enable Universal Outward Feeds (see "Procedure: Enabling Universal Outward Feeds" in this appendix), the system prompts you to determine whether the latest specification files should be used.

   System response:

   ```
   Do you wish to re-enable Universal Outward Feeds using the new specification
   file(s) before exiting? (default y) [y, n]:
   ```

   - If you answer **y**, Universal Outward Feeds is enabled or re-enabled with the new specification.
   - If you specify **n**, the old specification remains active until Universal Outward Feeds is re-enabled.

Procedure: Displaying or Retrieving the Installed Active Target Specification File

Command: $ xiadm gettargets

This option allows you to display the installed Active Target Specification File one page at a time or retrieve the installed Active Target Specification File to an ASCII file.

1. Type **xiadm gettargets**, or type **xiadm** and select **5** from the Universal Outward Feeds Administration menu.

   System response:

   ```
     Enter output file name, or press RETURN to view the file directly.
   ```

   - If you enter an output file name, the active target specification file is copied to the named file.
   - Or press **RETURN** to display the active target specification file a page at a time on your terminal screen.

Procedure: Editing the Installed Target Specification File

Command: $ xiadm chgtargets

This option allows you to edit the installed active target specification file. Only the System Administrator can edit this file, and a specification file with one or more errors may not be installed.

1. Type **xiadm chgtargets**, or type **xiadm** and select **6** from the Universal Outward Feeds Administration menu.
2. The system prompts you to choose an editor.

   ```
   Select editor (default vi) [ed, vi]:
   ```

   Press **RETURN** to select the default editor "vi," or type **ed**.

   - Check the value of your **$editor** environment variable to determine your default editor. If this variable is not set to either "ed" or "vi," the default editor is "vi."
3. Once you select an editor, the selected data element specification file is copied to a temporary file and the editor is invoked. When you have finished editing the temporary file, the system evaluates its contents.
   - If no errors are present, the new target specification file is installed.
   - If errors are present, the system informs you of the error and give you the opportunity to either re-edit the file or discard it.
4. [In menu mode only] If you exit the Universal Outward Feeds Administration menu after installing or updating one or more specification files but do not re-enable Universal Outward Feeds (see "Procedure: Enabling Universal Outward Feeds" in this appendix), the system prompts you to determine whether the latest specification files should be used:

   System response:

   ```
   Do you wish to re-enable Universal Outward Feeds using the new specification
   file(s) before exiting? (default y) [y, n]:
   ```

- If you say **y**, Universal Outward Feeds is enabled or re-enabled with the new specification.
- If you answer **n**, the old specification remains active until Universal Outward Feeds is re-enabled.

Procedure: Enabling Universal Outward Feeds

Command: $ xiadm enable

Before running this command, all data element specification files and the active target specification file must be installed. Each time you update a specification file, Universal Outward Feeds must be re-enabled. Only the system administrator can enable or re-enable Universal Outward Feeds.

1. Type **xiadm enable**, or type **xiadm** and select **7** from the Universal Outward Feeds Administration menu.

Once enabled, Universal Outward Feeds may be disabled by running the command **xiadm disable** at any time.

Procedure: Disabling Universal Outward Feeds

Command: $ xiadm disable

The following procedure explains how to disable Universal Outward Feeds. Only the System Administrator can disable Universal Outward Feeds.

1. Type **xiadm disable**, or type **xiadm** and select **8** from the Universal Outward Feeds Administration menu.

Once disabled, Universal Outward Feeds can be re-enabled at any time using the **xiadm enable** command.

Procedure: Reporting on All Installed Specification Files

Command: $ xiadm report

The following procedure explains how to generate a report on all installed specification files. The report consists of the installed active target specification file followed by each of the installed data element specification files.

1. Type **xiadm report**, or type **xiadm** and select **9** from the Universal Outward Feeds Administration menu.

   System response:

   ```
   Enter output file name, or press RETURN to view the report directly:
   ```

   - If you enter an output file name, the installed specification file report is written to the named file.
   - Or press **RETURN** to display the report a page at a time on your terminal screen.

A sample installed specification report follows:

```
        Universal Outward Feeds Specification File Report
        =================================================

Active Target Specification File:
--------------------------------

activate AP1 for { nj-generic2, co-generic2, co-system85 }

activate AP2 for { nj-generic2, nj-dimen3.8 }

Data Element Specification File AP1:
------------------------------------

# Universal Outward Feeds Data Element Specification file for
# Application I (AP1)

select { authc, accid, namdb } from auth

select { extn, state, namdb, setid, accid } from extn

select { dplba, fdac } from feadac

select { namdb, onum, suprv, auloc, aurm } from name

select { setid, plug1, plug2, stopt, sttyp, spkph, hdset, scord, lcord,
       pel, pe2, spid } from set

select { rnxcd, main } from rnx

select { rnxcc, main } from rnxcc

select {trkgp, dac, trknm, ttype, watsb, accid, vend, npnnx, subsw}
       from trkgp

Data Element Specification File AP2:
------------------------------------

# Universal Outward Feeds Data Element Specification file for
# Application II (AP2)

select { extn, namdb, lwcds, ap } from extn

select { namdb, onum, suprv, auloc, aurm, ufd1, ufd2, ufd3, ufd4, ufd5 }
       from name
```

Error Messages and Troubleshooting

Potential error messages returned by the **xiadm** command are summarized below:

The following section contains error messages returned while the system is validating the active target specification file. Each message is preceded by the file name and line number where the error occurs:

```
invalid application identifier <id>.

unknown application identifier <id>
   Install the data element specification file for this application before
   attempting to activate targets for this application.

duplicate specification for application id <id>.

invalid target identifier <id>.

unknown target <id>.

uninitialized target <id>.

redundant specification for target <id>.

syntax error.

unexpected character <character>
```

The following error messages may be returned while the system is validating a data element specification file. Each message is preceded by the file name and line number where the error occurred:

```
invalid file name <id>.

unknown file name <id>.

duplicate specification for file name <id>.

invalid field name <id>.

unknown field name <id>.

redundant specification for field name <id>.

file <filename> does not have a primary key.

primary key of file <filename> is not specified.

field name <field name> is invalid for file <filename>.

invalid file_limit <id>.

syntax error.

unexpected character <character>.
```

APPLICATION INITIALIZATION AND SYNCHRONIZATION

Manager IV comes with a pre-defined data element specification file that allows an Application to receive selected information from Manager IV. Two system administration tasks are associated with this feature: initializing and synchronizing the Application product database.

Each of these transactions retrieves the required data elements from the Manager IV product-image database to produce data transfer files in the standard format. (See "How Data is Transferred" at the beginning of this appendix.)

The **application-database initialize** command creates data transfer files suitable for the initialization of the Application database. These files have the prefix "in" rather than "tg," and use the verb **init** rather than **add**, **change**, or **remove**.

The **application-database audit** command creates data transfer files that allow the Application product to check for synchronization errors between the Application database and the Manager IV database. Data transfer files produced for synchronization (audit) purposes have the prefix "au" rather than "tg," and use the verb **audit** rather than **add**, **change**, or **remove**.

The data transfer files produced by either command are appended to the Application master file.

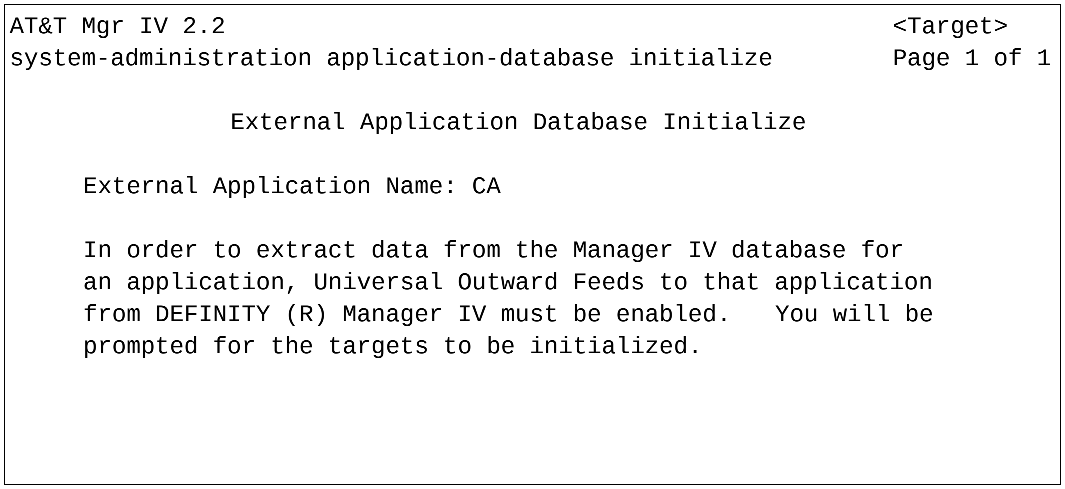
The following sections explain how to initialize and audit the Application database.

Initializing the Application Database

Command: system-administration application-database initialize

The following example is for the Cost Allocation (CA) Application. Use this command to initialize the CA product database.

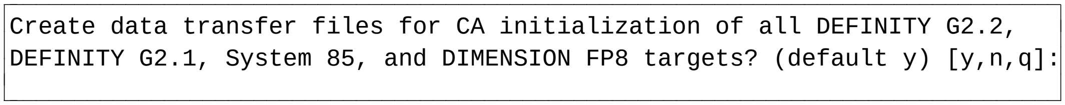
1. Type **system-administration application-database initialize**. The following screen appears:



```
AT&T Mgr IV 2.2                                             <Target>
system-administration application-database initialize       Page 1 of 1

               External Application Database Initialize

     External Application Name: CA

     In order to extract data from the Manager IV database for
     an application, Universal Outward Feeds to that application
     from DEFINITY (R) Manager IV must be enabled.   You will be
     prompted for the targets to be initialized.
```

2. Enter the External Application Name. In the example provided, this field defaults to "CA". You are allowed to enter any Application name. Press **RETURN** followed by **EXECUTE**.

3. System response:



```
Create data transfer files for CA initialization of all DEFINITY G2.2,
DEFINITY G2.1, System 85, and DIMENSION FP8 targets? (default y) [y,n,q]:
```

- If you answer **y**, the system begins processing the data transfer files for each initialized DEFINITY Generic 2, System 85, and DIMENSION target.
- If you answer **n**, the system prompts you before creating data transfer files for each target:

```
Create data transfer files for CA initialization of DEFINITY G2.1 target
mt-gen2? (default y) [y, n, q]:
```

  — Answer **y** to process the target indicated.

4. Processing consists of two steps.

   (Step 1:) The system verifies that there are no pending or failed service requests for the specified target. (Because Manager IV maintains a future rather than a current view of the switch image, it is important that no service requests are pending when this command is run).

```
Checking for pending and failed service requests against DEFINITY G2.1 target
mt-gen2 ...

The following Service Requests are pending:

  ausr0101aa  ausr0101ab   ausr0101ac   ausr0101ad  ausr0101ae
  busr0101aa  busr0101ab

The following Service Requests are failed:

  ausr0101ba  ausr0101bb  busr0101ba

Please use service-request remove and/or service-request run to
eliminate
all pending and failed service requests before attempting to create data
transfer files for this target.
```

   If the system has identified any failed or pending service requests for any targets in your network, use the **service-request remove** and/or **service-request run** commands to eliminate these failed and pending service requests; then run **application-database initialize** again. See *Getting Started with DEFINITY® Manager IV* for more information on the Service Request commands.

5. (Step 2:) If there are no failed or pending service requests against the target, the system creates a data transfer record for each record in the specified Manager IV product-image database files.

   System response is similar to the following:

```
Checking for pending and failed service requests against DEFINITY G2.1 target
mt-gen2...

Creating data transfer files for CA initialization of target mt-gen2...

             Processing data for CORE database file "fstdgt"...
             Processing data for CORE database file "feadac"...
             Processing data for CORE database file "name"...
             Processing data for CORE database file "set"...
             Processing data for CORE database file "extn"...
             Processing data for CORE database file "auth"...
             Processing data for CORE database file "trkgp"...
             Processing data for CORE database file "rnxcc"...

Data transfer files for target mt-gen2 created successfully.
```

6. If you have more targets, the system does one of the following:

   - If you answered **y** in step 1 above, the system continues to process the targets in your network with no further input from you.
   - If you answered **n** in step 1 above, the system prompts you before processing the next target:

     ```
     Create data transfer files for CA initialization of System 85 R2V4 target
     dr-system85? (default y) [y, n, q]:
     ```

   The system continues this process until all of your targets have been processed.

Auditing the Application Database

Command: system-administration application-database audit

The following example is for the Cost Allocation (CA) Application. Use this command to audit the CA product database.

1. Type **system-administration application-database audit**. The following screen appears.

```
AT&T Mgr IV 2.2                                             <Target>
system-administration application-database audit            Page 1 of 1

               External Application Database Audit

     External Application Name: CA

     In order to extract data from the Manager IV database for
     an application, Universal Outward Feeds to that application
     from DEFINITY (R) Manager IV must be enabled.   You will be
     prompted for the targets to be initialized.
```

2. Enter the External Application Name. In the example provided, this field defaults to "CA". You are allowed to enter any Application name. Press **RETURN** followed by **EXECUTE**.

3. System response:

   ```
   Create data transfer files for CA auditing of all DEFINITY G2.2,
   DEFINITY G2.2, System 85, and DIMENSION FP8 targets? (default y) [y,n,q]
   ```

   - If you answer **y**, the system begins processing the data transfer files for each initialized DEFINITY G2.1, System 85, and DIMENSION target.
   - If you answer **n**, the system prompts you before creating data transfer files for each target:

     ```
     Create data transfer files for CA auditing of DEFINITY G2.1 target
     mt-gen2? (default y) [y, n, q]
     ```

     — Answer **y** to process the target indicated.

4. Processing consists of two steps.

   (Step 1:) First the system verifies that there are no pending or failed Service Requests for the specified target. (Because Manager IV maintains a future rather than a current view of the switch image, it is important that no Service Requests are pending when this command is run).

   ```
   Checking for pending and failed service requests against DEFINITY G2.1 target
   mt-gen2 ...

   The following Service Requests are pending:

     ausr0101aa  ausr0101ab   ausr0101ac   ausr0101ad  ausr0101ae
     busr0101aa  busr0101ab

   The following Service Requests are failed:

     ausr0101ba  ausr0101bb  busr0101ba

   Please use service-request remove and/or service-request run
   to eliminate
   all pending and failed Service Requests before attempting to create data
   transfer files for this target.
   ```

   If the system has identified any failed or pending Service Requests for any targets in your network, use the **service-request remove** and/or **service-request run** commands to eliminate these failed and pending Service Requests, and then run the command **application-database audit**. See *Getting Started with DEFINITY® Manager IV* for more information on the Service Request commands.

5. (Step 2:) If there are no failed or pending service requests against the target, the system creates a data transfer record for each record in the specified Manager IV product-image database files.

   System response is similar to the following:

```
Checking for pending and failed service requests against DEFINITY G2.1 target
mt-gen2...

Creating data transfer files for CA audit of target mt-gen2...

             Processing data for CORE database file "fstdgt"...
             Processing data for CORE database file "feadac"...
             Processing data for CORE database file "name"...
             Processing data for CORE database file "set"...
             Processing data for CORE database file "extn"...
             Processing data for CORE database file "auth"...
             Processing data for CORE database file "trkgp"...
             Processing data for CORE database file "rnxcc"...

Data transfer files for target mt-gen2 created successfully.
```

6. If you have more targets, the system does one of the following:

   - If you answered **y** in step 1 above, the system continues to process the targets in your network with no further input from you.
   - If you answered **n** in step 1 above, the system prompts you before processing the next target:

     ```
     Create data transfer files for CA auditing of System 85 R2V4 target
     dr-system85? (default y) [y, n, q]:
     ```

   The system continues this process until all of your targets have been processed.

APPENDIX D. SUPPORTING DOCUMENTATION

This appendix contains information on documentation for DEFINITY ® Manager IV, related products (System 75/DEFINITY Generic 1 and System 85/DEFINITY Generic 2), and the UNIX operating system.

All of the following documentation can be ordered by calling the AT&T Customer Information Center (CIC) at 1-800-432-6600 or writing to:

AT&T Customer Information Center
ATTN: Customer Service Representative
P.O. Box 19901
Indianapolis, IN 46219

DEFINITY MANAGER IV DOCUMENTATION

Detailed information about specific aspects of Manager IV planning, installation, and day-to-day operation are included in the Manager IV manuals listed below.

Introduction to DEFINITY® Manager IV presents a general overview of Manager IV. The *Introduction* is designed to help customers become familiar with Manager IV and evaluate its benefits. It contains a description of Manager IV capabilities, a discussion of major benefits, an explanation of AT&T service and support, and a detailed description of each of the Manager IV applications.

Getting Started With DEFINITY® Manager IV provides the procedural and reference information necessary to use Manager IV. The first part of this guide includes a general overview of Manager IV, a system description, Manager IV application overviews, and instructions for administering the Manager IV user interface. The second part gives you detailed information about service requests.

The *DEFINITY® Manager IV Quick Reference* card puts Service Request commands, Escape Sequences, Scrapbook, Clipboard, and Utilities information at your fingertips.

DEFINITY® Manager IV Planning and Implementation Manual provides information on planning and implementing Manager IV. The manual helps customers determine their configuration needs and outlines the activities that must be completed by the customer and AT&T from the initial planning stages to Manager IV cutover.

DEFINITY® Manager IV Initialization, Installation and Maintenance provides the installer with procedural and reference information needed to install and initialize Manager IV on its processor. The manual also describes and suggests solutions for possible problems that may arise during the execution of these procedures. Customers may need to refer to some of the initialization procedures if they need to reconfigure Manager IV or if they install new equipment that changes the network configuration.

The manual also provides the service technician or the qualified customer with the procedural and reference information needed for routine software maintenance.

DEFINITY® Manager IV Query and Report Languages explains the commands used in the Query and Report Languages and provides instructions for using them to supplement standard reports.

Manager IV User Guides

The Manager IV user guides provide detailed procedures for using each Manager IV application. These guides each contain the following information:

- How the application fits into Manager IV’s overall structure
- How to access Manager IV and use the commands provided by the application
- Detailed procedures needed to perform the tasks related to the application
- A list of the application’s commands

Application administrators should refer to these guides for information about their specific application.

DEFINITY® Manager IV System Administration provides the Manager IV System Administrator with the reference and procedural information needed to monitor Manager IV and the products it supports. It enables the System Administrator to analyze and improve the overall performance of the system configuration.

The *DEFINITY® Manager IV System Administrator’s Checklist* is a quick reference card that reminds the System Administrator about tasks that should be performed regularly and offers a guide to backup and recovery.

DEFINITY® Manager IV Facilities Management Operations provides the FM user with the procedural and reference information needed to configure and control a telecommunications system. Procedures include configuring trunks and trunk groups, remotely accessing trunk-testing hardware, selecting network routing paths, and assigning and changing Facility Restriction Levels and authorization codes.

DEFINITY® Manager IV Terminal Change Management Operations provides the TCM user with the procedural and reference information needed to administer voice and data terminals and attendant consoles for the products supported by Manager IV.

SYSTEM 75 AND DEFINITY GENERIC 1 DOCUMENTATION

The documentation in support of DEFINITY® Generic 1 is structured similar to System 75. The following documents are common to System 75 and Generic 1:

DOCUMENT	ORDER NUMBER
Feature Description	555-200-201
Administration and Traffic Measurements	555-200-500
Voice Terminal Operations	555-200-701
Console Operations	555-200-700
Application Notes	555-209-000
Pocket Reference	555-200-202

The following documents are specific to DEFINITY Generic 1:

Introduction	555-200-024
System Description	555-204-200
Installation	555-204-104
Maintenance	555-204-105

SYSTEM 85 AND DEFINITY GENERIC 2 DOCUMENTATION

DOCUMENT	ORDER NUMBER
An Introduction to AT&T System 85	555-103-020
System 85 Feature Facts	555-102-751
An Introduction to DEFINITY® 75/85 Communications System Generic 2	555-104-020
DEFINITY® Communications System Generic 2 and System 85 System Description	555-104-201
DEFINITY® Communications System Generic 2 and System 85 Feature Description	555-104-301
System 85 Features Reference Manual	555-103-301
DEFINITY® 75/85 Communications System Administration Procedures	555-104-506
DEFINITY® Generic 2 Administration of Features and Hardware	555-104-507
System 85 Feature Translations Manual (Release 2, Version 1 and 2)	555-101-107
System 85 Feature Translations Manual (Release 2, Version 3)	555-102-107
System 85 Feature Translations Manual (Release 2, Version 4)	555-103-107
System 85 Maintenance Service Manual (R2V1 and R2V2)	555-101-108
System 85 Maintenance Service Manual (R2V3)	555-102-108
System 85 Maintenance Service Manual (R2V4)	555-103-108

UNIX OPERATING SYSTEM DOCUMENTATION

UNIX System V Release 3.1 Release Notes	305-565
UNIX System V Release 3.1 Administration Guide	305-569
UNIX System V Release 3.1 User’s Reference Manual	307-012
UNIX System V Release 3.1 System Administrator’s Reference Manual	305-570
UNIX System V Release 3.1 System Administrator’s Reference Manual Updates	305-571
UNIX System V Release 3.1 User’s Guide	307-231
Systems Software Development Tools User’s Guide	307-235
UNIX System V Release 3.1 Cartridge Tape Utilities Guide	306-006
Network Support Utilities Release Notes	307-233
Release 3 Streams Primer/ Remote Filesharing Utilities Release Notes	307-229

PROCESSOR DOCUMENTATION

DOCUMENT	ORDER NUMBER
AT&T 3B2 Computer UNIX System V Release 3 System Administrator’s Guide	305-611
AT&T 3B2 Computer UNIX System V Release 3 Owner/Operator Manual	305-612
AT&T 3B2 Computer UNIX System V Release 3 User’s and System Administrator’s Reference Manual	305-646
UNIX System V/386 Release 3.2 User’s/System Administrator’s Reference Manual	307-077
UNIX System V/386 Release 3.2 User’s Guide	307-079
UNIX System V/386 Release 3.2 Operations/System Adminstration Guide	307-085

APPENDIX E: PROC MODE APPLICATION

Maintenance (Proc Mode) is the Manager IV application which allows you to maintain AT&T DEFINITY Generic 2, System 85 R2V2-R2V4 and DIMENSION FP8 Issues 1.16 and 3.8 switches by running the following maintenance related tasks:

- Examine error and alarm logs to find all errors.
- Run error-detection tests of circuits to verify if the system is still defective.
- Run diagnostic tests.
- Resolve alarms in the alarm log and retire alarm indicators.
- Switch between the duplicated subsystems to place standby subsystems in service.
- Make circuits available or unavailable for service.
- Monitor system status.
- Reinitialize all or part of the system.

This guide is intended for Proc Mode users who have taken the preliminary training. If you are a new Proc Mode user, use the on-line help to get familiarized with Proc Mode applications and the commands for administering the maintenance procedures.

Detailed information on each maintenance procedure used with Generic 2 is provided in *DEFINITY® Communications System Generic 2 Maintenance Procedures* . For System 85 switches, refer to *AT&T System 85 Advanced Networking Switch R2V4 Maintenance* . The DIMENSION switches are described in *System Maintenance Procedures*.

ABOUT MAINTENANCE PROCEDURES

The maintenance tasks can be accessed from the Manager IV Systems Management User Executive (SMUE) via the system's procedures (procs) identified by three-digit numbers (600 series for Generic 2 and System 85; 500 series for DIMENSION). For Generic 2 and System 85, the following maintenance procs are supported:

General Switch Proc - 600
Provide status information about the entire switch or about switch components that can affect the entire switch.

General Switch Proc - 601
Provide environmental failure history log information, resolve environmental alarms and test cabinets for environmental failures.

Common-Control Procs - 610-614, 616, 618
Test the common control and associated components.

Network Area Procs - 620-625, 627, 631, 635, 640, 642-644, 646-648
Deal with the digital network and its peripherals. Procedures **631, 635, 640, 642-644** are auxiliary procs (they do not do any tests) used to monitor switch information.

Common-Control Peripheral Procs - 650-656
Test any equipment which can directly communicate with the common control through a non-network path.

Connection Status - 960-962

Show the connection status and let you trace a call through the switch.

Memory Word Display - 999

Shows the data contents of a memory address through the software tables.

Maint-1 or All User

To access Proc Mode, you need to be assigned as a *maint-1* or *all* class user via the **system-administration login add** or **system-administration login change** commands. The details on administration procedures are covered in *DEFINITY® Manager IV System Administration*.

Security:

Your System Administrator may have placed restrictions on your User ID. These restrictions can block your access to switch mode (Administration, or Disk/Tape Subsystem) and/or certain procedures.

As a *maint-1* class user, you will be restricted to the maintenance procs only. The restrictions are defined in the Proc Restriction List.

Proc Restriction File

Manager IV provides a default Proc Restriction file which restricts you to the maintenance procs only. This file contains a list of procs that you are not allowed to access as a regular user. The system will automatically restrict you from running procs **276, 277, 490, 495, 496, 497**, and **999**. These procs are not included in the Proc Restriction file. The following conventions apply to the Proc Restriction file:

- All comment lines start with "#".
- The file contains one proc per line. For example, **000** means the user is not allowed to access any of the procs associated with proc **000**.

Only the System Administrator is allowed to edit this file to override the restrictions.

Modes of Operation

Proc Mode supports two modes of operation: *basic* and *enhanced*. *Basic* mode is a built-in Proc Mode functionality that allows you to connect to and maintain the Generic 2, System 85 R2V2-R2V4 and DIMENSION switches. The *basic* mode software is delivered as a part of the Manager IV software.

Enhanced mode is supported only if the Switch Support Base (SSB) package is delivered with the Proc Mode *basic* functionality. In *enhanced* mode, you can access and maintain DEFINITY Generic 2 switches only; the SSB software is not available for the System 85 and DIMENSION switches.

Basic Mode

You can always access *basic* mode. In *basic* mode, the Proc Mode application operates in a manner similar to the System Management Terminal (SMT) or the Visual Maintenance and Administration Panel (VMAAP). Data can be entered from the command line or directly into the fields.

- Commands that depend on the information in the SSB to function properly are not available in *basic* mode. These include on-line help commands related to the procedures and the interpret string command that translates field encodes.
- *Basic* mode processes only numerical data. Therefore, you must enter the numerical codes associated with the character rather than the characters themselves.
- *Basic* mode does not have field labels nor does it display encode meanings.

- *Basic* mode does not accept universal equipment location specifications. Use the **el** command to translate universal equipment locations to traditional equipment location numbers. Press the Cmds function key or refer to Table 1 to see a complete list of commands and their meanings.

Enhanced Mode

In *enhanced* mode, Proc Mode provides you with a fully prompted interface (Switch Support Base) to Generic 2. The SSB interface contains descriptive field names, help messages and error messages for each proc supported. Data are displayed on the screens in fields that are organized in readable columnar format.

With the SSB software installed, you need to tell Manager IV where on the system the SSB files are located by specifying the SSB Environment Variable in the $SYSROOT/etc/envlist and /etc/envlist files. Also, edit $SSB/r2v5/path.ssb file so that the valiables ADM_PATH, MNT_PATH, and HLP_PATH point to the correct directories. Note that the variables point to an expanded path.

Proc Mode Commands and Function/Control Keys

Table 1. Enhanced and Basic Mode Commands

Cmd	Description	Enh	Bas
#	Enter a Comment	x	x
;	Advance One Field	x	x
@	One Second Pause	x	x
"..."	Interpret a Character String	x	
add	Add Data	x	x
ax	Add Data Execute	x	x
bas	Enter Basic Mode	x	
bo	Busy Out Facility	x	x
cdx	Clear Data Execute	x	x
ce	Clear Active Field Entry	x	x
cf	Change Active Field	x	x
chg	Change Data	x	x
cp	Select Customer Procedure	x	x
cx	Change Data Execute	x	x
dsp	Display Data	x	x
dx	Display Execute	x	x
el	Convert Equipment Location	x	x
enh	Enter Enhanced Mode		x
get	Get Switch Support Base File(s)	x	x
help, h	General Help and Information	x	x
hc, ?	Command Help	x	x
hf	Procedure Field Help	x	
hi	Procedure Input Help	x	
hist	Display Activity Log	x	x
log	Open or Close Activity Log File	x	x
m	Select Procedure Mode	x	x
nc	Next Circuit	x	x
nd	Next Data	x	x
nf	Next Fault	x	x
np	Next Procedure	x	x
nt	Next Text	x	x
nu	Next Unit	x	x
p	Select Procedure	x	x
ptx	Park Tape Execute	x	x
quit	Quit	x	x
rb	Release Busy Out	x	x
rld	Reload Switch Memory	x	x
rmv	Remove Data	x	x
rs	Reset Procedure	x	x
rtx	Run Tape Execute	x	x
run	Run a Script File	x	x
rx	Remove Data Execute	x	x
s	Stop Procedure	x	x
scroll	Enter Scroll Mode	x	x
stat	Display Status	x	x
sw	Switch Control Processors	x	x
t	Select Procedure Test	x	x
task	Enter Task Mode	x	x
v	Verify Procedure	x	x
visual	Exit Scroll Mode	x	x
w	Select Procedure Word	x	x
x	Execute Procedure	x	x

Table 2. Enhanced and Basic Mode Function/Control Keys

Key	Screen Label	Function
F3	Form	When cursor is on command line, moves cursor to screen form to accept entries.
F3	Line	When cursor is on screen, moves cursor from active field to the command line.
F4	Clear	When cursor is on screen, clears field.
F5	Help	Display a menu to access information about using the system (how to access on-line help, command syntax, a list of command options, a list of procedures, and information about procedures.)
F6*	Field	Display a range of valid entries (such as **1-120**) or a list of available field values displayed in a window.
F7*	Input	Display required input data.
F8	Cmds	a list of valid commands.

* Enhanced Mode only

ADMINISTERING MAINTENANCE PROCS

In Proc Mode, you can access the maintenance procs via the "Procedure Mode" screens. To invoke the "Procedure Mode" screen, you have to perform the following prerequisites:

1. Select Proc Mode by entering "maintenance" in the Select application field.
2. Select a target by entering the valid switch (the same as the target) name.
   - The switch name must have been previously defined via the **product add** transaction.

With the target established, you have a choice of viewing the Proc Mode Help Facility via the **proc info** command or connecting to the switch by entering the **proc run** command to access the selected maintenance proc.

Proc Mode Help Facility

Proc Mode supports the on-line Help Facility in *enhanced* mode only if the SSB software is installed. The Help Facility contains all information necessary to administer and maintain Generic 2 in Proc Mode. Via the Help Facility, you can display information about the procedures on your system. You may even display the procs themselves by using the F6 FIELD function key.

You are allowed to access the on-line help before connecting to the switch by using the **proc info** command. To invoke the on-line help from within a Test screen (when connected to the switch), enter **h** or **help** at the command line or press the F5 HELP function key.

To access Help from any maintenance *test* screen, enter **h** or **help** at the command line or press F5 HELP function key. For a detailed description of the Help Facility, refer to *DEFINITY Communications System Generic 2 Maintenance Procedures*.

Connect to the Switch

Proc Mode allows you to directly connect to all switch types via the **proc run** command, thus minimizing load on Manager IV. When you enter the **proc run** command, Proc Mode will try to establish a connection to the specified switch. If a connection cannot be established, the appropriate error codes will be returned.

1. Enter the **proc run** command to establish connection to the specified switch.
   - The **proc run** transaction works only for a dial out connection. If the connection is defined as "dedicated", the **proc run** transaction fails.

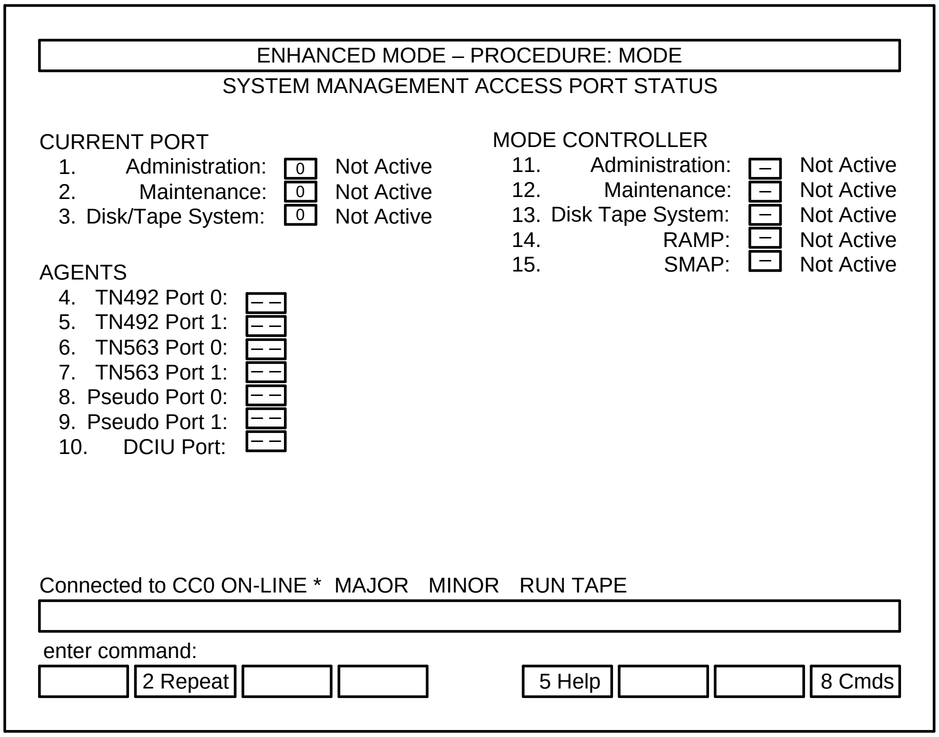
WARNING:
Before the connection is established, the warning message will be generated: "THE MANAGER IV DATABASE WILL NOT REFLECT CHANGES DONE WITH THIS TRANSACTION." This is a reminder that any administration done via Proc Mode will directly affect the switch but not the Manager IV database which may result in "out-of-sync" condition. Therefore, if you modify the switch configuration in Proc Mode, you must either update the Manager IV database to keep it "in sync" with the switch, or report any switch updates to the System Administrator.

   - With the connection established, and depending on the switch (Generic 2 or earlier release) selected and the SSB software, the Enhanced or Basic Mode screen will be displayed.

Proc Mode Screens

Proc Mode is a screen-based application that facilitates your interactive session with the switch via prompts, error and help messages.

If a Generic 2 switch has been specified as a target, and the SSB software is present, Proc Mode defaults to the *enhanced* mode, and the input "Procedure Mode" screen is as follows:



```
                 ENHANCED MODE – PROCEDURE: MODE
              SYSTEM MANAGEMENT ACCESS PORT STATUS

CURRENT PORT                             MODE CONTROLLER
  1.      Administration: [0]  Not Active  11.     Administration: [–]  Not Active
  2.        Maintenance:  [0]  Not Active  12.       Maintenance:  [–]  Not Active
  3. Disk/Tape System:    [0]  Not Active  13. Disk Tape System:   [–]  Not Active
                                           14.              RAMP:  [–]  Not Active
AGENTS                                     15.              SMAP:  [–]  Not Active
  4.  TN492 Port 0:  [– –]
  5.  TN492 Port 1:  [– –]
  6.  TN563 Port 0:  [– –]
  7.  TN563 Port 1:  [– –]
  8. Pseudo Port 0:  [– –]
  9. Pseudo Port 1:  [– –]
 10.     DCIU Port:  [– –]

Connected to CC0 ON-LINE *  MAJOR   MINOR   RUN TAPE

 enter command:
[      ] [2 Repeat] [      ] [      ]     [5 Help] [      ] [      ] [8 Cmds]
```

In *enhanced* mode, this screen layout applies to all maintenance procs.

Proc ID Line

> The Proc ID Line occupies the top highlighted line of the screen. This line identifies *enhanced* or *basic* mode and the selected proc number.

Switch Modes

> Fields 1–3 of the Proc Mode screen list the available switch modes, their numbers, names, and "Active" or "Not Active" state depending on the mode chosen. Depending on your class of user, select "Administration," "Maintenance," "Disk/Tape Subsystem," or any combination of these.
>
> Administration mode is selected by entering **1** on the command line. To release the mode for other users, enter **1** again. Similarly, select Maintenance mode by entering **2** and Disk/Tape mode by entering **3**.
>
> The Proc Fields Area is populated with the field descriptions and data. Fields 11–15 tell which port has control of a switch mode. Fields 4–10 display a code that tells which agent has control of the given port.

Status Line

> The Status Line indicates the state of the switch and of your connection to the switch. Six status indicators are available: *MAJOR*, *MINOR*, *RUN TAPE*, *BUSY OUT*, *IN USE*, and *WAIT*. The indicators interpretation is covered in detail in *DEFINITY Manager II MS-DOS® Version Operation*.

Message/Help Line

The Message/Help Line is used for displaying error and help messages.

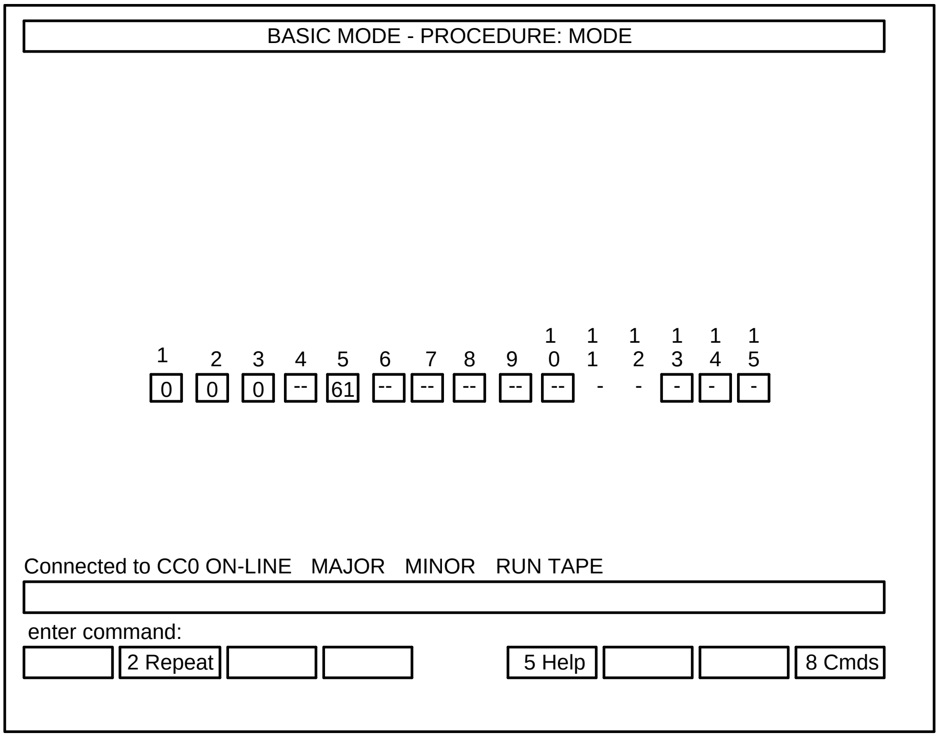
Command Line

The Command Line starts with the prompt *enter command:* . All Proc Mode commands are typed at this command line.

Function Keys (F1 through F8)

Labels for the active Function Keys are displayed in this area.

If a Generic 2 switch has been specified but the SSB software is not installed, or if a System 85 R2V3 or R2V4 switch has been requested, Proc Mode defaults to the *basic* mode, and the Procedure Mode screen looks as follows:



BASIC MODE - PROCEDURE: MODE

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	--	61	--	--	--	--	--	-	-	-	-	-

Connected to CC0 ON-LINE   MAJOR   MINOR   RUN TAPE

enter command:

The screen description for the Enhanced Mode screen applies to the Basic Mode screen, as well. However, on these two screens, the same information is presented in different manner; the field descriptions and the way the fields are organized are completely different.

- The selection items in the Selection Menu and the proc fields in the Proc Fields Area are represented by numbers positioned side-by-side.
- The field numbers appear above each field.

For the screen and command description in the DIMENSION switches, refer to *System Maintenance Procedures*.

Maintenance procedures consist of a series of "tests". Depending on the type of maintenance operation, a maintenance proc can have 1-6 test screens with the fields specifically defined for the particular *test*. For each test screen, the fields and the names may be different but the screen layout will be the same as described above. You can access any *test* screen by entering the appropriate command at the command line.

Proc Mode Commands

The "Procedure Mode" screens allow you to enter commands to run procs. For example, to run proc **600**, type in **p** (for the "proc" command) followed by a valid proc number at the enter command prompt.

p600 or **p 600** and press **Return**.

Most procedures have numbered sub-procedures, called *tests*. When you select a procedure, *Test* number **1** is automatically displayed. The command as entered above will invoke the screen for Proc **600** Test **1**. To view a test other than Test **1**, you have to specify **t** (for "test") as part of the command. For example, to invoke the Proc 600 Test 2 screen, enter:

p 600 t 2 and press **Return**.

Some procs are display only, like Proc **600** Test **1** and Proc **601** Test **1**. You can only view these procs to examine alarms, errors and failure history in the error and history logs. Other procs, for example, Proc **620**, allow you to enter data in the fields to run tests on the specified hardware.

Data can be entered in two ways:

From the Command Line

Just by typing the data on the command line. You can enter one command or field entry at a time, or enter a string, leaving spaces between each entry.

- Basic mode does not accept a "string" of data entered in quotes; you must enter numerical codes.

When you press **Return**, the data will appear in the field(s) on the screen. For example, to change the Module (field 3) to value **3** in Proc **620** Test **2**, enter:

cf 3 3 and press **Return**

Directly in the Active (Highlighted) Field

By using the function keys and commands. For example, to change Proc **620** Test **2** Field **3** to **3**:

- Press **Form** to move the cursor to an active field.
- Press **Backspace** to remove a character or use **Clear** to blank the entire field.
- Type **3** in the active field. Press one of these keys: **Return**, **Tab**, → or ▼ to move the cursor to next field (Leaves next field intact). If you need to move the cursor to the preceding field, use any of these: **Shift-Tab**, ←, or ▲.
- Return to command line by pressing **Line** . When you exit the last field on the screen, the cursor automatically returns to the command line.

For more details on how to enter data in the active field, refer to Table 2. For a complete list of commands, press **Cmds** for on-line help, or refer to Table 1 later in this document.

MAINTAINING THE SWITCH

To provide the efficient services that ensure the proper switch operation, observe the following guidelines:

1. Start your switch routine check up or troubleshooting with Proc **600**. Use Test **1** and Test **2** to examine the Periodic Maintenance Information Data Structure (PMIDS) error log.
2. Go to the maintenance procedure that the test directs you to (Procedure Reference, field 15), and retest the problem that raised the alarm.

The second way is to delete any invalid alarms from the PMIDS error log.

Caution: Deleting alarms is not a good practice and not a normal maintenance function.

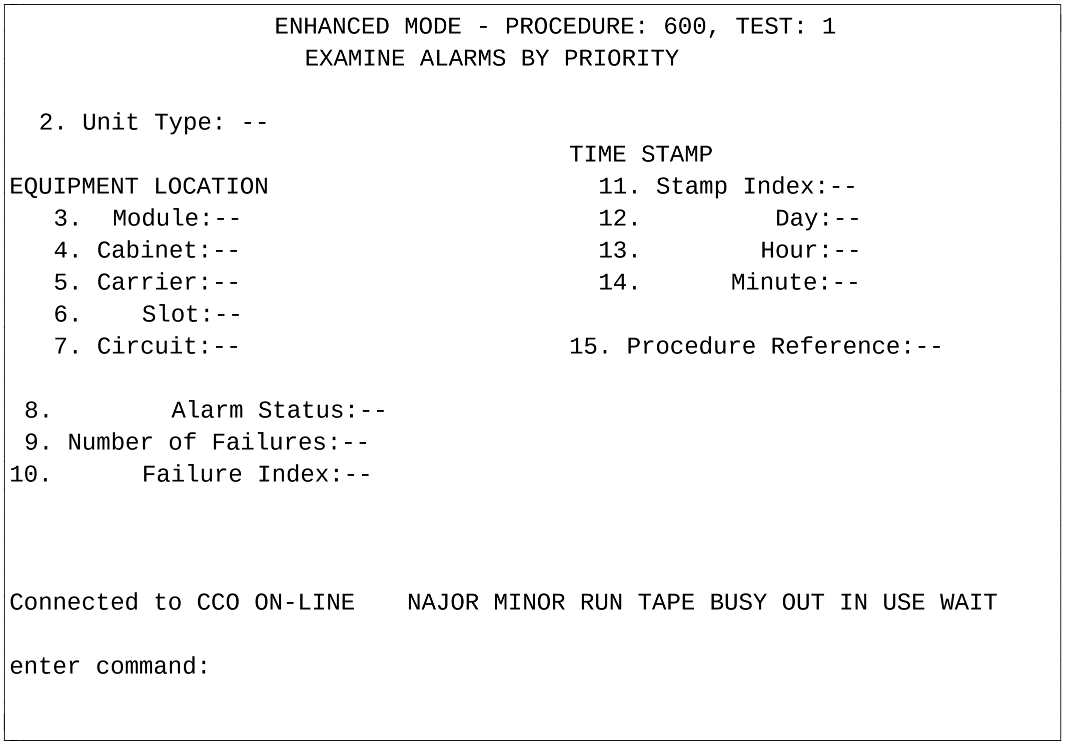
Detailed guidelines for Generic 2 are provided in *DEFINITY Communications System Generic 2 Maintenance Procedures*. For System 85 switches, refer to *AT&T System 85 Advanced Networking Switch R2V4 Maintenance*. The DIMENSION switches are described in *System Maintenance Procedures*.

Examine Alarms and Errors in Enhanced Mode

Use Proc **600** Test **1** and Test **2** to examine the PMIDS error log.

Procedure: Proc 600 Test 1 (Command line)

1. To examine the PMIDS error log, enter the command **p600** and press **Return**. The Proc **600** Test **1** screen displays.



```
                  ENHANCED MODE - PROCEDURE: 600, TEST: 1
                    EXAMINE ALARMS BY PRIORITY

  2. Unit Type: --
                                       TIME STAMP
EQUIPMENT LOCATION                       11. Stamp Index:--
   3.  Module:--                         12.         Day:--
   4. Cabinet:--                         13.        Hour:--
   5. Carrier:--                         14.      Minute:--
   6.    Slot:--
   7. Circuit:--                       15. Procedure Reference:--

 8.        Alarm Status:--
 9. Number of Failures:--
10.      Failure Index:--



Connected to CCO ON-LINE    NAJOR MINOR RUN TAPE BUSY OUT IN USE WAIT

enter command:
```

The Test **1** screen is display only. You can use the Test **1** screen for examining alarms by priority or for resolving alarms. WAIT will appear and stay until sorting is completed.

To examine alarms by priority,

1. Enter **x** to sort active alarms in the PMIDS error log. Press **Return**. Failure Index (field 10) will show total number of active alarms.
2. Enter **nc** to see each alarm.
   - Unit Type (field 2) may show the unit type of the alarm or error.
   - Equipment Location (fields 3-7) may show the equipment location of the circuit that caused the alarm.
   - Also, the rest of the fields will be populated with the data pertinent to this particular alarm.
   - Go to the procedure shown in Procedure Reference (field 15) to repair the failure that caused the alarm and then return to Proc **600** Test **1**. For example, field 15 shows 20. This means you must run Proc **620** to diagnose the problem. If there is no entry in field 15, refer to *DEFINITY Communications System Generic 2 Maintenance Repair Strategies (555-104-118)* and follow the repair steps for failures that are not alarmed.

To resolve alarms,

1. Enter **x** and then **nc** until the alarm you want to resolve appears on the screen.
2. Enter **cdx** to resolve alarms.
3. Enter **t3** to view the resolved alarm in Test **3**.
4. To examine alarms by unit type and search for errors, enter **t2**.

Methods of fault detection and troubleshooting the Generic 2 switch are detailed in *DEFINITY Communications System Generic 2 Maintenance Procedures*. Also, use the on-line Help Facility for reference. For System 85 refer to *AT&T System 85 Advanced Networking Switch R2V4 Maintenance*. The DIMENSION switch is described in detail in *System Maintenance Procedures*.

Procedure: Proc 600 Test 1 (Active field entry)

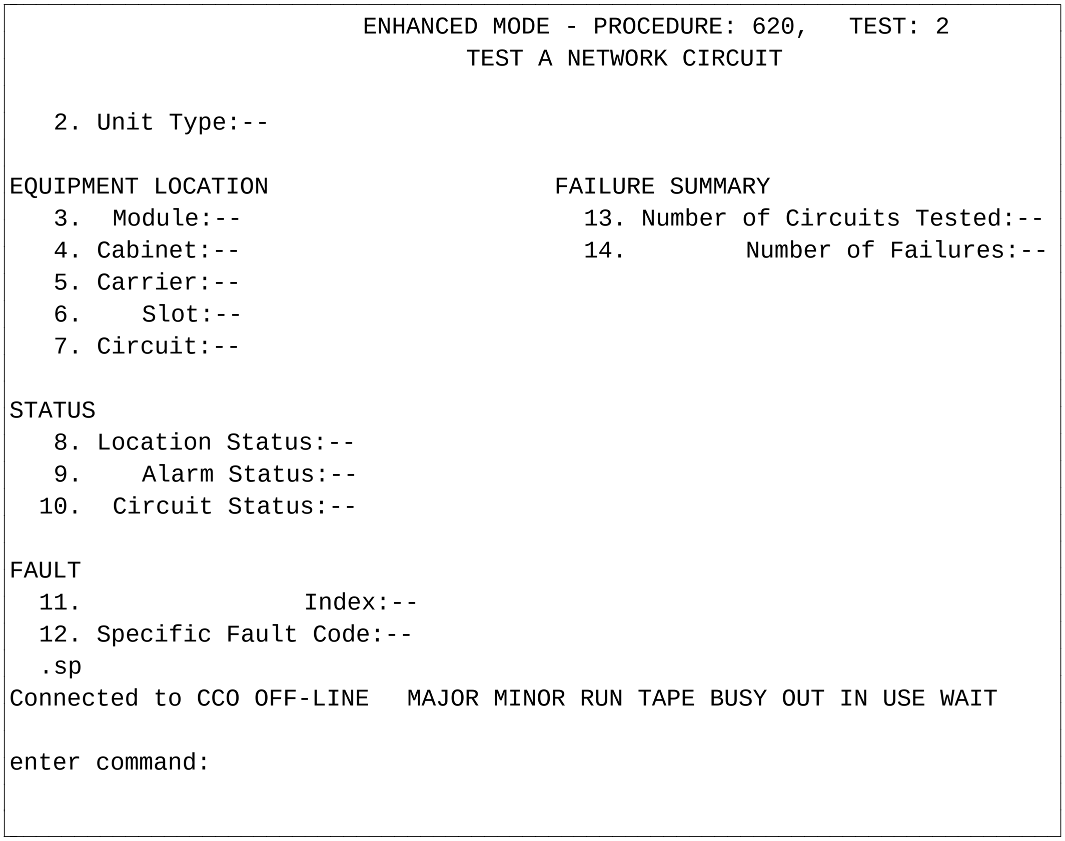
To perform Proc 600 Test 1 using the active field entry, follow the instructions provided in "Proc Mode Commands" earlier in this chapter.

Isolate the Problem in Enhanced Mode

To isolate the problem, run the maintenance test as indicated in Proc **600** Test **1** Field **15** (Procedure Reference).

Procedure: Proc 620 Test 2 (Command Line)

1. To start the procedure, enter **p620 t2**.
2. If you are already in Proc **1620** Test **1**, enter **t2**. The following screen appears.



```
                        ENHANCED MODE - PROCEDURE: 620,   TEST: 2
                                TEST A NETWORK CIRCUIT

   2. Unit Type:--

EQUIPMENT LOCATION                    FAILURE SUMMARY
   3.  Module:--                        13. Number of Circuits Tested:--
   4. Cabinet:--                        14.        Number of Failures:--
   5. Carrier:--
   6.    Slot:--
   7. Circuit:--

STATUS
   8. Location Status:--
   9.    Alarm Status:--
  10.  Circuit Status:--

FAULT
  11.               Index:--
  12. Specific Fault Code:--
  .sp
Connected to CCO OFF-LINE   MAJOR MINOR RUN TAPE BUSY OUT IN USE WAIT

enter command:
```

The switch highlights field 2. Use Test 2 screen to run tests on the selected circuit or a range of circuits. First, you need to select such circuit(s). This screen allows you to choose a single or a range of circuits by unit type, equipment location, or by unit type and by equipment location.

To select all network circuits in the switch:

- Enter **cf2** and then enter **;** so fields 2 and 3 contain a dash. If you skip field 3, the rest of the equipment location field will contain dashes.

To select a circuit by unit type:

- If you do not know a unit type, enter **nu** until the unit type you want to test appears. Unit types appear in numerical order.
- Enter **cf2** and then enter the selected unit type in field 2.

To select a circuit by equipment location:

- Enter **cf3** and enter the Module number in field 3 (select all circuits in a module), or enter the Module number and the Cabinet number in fields 3 and 4 (for all circuits in a Cabinet), or enter the Module number and the Cabinet number and Carrier in fields 3, 4, and 5 (for all circuits in a Carrier), or enter the Module number, the Cabinet number, Carrier, and Slot in fields 3, 4, 5, and 6 (for all circuits in a Slot).

- To select a specific circuit,
  - Enter a Unit number or partial equipment location, then enter **nc** until the circuit you want to test appears in fields 3-7.
  - If the circuit you want is already on the screen, enter **cf3** and then enter the module, carrier, cabinet, slot, and circuit.

- If you selected the unit types that must be busied out, enter **bo**.
- With a selection completed, enter **x** to test this circuit. WAIT appears on the screen. When test is done, WAIT disappears.

3. To see the specific fault code recorded for the failure, enter **nc**. This code will be displayed in Field 12.

Procedure: Proc 600 Test 1 (Active field entry)

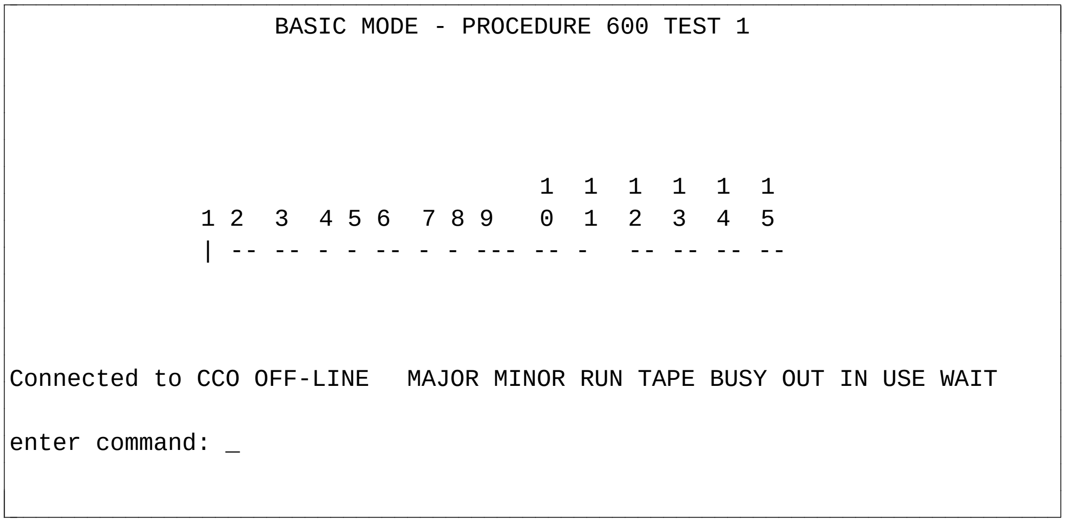
To populate the active fields directly, follow the instructions provided in "Proc Mode Commands" earlier in this chapter. Use the on-line help to get more information on how to administer maintenance procs, or refer to *DEFINITY Communications System Generic 2 Maintenance Procedures* .

Examine Alarms and Errors in Basic Mode

Use proc **600** Test **1** to examine the PMIDS error log.

Procedure: Proc 600 Test 1 (Command line)

1. To examine the PMIDS error log, enter the command **p600** and press **Return**. The Proc **600** Test **1** screen displays.



```
                  BASIC MODE - PROCEDURE 600 TEST 1




                                    1  1  1  1  1  1
             1 2  3  4 5 6  7 8 9   0  1  2  3  4  5
             | -- -- - - -- - - --- -- -  -- -- -- --



Connected to CCO OFF-LINE   MAJOR MINOR RUN TAPE BUSY OUT IN USE WAIT

enter command: _
```

2. Test **1** screen is display only. You can use the Test **1** screen for examining alarms by priority or for resolving alarms. WAIT will appear until sorting is completed.

To examine alarms by priority,

1. Enter **x** to sort active alarms in the PMIDS error log. Press **Return**. Failure Index (field 10) will show the total number of active alarms.
2. Enter **nc** to see each alarm.
   - Unit Type (field 2) may show the unit type of the alarm or error.
   - Equipment Location (fields 3-7) may show the equipment location of the circuit that caused the alarm.
   - Also, the rest of the fields will be populated with the data pertinent to this particular alarm.
   - Go to the procedure shown in Procedure Reference (field 15) to repair the failure that caused the alarm and then return to Proc **600** Test **1**. For example, field 15 shows 20. This means you must run Proc **620** to diagnose the problem.

To resolve alarms,

1. Enter **x** and then **nc** until the alarm you want to resolve appears on the screen.
2. Enter **cdx** to resolve alarms.
3. Enter **t3** to view the resolved alarm in Test **3**.
4. To examine alarms by unit type and search for errors, enter **t2**.

Methods of fault detection and troubleshooting the switch are detailed in *AT&T System 85 Advanced Networking Switch R2V4 Maintenance*. Also, use the on-line Help Facility for reference.

Procedure: Proc 600 Test 1 (Active field entry)

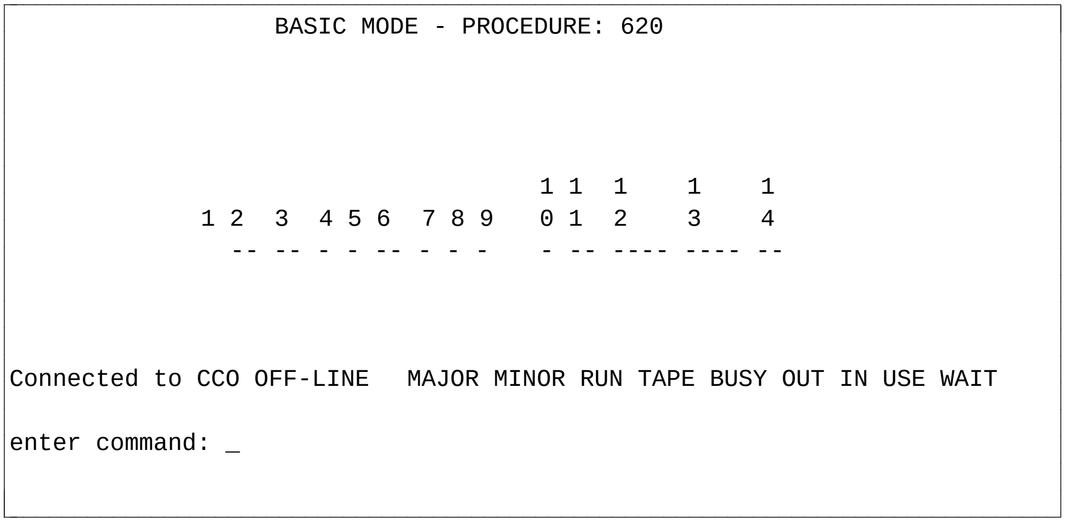
To perform Proc 600 Test 1 using the active field entry, follow the instructions provided in "Proc Mode Commands" earlier in this chapter.

Isolating the Problem in Basic Mode

To isolate the problem, run the maintenance test as indicated in Proc **600** Test **1** Field **15** (Procedure Reference).

Procedure: Proc 620 Test 2 (Command Line)

1. To start the procedure, enter **p620 t2**.
2. If you are already in Proc **1620** Test **1**, enter **t2**. The following screen appears.



```
                  BASIC MODE - PROCEDURE: 620




                                     1 1  1    1    1
             1 2  3  4 5 6  7 8 9    0 1  2    3    4
               -- -- - - -- - - -    - -- ---- ---- --



Connected to CCO OFF-LINE   MAJOR MINOR RUN TAPE BUSY OUT IN USE WAIT

enter command: _
```

The switch highlights field 2. Use Test 2 screen to run tests on the selected circuit or a range of circuits. First, you need to select such circuit(s). This screen allows you to choose a single or a range of circuits by unit type, or equipment location, or by unit type and by equipment location.

To select all network circuits in the switch:

- Enter **cf2** and then enter **;** so fields 2 and 3 contain dash. If you skip field 3, the rest of the equipment location field will contain dashes.

To select a circuit by unit type:

- If you do not know a unit type, enter **nu** until the unit type you want to test appears. Unit types appear in numerical order.
- Enter **cf2** and then enter the selected unit type in field 2.

To select a circuit by equipment location:

- Enter **cf3** and enter the Module number in field 3 (select all circuits in a module), or enter the Module number and the Cabinet number in fields 3 and 4 (for all circuits in a Cabinet), or enter the Module number and the Cabinet number and Carrier in fields 3, 4, and 5 (for all circuits in a Carrier), or enter the Module number, the Cabinet number, Carrier, and Slot in fields 3, 4, 5, and 6 (for all circuits in a Slot).

- To select a specific circuit,
    - Enter a Unit number or partial equipment location, then enter **nc** until the circuit you want to test appears in fields 3-7.
    - If the circuit you want is already on the screen, enter **cf3** and then enter the module, carrier, cabinet, slot, and circuit.
- If you selected the unit types that must be busied out, enter **bo**.
- With a selection completed, enter **x** to test this circuit. WAIT appears on the screen. When test is done, WAIT disappears.

3. To see the specific fault code recorded for the failure, enter **nc**. This code will be displayed in Field 12.

Procedure: Proc 620 Test 2 (Active field entry)

To populate the active fields directly, follow the instructions provided in "Proc Mode Commands" earlier in this chapter. To get more information on administering maintenance procs, refer to *AT&T System 85 Advanced Networking Switch R2V4 Maintenance* .

APPENDIX F. HIGH CAPACITY BACKUP AND RECOVERY FOR 3B2

IMPORTANT PREREQUISITES:

Before you start Backup and Recovery procedures, the following prerequisites must be performed:

1. *Confirm that the* **x-Tape** *package contains all pieces of equipment required for installing the unit with most common 3B2 configurations:*

   - *x-Tape™ drive*
   - *Power cord*
   - *3B2 x-Tape software diskette*
   - *SCSI Extension Cable*
   - *Internal-to-external SCSI cable and SCSI terminator included with the "SCSI Connect Kit" (AT&T #73277). You will need this kit if this is the first external SCSI device that you are connecting to a 3B2/500, 3B2/600, 3B2/700, and 3B2/1000. If you have purchased the SCSI Host Adapter separately, the required cable and terminator are included in the host adapter package.*
   - *Data-grade 8mm tape cartridge.*

2. *Using the* **sysadm listpkg**, *verify that your 3B2 is running UNIX 3.2.1 Version 3 or later release which includes "AT&T 3B2 SCSI Cartridge Tape Utilities Release 3.0" and "AT&T 3B2 SCSI Host Adapter Utilities Release 3.0".*

   For detailed instructions, use "x-Tape for AT&T 3B2 Installation and Operation Guide" prepared by DBM Associates. If the Guide is not available, contact DBM Associates at (908) 534-1665.

WARNING:
The speed and capacity of the x-Tape allow the capability to store a full backup on a single cartridge, therefore allowing unattended backups. We do not recommend or support the storage of multiple backups on a single cartridge, as this procedure does not offer you the best protection for your backups.

Manager IV is highly user-interactive and certain "housekeeping," (or backup) operations must be performed to ensure that the system functions properly. Some of the backup procedures are conducted regularly; others are performed as needed.

Recovery procedures are performed in the event of a problem. One of your most important roles as System Administrator is to recover any files, file systems, or databases that are lost due to hardware failure, power down, or user error. Recovery means restoring the system to a state as close as possible to its state prior to corruption.

Manager IV allows you to back up and recover from the following backup devices: QIC, 9-track, or high capacity (8mm) tape. You must use the backup or recovery tool that supports the tape you choose. The QIC and 9-track tapes are supported by the administration program **bradm**, as described in detail in "Backing up Manager IV Databases" and "Recovering Manager IV Databases" in Chapter 6. The 8mm tapes are supported by the Manager IV **Full Backup**, **Log Backup**, and **Recovery Procedures**.

IMPORTANT:
You may not use the **bradm full_dump**, **bradm log_dump**, or **bradm recovery** commands with 8mm tape. The 8mm tape can be accessed and administered only by using the Manager IV **Full Backup**, **Log Backup**, and **Recovery Procedures** that use the **dd** command to copy and store the data.

The **Backup** and **Recovery Procedures** operate the backup and recovery for the 8mm tape in the same manner as the corresponding **bradm** commands administer the QIC and 9-track tapes. The **Full Backup** and **Log Backup Procedures** are explained in detail in Table F-1; the **Recovery Procedures** are described later in this chapter.

Manager IV does not provide for the backup and recovery procedures of the UNIX filesystems; you are required to use the standard UNIX commands. For more details, refer to *AT&T 3B2 Computer System Administration Guide*.

BACKING UP MANAGER IV DATABASES ONTO THE 8MM TAPE

Software maintenance conducted regularly by the Manager IV System Administrator includes administering the transaction logs and backing up databases to the 8mm tape. The 8mm tape provides you with more efficient backup and recovery procedures: the tape can accommodate up to 2.2 GBytes of data. The following table provides details on backing up the entire Manager IV database and the transaction logs:

Table F-1. Schedule of Software Maintenance

MAINTENANCE FUNCTION	FREQUENCY	RUNNING MODE	PURPOSE
Log Backup Procedure: (backing up the database transaction logs to the 8mm tape) **dd if=/dev/rlog**(*1 ... n*) **bs=64k of=/dev/rmt/c1t7d0s0**	Daily, or as logs become full (done manually upon demand). The system console displays a message requesting the log dump.	Multi-user	Copies only the current unmounted log area which was the previous active log area containing latest entries. **Notes:** ● If not done: - No further Manager IV transactions can be executed due to lack of available disk slice space. - Inability to fully recover changes made to core database.
Full Backup Procedure: (backing up the Manager IV database to the 8mm tape) **dd if=/dev/rlog**(*1 ... n*) **bs=64k of=/dev/rmt/c1t7d0s0n** **dd if=/dev/coredb**(*00 .. ##*) **of=/dev/rmt/c1t7d0s0n bs=64k** **>/dev/rmt/c1t7d0s0**	Weekly (done manually during off-peak hours).	Any UNIX system state with Manager IV shut down (**stopsm**).	Copies the transaction logs and all stored data.

Note: Following is a brief explanation of the commands in the table. It is *important* to read this information to get a better understanding of how the **Log Backup Procedure** and **Full Backup Procedure** are implemented.

- The raw devices: **coredb00 ... coredb##** represent the primary storage where the core database is located.
- The journals are stored in the raw disk partitions: **/dev/rlog1 ... /dev/rlogn**.
- The command **>/dev/rmt/c1t7d0s0** rewinds the tape.
- **c1t7d0s0(n)** specifies the 8mm tape: **c1** is a slot number of the Controller card; **t7** is the Smaller Computer Standard Interface (SCSI) target controller ID for the drive, **n** when specified means "no rewind".
- **bs=64k** designates the block size.

Administration of Manager IV Host Processor

Administration of your host processor is done using the Manager IV **Backup** and **Recovery Procedures** and administration program, **bradm**.

Log in as **root** to perform all **Backup** and **Recovery Procedures** and **bradm** commands.

The following list describes each of the backup procedures (**Full Backup** and **Log Backup**) and **bradm** commands that are available to you when using the 8mm tape.

bradm ?

Displays the command list and a short description of each command.

bradm crash

Run automatically by **startsm** if Manager IV was booted after an abnormal shutdown. It checks to make sure that databases and log devices are in sync.
A warning message is displayed if there is no log device to clean.
Running mode: Manager IV shut down.

Full Backup Procedure Commands:

Dump the logs and core database to the 8mm tape.
Running mode: Manager IV shut down.

dd if=/dev/rlog(*1 ... n*) **of=/dev/rmt/c1t7d0s0n bs=64k**
dd if=/dev/coredb(*00 ... ##*) **of=/dev/rmt/c1t7d0s0n bs=64k**
>/dev/rmt/c1t7d0s0

bradm help <command>

Displays additional instructions on how to use a command.

Log Backup Procedure Commands:

Used to back up a full log device onto the 8mm tape. A warning message is displayed if there is no full log device to back up (one or more log entries qualifies the log as full), or if there is no tape mounted to record the backup.
Running mode: multi-user with Manager IV up.

dd if=/dev/rlog(*1 ... n)* **bs=64k of=/dev/rmt/c1t7d0s0**

bradm log_sw

Used to switch (swap) log devices on demand. The active log device is switched off and the standby log device is switched on and becomes the active log device. This command is usually run automatically by the system and will not be activated if a standby log device has not been mounted.
Running mode: multi-user with Manager IV up.

bradm menu

Displays the command list and a short description of each command.

bradm log_info

Displays status information about the logs.

Scheduling Backups

Manager IV provides procedures for backing up and restoring the core database and journals. In addition to this, you should regularly back up your users' areas. This can be done by using one of the available UNIX System options. It is recommended that the UNIX command **cpio** be used for ease of backup and recovery. It is also recommended that you back up your application at least once after installation and also after any software updates. Your users' areas should be backed up at least once a week and kept for four weeks before you recycle your tapes.

Backups require that you mount 8mm scratch tapes on the system to capture data for storage off-line. A full backup of the entire Manager IV system should be done once a week. This ensures that at least once a week you capture all the changes that have been made to the system.

In addition to weekly full backups, it is recommended that you perform a log dump each day or as necessary to back up the database incremental changes.

Procedure: Backing up the Manager IV Database

Commands:

dd if=/dev/rlog*(1 ... n)* **of=/dev/rmt/c1t7d0s0n bs=64k**
dd if=/dev/coredb*(00 ...##)* **of=/dev/rmt/c1t7d0s0n bs=64k**
>/dev/rmt/c1t7d0s0

The **dd** command is used to copy all stored data from the specified raw disk partitions to the 8mm tape. Following is the **Full Backup Procedure** used in Manager IV to back up the core database and the transaction logs to the 8mm tape.

Full Backup Procedure

1. Log in as **root** and enter your system password.
2. Enter **. /etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. Shut down Manager IV. Enter **stopsm**.
6. Enter the commands to save the journals **/dev/rlog***(1 ... n)* to the tape:

   ```
   dd if=/dev/rlog1 of=/dev/rmt/c1t7d0s0n bs=64k
    dd if=/dev/rlog2 of=/dev/rmt/c1t7d0s0n bs=64k
   ```

   For each of the above listed commands, the number of the *records in* and *records out* will be displayed.

   Note:

   The number of *records in* and *records out* depend on the actual size of the files you are backing up or recovering.

   In this example, the screen is as follows:

   ```
   610+1 records in
   610+1 records out
   ```

7. Enter the commands to save the core database:

   ```
   dd if=/dev/coredb00 of=/dev/rmt/c1t7d0s0n bs=64k
    .
    .
    .
    dd if=/dev/coredb## of=/dev/rmt/c1t7d0s0n bs=64k
    >/dev/rmt/c1t7d0s0
   ```

   The number of *records in* and *records out* appears on the screen.

   ```
   1818+1 records in
   1818+1 records out
   ```

8. Get the journal *size* by entering the command:

   logadm -list /dev/rlog1.

9. Reset the journals:

   ```
   logadm -lglb /dev/rlog1 size
   logadm -lglb /dev/rlog2 size
   ```

10. Restart Manager IV by entering **startsm**.

Performing a Tape Run

Once you have done a full backup, it is recommended that you also do a **tape run** from TCM or FM **admin** at the switch. This will preserve the information at the switch, allowing you to synchronize the data in the switch and the Manager IV database should the two become unsynchronized at any time. Do this in addition to the regularly scheduled tape run, which you set with **admin daily-tape-run schedule**. Refer to "Backing up PBX Downloads" in Chapter 3 for details on **admin daily-tape-run schedule**.

Cron Service Procedures

Cron is a UNIX operating system utility that performs scheduled tasks automatically at specified times. These include checking the status of the transaction logs and switching the log devices.   If cron is not operating, these tasks must be completed manually.

The results of all cron activity are mailed to appropriate users such as smsa, smgr, uucp, adm, and root. The Manager IV System Administrator should monitor all mail to these users and make note of any problems requiring administrative action.

The following table identifies the database maintenance service procedures performed automatically by cron. Procedures for manual execution follow the table.

Table F-2. Cron Service Procedures

SERVICE TASK	FREQUENCY	RUNNING MODE	PURPOSE
Check status of transaction log devices.	Every 30 minutes (done automatically during workday).	● normally: cron-controlled ● manually: multi-user	● Determines if only the active log area is available. ● Generates **log_dump** request at system front console. **Notes:** ● If cron fails to run, both log areas become full. No Manager IV transactions can be executed due to lack of available disk slice space. ● An unusually high number of log entries can fill active log area before **ck_log** does its inspection of remaining disk slice space.
Switch log devices.	Daily (done automatically during off-peak hours).	● normally: cron-controlled ● manually: multi-user	Switches log areas on disk. **Note:** If Manager IV is down when cron is scheduled to run **log_sw**, the transaction log areas are not switched.

Procedure: Switching Log Devices

Command: # bradm log_sw

The **log_sw** command is automatically performed every day by cron during off-peak hours (or as needed by database software). If the processor is down when cron is scheduled to run **log_sw**, this command will not be executed. It can be performed manually in multi-user mode.

Use the command **log_sw** to change the active log area to standby status for copying to tape and to activate the standby log area for recording.

Once you enter the command **log_sw**, you will receive a message that reads "log_sw completed successfully." The active and standby log areas have been switched and the standby log area should be backed up to tape as soon as possible.

You may not fill the active log area during the course of a workday. This would occur when very few changes are made to the database. Depending upon the number of changes, a single active log area may not become filled for several days, weeks, or months. Thus, a single, unfilled log area may contain changes entered over a long time period. If an unexpected disk loss occurs, perhaps because of a head crash, all of those entries will be lost. Because it is more difficult to remember all of the changes entered over several weeks than it is to remember a single day's entries, the log areas are forcibly switched every day. This sets aside the partially filled log area for later backup and directs all new journal entries to a fresh log area.

Procedure: Backing up the Full Transaction Logs

Command:

```
dd if=/dev/rlog(1 ... n) bs=64k of=/dev/rmt/c1t7d0s0
```

The **Log Backup Procedure** allows you to copy the database transaction logs to the 8mm tape if the logs become full. In the event of a system failure, use this Procedure to save the current Transaction Logs. Refer to "Procedure: Restoring the Core Database"later in this appendix. The **Log Backup Procedure** uses the **dd** command to copy all stored data from the specified raw disk partitions to the 8mm tape.

All changes to the core database are recorded in the transaction log as journal entries. Two separate journal areas operate alternately. One area serves as the active device to record new changes, while the other area remains in the standby mode. When the active log (journal area) becomes full, the logs are switched and the standby area becomes the new active device, while the full journal area is placed in the "full" mode. The **Log Backup Procedure** backs up the contents of the filled device. Logs are sequentially numbered for identification. After the log area is backed up, the log area is "scratched" (reset to 0) so that it can become the standby area.

A **Log Backup Procedure** must be performed in multi-user mode with Manager IV up.

Log Backup Procedure

Start a **Log Backup Procedure** by mounting a tape. Use a separate tape for each log backup.

1. Log in at the system console as **root**
2. Enter **./etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. To determine which log to dump, enter:

   logadm -old.

This command will print "/dev/rlog1", "/dev/rlog2" or nothing if the log is empty. If "dev/rlog1" displays, it is the log to dump.

6. To dump the log, enter:

   dd if=/dev/rlog*(1 ... n)* **bs=64k of=/dev/rmt/c1t7d0s0**

   This command depends on the log you want to copy. In this example, the screen is as follows:

```
610+1 records in
610+1 records out
```

7. To get information for the tape label, enter:

   logadm -list /dev/rlog*(1 ... n)*

   On the screen, the journal sequence, size and mount flag (should be "n") appear. In this example, the following information appears:

```
  14  78120  n  /dev/rlog1
```

   The numbers will depend on the actual journal sequence and size on your system. Put this information on the label.

8. Initialize the log file by entering the command:

   logadm -lglb /dev/rlog*(1 ... n) size.*

   Note:
   Use the journal *size* as displayed by the **logadm -list** command (78120 in this example).

9. To remount the journal, enter:

   logadm -mall

Procedure: Displaying Database Journaling Status

Command: # bradm log_info

This procedure reports on the status of the database journaling process.

1. Enter **bradm log_info [-s] [-l [log1][log2]] -c**

   The options are defined as follows:

   — **-s** prints current mounted log device information.

   — **-l [log1]** prints the long listing of log 1.

   — **-c** prints status information.

RECOVERING MANAGER IV DATABASES

The Manager IV core database and log devices are partitioned throughout the processor disks.

Journaling, or the storage of system information on the 8mm backup tapes, is a critical part of the recovery process. If you fail to do backups—full backups (**Full Backup Procedure**) weekly and incremental backups (**Log Backup Procedure**)—as necessary, your system cannot be restored adequately.

In addition to the information on the backup tapes you make, Manager IV provides a method for restoring information about completed transactions in the transaction log. As a user successfully enters data for a transaction, the information that changes the Manager IV database is stored in the active transaction log. To add additional insurance that this information is protected against loss, the transaction log is located on a disk separate from the disk where the Manager IV core database resides. Thus, if the core database (which stores switch information) is corrupted, the transaction log is protected.

Using the Recovery Procedure and Bradm Command

In the event of a system crash, use the **Recovery Procedure** to restore the core database and the Transaction Logs from the Full Backup 8mm tape. The **bradm** commands that can be used for recovery processes are **bradm crash, bradm help, bradm menu**, and **bradm log_info**. See "Administration of the Manager IV Host Processor" in this chapter for more information on the **bradm** tool.

When recovering the core database, you must begin with the latest Full Backup 8mm tape, and supplement that information with information from additional Transaction Log 8mm tapes.

Procedure: Restoring the Core Database

Command:

```
dd if=/dev/rmt/c1t7d0s0n of=/dev/coredb00 bs=64k
.
.
.
dd if=/dev/rmt/c1t7d0s0n of=/dev/coredb## bs=64k
>/dev/rmt/c1t7d0s0
```

Major recovery of the Manager IV database from the 8mm tape is done through the **Recovery Procedure**. The **Recovery Procedure** is identical to the **bradm recovery** command used with the QIC and 9-track tapes. In the **Recovery Procedure**, you are required to perform three major steps:

- Save the current Transaction Logs
- Restore the core database from a Full Backup
- Apply the Transaction Logs to the core database.

Before starting the **Recovery Procedure**, mount the 8mm tape.

Core Recovery Procedure

WARNING: Always start **Core Recovery Procedure** from saving the current Transaction Logs.

Before restoring the core database, it is necessary to save the journals which had not yet been backed up at the time of the failure. The procedure for this is *almost* identical to the procedure for normal backup of journals. Make sure you use a separate tape for saving each current Transaction Log.

Saving the Current Transaction Logs

1. Log in at the system console as **root**
2. Enter **./etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. To determine which log to save, enter:

   logadm -old -ab.

   This command will print "/dev/rlog1", "/dev/rlog2" or nothing if the log is empty.
6. To dump the log, enter:

   dd if=/dev/rlog*(1 ... n)* **bs=64k of=/dev/rmt/c1t7d0s0**

   This command depends on the log you want to save. In this example, the screen is as follows:

   ```
   610+1 records in
   610+1 records out
   ```

7. To get information for the tape label, enter:

   logadm -list /dev/rlog*(1 ... n)*

   On the screen, the journal sequence, size and mount flag (should be "n") appear. In this example, the following information appears:

   ```
     14  78120  n  /dev/rlog1
   ```

   The numbers will depend on the actual journal sequence and size on your system. Put this information on the label.
8. Initialize the log file by entering the command:

   logadm -lglb /dev/rlog*(1 ... n) size.*

   Note:
   Use the journal *size* as displayed by the **logadm -list** command (78120 in this example).

Recovering the Core Database

1. Log in as **root** and enter your system password.
2. Skip over the Logs on the Full Backup tape:

   ```
   </dev/rmt/c1t7d0s0n
   </dev/rmt/c1t7d0s0n
   ```

3. Restore the core database from the Full Backup tape by entering:

   ```
     dd if=/dev/rmt/c1t7d0s0n of=/dev/coredb00 bs=64k
     .
     .
     .
     dd if=/dev/rmt/c1t7d0s0n of=/dev/coredb## bs=64k
     >/dev/rmt/c1t7d0s0
   ```

   In this example, the screen is as follows:

   ```
   1881+1 records in
   1881+1 records out
   ```

   Note:

   Disregard the error message "**dd:write error: Error 0"** that appears only if the **dd** command is used to recover a disk slice whose length, in 512 byte blocks, is an odd number. The tape drive cannot save an odd number of blocks; therefore, the data will be padded with an extra block which will not fit on the disk slice.

4. Apply the Transaction Logs to the core database as described in "Procedure: Restoring a Transaction Log".

Procedure: Restoring a Transaction Log

This procedure explains how to apply (restore) the Transaction Logs saved to the Log Backup 8mm tape(s) to the core database. Manager IV is down.

Log Recovery Procedure

1. Log in at the system console as **root**
2. Enter **. etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. Enter **skill -u**. This command kills semaphores lingering from crash.
6. Enter **echo $SYSROOT/etc/fmboot -m |su smdba**
7. To determine which log to apply, enter:

   ```
   devadm
   ls -l
    /dev/coredb00
    q
   ```

The following screen appears:

```
fsname  devno  devnm  pgno  npgs log  (m)  time
prod  0  /dev/coredb00 0 50000 32 (n) Fri Feb 3 10:59:13 19
```

In this example, under the **log** column, **32** is displayed (this number depends on the actual sequence number of the latest log applied). The log to be loaded must be one number higher, i.e. **33** in this example.

8. Load log **33** from the backup media:

   ```
   dd if=/dev/rmt/c1t7d0s0 of=/dev/rlog1 bs=64k
   ```

   The system displays a number of *records in* and *out*.

9. Apply the log:

   ```
   devadm
   redo -c
   ```

   The system responds with the message:

   Log device name #33? _

   Enter:

   ```
   /dev/rlog1
   ```

   The system displays "Restoration completed". Enter:

   ```
   q
   ```

10. Initialize the log by entering:

    ```
    logadm -lglb /dev/rlog1 size
    ```

    Note:

    Use the journal *size* as displayed by the **logadm -list** command (78120 in this example). The *size* is the same for both journals.

11. Repeat steps 8 through 10 for each journal including the logs saved by the procedure "Backing Up the Full Transaction Logs".

APPENDIX G. HIGH CAPACITY BACKUP AND RECOVERY FOR 386 PC AT

IMPORTANT PREREQUISITES:

Before you start Backup and Recovery procedures, the following prerequisites must be performed:

1. *Confirm that the* **x-Tape** *package contains all pieces of equipment required for installing the unit with most common 386 configurations:*

   - *x-Tape™ drive*
   - *Power cord*
   - *386 x-Tape software diskette*
   - *SCSI Extension Cable*
   - *Internal-to-external SCSI cable and SCSI terminator included with the "SCSI Connect Kit" (AT&T #73277). You will need this kit if this is the first external SCSI device that you are connecting to a 386 PC AT. If you have purchased the SCSI Host Adapter separately, the required cable and terminator are included in the host adapter package.*
   - *Data-grade 8mm tape cartridge.*

2. *Using the* **displaypkg**, *verify that your 386 is running UNIX 3.2.2 or later release which includes "AT&T 386 SCSI Cartridge Tape Utilities Release 3.0" and "AT&T 386 SCSI Host Adapter Utilities Release 3.0".*

   For detailed instructions, use "x-Tape for AT&T 386 Installation and Operation Guide" prepared by DBM Associates. If the Guide is not available, contact DBM Associates at (908) 534-1665.

WARNING:
The speed and capacity of the x-Tape allow the capability to store a full backup on a single cartridge, therefore allowing unattended backups. We do not recommend or support the storage of multiple backups on a single cartridge, as this procedure does not offer you the best protection for your backups.

Manager IV is highly user-interactive and certain "housekeeping," (or backup) operations must be performed to ensure that the system functions properly. Some of the backup procedures are conducted regularly; others are performed as needed.

Recovery procedures are performed in the event of a problem. One of your most important roles as System Administrator is to recover any files, file systems, or databases that are lost due to hardware failure, power down, or user error. Recovery means restoring the system to a state as close as possible to its state prior to corruption.

Manager IV allows you to back up to and recover from the following backup devices: QIC, 9-track, or high capacity (8mm) tape. You must use the backup or recovery tool that supports the tape you choose. The QIC and 9-track tapes are supported by the administration program **bradm**, as described in detail in "Backing Up Manager IV Databases" and "Recovering Manager IV Databases" in Chapter 6. The 8mm tapes are supported by the Manager IV **Full Backup**, **Log Backup**, and **Recovery Procedures**.

IMPORTANT:
You may not use the **bradm full_dump**, **bradm log_dump**, or **bradm recovery** commands with 8mm tape. The 8mm tape can be accessed and administered only by using the Manager IV **Full Backup**, **Log Backup**, and **Recovery Procedures** that use the **dd** command to copy and store the data.

The **Backup** and **Recovery Procedures** operate the backup and recovery for the 8mm tape in the same manner as the corresponding **bradm** commands administer the QIC and 9-track tapes. The **Full Backup** and **Log Backup Procedures** are explained in detail in Table G-1; the **Recovery Procedures** are described later in this chapter.

Manager IV does not provide for the backup and recovery procedures of the UNIX filesystems; you are required to use the standard UNIX commands. For more details, refer to *AT&T 3B2 Computer System Administration Guide*.

BACKING UP MANAGER IV DATABASES ONTO THE 8MM TAPE

Software maintenance conducted regularly by the Manager IV System Administrator includes administering the transaction logs and backing up databases to the 8mm tape. The 8mm tape provides you with more efficient backup and recovery procedures: the tape can accommodate up to 2.2 GBytes of data. The following table provides details on backing up the entire Manager IV database and the transaction logs:

Table G-1. Schedule of Software Maintenance

MAINTENANCE FUNCTION	FREQUENCY	RUNNING MODE	PURPOSE
Log Backup Procedure: (backing up the database transaction logs to the 8mm tape) **dd if=/dev/rlog**(*1 ... n*) **bs=64k of=/dev/scsi/xtape1**	Daily, or as logs become full (done manually upon demand). The system console displays a message requesting the log dump.	Multi-user	Copies only the current unmounted log area which was the previous active log area containing latest entries. **Note:** ● If not done: - No further Manager IV transactions can be executed due to lack of available disk slice space. - Inability to fully recover changes made to core database.
Full Backup Procedure: (backing up the Manager IV database to the 8mm tape) **dd if=/dev/rlog**(*1 ... n*) **bs=64k of=/dev/scsi/xtape1n** **dd if=/dev/coredb**(*00 .. ##*) **of=/dev/scsi/xtape1n bs=64k** **>/dev/scsi/xtape1**	Weekly (done manually during off-peak hours).	Any UNIX system state with Manager IV shut down (**stopsm**).	Copies the transaction logs and all stored data.

Note: Following is a brief explanation of the commands used in the table. It is *important* to read this information to get a better understanding of how the **Log Backup Procedure** and **Full Backup Procedure** are implemented.

- The raw devices: **coredb00 ... coredb##** represent the primary storage where the core database is located.
- The journals are stored in the raw disk partitions: **/dev/rlog1 ... /dev/rlogn**.
- The command **>/dev/scsi/xtape1** rewinds the tape.
- **xtape1** specifies the 8mm tape with rewind after reading or writing.
- **xtape1n** specifies the 8mm tape without rewind after reading or writing.
- **bs=64k** designates the block size.

Administration of Manager IV Host Processor

Administration of your host processor is done using the Manager IV **Backup** and **Recovery Procedures** and administration program, **bradm**.

Log in as **root** to perform all **Backup** and **Recovery Procedures** and **bradm** commands.

The following list describes each of the backup procedures (**Full Backup** and **Log Backup**) and **bradm** commands that are available to you when using the 8mm tape.

bradm ?

Used to display the command list and a short description of each command.

bradm crash

Run automatically by **startsm** if Manager IV was booted after an abnormal shutdown. It checks to make sure that databases and log devices are in sync.
A warning message is displayed if there is no log device to clean.
Running mode: Manager IV shut down.

Full Backup Procedure Commands:

Dump the logs and core database to the 8mm tape.
Running mode: Manager IV shut down.

dd if=/dev/rlog(*1 ... n*) **of=/dev/scsi/xtape1n bs=64k**
dd if=/dev/coredb(*00 ... ##*) **of=/dev/scsi/xtape1n bs=64k**
>/dev/scsi/xtape1

bradm help <command>

Displays additional instructions on how to use a command.

Log Backup Procedure Commands:

Used to back up a full log device onto the 8mm tape. A warning message is displayed if there is no full log device to back up (one or more log entries qualifies the log as full), or if there is no tape mounted to record the backup.
Running mode: multi-user with Manager IV up.

dd if=/dev/rlog(*1 ... n)* **bs=64k of=/dev/scsi/xtape1**

bradm log_sw

Used to switch (swap) log devices on demand. The active log device is switched off and the standby log device is switched on and becomes the active log device. This command is usually run automatically by the system and will not be activated if a standby log device has not been mounted.
Running mode: multi-user with Manager IV up.

bradm menu

Used to display the command list and a short description of each command.

bradm log_info

Used to display status information about the logs.

Scheduling Backups

Manager IV provides procedures for backing up and restoring the core database and journals. In addition to this, you should regularly back up your users' areas. This can be done by using one of the available UNIX System options. It is recommended that the UNIX command **cpio** be used for ease of backup and recovery. It is also recommended that you back up your application at least once after installation and also after any software updates. Your users' areas should be backed up at least once a week and kept for four weeks before you recycle your tapes.

Backups require that you mount 8mm scratch tapes on the system to capture data for storage off-line. A full backup of the entire Manager IV system should be done once a week. This ensures that at least once a week you capture all the changes that have been made to the system.

In addition to weekly full backups, it is recommended that you perform a log dump each day or as necessary to back up the database incremental changes.

Procedure: Backing up the Manager IV Database

Commands:

```
dd if=/dev/rlog(1 ... n) of=/dev/scsi/xtape1n bs=64k
dd if=/dev/coredb(00 ...##) of=/dev/scsi/xtape1n bs=64k
>/dev/scsi/xtape1
```

The **dd** command is used to copy all stored data from the specified raw disk partitions to the 8mm tape. Following is the **Full Backup Procedure** used in Manager IV to back up the core database and the transaction logs to the 8mm tape.

Full Backup Procedure

1. Log in as **root** and enter your system password.
2. Enter **. /etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. Shut down Manager IV. Enter **stopsm**.
6. Enter the commands to save the journals **/dev/rlog***(1 ... n)* to the tape:

   ```
   dd if=/dev/rlog1 of=/dev/scsi/xtape1n bs=64k
    dd if=/dev/rlog2 of=/dev/scsi/xtape1n bs=64k
   ```

   For each of the above listed commands, the number of the *records in* and *records out* will be displayed.

   Note:

   The number of *records in* and *records out* depend on the actual size of the files you are backing up or recovering.

   In this example, the screen is as follows:

   ```
   610+1 records in
   610+1 records out
   ```

7. Enter the commands to save the core database:

   ```
   dd if=/dev/coredb00 of=/dev/scsi/xtape1n bs=64k
     .
     .
     .
    dd if=/dev/coredb## of=/dev/scsi/xtape1n bs=64k
    >/dev/scsi/xtape1
   ```

   The number of *records in* and *records out* appears on the screen.

   ```
   1818+1 records in
   1818+1 records out
   ```

8. Get the journal *size* by entering the command:

   logadm -list /dev/rlog1.

9. Reset the journals:

   logadm -lglb /dev/rlog1 *size*
   logadm -lglb /dev/rlog2 *size*

10. Restart Manager IV by entering **startsm**.

Performing a Tape Run

Once you have done a full backup, it is recommended that you also do a **tape run** from TCM or FM **admin** at the switch. This will preserve the information at the switch, allowing you to synchronize the data in the switch and the Manager IV database should the two become unsynchronized at any time. Do this in addition to the regularly scheduled tape run, which you set with **admin daily-tape-run schedule**. Refer to "Backing up PBX Downloads" in Chapter 3 for details on **admin daily-tape-run schedule**.

Cron Service Procedures

Cron is a UNIX operating system utility that performs scheduled tasks automatically at specified times. These include checking the status of the transaction logs and switching the log devices. If cron is not operating, these tasks must be completed manually.

The results of all cron activity are mailed to appropriate users such as smsa, smgr, uucp, adm, and root. The Manager IV System Administrator should monitor all mail to these users and make note of any problems requiring administrative action.

The following table identifies the database maintenance service procedures performed automatically by cron. Procedures for manual execution follow the table.

Table G-2. Cron Service Procedures

SERVICE TASK	FREQUENCY	RUNNING MODE	PURPOSE
Check status of transaction log devices.	Every 30 minutes (done automatically during workday).	● normally: cron-controlled ● manually: multi-user	● Determines if only the active log area is available. ● Generates **log_dump** request at system front console. **Notes:** ● If cron fails to run, both log areas become full. No Manager IV transactions can be executed due to lack of available disk slice space. ● An unusually high number of log entries can fill active log area before **ck_log** does its inspection of remaining disk slice space.
Switch log devices.	Daily (done automatically during off-peak hours).	● normally: cron-controlled ● manually: multi-user	Switches log areas on disk. **Note:** If Manager IV is down when cron is scheduled to run **log_sw**, the transaction log areas are not switched.

Procedure: Switching Log Devices

Command: # bradm log_sw

The **log_sw** command is automatically performed every day by cron during off-peak hours (or as needed by database software). If the processor is down when cron is scheduled to run **log_sw**, this command will not be executed. It can be performed manually in multi-user mode.

Use the command **log_sw** to change the active log area to standby status for copying to tape and to activate the standby log area for recording.

Once you enter the command **log_sw**, you will receive a message that reads "Log devices were switched at: Date/time." The active and standby log areas have been switched and the standby log area should be backed up to tape as soon as possible.

It is possible to not fill the active log area during the course of a workday. This would occur when very few changes are made to the database. Depending upon the number of changes, a single active log area may not become filled for several days, weeks, or months. Thus, a single, unfilled log area may contain changes entered over a long time period. If an unexpected disk loss occurs, perhaps because of a head crash, all of those entries will be lost. Because it is more difficult to remember all of the changes entered over several weeks than it is to remember a single day’s entries, the log areas are forcibly switched every day. This sets aside the partially filled log area for later backup and directs all new journal entries to a fresh log area.

Procedure: Backing up the Full Transaction Logs

Command:

dd if=/dev/rlog*(1 ... n)* **bs=64k of=/dev/scsi/xtape1**

The **Log Backup Procedure** allows you to copy the database transaction logs to the 8mm tape if the logs become full. In the event of a system failure, use this Procedure to save the current Transaction Logs. Refer to "Procedure: Restoring the Core Database" later in this appendix. The **Log Backup Procedure** uses the **dd** command to copy all stored data from the specified raw disk partitions to the 8mm tape.

All changes to the core database are recorded in the transaction log as journal entries. Two separate journal areas operate alternately. One area serves as the active device to record new changes, while the other area remains in the standby mode. When the active log (journal area) becomes full, the logs are switched and the standby area becomes the new active device, while the full journal area is placed in the "full" mode. The **Log Backup Procedure** backs up the contents of the filled device. Logs are sequentially numbered for identification. After the log area is backed up, the log area is "scratched" (reset to 0) so that it can become the standby area.

A **Log Backup Procedure** must be performed in multi-user mode with Manager IV up.

Log Backup Procedure

Start a **Log Backup Procedure** by mounting a tape. Use a separate tape for each log backup.

1. Log in at the system console as **root**
2. Enter **./etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. To determine which log to dump, enter:

   logadm -old.

This command will print "/dev/rlog1", "/dev/rlog2" or nothing if the log is empty. If "dev/rlog1" displays, it is the log to dump.

6. To dump the log, enter:

   dd if=/dev/rlog*(1 ... n)* **bs=64k of=/dev/scsi/xtape1**

   This command depends on the log you want to copy. In this example, the screen is as follows:

   ```
   610+1 records in
   610+1 records out
   ```

7. To get information for the tape label, enter:

   logadm -list /dev/rlog*(1 ... n)*

   On the screen, the journal sequence, size and mount flag (should be "n") appear. In this example, the following information appears:

   ```
    14  78120  n  /dev/rlog1
   ```

   The numbers will depend on the actual journal sequence and size on your system. Put this information on the label.

8. Initialize the log file by entering the command:

   logadm -lglb /dev/rlog*(1 ... n) size.*

   Note:
   Use the journal *size* as displayed by the **logadm -list** command (78120 in this example).

9. To remount the journal, enter:

   logadm -mall

Procedure: Displaying Database Journaling Status

Command: # bradm log_info

This procedure reports on the status of the database journaling process.

1. Enter **bradm log_info [-s] [-l [log1][log2]] -c**

   The options are defined as follows:

   — **-s** prints current mounted log device information.

   — **-l [log1]** prints the long listing of log 1.

   — **-c** prints status information.

RECOVERING MANAGER IV DATABASES

The Manager IV core database and log devices are partitioned throughout the processor disks.

Journaling, or the storage of system information on the 8mm backup tapes, is a critical part of the recovery process. If you fail to do backups—full backups (**Full Backup Procedure**) weekly and incremental backups (**Log Backup Procedure**)— as necessary, your system cannot be restored adequately.

In addition to the information on the backup tapes you make, Manager IV provides a method for restoring information about completed transactions in the transaction log. As a user successfully enters data for a transaction, the information that changes the Manager IV database is stored in the active transaction log. To add additional insurance that this information is protected against loss, the transaction log is located on a disk separate from the disk where the Manager IV core database resides. Thus, if the core database (which stores switch information) is corrupted, the transaction log is protected.

Using the Recovery Procedure and Bradm Command

In the event of a system crash, use the **Recovery Procedure** to restore the core database and the Transaction Logs from the Full Backup 8mm tape. The **bradm** commands that can be used for recovery processes are **bradm crash, bradm help, bradm menu**, and **bradm log_info**. See "Administration of the Manager IV Host Processor" in this chapter for more information on the **bradm** tool.

When recovering the core database, you must begin with the latest Full Backup 8mm tape, and supplement that information with information from additional Transaction Log 8mm tapes.

Procedure: Restoring the Core Database

Command:

```
dd if=/dev/scsi/xtape1n of=/dev/coredb00 bs=64k
.
.
.
dd if=/dev/scsi/xtape1n of=/dev/coredb## bs=64k
>/dev/scsi/xtape1
```

Major recovery of the Manager IV database from the 8mm tape is done through the **Recovery Procedure**. The **Recovery Procedure** is identical to the **bradm recovery** command used with the QIC and 9-track tapes. In the **Recovery Procedure**, you are required to perform the three major steps:

- Save the current Transaction Logs
- Restore the core database from a Full Backup
- Apply the Transaction Logs to the core database.

Before starting the **Recovery Procedure**, mount the 8mm tape.

Core Recovery Procedure

WARNING:

Always start **Core Recovery Procedure** from saving the current Transaction Logs.

Before restoring the core database, it is necessary to save the journals which had not yet been backed up at the time of the failure. The procedure for this is *almost* identical to the procedure for normal backup of journals. Make sure you use a separate tape for saving each current Transaction Log.

Saving the Current Transaction Logs

1. Log in at the system console as **root**
2. Enter **./etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. To determine which log to save, enter:

   logadm -old -ab.

   This command will print "/dev/rlog1", "/dev/rlog2" or nothing if the log is empty.
6. To dump the log, enter:

   dd if=/dev/rlog*(1 ... n)* **bs=64k of=/dev/scsi/xtape1**

   This command depends on the log you want to save. In this example, the screen is as follows:

   ```
   610+1 records in
   610+1 records out
   ```

7. To get information for the tape label, enter:

   logadm -list /dev/rlog*(1 ... n)*

   On the screen, the journal sequence, size and mount flag (should be "n") appear. In this example, the following information appears:

   ```
     14  78120  n  /dev/rlog1
   ```

   The numbers will depend on the actual journal sequence and size on your system. Put this information on the label.
8. Initialize the log file by entering the command:

   logadm -lglb /dev/rlog*(1 ... n) size.*

   Note:
   Use the journal *size* as displayed by the **logadm -list** command (78120 in this example).

Recovering the Core Database

1. Log in as **root** and enter your system password.
2. Skip over the Logs on the Full Backup tape:

   </dev/scsi/xtape1n/
   </dev/scsi/xtape1n

3. Restore the core database from the Full Backup tape by entering:

   dd if=/dev/scsi/xtape1n of=/dev/coredb00 bs=64k
   .

```
.
.
dd if=/dev/scsi/xtape1n of=/dev/coredb## bs=64k
>/dev/scsi/xtape1
```

In this example, the screen is as follows:

```
1881+1 records in
1881+1 records out
```

Note:

> Disregard the error message "**dd:write error: Error 0**" that appears only if the **dd** command is used to recover a disk slice whose length, in 512 byte blocks, is an odd number. The tape drive cannot save an odd number of blocks; therefore, the data will be padded with an extra block which will not fit on the disk slice.

4. Apply the Transaction Logs to the core database as described in "Procedure: Restoring a Transaction Log".

Procedure: Restoring a Transaction Log

This procedure explains how to apply (restore) the Transaction Logs saved to the Log Backup 8mm tape(s) to the core database. Manager IV is down.

Log Recovery Procedure

1. Log in at the system console as **root**
2. Enter **. etc/envlist**
3. Enter **. $SYSROOT/etc/envlist.br**
4. Enter **PATH=$PATH:$SYSGEN:/etc:$SYSROOT/etc**
5. Enter **skill -u**. This command kills semaphores lingering from crash.
6. Enter **echo $SYSROOT/etc/fmboot -m |su smdba**
7. To determine which Log to apply, enter:

   ```
   devadm
   ls -l
    /dev/coredb00
    q
   ```

   The following screen appears:

   ```
   fsname devno devnm    pgno  npgs   log  (m)  time
   prod  0  /dev/coredb00 0  50000  32 (n) Fri Feb 3 10:59:13 19
   ```

   In this example, under the **log** column, **32** is displayed (this number depends on the actual sequence number of the latest log applied). The log to be loaded must be one number higher, i.e. **33** in this example.

8. Load Log **33** from the backup media:

   ```
   dd if=/dev/scsi/xtape1 of=/dev/rlog1 bs=64k
   ```

The system displays a number of *records in* and *out*.

9. Apply the Log:

   devadm
   redo -c

   The system responds with the message:

   Log device name #33? _

   Enter:

   /dev/rlog1

   The system displays "Restoration completed!". Enter:

   q

10. Initialize the Log by entering:

    logadm -lglb /dev/rlog1 *size*

    Note:

    Use the journal *size* as displayed by the **logadm -list** command (78120 in this example). The *size* is the same for both journals.

11. Repeat steps 8 through 10 for each journal including the Logs saved by the procedure "Backing Up the Full Transaction Logs".

INDEX