DMS-100 Family

SuperNode Data Manager Exception Reporting
User Guide

NORTEL NETWORKS™
How the world shares ideas.

DMS-100 Family

SuperNode Data Manager Exception Reporting

User Guide

Publication history

April 2001

SDMCom015 and up Standard 09.01. Upversioned for Gate SDMCom015 Gate 3.

October 2000

SDMCom014 and up Standard 08.02. Upversioned for the SDM00014 Gate 3 release.

August 2000

SDMCom014 and up Preliminary 08.01. Upversioned for the SDM00014 Gate 3 release.

June 2000

SDMCom013 and up Standard 07.02. Upissued for the SDMN0013 Gate 3 release.

Februrary 2000

SDMCom013 and up Standard 07.01. Upversioned for SDMCom013 release for changes made to the installation procedures.

August 1999

SDMCom012 and up Standard 06.01. Upversioned for SDMCom012 release for changes made to the installation procedures.

May 1999

SDMCom011 and up Standard 05.02. Upissued to incorporate editing changes.

February 1999

SDMCom011 and up Standard 05.01. Upversioned to correct publication history and ordering codes.

December 1998

SDMCom010 and up Standard 04.06. Upissued to resolve cross references.

October 1998

SDMCom010 and up   Standard 04.05. Upissued to reflect the change to the middle layer number back to 5051.

April 1998

SDMCom009 and up   Standard 04.04. Upissued to add installation steps for DCE tools in the "Installing client common resources and DCE tools software" procedure.

February 1998

SDMCom009 and up   Standard 04.03. Upissued to replace incorrect graphic.

February 1998

SDMCom009 and up Standard 04.02. Upissued to incorporate editing changes.

February 1998

SDMCom009 and up   Standard 04.01. Upversioned to make changes to the ER client software installation procedure.

January 1998

SDMComF08 and up   Standard 03.02. Upissued to update the information on the knowledge base (chapter 1)

October 1997

SDMComF084 and up   Standard 03.01. Upversioned to delete references to DataVision Viewer 2.2. Also added flowcharts in chapters 2 and 3.

August 1997

SDMComF07 and up   Standard 02.04. Upissued to finalize changes introduced in SDMN0003 Release software.

June 1997

SDMComF07   Preliminary 02.03. Upissued to remove references to SWERs and TRAPS and "delete/keep log types not broadcast" options, and to include editorial and pagination corrections.

May 1997

SDMComF07   Preliminary 02.02. Upissued to include changes to the installation procedures (Chapter 2) and the reference to a new version of the DataVision Viewer 2.2 User Guide. ("About this document").

March 1997

SDMComF07   Draft 02.01. Upversioned to include changes introduced in SDMComF07 Release software.

May 1995

SDML0002   Standard 01.02. Upissued to include changes introduced in SDM02.1 Maintenance Release software.

October 1994

SDML0002   Preliminary 01.01. First release of this document.

Contents

About this document

This document describes the SuperNode Data Manager (SDM) Exception Reporting application, including procedures for installing and running the application, and using the graphical user interface (known as the Log Customization Utility). The document is intended for system administrators and maintenance personnel.

Organization of this document

The following table describes the organization of this document.

Table 1

Chapter	Title	Description
1	Understanding Exception Reporting	Describes the application and lists all of the category 0 and 1 log types.
2	ER server software installation or upgrade	Explains how to install the server software on the SDM.
3	ER client software installation or upgrade	Explains how to install the client software on client workstations.
4	Using the Log Customization Utility	Describes the Log Customization Utility and how to invoke the Log Customization Utility on a client workstation. Explains how to use and edit the windows. Describes the steps for logging in to the utility as well as logging out.
5	Threshold management	Describes the procedures for changing the threshold information using the Log Customization Utility.
6	Log reports	Describes the log report generated by the Exception Reporting application and defines all of the category 0 and 1 log types.
7	Appendix: ER status messages	Describes the ER status messages, what each message means, and what actions you must take to resolve problems.

How to check the version and issue of this document

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

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

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

To determine which version and issue of this document applies to the software in your office, check the release information in *DMS-100 Family Guide to Northern Telecom Publications*, 297-1001-001.

References in this document

The following documents are referred to in this document:

- *SuperNode Data Manager Fault-tolerant User Guide, 297-5061-906*

- Log Report Reference Manual, 297-XXX-840 (Note - XXX=8041 for LEC or 8021 for LET offices)

- OSF DCE Administration Guide — Core Components, ISBN 0–13–185844–0, Release 1.1 (1995), Open Software Foundation, Inc., 11 Cambridge Center, Cambridge, MA 02142

What precautionary messages mean

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

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

Examples of the precautionary messages follow.

ATTENTION Information needed to perform a task

ATTENTION

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

DANGER Possibility of personal injury

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

WARNING Possibility of equipment damage

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

CAUTION Possibility of service interruption or degradation

> **CAUTION**
> **Possible loss of service**
> Before continuing, confirm that you are removing the card from the inactive unit of the peripheral module (PM). Subscriber service is lost if you remove a card from the active unit.

Writing conventions

This section describes the writing conventions used in this document.

Input prompt

An input prompt (> or #) indicates that the information that follows is a command:

>**LIST**

Commands and fixed parameters

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

>**LIST ALL**

UNIX commands and fixed parameters that are entered at the SDM are shown in lowercase and uppercase letters, depending on the UNIX syntax:

>echo $TERM

Variables

Variables that are entered at a MAP terminal are shown in lowercase letters:

>TABLE table_name

UNIX variables that are entered at the SDM are shown in italicized lowercase letters:

>setenv TERM *term_type*

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

Responses

The result of an action is described using italic text. System responses are shown in the following typeface:

```
WARNING: Are you sure you want to Busy the SDM?
Please Confirm ('y' or 'n'):
```

1 Understanding Exception Reporting

This chapter describes the DMS SuperNode Data Manager (SDM) Exception Reporting application, including how it relates to SDM, the architecture of the application, and the source logs.

Overview

The SDM Exception Reporting application performs event correlation using an expert system, and generates exception reports to alert operating company personnel of any detected conditions that may require attention. The expert system is controlled by a knowledge base that analyzes the incoming log stream to identify log exceptions, based on the type and volume of logs received, and on call traffic information from the switch.

How the Exception Reporting application relates to SDM

SDM is the Nortel Networks operations, administration, and maintenance (OA&M) processing complex for the DMS SuperNode switch. SDM is a high-performance UNIX computing platform and software applications environment that allows operating companies to operate, administer, maintain, and provision DMS SuperNode components and services. The Exception Reporting application delivers exception reports to the SDM Log Delivery application.

Exception Reporting architecture

The Exception Reporting application uses a third-party expert system on the SDM to correlate selected DMS SuperNode logs (including SDM logs) into actionable exception report logs. The application uses an inference engine to generate exception reports. The inference engine processes the incoming logs and call traffic information and, if certain conditions are met, generates exception logs.

Inference engine

The inference engine is the software that uses the knowledge base information to detect, track, and provide notification of potential problems. The inference engine generates exception report logs based on logs sent to the inference engine by the SDM log delivery software.

When a log is received, the inference engine checks the knowledge base to see if a rule exists for that log type. If no rules are associated with that log type or the rules have been disabled, no further action is taken.

Otherwise, the inference engine applies the associated rules to process the log data, in relation to the current time, threshold values, and recent call statistics. If required, an exception report is generated.

Exception report logs

All exception report logs are generated with the same log name (EXC). You can specify a log number for EXC reports, in the range 900–999. The default log number for all EXC reports is 900.

The body of every exception report contains the following information:

- a component field that shows component information (if any) that the system used in generating the exception report (only for log types that can be tracked on a component level)

- an event field that explains why the exception report was generated

- an information field that indicates the number of logs and their type, covered by the exception report.

- a correlation ID field that contains a unique identifier that can be used to link repeat notifications

All calculations in the inference engine are based on the time when the log is received, according to the SDM clock. The timestamp on an incoming log header is ignored. All exception reports are generated using SDM time.

Knowledge base

The SDM knowledge base uses rules to analyze the incoming DMS SuperNode and SDM log streams and identify the log reports that are associated with specific scenarios.

You can set threshold values to specify that if a certain number of logs of a given type are received within a specific time interval, the system generates an exception report. Or you can set traffic-based thresholds that cause the system to generate an exception report when a certain number of logs of a given type have been received within the duration of a specific number of calls.

Log types that are tracked at the system level only are called Category 0 logs. Log types that are tracked at the component level are called Category 1 logs. Log types that are tracked at both the component and system level are also called Category 1 logs. For more information about Category 0 and 1 logs, refer to Table Table 1-1, " Category 0 and 1 logs,".

How the knowledge base works

The system or component threshold values specify how many logs of the same log type are received before an exception report is generated.

The time interval specifies how many hours, minutes, or seconds elapse before an exception report is generated. The traffic interval specifies how many calls elapse (using a formula based on a set of OM registers) before an exception report is generated.

When the rate of log generation reaches the threshold, the system generates an exception report and sets the interval. Once the interval has expired and the rate of log generation reaches the threshold, the system generates a repeat notification. The notification lets you know how many logs the system generated within the interval. If the interval expires and the rate of log generation has not reached the threshold, then the system does not generate a repeat notification. Instead, normal monitoring resumes and the system waits until the rate of log generation again reaches the threshold, regardless of the interval.

Thresholding and suppression by way of LOGUTIL

All logs processed by the SDM, including those analyzed by the Exception Reporting application, are subject to suppression or thresholding controls. The suppression or thresholding controls are configured by the DMS LOGUTIL tool. The DMS LOGUTIL tool examines each log to see if it is a suppressed log or a threshold log.

The Exception Reporting application does not receive suppressed logs. Therefore, suppressed logs do not cause the system to generate an exception report.

The Exception Reporting application does receive logs that have reached the threshold. However, the number of logs reported is the number of logs that have reached the threshold, not the number of logs received.

> **CAUTION**
> **Risk of inaccurate reporting**
> To ensure accurate analysis of log data, threshold and suppression controls applied by using the LOGUTIL should be disabled for any logs analyzed by Exception Reporting.

An SDM615 log report is generated daily (8:00 a.m., local time), listing the report names of all logs received for which the threshold capability has been enabled and Exception Reporting criteria have been specified. Either remove

the threshold settings (using LOGUTIL) or adjust the Exception Reporting criteria, to ensure the accuracy of any exception reports generated.

Source log categories

A log category is a common group of log types that the knowledge base handles in a generic fashion. The knowledge base analyzes two categories of log types: category 0 and category 1; category 1P (prime) logs are a subset of category 1 logs. The Exception Reporting application provides default values of thresholds, exception report severity, and interval definitions for each log category. These values can be customized, on the basis of log type, to track category 1 problems on the system level, an individual component level, both levels, or not at all (no exception report). These values can also be customized, on the basis of log type, to track category 0 problems on the system level or not at all.

The operating company can modify the threshold values through the Log Customization Utility graphical user interface (GUI). Users can specify the following:

- no exception report logs be generated for a given log type by disabling its system and component thresholds

- exception report logs, for a given category 1 log type, be generated only on the basis of individual components

- exception report logs be generated for a log type only on the basis of its system threshold

- exception report logs for a given category 1 log type are generated based on both the component threshold and the system threshold

Category 0 logs

For category 0 logs, the Exception Reporting application provides the ability to track problems on the system level only.

System threshold values can be set to specify that if a certain number of logs of a given type are received within a set interval, an exception report log with a particular severity is generated. One of four severity levels can be specified: none, minor, major, and critical.

The severity level of the exception reports is independent of the severity of the originating logs because the inference engine does not look at the severity of the incoming log when it processes it. For example, the inference engine makes no distinction between receiving four critical logs and receiving four minor logs.

The following example shows a severity threshold defined for log type C7UP116, a category 0 log type.

Figure 1-1 Severity threshold for a Category 0 log

| Office Name | Threshold Settings | | | | Exception Log | | Tracking | |
	System	Compon.	in every	Criteria	Severity	Number	S	C
Log Name: C7UP116								
ECCOMB_SD	1	15	5	hours	none	900	√	
FCC1_0	20	0	300	CMCalls	minor	900	√	√
ottwaonxxt01	15	0	3	CMCalls	minor	900	√	√
ottwaonye69	7	0	3	CMCalls	minor	900	√	√
ottwaonye6a	20	0	300	CMCalls	minor	900	√	√
ottwonye61							√	√
OTWAON10FC	30	2	3	CMCalls	none	900	√	√

View: By Log   Total: 7   Viewing: all   Sorted by "Office Name" no changes

This example indicates that the knowledge base generates an exception report with severity "none" when one C7UP116 log is received from the office shown, within 5 hours.

If this rule is disabled (that is, if tracking is disabled), no exception reports are generated.

Category 1 logs

For category 1 logs, the Exception Reporting application provides the ability to track problems from the system and from the component level. Again, all exception reports generated (whether at the system or the component level) will have a specified severity, independent of the severity of the incoming logs.

Component-level tracking generates exception reports when the number of logs, whose component identifier shows the same value, exceeds a specified threshold. The component identifier is specific to the log type and can not be customized.

The various component identifiers used by category 1 logs are the following:

- trunk ID
- route ID
- Common Language Location Identifier (CLLI)
- subsystem number
- network plane
- message switch (MS) number
- name of a failed test
- failure reason codes
- peripheral module (PM)
- line equipment number (LEN)

The following example shows a severity threshold defined for log type C7UP100, a category 1 log type.

Figure 1-2 Severity threshold for Category 1 log

| Log Name | C7UP100 ▼ | | | | Apply... | | | |

Office Name	Threshold Settings				Exception Log		Tracking	
	System	Compon.	in every	Criteria	Severity	Number	S	C
ECCOMB_SD	19	15	3	CMCalls	none	900	✓	
FCC1_0	20	0	300	CMCalls	minor	900	✓	✓
ottwaonxxt01	15	0	3	CMCalls	minor	900	✓	✓
ottwaonye69	7	0	3	CMCalls	minor	900	✓	✓
ottwaonye6a	20	0	300	CMCalls	minor	900	✓	✓
ottwonye61 ⑦							✓	✓
OTWAON10FC	30	2	3	CMCalls	none	900	✓	✓

View: By Log   Total: 7   Viewing: all   Sorted by "Office Name" no changes

This example indicates that the knowledge base generates an exception report with severity "none" when 19 C7UP100 logs, or 15 C7UP100 logs with identical component-identifier values, are received from the office shown within the duration of 3 CM Calls.

Category 1P (prime)

This category has logs with two component identifiers, where either component can be faulty. For example, trunk logs can indicate a problem on either the originating side, terminating side, or both sides of the trunk.

For example, the following C7UP102 log is received:

```
C7UP102 JUL06 10:19:04 3716 FLT REL DUE TO ABNORMAL
COND
ORIG LEN HOST 44 0 03 24 DN 4297508 TERM CKT
HLFXNS0103T2 761
REPORTED BY CKT HLFXNS0103T2 761
REASON = EXPECTED: ACM/ANM RECEIVED: NOTHING
CLDNO = 18003699330
```

This log indicates a problem between the components LEN HOST 44 0 03 24 and the trunk identified by HLFXNS0103T2 761. Category 1P logs have component-level tracking against both of their component identifiers, independently. An exception report generates when the number of logs with the same value of either component identifier exceeds a specified threshold. Again, the two component identifiers are specific to the log type and cannot be customized. The following example shows severity thresholds as defined for log type C7UP102, a category 1P log.

Figure 1-3 Severity threshold for a Category 1P log

| Log Name | C7UP102 ▼ | | | | | | | Apply... |

| | Threshold Settings | | | | Exception Log | | Tracking | |
Office Name	System	Compon.	in every	Criteria	Severity	Number	S	C
ECCOMB_SDM								
FCC1_0								
ottwaonxxt01	13	3	2	minutes	major	900		
ottwaonye69	13	3	2	minutes	major	900		
ottwaonye6a	20	0	300	CMCalls	minor	900	✓	✓
ottwonye61	⑦						✓	✓
OTWAON10FCC	30	2	3	CMCalls	none	900	✓	✓

| View: By Log | Total: 7 | Viewing: all | Sorted by "Office Name" no changes |

This example indicates that the knowledge base generates an exception report, with severity "major", when 13 C7UP102 logs, or 3 C7UP102 logs with identical values for either of their component identifiers, are received from the office shown, within 2 minutes.

List of logs and categories

The following table lists the source log types used for this release, and indicates their categories.

Table 1-1
Category 0 and 1 logs (Sheet 1 of 2)

Log type	Category	Log type	Category	Log type	Category
AUDT110	1	CM103	0	MM113	0
AUDT113	1	CM104	0	MS103	0
AUDT116	1	CM111	0	MS303	1
AUDT201	1	CM112	0	MS304	1
AUDT603	1	CM115	0	MS305	1
C7UP100	1	CM116	0	MS306	1
C7UP101	1P	CM120	0	MS307	1
C7UP102	1P	CM122	0	MS313	1
C7UP107	1	CM134	0	NET130	0
C7UP111	1	CM141	0	NETM104	0
C7UP112	1P	CM145	0	NETM109	0
C7UP116	0	ENET111	1	NETM112	0
CCS101	1	ENET120	1	NETM116	0
CCS103	1	ENET203	1	PM100	1
CCS107	1	ENET205	1	PM101	1
CCS153	1	ENET211	1	PM102	1
CCS154	1	ENET502	0	PM107	1
CCS158	1	ENET505	0	PM109	1
CCS164	1	LINE100	1	PM110	1
CCS167	1	MM100	0	PM114	1
CCS168	1	MM101	0	PM115	1
CCS170	1	MM110	0	PM116	1
CCS175	1	MM111	0	PM117	1
CCS204	1	MM112	0	PM118	1

Table 1-1   (Continued)
Category 0 and 1 logs (Sheet 2 of 2)

Log type	Category	Log type	Category	Log type	Category
PM125	1	PM189	1	TRK107	1
PM179	1	SLM403	0	TRK113	1P
PM181	1	SYNC203	0	TRK117	1
PM183	1	SYNC206	0	TRK123	1P
PM187	1	SYNC209	0		

2 ER server software installation or upgrade

This chapter describes how to install or upgrade the Exception Reporting (ER) server software on the SuperNode Data Manager (SDM). You must complete the installation procedures in the order outlined in this chapter.

You must have root user privileges to perform the installation procedures in this chapter.

The SDM software packages contain both the server software and the client software. The Software Inventory Manager (SWIM) feature allows you to install one or more application on the SDM using one procedure.

Note: Nortel Networks recommends that you use the batch installation steps when instructed, to reduce the amount of time required to install SDM applications.

You must complete the installation and configuration procedures in the order outlined in this chapter. This chapter discusses the following topics:

* Limitations and restrictions
* Compiling a list of server software filesets
* Installing or upgrading the ER software image on the SDM
* Configuring the server application software using SWIM
* Starting the ER server on the SDM
* Removing an ER server

Limitations and restrictions

The following limitations and restrictions apply to installing ER:

* The SDM for the remote client workstation must be configured in the DCE cell before installing ER software. For information on DCE, refer to the

DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide, 297-5061-906.

- The NA009, NA0010, NA0011, or NA0012 computing module (CM) software must be installed.

The following limitations and restrictions apply to running ER:

- The maximum number of offices supported by the ER client is 300.

- The maximum number of log types supported by the ER application is 200.

- The state of the ER application should appear as InSv. If it is ISTb, then call-based thresholding is not functional, although all other aspects of the application are supported. The ER application appears as ISTb when the Operation Measurements application is initializing.

- When multiple ER applications are updating data on the same SDM, data that is stored on the SDM reflects the last change made.

- Avoid log suppression and thresholding on the CM through the LOGUTIL system for log types that are being tracked by the ER application. CM log thresholding is monitored by the ER application, which reports an SDM615 log daily, listing any logs being stored on the CM that are being tracked by the expert system.

- EXC logs cannot be added to the list of logs tracked by ER. This restriction is required to prevent exception looping.

- Only category 0 logs can be deleted.

- If the type of thresholding is changed between call-based thresholding and time-based thresholding while the threshold is currently enabled, there will be a transitional period where results are unpredictable.

  Note: Each of the following limitations and restrictions are followed by the recommended action, shown in italic text.

- Under certain SDM-CM link conditions, the OM application will fail to remain InSv. Under this condition, the OM application moves from InSv to ISTb and back to InSv within 75 seconds. This cycle is repeated three

times, after which the OM application is failed. This condition occurs when the following sequence happens:

— All applications are InSv.

— All DS512 links move to a state other than OPEN.

— One or more DS512 links change to OPEN after 1 min. or more of being in the previous state.

The corrective action is to change the SDM state to OFFL, then change the SDM state to ManB and InSv.

• Only one Log Customization Utility application should apply changes to one SDM at a time. If more than one user applies a large number of changes simultaneously, a few of the changes may fail, with the message "Communications failure (dce/rpc)" appearing in the Event Logger window.

If this occurs, the log parameters not applied will have a change flag still set, next to the parameter. The failed changes can be reapplied by performing another Apply operation.

The following are prerequisites for installing the server software:

• installation of the SDM base software

• system administrator (root) and maintenance (maint) access to the SDM

• sdm_admin or cell_admin privileges for the DCE cell

Compiling a list of server software filesets

ATTENTION

Nortel Networks recommends that you use the batch installation steps in this section to reduce the amount of time required to install SDM applications.

Prerequisite for batch installation of SDM application software

You must have a list of software filesets for each application you wish to install or upgrade. Before beginning the installation procedures, refer to the user guide of each application for a list of filesets.

ER filesets

Before you begin the installation procedure for ER, you must record the name of its server fileset as shown in the SWIM display of the server's Remote Maintenance Interface (RMI). You must refer to this information during the installation procedures that follow in this chapter.

The SWIM menu displays the ER fileset in one of the following forms:

- SDM_SURV.excrep (name view)

- ER (description view)

    Note 1: The VIEW command on the SWIM main menu allows you to change the way the system displays the filesets. Use VIEW to toggle between the fileset name view and the fileset description view.

    Note 2: If you also wish to install other applications at this time, refer to the fileset descriptions in their respective NTPs.

Once you have recorded the fileset information, you can, if necessary, refer to other SDM application NTPs for fileset information regarding other applications. If you have completed the list of filesets for all of the applications you wish to install, go directly to the procedure, "Installing the software on the SDM server using SWIM".

Installing or upgrading the ER software on the SDM server using the SWIM

The following section describes how to install the SDM server software using SWIM.

SDM server software package

Use the following procedure to install a software install image from a digital audio tape (DAT), or from an SDM hard disk drive. This procedure applies to an initial installation of ER software only.

You must have root user access to the SDM to perform this procedure.

ATTENTION

Make sure that the SDM is configured in the DCE cell before performing this procedure. Refer to the SuperNode Data Manager Fault-tolerant User Guide for information about how to configure the SDM in a DCE cell.

Installing the software using SWIM

The SWIM package is part of the SDMN0012 base software release. SWIM provides the user interface (UI) for local SDM software installation and maintenance. You can access SWIM from the Remote Maintenance Interface (RMI). For more information on SWIM, see the *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide.* Nortel Networks recommends that

you use the batch installation steps in this section to reduce the amount time required to install SDM applications.

ATTENTION

Before you can perform an installation using SWIM, you must have the SDMPL012 software installed on the SDM.

The following flowchart summarized the installation procedures for the SFT software.

Figure 2-1 Summary of Installing or upgrading the software image using SWIM

This flowchart summarizes the procedure.

Use the instructions that follow this flowchart to perform the procedure.

Log into the SDM as the root user

Select the source device

Select the application fileset

Select another application fileset?   Y

N

Apply the fileset(s)

End
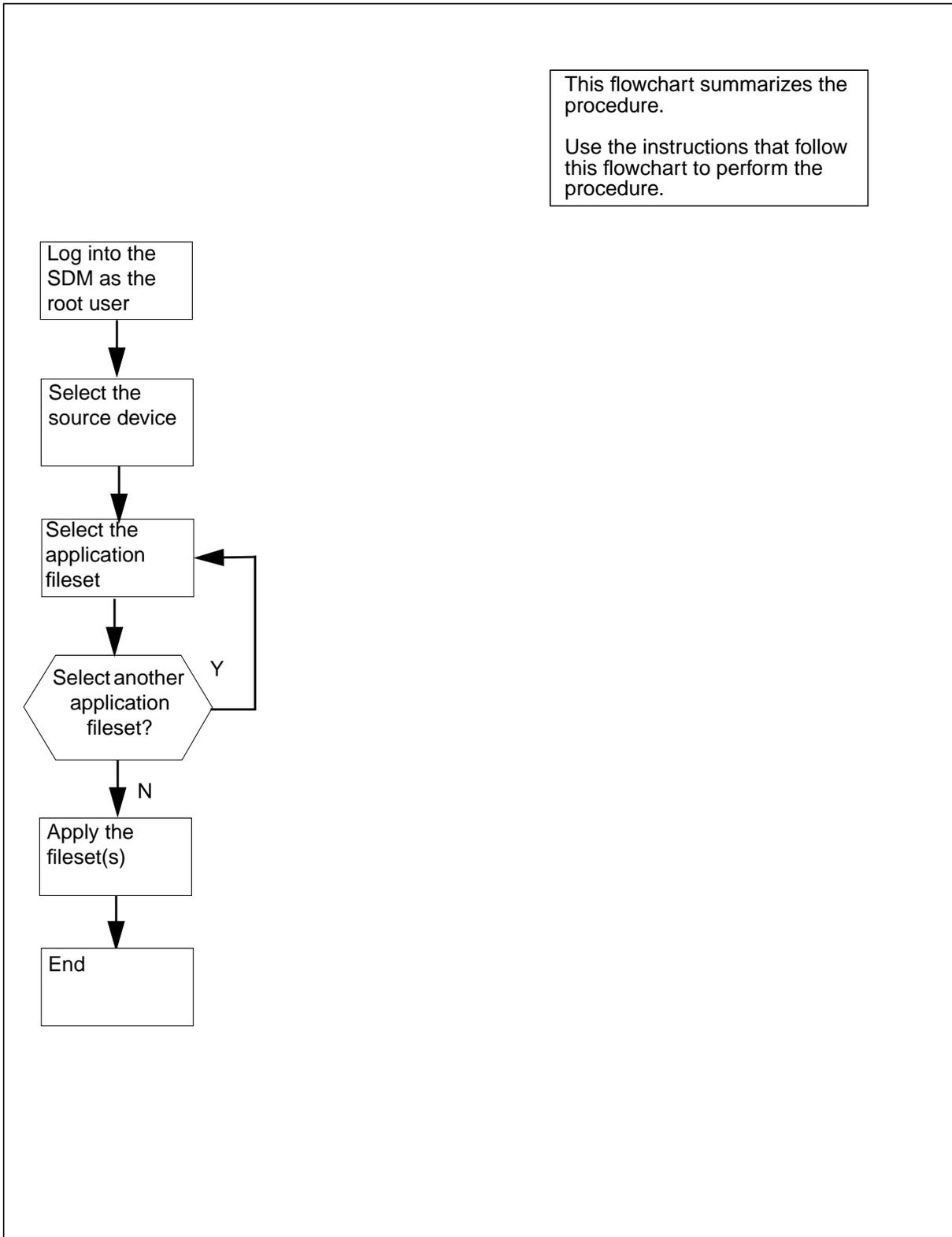
Procedure 2-1 Installing or upgrading the software on the SDM server using SWIM

At the local or remote VT100 console

1   Log into the SDM as the root user.

2   Determine if you are installing the software image using the tape, or the disk.

If	Do
you are using the tape	step 3
you are using the disk	step 5

At the SDM tape drive

3   Insert the tape containing the SDM application packages into the SDM tape drive.

Figure 2-2 shows how to insert the tape into the DAT drive.

Figure 2-2 Inserting the tape into the DAT drive in domain 0 (slot 2)
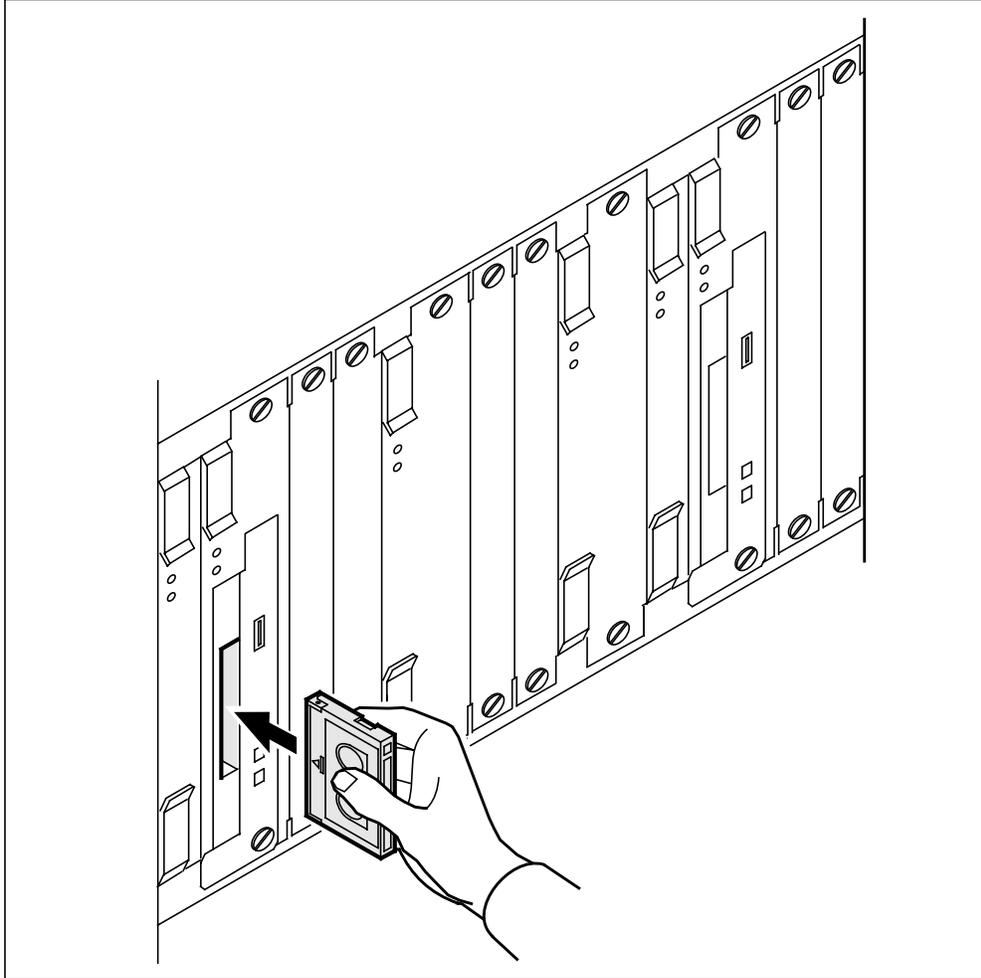
At the local or remote VT100 console

4　　Access the SDM maintenance interface, and the application source by typing

　　　`#sdmmtc apply n`

　　　and pressing the Enter key.

　　　where

　　　　n
　　　　　is the domain where you have inserted the tape.

If	Do
you inserted the tape into the tape drive in slot 2 (domain 0)	sdmmtc apply 0, and go to step 6.
you inserted the tape into the tape drive in slot 13 (domain 1)	sdmmtc apply 1, and go to step 6.

5   Access the SDM maintenance interface, and select the source by typing

#sdmmtc apply *directory*

and pressing the Enter key.

where

> **directory**
> is the name of the directory for the disk.

6   The system displays a list of filesets that are available on the tape drive. Each fileset has an identification number shown in the column under the number symbol.

Example response of the Apply menu level:

```
Source Device: Tape drive on the main chassis slot 2
# Fileset Description            Current     Available
1 Client Common Resources        13.0.13.0  14.0.14.0 i
2 Log Delivery Service           13.0.13.0  14.0.14.0 i
3 Platform Maintenance           13.0.13.0  14.0.14.0 i
4 OM Access Service              13.0.13.0  14.0.14.0 i
5 Table Access Service           13.0.13.0  14.0.14.0 i
6 Enhanced Terminal Access       NA         14.0.14.0 i
7 Installation & Upgrade Tools   13.0.13.0  14.0.14.0 i
8 Installation & Upgrade Lists   13.0.13.0  14.0.14.0 i
9 Secure File Transfer           NA         14.0.14.0 i
10 Exception Reporting           NA         14.0.14.0 i
```

> **Note 1:** *You can use the Up/Down commands to view additional filesets if the list extends beyond one screen. Also, you can use the Filter command to shorten the list.*

> **Note 2:** *When shown in the fileset list, install fileset images appear with a letter **i** to separate them from corrective content images. If you apply the install image, the system removes all archived versions of that fileset from the SDM hard disk. For more information about the Apply command menu, see the DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide.*

7   Select the application fileset that you want to install. If necessary, refer to the list of filesets that you recorded in the previous section titled "Compiling a list of server software filesets". To select the application fileset, type

>select *n*

and press the Enter key.

where

> **n**
> is the identification number listed next to the fileset shown in the column under the number symbol (#) in the SWIM Apply level.

In the example response shown in step 6, the identification number for Enhanced Terminal Access is 6, for Secure File Transfer, the number is 9, for Exception Reporting the number is10.

After you have selected a fileset, the system highlights the fileset on the terminal. The system displays the total number of selected filesets on the top right corner of the SDM maintenance interface.

8   Repeat step 7 for any other application filesets that you wish to install. When you have selected the filesets you want to install, go to the next step.

9   Apply the selected software fileset(s) by typing

>**apply**

and pressing the Enter key.

> *Note 1:* The system checks for warnings or errors before it exercises the apply command. If you have selected any filesets that also require installation of other filesets, the system generates a warning message. The warning message indicates that the SDM will apply the matching filesets even though you have not selected them.

> *Note 2:* If the system warns that the newly installed fileset is in the failed state, you must remove and reinstall the fileset. For the procedure to remove a fileset, refer to the *SuperNode Data Manager Upgrade Guide, 297-5051-304.* If the newly installed fileset appears in the failed state at the second attempt, contact your next level of support.

10   Exit the SDM maintenance interface by typing

>**quit all**

and pressing the Enter key.

11   You have completed this procedure.

Check that the SDM has configured the software for each application you installed. If the SDM did not configure the software for the application, you must configure the software manually. Refer to the procedure "Configuring the server application software using SWIM".

Configuring the server application software using SWIM

The following section describes how to configure the server application software using SWIM. SWIM lets you install and maintain the local SDM software. You can access SWIM from the RMI. For more information about SWIM, see the *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide.*

ATTENTION
Before you can perform an installation using SWIM, you must have the SDM base software installed on the SDM.

Preparing the Distributed Computing Environment (DCE) for the application software

Before configuring the ER application software, DCE must be commissioned and in-service. You must have a DCE account with administrative privileges to add application servers such as ER, ETA, and Secure File Transfer.

ATTENTION

If you use the sdm_admin account to perform this procedure, and the account does not exist, you can use the cell_admin account instead. You also can exit the procedure, and go to the "DCE Creating an SDM administration account" procedure to create the sdm_admin account. Return to this procedure after you have created an sdm_admin account.

CAUTION
Risk of revealing the administrative user password
If you use telnet to access the SDM remotely, and use the default sdm_admin or cell_admin "master administrator" account to add the application server, the system sends the password of the administrative user in clear text across the network. To prevent this security risk, Nortel Networks recommends that you execute the command from a terminal attached to the SDM console port.

Both the sdm_admin and cell_admin accounts have the required privileges to make changes to the DCE cell. However, the sdm_admin account functions as a sub-administrator with limited privileges. The sdm_admin account performs administrative tasks related to the SDM within the DCE cell.

The sub-administrator account requires the following privileges:

- the ability to create accounts

- the ability to add a permission to the SDM server organization

- the ability to a add permission to the sdm-servers-using-cds group

- the ability to insert and modify a permission to the access control list (ACL on the /.:/subsys/NT/SDM CDS directory.

Configuring the application software

The following flowchart summarizes the installation procedures for configuring the application software.

Note: To complete the procedure for configuring the application software, perform the step-action procedures that follow the flowchart.

Figure 2-3 Summary of Configuring the server application software using SWIM
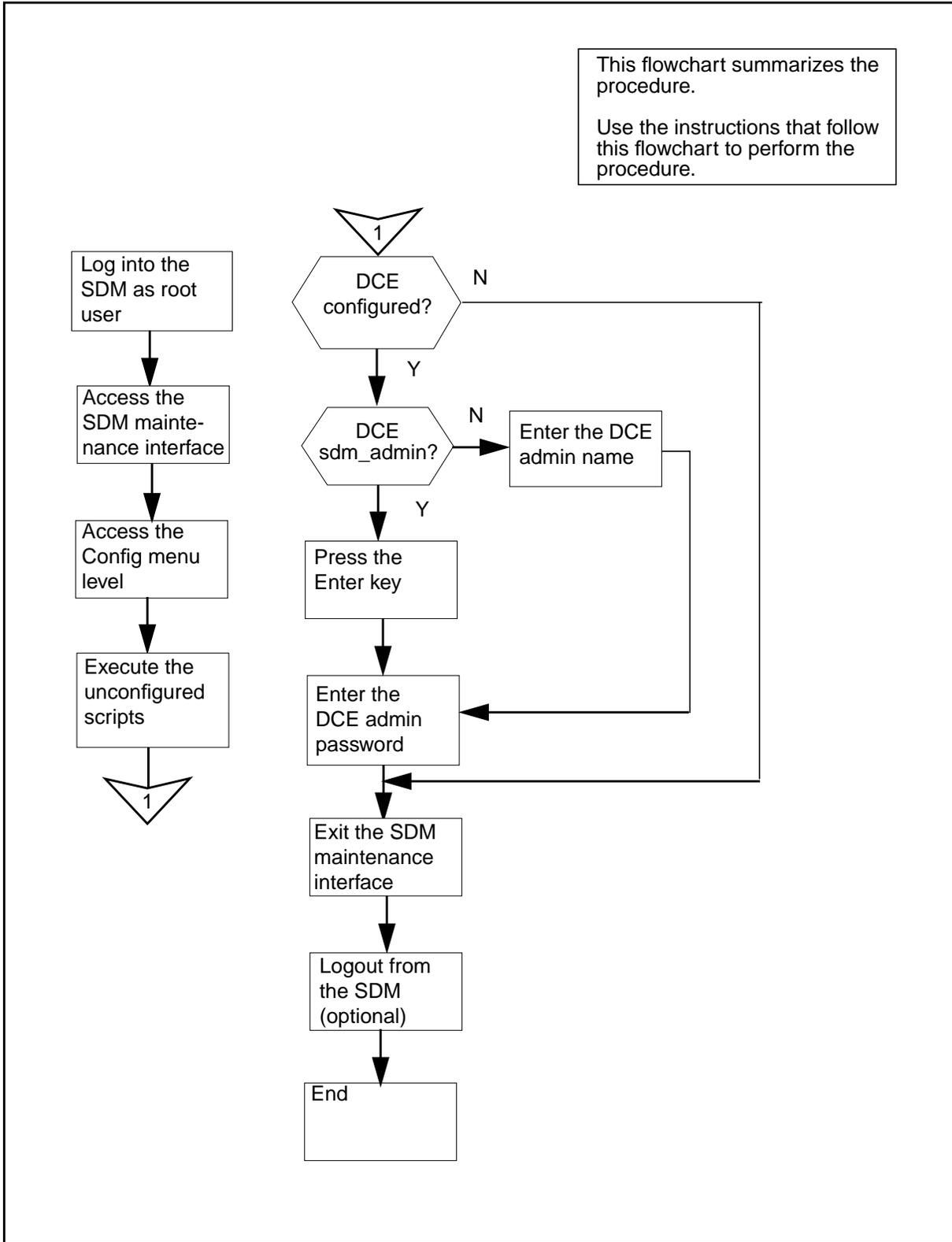
Procedure 2-2 Configuring the server application software using SWIM

At a local or remote VT100 console:

1   Log into the SDM as the root user.

2   Access the SDM RMI by typing

`#sdmmtc`

and pressing the Enter key.

The system displays the top menu level of the RMI.

3   Access the Config menu by typing

`>config`

and pressing the Enter key.

The system displays the Config menu that lists the filesets available for installation.

Example response:

```
# Fileset Description       Status
1 Enhanced Terminal Access  Unconfigured
2 Secure File Transfer      Secure and Normal FTP Access
3 Exception Reporting       Configured
```

4   Execute the unconfigured interactive configuration scripts by typing

`>config `*`n`*

and pressing the Enter key.

where

> ***n***
>   is the number next to the fileset you want to configure.

5   If you have commissioned DCE, the following prompt appears:

```
Please enter the DCE administrator id: [sdm_admin]
```

If	Do
DCE is not commissioned	Step 6
DCE is commissioned	Step 7

6   Press the Enter key.

The system returns to the SDM maintenance interface screen.

Go to step 9.

7   The system prompts you to enter a DCE administrator name. To accept the default DCE account (cell_admin), press the Enter key, or enter another DCE administrator account.

Example response:

```
Enter the password for the DCE administrator sdm_admin:
```

> ***Note:*** You can also type another DCE account with administrative privileges (cell_admin), as described at the beginning of this procedure.

8   At the "Password:" prompt, type

password

and press the Enter key. The system configures the fileset and returns you to the Config menu level.

where

> **password**
> is the password for the DCE administrator account name.

9   To exit from the SDM maintenance interface, type

>quit all

and press the Enter key.

10   To logout from the SDM, type

#exit

and press the Enter key.

> **Note:** At this time, you do not have to logout from the SDM. You can continue with other procedures.

11   You have completed this procedure.

Starting the ER server on the SDM

Use the following procedure to start the ER server on the SDM.

The following flowchart summarizes the procedure to start the ER server on the SDM. To complete the procedure, perform the step-action procedure that follows the flowchart.

Figure 2-4 Summary of Starting the ER server on the SDM

```
┌─────────────────────────────────────────────────────────────────┐
│                                                                   │
│                                          ┌──────────────────────┐ │
│   ┌──────────────────┐                   │ This flowchart       │ │
│   │ Log into the SDM │                   │ summarizes the       │ │
│   │ as the mainte-   │                   │ procedure.           │ │
│   │ nance user       │                   │                      │ │
│   └──────────────────┘                   │ Use the instructions │ │
│            │                             │ that follow          │ │
│            ▼                             │ this flowchart to    │ │
│   ┌──────────────────┐                   │ perform the          │ │
│   │ Access the       │                   │ procedure.           │ │
│   │ RMI              │                   └──────────────────────┘ │
│   └──────────────────┘                                            │
│            │                                                      │
│            ▼                                                      │
│   ┌──────────────────┐                                           │
│   │ Access the       │                                           │
│   │ Appl menu        │                                           │
│   │ level            │                                           │
│   └──────────────────┘                                           │
│            │                                                      │
│            ▼                                                      │
│   ┌──────────────────┐                                           │
│   │ Start the ER     │                                           │
│   │ application      │                                           │
│   └──────────────────┘                                           │
│            │                                                      │
│            ▼                                                      │
│   ┌──────────────────┐                                           │
│   │ End              │                                           │
│   └──────────────────┘                                           │
│                                                                   │
└─────────────────────────────────────────────────────────────────┘
```
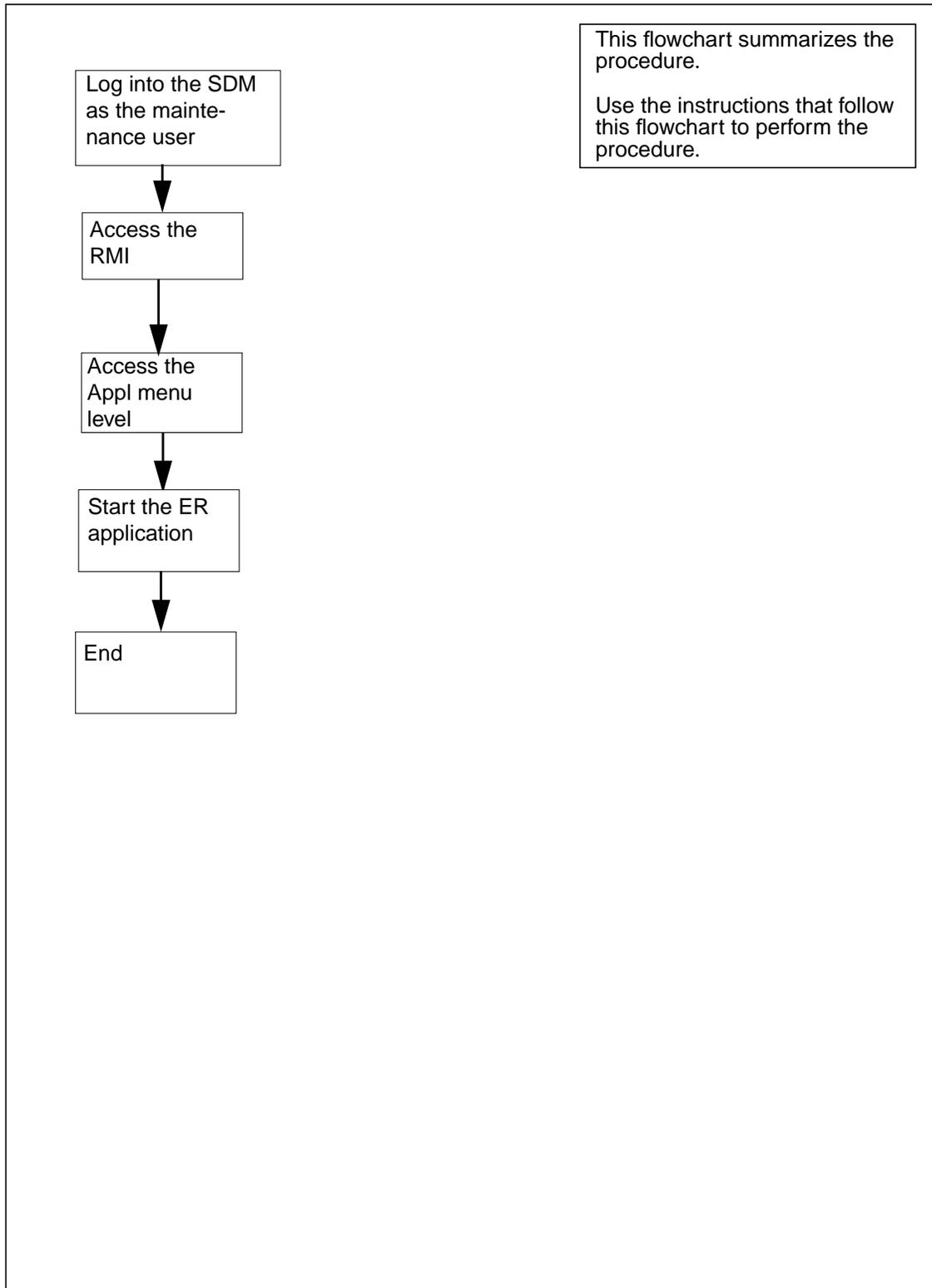
Procedure 2-3 Starting the ER server on the SDM

At the local or remote VT100 console

1   Log into the SDM as the maint user.

2   Access the SDM maintenance interface by typing

maint: sdmmtc

and pressing the Enter key.

3   Go to the application (Appl) menu level by typing

>appl

The application menu lists the software packages installed on the SDM.

4   Find the ER application in the display. The version number is the same as the one displayed when the software was installed.

Example of the application menu level

```
# Package Description    Version       State
1 Table Access Service   9.0.21.0      InSv
2 Operation Measurements 9.0.21.0      InSv
3 Log Delivery Service   9.0.21.0      InSv
4 Exception Reporting    9.0.21.0      OffL
```

5   Busy the ER application by typing

Bsy *er_application_id*

and pressing the Enter key.

where

   er_application_id
         is the number shown for the ER application. The example shows how the software packages are listed at the application (Appl) menu level.

The system responds saying that the application is in-service and that if you busy it, a service interruption will result. Confirm the busy command.

6   Start the ER application by typing

>Rts *er_application_id*

and pressing the Enter key.

where

   er_application_id
         is the number shown for the ER application. The example shows how the software packages are listed at the application menu level. To start the ER application, in this example, you would type RTS 4.

   Note: The state of ER displayed must be InSv. The ER application is dependent on the DCE service on the SDM and the Operation Measurements application. If either are not in service, the state of ER will be ISTb.

7   You have completed this procedure.

Removing an ER server

When the ER application is not required on the SDM, you must release the resources that were claimed by the application server. The same procedure can also be used to clear problems with an application server. It might be necessary to remove the server from the DCE cell, then re-create the server using the add_lcu_server command.

Problems with an application server include the following:

- the server identifies a mismatch resulting from a change to the switch Common Language Location Identifier (CLLI)

- the server is unable to authenticate itself because of key tab problems, which can occur if the SDM data files are restored from a backup tape

---

CAUTION
Risk of revealing the administrative users password
If you use telnet to access the SDM remotely, and use the default sdm_admin or cell_admin "master administrator" account to execute the DCE control program (dcecp) commands, the administrative user password is sent in clear text across the network. To prevent this, Nortel Networks recommends that you execute commands from a terminal attached to the SDM console port.

To perform this procedure, you must have a DCE account with administrative privileges and root user access to the SDM.

Figure 2-5 Summary of removing an ER server
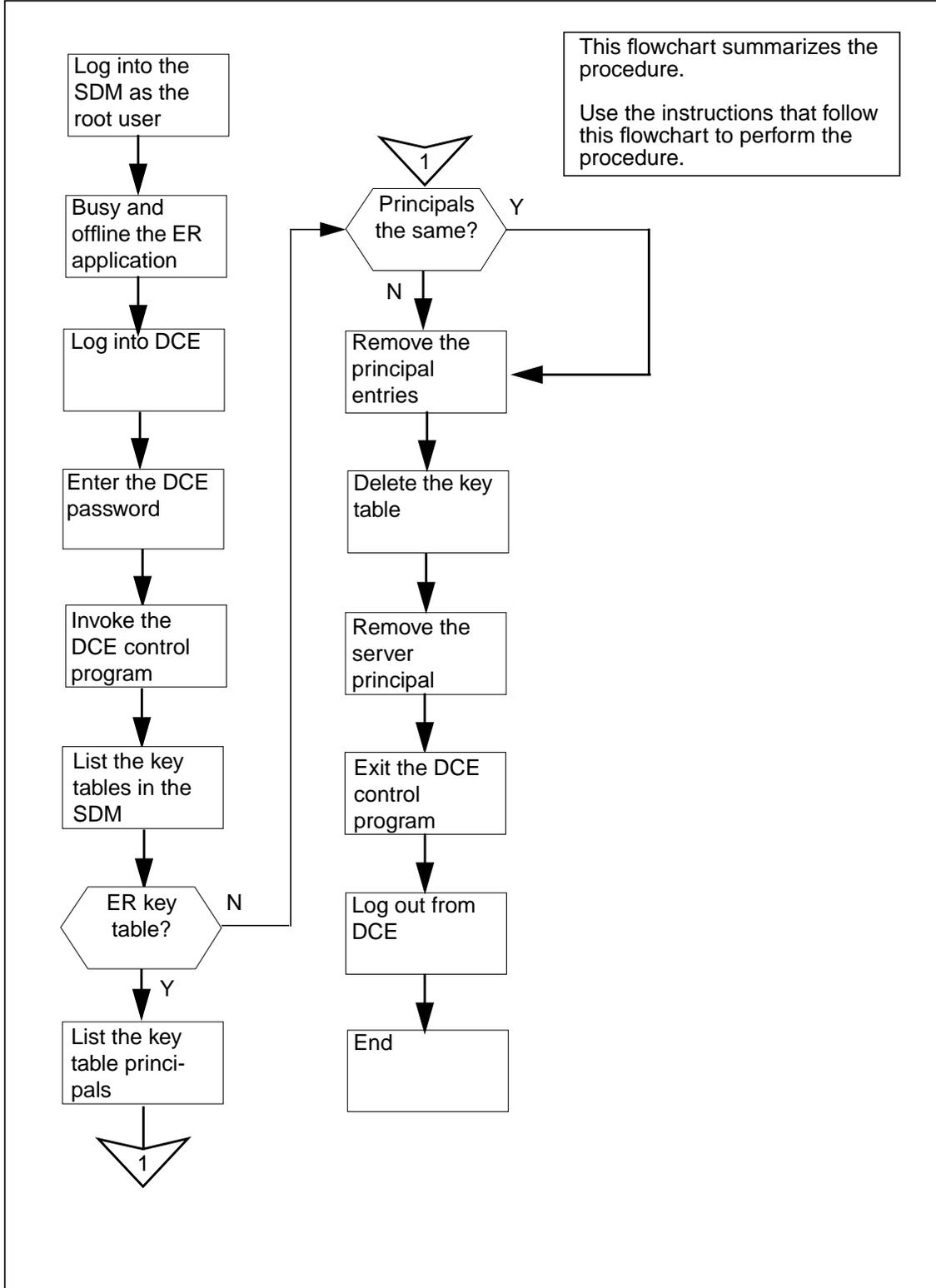
Procedure 2-4 Removing an ER server

At the local or remote VT100 console

1   Log into the SDM as the root user.

2   Access the SDM maintenance level by typing

      #sdmmtc

      and pressing the Enter key.

3   Access the Application level by typing

      >appl

      and pressing the Enter key.

4   Busy the Exception Reporting application by typing

      >bsy application *n*

      and pressing the Enter key.

      where

          n
             is the number for the Exception Reporting application.

5   Offline the Exception Reporting application by typing

      >offl application *n*

      and pressing the Enter key.

      where

          n
             is the number for the Exception Reporting application.

6   Go back to the SDM restricted shell by typing

      >quit all

      and pressing the Enter key.

7   Log into DCE using the administrators userID by typing

      #dce_login *DCE_admin_user*

      and pressing the Enter key.

      where

          DCE_admin_user
             is the userID for the DCE system administrator.

8   Enter your DCE password by typing

      >*password*

      and pressing the Enter key.

      where

          password
             is the password for the administrator userID.

9   Invoke the DCE control program (dcecp) by typing

      >dcecp

      and pressing the Enter key.

10   List the key tables in the SDM by typing

`dcecp>key catalog -simplename`

and pressing the Enter key.

11   Determine if the key table list contains a key table called lcu_ktab.

If	Do
the list contains the lcu_ktab key table	step 12
the list does not contain the lcu_ktab key table	step 16

12   List the principals that are supported by the key table by typing

`dcecp>key list lcu_ktab`

and pressing the Enter key.

The list from the command executed in step 12 must contain entries that follow the format: /.../

cell name/sdm/*clli*/*principal name*.

where

> **cell name**
>   *is the cell in which the SDM resides.*

> **clli**
>   *is the Common Language Location Identifier (CLLI) of the switch to which the SDM is connected.*

> **principal name**
>   *is the userID of the server.*

13   Determine if the principal names of all members in the list are "lcu_server".

If	Do
all principal names are "lcu_server" and match lcu_server	step 14
not all principal names are "lcu_server"	step 16

14   Remove the entries for the principal in the key table by typing

`dcecp>key remove lcu_ktab`
`-member/.../cellname/sdm/clli/lcu-server`

and pressing the Enter key.

where

> **cellname**
>   *is the cell in which the SDM resides.*

> **clli**
>   *is the Common Language Location Identifier (CLLI) of the switch to which the SDM is connected.*

15   Delete the key table by typing

   dcecp>key delete lcu_ktab

   and pressing the Enter key.

16   Remove the principal for the SDM application server by typing

   dcecp>principal delete sdm/*clli*/lcu-server

   and pressing the Enter key.

   where

   clli
      is the Common Language Location Identifier (CLLI) of the switch to which the SDM is connected.

17   Exit dcecp by typing

   dcecp>exit

   and pressing the Enter key.

18   Log out from DCE by typing

   >exit

   and pressing the Enter key.

19   You have completed this procedure.

3 ER client software installation or upgrade

This chapter describes the Exception Reporting (ER) application client software installation or upgrade procedures.

The SDM software packages contain both the server software and the client software. The Software Inventory Manager (SWIM) feature allows you to install one or more application software packages on a client workstation during one procedure.

Note: Nortel Networks recommends that you use the batch installation steps when instructed, to reduce the amount of time required to install SDM applications

This chapter discusses the following topics:

- Limitations and restrictions
- Compiling a list of client software filesets
- Installing or upgrading the client software packages on the client workstations

Limitations and restrictions

The following limitations and restrictions apply to installing Exception Reporting:

- The following platforms support the Exception Reporting client:

    — Hewlett-Packard 700/800 series workstations running the HP-UX 10.20 operating system (or higher) with year 2000 enhancements

    — Sun SPARC workstations running the Solaris 2.5 operating system (or higher) with year 2000 enhancements

    — Sun SPARC workstations running the year 2000 compliant Solaris 2.6 operating system (or higher)

    — Sun SPARC workstations running the year 2000 compliant Solaris 7.0 operating system

    — IBM RS6000 workstations running AIX 4.1.5 (or higher) operating system

- The workstation must use Open System Foundation (OSF) Distributed Computing Environment (DCE) version 1.1.

- The SDM for the remote client workstation must be configured in the DCE cell before installing Exception Reporting software. For information on DCE, refer to the *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

- The NA010, NA0011, NA0012, NA0013, or NA0014 computing module (CM) software must be installed.

- The DISPLAY environment variable must always be set, even if you are starting the interface from the console.

The following limitations and restrictions apply to running Exception Reporting:

- You must configure the Hewlett-Packard 700 or 800 series client workstation with a maxfiles value greater than or equal to 256. Use the kernel configuration of the client workstation to set the value of the maxfiles parameter. Only the network administrator and operating company personnel with UNIX root permissions can modify the maxfiles value.

- The maximum number of offices supported by the Exception Reporting client is 300.

- The maximum number of log types supported by the Exception Reporting application is 200.

- The state of the Exception Reporting application should appear as InSv. If it is ISTb, then call-based thresholding is not functional, although all other aspects of the application are supported. The Exception Reporting

application appears as ISTb when the Operation Measurements application is initializing.

- When multiple Exception Reporting applications are updating data on the same SDM, data that is stored on the SDM reflects the last change made.

- Avoid log suppression and thresholding on the CM through the LOGUTIL system for log types that are being tracked by the Exception Reporting application. CM log thresholding is monitored by the Exception Reporting application, which reports an SDM615 log daily, listing any logs being stored on the CM that are being tracked by the expert system.

- EXC logs cannot be added to the list of logs tracked by Exception Reporting. This restriction is required to prevent exception looping.

- The DISPLAY environment variable must always be set for the graphical user interface, even if the user is starting from the console.

- Only category 0 logs can be deleted. Since it is not possible to add category 1 and 1-prime (1P) logs, these logs cannot be deleted.

- If the type of thresholding is changed between call-based thresholding and time-based thresholding while the threshold is currently enabled, there will be a transitional period where results are unpredictable. It is recommended to first disable tracking before changing from one type of thresholding to another.

Note: Each of the following limitations and restrictions are followed by the recommended action, shown in italic text.

- Under certain SDM-CM link conditions, the OM application will fail to remain InSv. Under this condition, the OM application moves from InSv to ISTb and back to InSv within 75 seconds. This cycle is repeated three times, after which the OM application is failed. This condition occurs when the following sequence happens:

  — All applications are InSv.

  — All DS512 links move to a state other than open.

  — One or more DS512 links change to open after 1 min. or more of being in the previous state.

  The corrective action is to change the SDM state to OFFL, then change the SDM state to ManB and InSv.

- Certain models of X-terms may experience problems displaying the Log Customization Utility if the "Backing Store" option on the X-term is set to "Disabled". The user may notice some dialogs are not drawn properly.

Refreshing the display or reducing the display to an icon and maximizing the icon will clear the problem.

- Only one user should apply changes to one SDM at a time using the Log Customization Utility. If more than one user applies a large number of changes simultaneously, a few of the changes may fail, with the message "Communications failure (dce/rpc)" appearing in the Event Logger window.

If this occurs, the log parameters not applied will have change flags still set next to them. The failed changes can be reapplied by performing another Apply operation.

The following are prerequisites for installing the software:

- installation of the SDM Base software
- root and maintenance (maint) user class access to the SDM
- cell_admin privileges for the DCE cell, or sdm_admin privileges for the applications
- DCE account with administrative privileges
- execute access to the following executable on the SDM:
  — ftp
- an X Windows-based client machine where the client software is supported
- root user class access to the client machine
- execute access to the following executable files on the client machine:
  — un-compress
  — tar

Compiling a list of client software filesets

Nortel Networks recommends that you use the batch installation steps in this section to reduce the amount of time required to install SDM applications.

Instructions for batch installation of SDM application software

You must have a list of software filesets for each application you wish to install or upgrade. Before beginning the installation procedures, refer to the user guide of each application for a list of filesets.

ER filesets

Before you begin the installation procedure of ER, you must record the names of the client filesets. You must refer to this information during the installation procedures that follow in this chapter.

Each client program is stored as a .tar.Z file with the following structure: *clientname-version*.tar.Z.

where

clientname is the client name of the application

version   is the version number for that client

Record the following ER client software fileset names:

- clientcommon_15.x.x.x.tar.Z
- dcetools_15.x.x.x.tar.Z
- erclient_15.x.x.x.tar.Z

> *Note:* If you wish to install other applications at this time, refer to the fileset descriptions in the respective NTPs.

Once you have recorded the fileset information, you can, if necessary, refer to other SDM application NTPs for fileset information regarding other applications. If you have completed the list of filesets for all of the applications you wish to install, go directly to "Installing CIL on the client workstation".

Installing CIL on the client workstation

Install the SDM Client Installer and Launcher (CIL) tool on the client workstation. Then use the CIL tool to install the Exception Reporting application on the workstation.

Application

Use the following procedure to install the CIL tool on client workstations. Nortel Networks recommends that you use the batch installation steps in this section to reduce the amount of time required to install SDM applications on client workstations.

You must know the following information to perform this procedure:

- the platform node names of the client workstations
- the IP addresses and root passwords of the client workstations
- the root user password of the SDM
- the client software fileset names

Repeat this procedure for every client workstation.

Interval

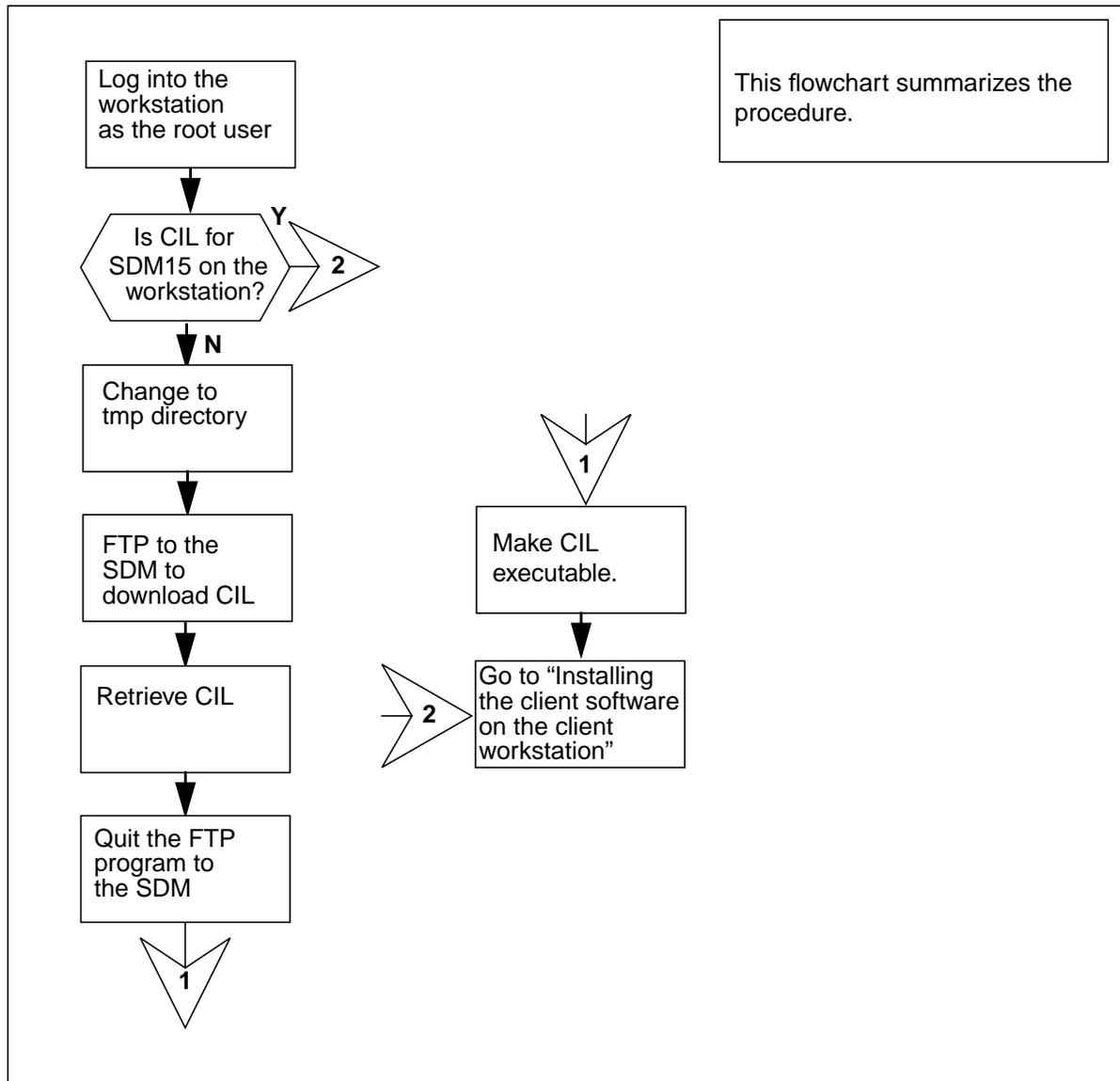Perform this procedure when you are installing SDM applications for the first time.

Common procedures

This procedure refers to "Installing or upgrading the client software on the client workstation".

Action

The flowchart that follows provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the routine maintenance procedure.

Summary of installing CIL on the client workstation

```
┌─────────────────────────────────────────────────────────────────┐
│                                                                   │
│   ┌──────────────┐                    ┌──────────────────────┐    │
│   │ Log into the │                    │ This flowchart       │    │
│   │ workstation  │                    │ summarizes the       │    │
│   │ as the root  │                    │ procedure.           │    │
│   │ user         │                    └──────────────────────┘    │
│   └──────────────┘                                                │
│          │                                                        │
│          ▼          Y                                             │
│      ╱ Is CIL for ╲ ──▷ 2                                         │
│     ⟨  SDM15 on the ⟩                                             │
│      ╲ workstation?╱                                              │
│          │  N                                                     │
│          ▼                                                        │
│   ┌──────────────┐                                                │
│   │ Change to    │              ▽                                 │
│   │ tmp directory│              1                                 │
│   └──────────────┘                                                │
│          │                                                        │
│          ▼                 ┌──────────────┐                       │
│   ┌──────────────┐         │ Make CIL     │                       │
│   │ FTP to the   │         │ executable.  │                       │
│   │ SDM to       │         └──────────────┘                       │
│   │ download CIL │                │                               │
│   └──────────────┘                ▼                               │
│          │                 ┌──────────────────┐                   │
│          ▼            2    │ Go to "Installing│                   │
│   ┌──────────────┐   ▷     │ the client       │                   │
│   │ Retrieve CIL │         │ software on the  │                   │
│   └──────────────┘         │ client           │                   │
│          │                 │ workstation"     │                   │
│          ▼                 └──────────────────┘                   │
│   ┌──────────────┐                                                │
│   │ Quit the FTP │                                                │
│   │ program to   │                                                │
│   │ the SDM      │                                                │
│   └──────────────┘                                                │
│          │                                                        │
│          ▽                                                        │
│          1                                                        │
│                                                                   │
└───────────────────────────────────────────────────────────────────┘
```

Procedure 3-1 Installing CIL on the client workstation

At the client workstation

1

> ⚠ **CAUTION**
> **Risk of revealing the administrative user password**
> If you use telnet to access the client workstation remotely,
> and use the default sdm_admin or cell_admin account to
> execute the DCE control program (dcecp) commands, the
> system sends the administrative user password in clear text
> across the network. To prevent this, Nortel Networks
> recommends that you execute the commands from a terminal
> attached to the workstation console port.

At the local or remote VT100 console, log into the client workstation as the root user.

2   Determine if the client installer and launcher (CIL) tool for the SDM15 release exists on the client workstation.

If	Do
CIL for SDM15 exists on the client workstation	step 10
CIL for SDM15 does not exist on the client workstation	step 3

3   Change to the temporary directory by typing,

#cd /tmp

and pressing the Enter key.

> *Note:* You can change to any directory as long as it is a directory to which you can download new files.

4   Open a connection to an SDM which has at least SDMN0012 installed. Open a file transfer protocol (FTP) connection by typing,

#ftp> *ip_address*

and pressing the Enter key.

where

> ***ip_address***
> is the IP address of the SDM.

5   Log into the SDM as an anonymous user by typing,

Name: ftp

and pressing the Enter key.

6   When the system asks you for a password, ignore the prompt and press the Enter key to continue the procedure.

7   Retrieve the CIL program by typing,

ftp> get cil

and pressing the Enter key.

8   Quit the connection to the SDM by typing,

`ftp> quit`

and pressing the Enter key.

9   Make the CIL program executable by typing,

`#chmod +x cil`

and pressing the Enter key.

10   You have completed installing CIL on the client workstation. Proceed to the next procedure (Installing the client software on the client workstation) to install the software application.

Installing or upgrading the client software on the client workstation
Application
Use this procedure to install or upgrade client software on the client work station using the client installer and launcher (CIL). Ensure that you install CIL on the client workstation before you install the software application.

ATTENTION
The clientcommon fileset must be installed before installing the ER application.

Interval
Perform this procedure when you are installing the ER application for the first time, or upgrading to the latest version of the ER application on the client workstation.
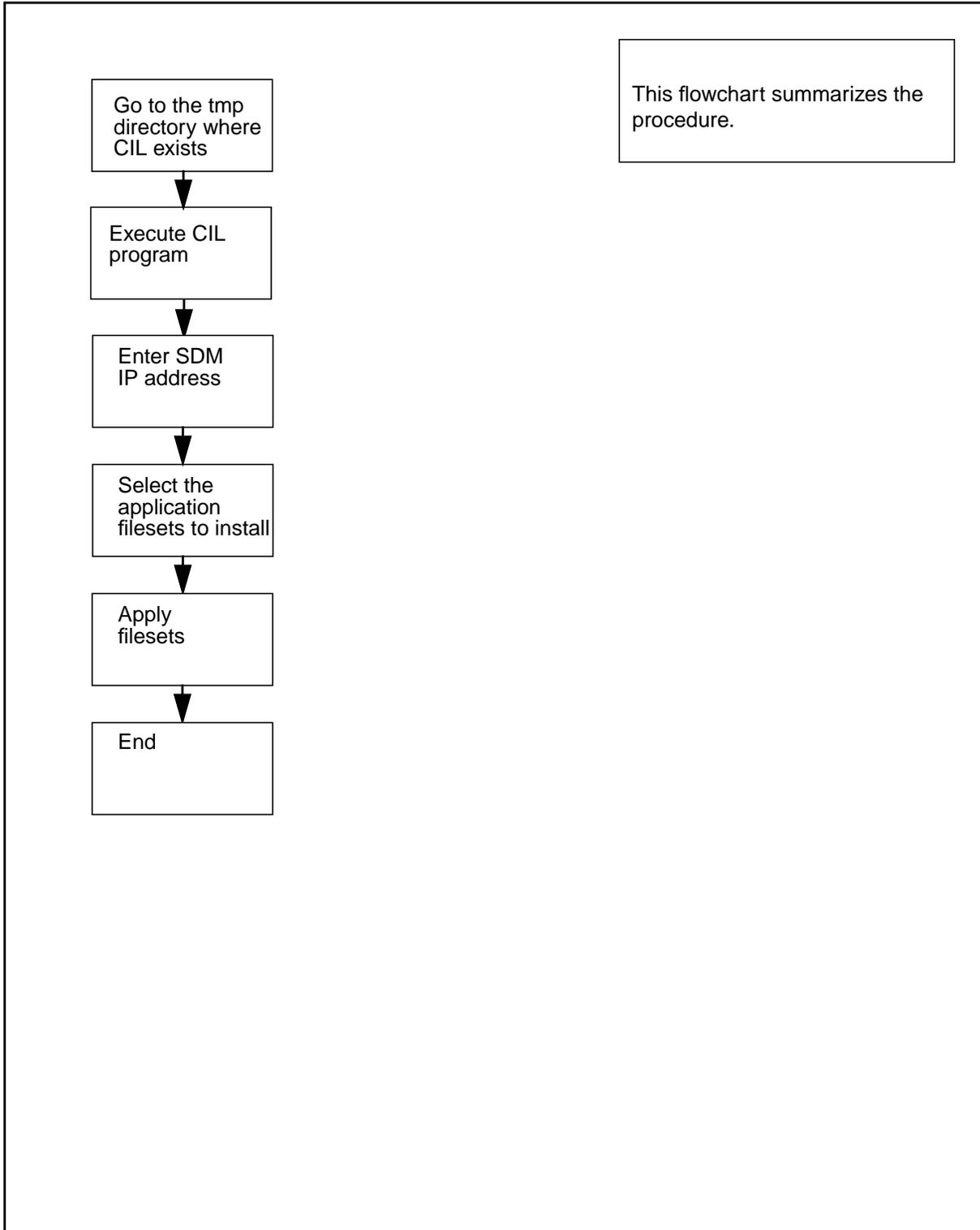
Common procedures
This procedure does not refer to any common procedures.

Action
The flowchart that follows provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the routine maintenance procedure.

Summary of installing or upgrading the client software on the client workstation

Go to the tmp
directory where
CIL exists

Execute CIL
program

Enter SDM
IP address

Select the
application
filesets to install

Apply
filesets

End

This flowchart summarizes the
procedure.

Procedure 3-2 Installing or upgrading the client software on the client workstation

At the client workstation

1   Access the tmp directory where the client installer and launcher (CIL) tool exists by typing

#cd /tmp

and pressing the Enter key.

2   Execute CIL by typing,

#./cil

and pressing the Enter key.

Response:

```
        SDM CLIENT SOFTWARE INSTALLATION

Enter the IP address or hostname of the SDM that you want
to download the client software from.

SDM's Address:
```

3   At the CIL menu, connect to the SDM by typing

SDM's Address: *sdm*_name

and pressing the Enter key.

where

   sdm_name
        is the IP address or the host name of the SDM.

Example response:

```
        SDM CLIENT SOFTWARE INSTALLATION

After you enter 'Apply', the selected filesets are FTPed
from the SDM to the /tmp directory. The filesets are then
installed into the /sdm directory. Type 'Help' for a list
of commands. Type 'Quit' to exit this program.

Client software source: the SDM at bmerye6b
    # Fileset Name
    1 ata_client_15.0.8.0.tar.Z
    2 dcetools_15.0.8.0.tar.Z
    3 sft_client_15.0.8.0.tar.Z
    4 ata_client_15.0.8.0.tar.Z
    5 clientcommon_15.0.8.0.tar.Z
    6 er_client_15.0.8.0.tar.Z
    7 guide_15.0.8.0.tar.Z
    8 logreceiver_15.0.8.0.tar.Z
                            Client Software: 1 to 8 of 8

cil>
```

4   Use the folllowing table to determine your next step.

Table 3-1

If	Do
the clientcommon resources (filesets) are not installed	step 5
the clientcommon resources (filesets) are installed	step 7

5   Select the clientcommon fileset to install on the client workstation by typing

`cil>select n`

and pressing the Enter key.

where

> **n**
>   is the entry number of the clientcommon fileset on the list.

> **Note:** To deselect any filesets, select the fileset a second time. To deselect all filesets, type *select none.*

6   Install the selected fileset by typing

`cil>apply`

and pressing the Enter key.

7   Select each Exception Reporting application fileset for installation on the client workstation by typing

`cil>select n`

and pressing the Enter key.

where

> **n**
>   is the entry number of the fileset on the list.

> **Note:** To deselect any filesets, select the fileset a second time. To deselect all filesets, type *select none.*

8   Install the selected filesets by typing

`cil>apply`

and pressing the Enter key.

9   You have completed this procedure.

4 Using the Log Customization Utility

This chapter describes how to use the Log Customization Utility, which is the graphical user interface (GUI) for the Exception Reporting (ER) application.

Note: For information about changing the threshold values using the Log Customization Utility, see chapter "Threshold management".

Requirements

Before starting to use the utility, confirm that you have access to an X Windows-based client machine which supports the appropriate client software. Software release SDM15 supports the following platforms:

- Hewlett-Packard 700/800 series workstations running the HP-UX 10.20 operating system (or higher) with year 2000 enhancements

- Sun SPARC workstations running the Solaris 2.5 operating system (or higher) with year 2000 enhancements

- Sun SPARC workstations running the year-2000 compliant Solaris 2.6 operating system (or higher)

- Sun SPARC workstations running the year-2000 compliant Solaris 7.0 operating system

- IBM RS6000 workstations running AIX 4.1.5 (or higher) operating system

Your workstation must use Open System Foundation (OSF) Distributed Computing Environment (DCE) version 1.1.

Selecting menu items

How you select a menu item differs depending on your workstation. Use the following guide to select a menu item:

- Press the right mouse button if you are using a Sun workstation.

- Press the left mouse button if you are using a Hewlett-Packard workstation.

Note: This guide may vary depending on how you have configured your mouse button.
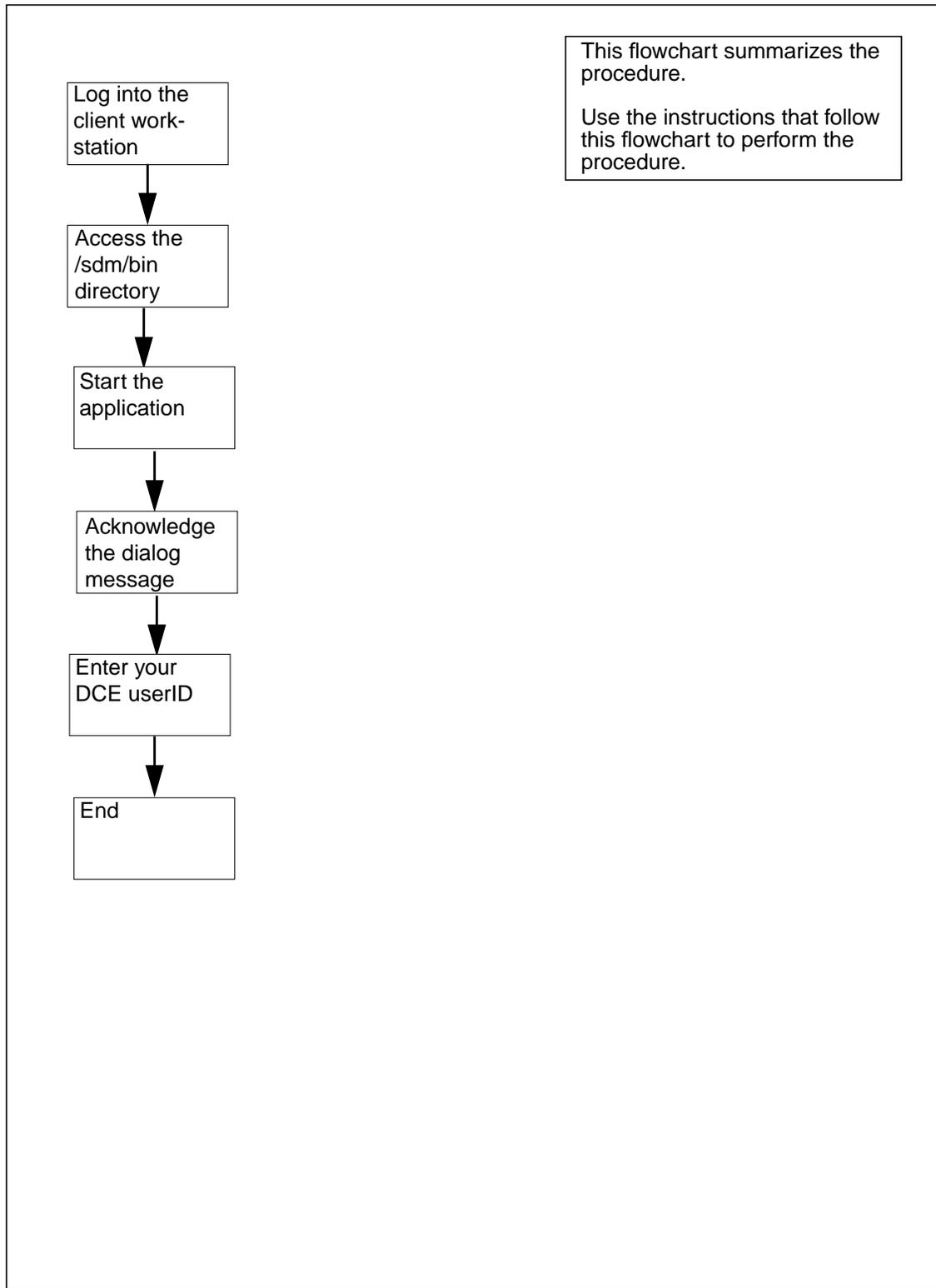
Accessing the Log Customization Utility

Before starting the Log Customization Utility, you must log in to the Distributed Computing Environment (DCE) cell. A DCE administrator can set up a userID for you.

Running the Log Customization Utility

Use the following procedure to start the Log Customization Utility. Depending on how your workstation is configured, you might be automatically logged into DCE when you log in to your workstation. If this is not the case, you are prompted for your DCE principal name and password when you start the Log Customization Utility.

> *Note:* The DISPLAY environment variable must always be set, even if the user is starting the interface from the console.

Figure 4-1 Summary of starting the Log Customization Utility

Procedure 4-1 Running the Log Customization Utility

At the VT100 console:

1   Log into the client workstations as any user (other than root).

> ***Note:*** If you log in as root, type dce_login, followed by your DCE login ID. At the password prompt, enter your password.

2   Type

>cd /sdm/bin

and press the Enter key.

3   Start the application, by typing

>./erclient

and press the Enter key.

After a few seconds, the Log Customization Utility copyright dialog appears:

> ***Note:*** If you log in as root, you will not see the copyright message in the Log Customization Utility window, and the DCE Login window is not displayed afterward.

<table>
<tr><td>i</td><td>Copyright 1998 Northern Telecom
All Rights Reserved.

Log Customization Utility

Release 13.0.0.0</td></tr>
<tr><td colspan="2" align="center">OK</td></tr>
</table>
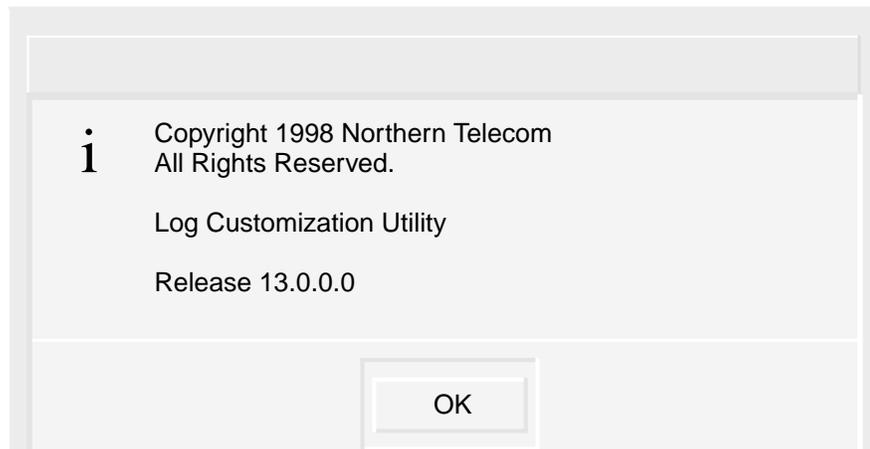
4   Acknowledge the copyright dialog message by clicking on the OK button.

If applicable, the DCE Login window appears:
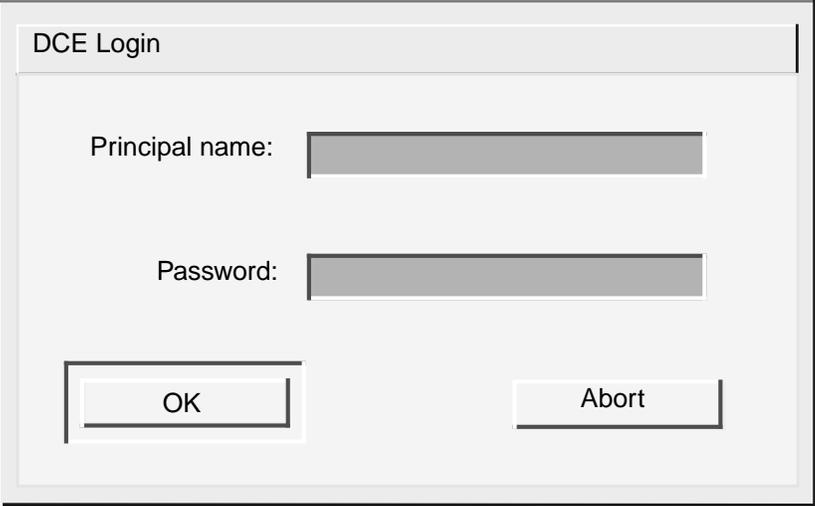
```
┌─────────────────────────────────────────────────────────┐
│ DCE Login                                              │ │
├─────────────────────────────────────────────────────────┤
│                                                         │
│                                                         │
│      Principal name:   ┌──────────────────────────┐     │
│                        │                          │     │
│                        └──────────────────────────┘     │
│                                                         │
│                                                         │
│         Password:      ┌──────────────────────────┐     │
│                        │                          │     │
│                        └──────────────────────────┘     │
│                                                         │
│      ┌──────────────┐                ┌──────────────┐   │
│      │     OK       │                │    Abort     │   │
│      └──────────────┘                └──────────────┘   │
│                                                         │
└─────────────────────────────────────────────────────────┘
```

5   Enter your DCE principal name, press Tab, enter your password, and click on
             the OK button.

             Note: Pressing Return after entering your principal name causes the
             password field to be accepted as a blank value.

             *The Log Customization Utility appears on the desktop, similar to the following
             screen:*

Figure 4-2 Log customization utility

| File   Edit   Action   View | | | | | | Help |

| Office Name: | OTWAON10FCC | | Apply... |

|	Threshold Settings				Exception Log		Tracking	
Log Name	System	Compon.	in every	Criteria	Severity	Number	S	C
AUDT201	15	5	1	hours	minor	900	√	√
C7UP100	20	5	300	CMCalls	minor	900	√	√
C7UP101	9	2	1	hours	none	900	√	√
C7UP102	10	5	2	minutes	minor	900	√	√
C7UP107	27	5	65000	CMCalls	minor	900	√	√
C7UP111	3	2	1000	LineCalls	none	900	√	√
C7UP112	13	5	1	minutes	minor	900	√	√
C7UP116	10		5	hours	none	910	√	
CCS154	30	5	20	seconds	minor	900	√	√
CCS167	15	5	6	hours	minor	900	√	√
CCS168	5	5	6	hours	minor	900		
CCS204	5	5	50	seconds	minor	900	√	√
CM103	1		6	minutes	minor	900	√	
CM104	1		8	minutes	major	900	√	
CM111	1		10	minutes	critical	900	√	
CM112	1		600	LineCalls	minor	900	√	
CM115	1		1	hours	minor	900	√	
CM116	1		1	hours	critical	900		

| View: By Office | Total: 59 | Viewing: all | Sorted by "Log Name" | no changes. |

6 You have completed this procedure.

Tracking events using the event logger

In the case of an error or other significant event when communicating with an office, the event logger dialog is displayed, as follows.

Figure 4-3 Event logger dialog
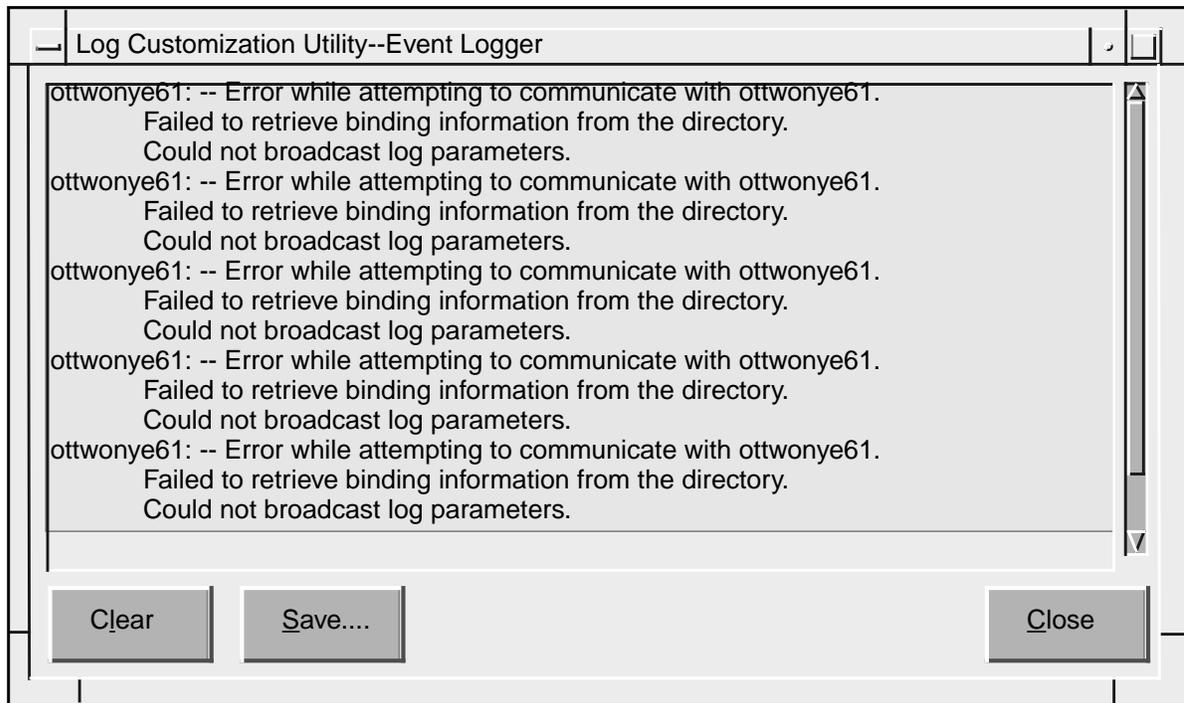
Each event is appended to the dialog's output. You can scroll to previous events by using the scroll bar. Use the Clear button to clear the records. Use the Save... button to save the events to a file. Use the Close button to close the dialog.

If the dialog is closed, a new dialog is displayed when another event occurs. If the dialog is not closed, events are displayed in the current dialog. The dialog

is always brought in front of all other windows when a new event occurs. This
brings the event to your attention. To prevent this, reduce the dialog to an icon.

> **CAUTION**
> **Risk of software error**
> If an error dialog containing a Trace Back button appears,
> this indicates a potentially serious software error. Have
> your system administrator click on Trace Back and record
> the data that is provided in the system response for
> analysis purposes, then click on OK to continue. If
> required, contact Nortel Networks for assistance.

Log Customization Utility views

The Log Customization Utility window can appear in one of three views:

- By Office

- By Log

- Default File

In the By Office view, a pull-down menu provides a choice of office names.
Beneath the menu, a table lists log types and their parameters, for the chosen
office.

In the By Log view, a pull-down menu provides a choice of log types. Beneath
the menu, a table lists office names and their parameters, for the chosen log
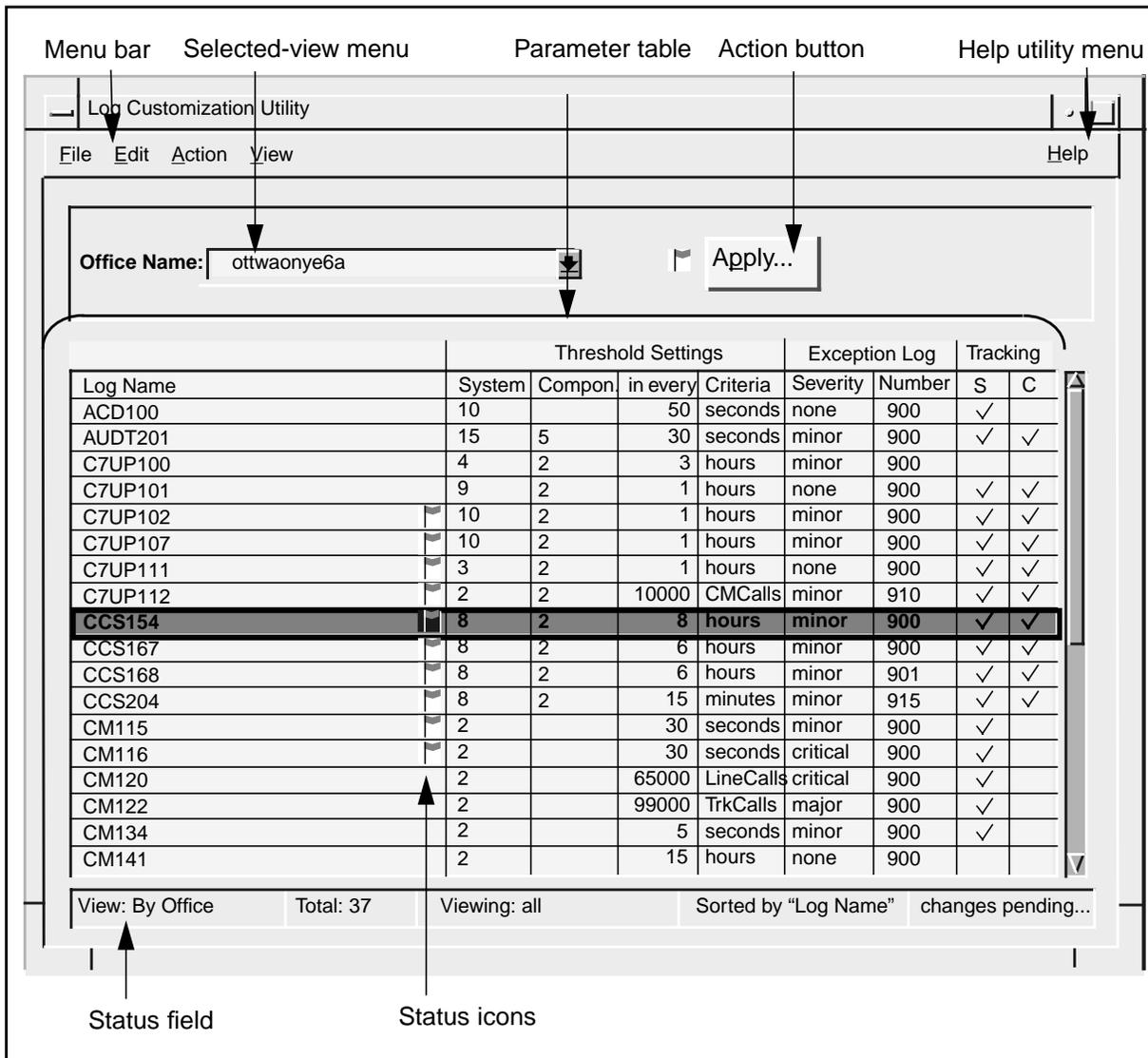type.

In the Default File view, a list of files (saved on the workstation) provides a
choice of default files. When a default file is chosen, the parameter table for
the default file, lists log types and their parameters.

The three views have a similar appearance, containing common parts. These
parts are described in the following section, using examples of the views.
Subsequent sections describe how to use command menus, how to access
HELP information, and how to logout from the Log Customization Utility.

Parts of the Log Customization Utility

The Log Customization Utility consists of several parts: the menu bar,
including a help utility menu, the selected-view menu (based on the view), the
parameter table (also known as a list box), plus action buttons and status icons
and fields. The following figure shows the various parts (using the By Office
view).

Figure 4-4 Log Customization Utility

Menu bar   Selected-view menu   Parameter table   Action button   Help utility menu

Log Name	System	Compon.	in every	Criteria	Severity	Number	S	C
ACD100	10		50	seconds	none	900	✓	
AUDT201	15	5	30	seconds	minor	900	✓	✓
C7UP100	4	2	3	hours	minor	900		
C7UP101	9	2	1	hours	none	900	✓	✓
C7UP102	10	2	1	hours	minor	900	✓	✓
C7UP107	10	2	1	hours	minor	900	✓	✓
C7UP111	3	2	1	hours	none	900	✓	✓
C7UP112	2	2	10000	CMCalls	minor	910	✓	✓
CCS154	**8**	**2**	**8**	**hours**	**minor**	**900**	**✓**	**✓**
CCS167	8	2	6	hours	minor	900	✓	✓
CCS168	8	2	6	hours	minor	901	✓	✓
CCS204	8	2	15	minutes	minor	915	✓	✓
CM115	2		30	seconds	minor	900	✓	
CM116	2		30	seconds	critical	900	✓	
CM120	2		65000	LineCalls	critical	900	✓	
CM122	2		99000	TrkCalls	major	900	✓	
CM134	2		5	seconds	minor	900	✓	
CM141	2		15	hours	none	900		

Office Name: ottwaonye6a   Apply...

Threshold Settings   Exception Log   Tracking

View: By Office   Total: 37   Viewing: all   Sorted by "Log Name"   changes pending...

Status field   Status icons

Menu bar

The Menu bar, beneath the title bar, displays the available menus for the Log Customization. The available menus are: File, Edit, Action, View, and Help (at the right end).

Selected-view menu

In the By Office view, the Selected-view menu shows the selected office and provides access to a list of available offices. In the By Log view, the Selected-view menu shows the selected log type and provides access to a list of all available log types. In the Default File view, the menu is replaced with the selected default file name.

To view the office or log type list as appropriate, click on the down arrow, then use the scroll bar to scroll through the list. Both lists are in alphabetical order.

Parameter table

In the By Office view and Default File view, the parameter table lists (in the left column) the available log types for the selected office or default file. In the By Log view, the table lists the available offices for the selected log type. Both lists have selectable rows in alphabetical order.

The center four columns of the table show the threshold settings and let you edit the values. The section is divided into columns that contain thresholds for the system, component, and interval, plus the interval criteria (time or call based). Call-based interval criteria show an "OM equation name," which specifies a formula based on a set of OM registers.

The next two columns to the right show exception log severities and log numbers, and let you edit the values.

The right two columns of the table show whether tracking for the system-level and component-level tracking is enabled or disabled, and let you change the settings.

The parameter table (also known as a list box) contains rows of log parameters. Depending on the view, the parameters belong to one office, all offices, or a local file. Each row contains nine fields. These fields are as follows:

- Log Name/Office Name. The first field in each row is the key to the row. It is either the name of the log for that row (in the By Office and Default File views) or the name of the office the selected log belongs to (in the By Log view).

- Threshold Settings--System. This field contains the system threshold value. This is the value that must be reached (for that log name) before a system exception log is produced.

- Threshold Settings--Compon. This field contains the component threshold value. This is the value that must be reached (for any component of that log name) before a component exception log is produced.

  Threshold Settings--in every. This field contains the interval within which the system or component thresholds must be reached before an exception log is produced.

  Threshold Settings--Criteria. This field contains the unit of measurement to which the "in every" field applies. Thresholds can be set on the basis of time or the basis of call traffic. To specify time-based thresholding, choose hours, minutes, or seconds for the criteria. To specify call-based

thresholding, choose an OM equation name. The OM equation name specifies a formula based on a set of OM registers.

Exception Log--Severity. This field indicates what level of severity is included in the exception log if one is produced for that log name.

Exception Log--Number. The log name of every exception log is EXC. This number field indicates what log number is used. For example, if 900 is coded, an EXC900 log is produced when an exception occurs.

Tracking--S. This field indicates whether system tracking is enabled. If a check mark is present in this field, tracking is enabled. Therefore, an exception log is produced if system thresholds are reached. If tracking is disabled, exception logs are not produced as a result of reaching system thresholds.

Tracking--C. This field indicates whether component tracking is enabled. If a check mark is present in this field, tracking is enabled. Therefore, an exception log is produced if component thresholds are reached. If tracking is disabled, exception logs are not produced as a result of reaching component thresholds.

Action buttons

Several action buttons are available, depending on the view. The actions buttons are used to effect changes in log tracking after new parameter values have been entered in the Log Customization Utility. Except for a Stop button, these actions are also available from the Menu bar menus.

Status icons

The left column can include status icons that indicate either operations in progress, changed values, or connectivity problems.

Change-flag icon

All changes made, including edit, add, and delete operations, affect only the utility's local memory. Whenever an edit operation is made that changes a value, a change flag appears next to the log name or office name. This is a reminder that the data has been changed and needs to be applied or saved to take effect. In addition, a global change flag located above the parameter table indicates that at least one change is pending.
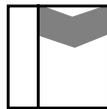
The change-flag icon indicates that threshold values have been changed but not applied. The change-flag icon disappears when the values are applied.

Operation-in-progress icon

The operation-in-progress icon indicates a pending request from the client to the SDM. This icon normally appears only briefly when changes are applied.
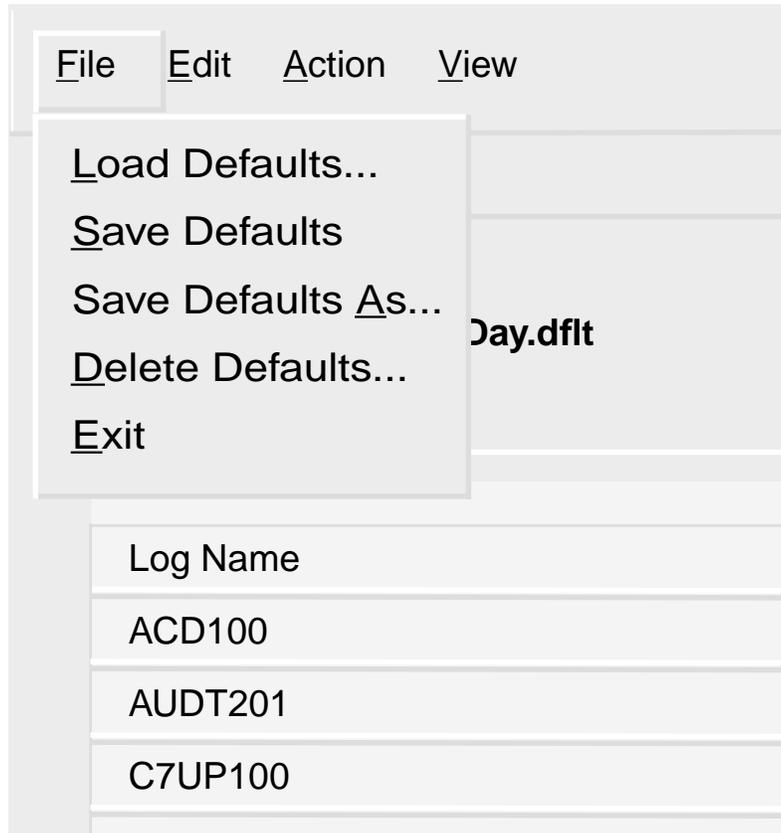
Loss-of-connection icon

The loss-of-connection icon indicates that your workstation cannot connect to the SDM for the switch.

File menu

The pull-down File menu is used for changes in the Default File, the view, and to exit from the Log Customization Utility. The following diagram shows the pull-down File menu.

Figure 4-5 File menu

File	Edit	Action	View

Load Defaults...

Save Defaults

Save Defaults As...

Delete Defaults...

Exit

Day.dflt

Log Name

ACD100

AUDT201

C7UP100

The File menu contains the following options:

- Load Defaults - This option is only available in the Default File view. It loads a new default file.

- Save Defaults - This option is only available in the Default File view. It saves the current default file. A backup file is created before saving. The name of the backup filename is the name of the current file with a tilde (~) appended to the end, that is, <filename>~.

- Save Defaults As - This option is available in the By Office view and Default file views. It saves the current log parameters to a default file.

- Delete Defaults - This option is available in the By Office view and Default file views. It deletes a default file.

- Exit - This option exits the utility.

Edit menu

The Edit menu is used to make changes in values stored by the Log Customization Utility. The Edit menu can also be used by holding down the right mouse button when the cursor is positioned anywhere in the parameter table. The following diagram shows the Edit menu.
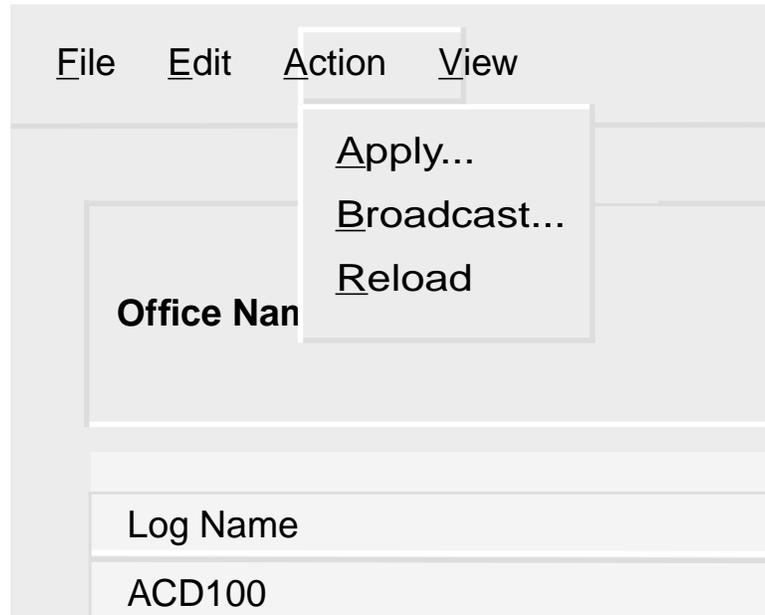
Figure 4-6 Edit menu
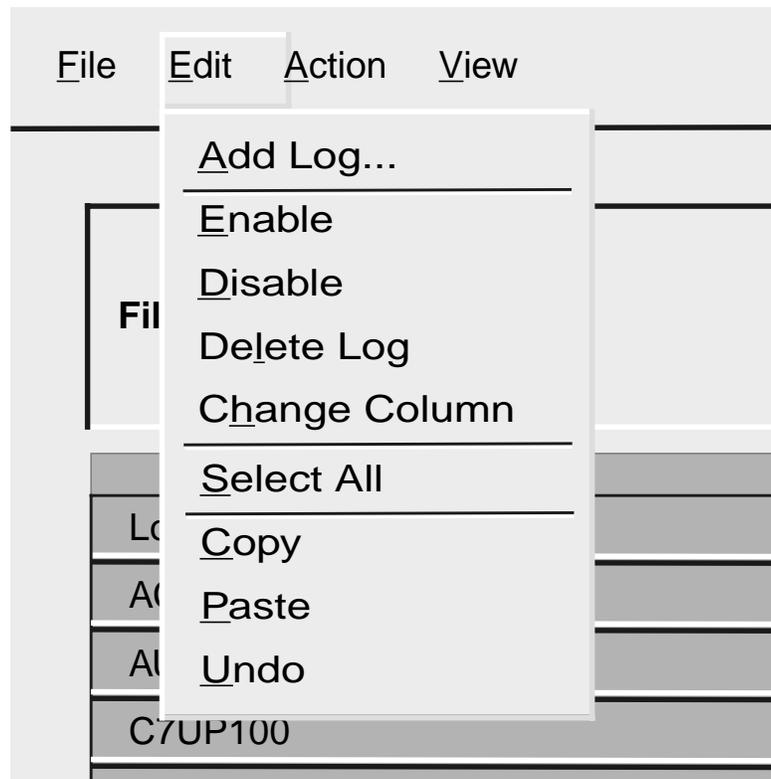
The Edit menu contains the following options:

*   Add Log - This option is available in the By Office view and Default file views. It adds a new category 0 log parameter.

*   Enable - This option is available in all views when at least one log parameter is highlighted in the parameter table. It sets both the system and component tracking on for all highlighted logs.

*   Disable - This option is available in all views when at least one log parameter is highlighted in the parameter table. It sets both the system and component tracking off for all highlighted logs.

*   Delete Log - This option is available in the By Office view and Default file views when exactly one log is highlighted and that log is a category 0 log. This option deletes the highlighted category 0 log. Deleting a log causes the global change flag to be displayed.

*   Change Column - This option is available in all views when a column other than the "Log Name/Office Name" or "Tracking" columns are highlighted. It changes the value stored in that column for every log parameter.

*   Select All - This option is available in all views. It selects (highlights) all rows in the parameter table.

*   Copy - This option is available in the By Office view and Default file views when at least one row in the parameter table is highlighted. It copies any highlighted log entries to a copy buffer. The copy buffer survives until the utility is exited.

*   Paste - This option is available in the By Office view and Default file views when a copy operation was previously performed. It copies the log entries stored in the copy buffer to the current log parameter table. Log entries in the copy buffer that are already present in the table overwrite existing values. Log entries not already present are added.

*   Undo - This option is available in all views when at least one editing operation has been performed, but the changes have not been applied. This option reverses the effect of the last single edit.

Action menu

The Action menu is used to change log tracking after changes have been made within the Log Customization Utility.
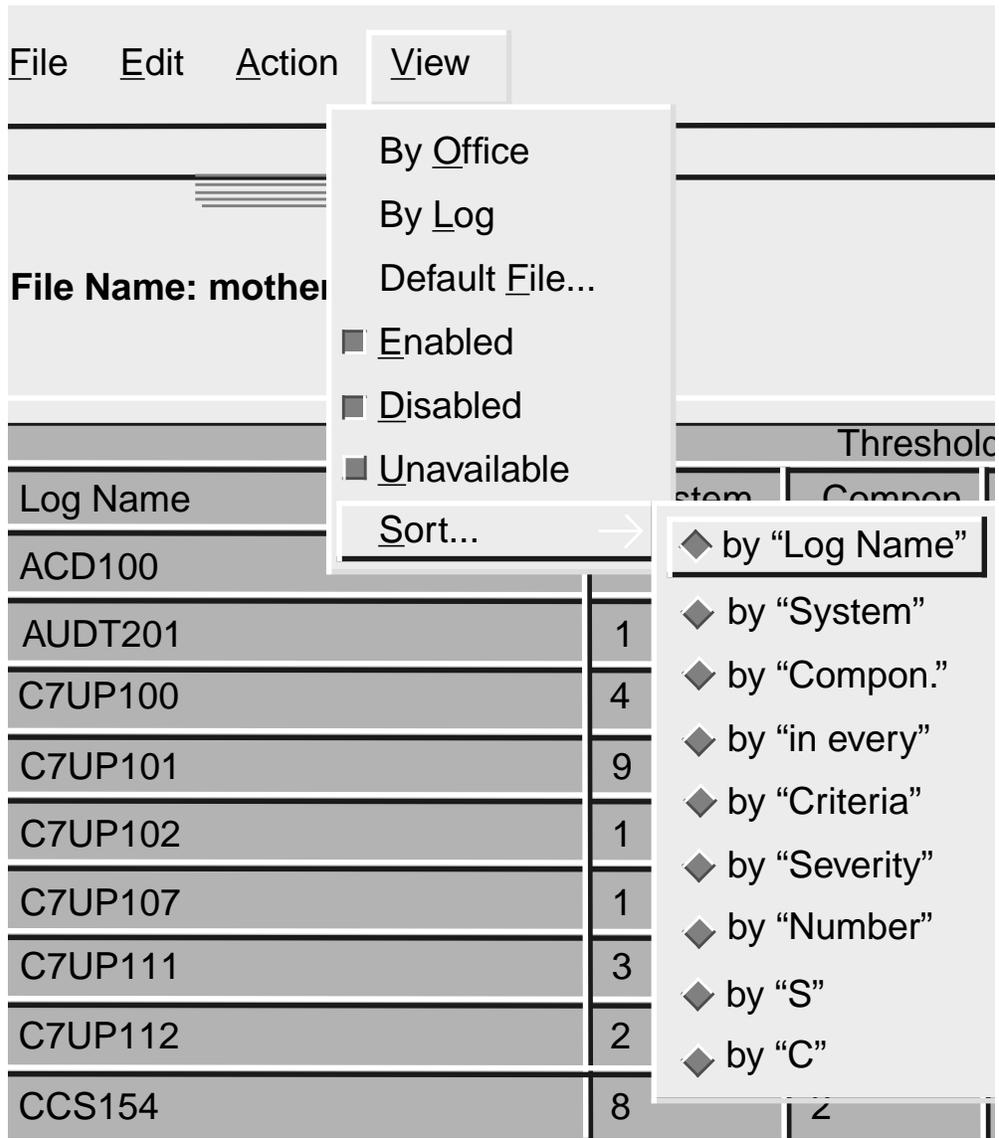
Figure 4-7 Action menu

File	Edit	Action	View

> Apply...
> Broadcast...
> Reload

Office Nam

Log Name

ACD100

The Action menu contains the following options:

- Apply - This option is available in the By Office view and By Log file views. In the By Office view, it applies any changed values in the parameter table to exception reporting for the current office. In the By Log view, it applies any changed values in the parameter table to exception reporting for offices in which the corresponding logs are being tracked. Before applying changes, a dialog is presented warning that once logs are applied, the operation cannot be canceled.

- Broadcast - This option is only available in the Default File view. It broadcasts all log parameters in the file to selected offices.

- Reload - This option is available in the By Office view and By Log file views. It reloads the log entries.

View menu

The pull-down View menu is used to change the view displayed by the Log Customization Utility. The following diagram shows the pull-down View menu.

Figure 4-8 View menu

| File | Edit | Action | View |

By Office
By Log
Default File...
☐ Enabled
☐ Disabled
☐ Unavailable
Sort... →

File Name: mother

Threshold

Log Name		System	Compon.

◆ by "Log Name"
◆ by "System"
◆ by "Compon."
◆ by "in every"
◆ by "Criteria"
◆ by "Severity"
◆ by "Number"
◆ by "S"
◆ by "C"

Log Name		
ACD100		
AUDT201	1	
C7UP100	4	
C7UP101	9	
C7UP102	1	
C7UP107	1	
C7UP111	3	
C7UP112	2	
CCS154	8	2

The View menu contains the following options:

- By Office - This option is available in the By Log view and Default File views. It changes the view to the By Office view.

- By Log - This option is available in the By Office view and Default File views. It changes the view to the By Log view.

- Default File - This option is available in the By Office view and By Log views. It changes the view to the Default File view.

- Enabled - This option is available in all views. When the check box next to the option is selected, enabled logs are shown in the log parameter table.

Otherwise, they are filtered and not shown. By default, the check box is selected. Choosing this option deselects or reselects the check box.
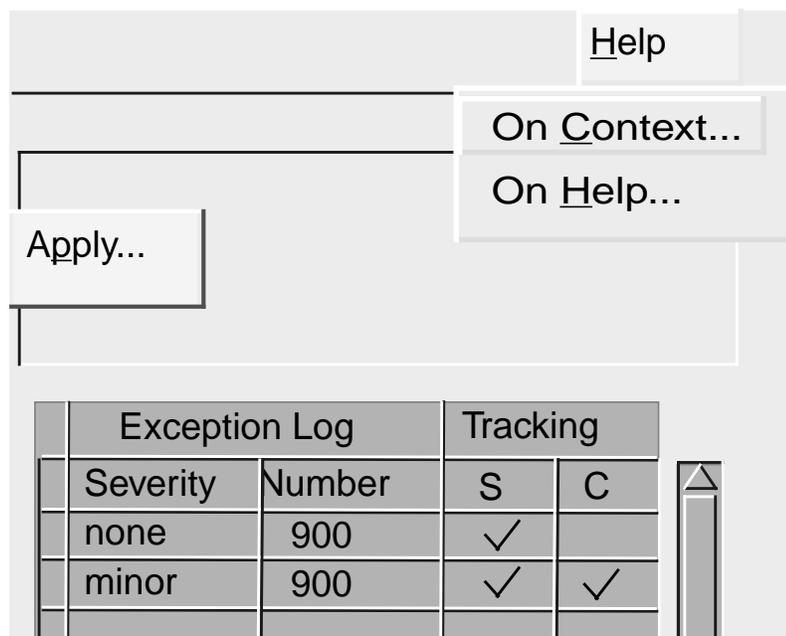
- Disabled - This option is available in all views. When the check box next to this option is selected, disabled logs are shown in the log parameter table.   By default, the check box is selected.

- Unavailable - This option is only available in the By Log view. When the check box next to the option is selected, offices that do not have threshold data for this log are shown in the parameter table. Otherwise, they are filtered and not shown. By default, the check box is selected. Selecting this option deselects or reselects the check box.

- Sort - This option is available in all views. A submenu is attached to this option. This submenu shows a list of all columns. The logs are sorted by one of these columns. The radio button in this list indicates the column by which the logs are sorted. Select a different column to sort the logs again.

Help utility menu

The Help utility menu, at the right end of the menu bar, provides information on the Log Customization Utility window, menu commands, and the Help utility. The Help utility is context sensitive; that is, you can obtain information on a specific topic by clicking on the appropriate area of the window.

The following diagram shows the pull-down Help menu.

Figure 4-9 Help menu

The Help menu contains the following options:

- On Context - This option is available in all views. It provides context-sensitive help.

- On Help - This option is available in all views. It provides help on how to use context-sensitive help.

Action buttons

The following Action buttons appear, depending on the view. They have the same affect as certain menu commands.

Apply button

The Apply... button is visible in the By Office and By Log views. It performs the same function described by the Apply... option in the Action menu.

Save button

The Save button is visible in the Default File view. It performs the same function described by the Save Defaults option in the File menu.

Broadcast button

The Broadcast... button is visible in the Default File view. It performs the same function described by the Broadcast... option in the Action menu.

Stop button

The Stop button is visible in all views when the utility is communicating with one or more servers. Normally, the operations initiated by other action buttons, are performed quickly. In cases where an operation is suspended, press the Stop button to abandon the current operation.
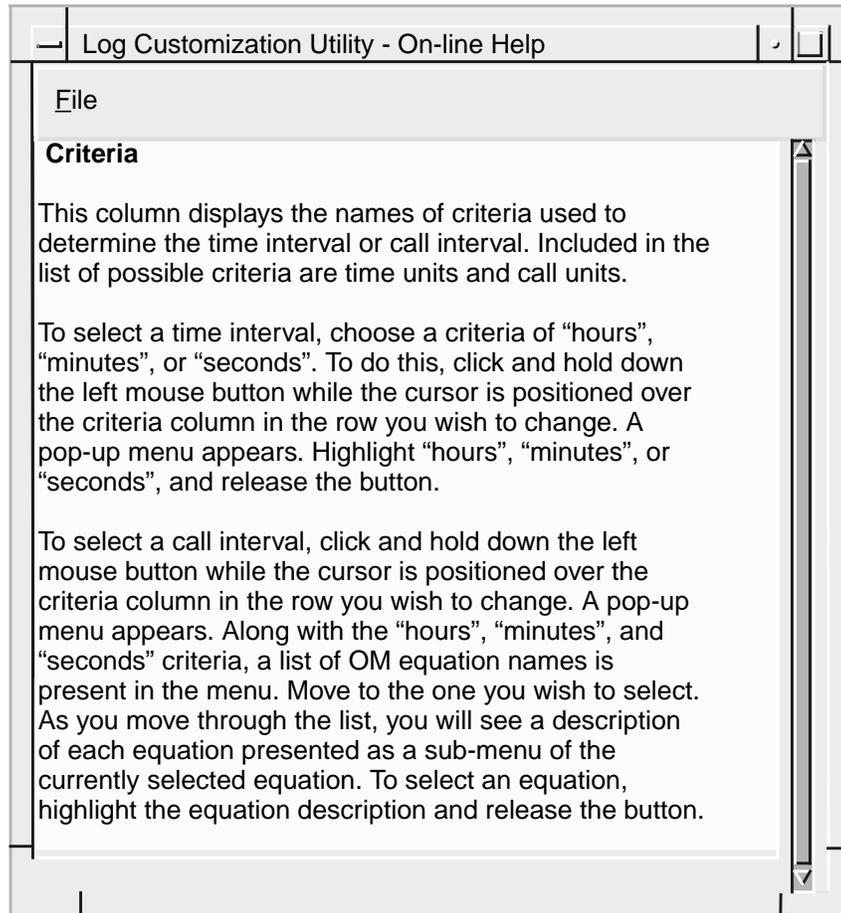

ATTENTION

Using the Stop button is risky when used on an apply or broadcast operation, because it is impossible to determine which operations have already been processed, and could lead to inconsistent data stored on the SDM.

On-line help dialog

The on-line help dialog is shown in the following illustration.

Figure 4-10 On-line help


```
┌─────────────────────────────────────────────────────┐
│ ─│ Log Customization Utility - On-line Help   │ ⌐│□│ │
│  ┌──────────────────────────────────────────────┐    │
│  │ File                                         │    │
│  │──────────────────────────────────────────────│ △  │
│  │ Criteria                                     │    │
│  │                                              │    │
│  │ This column displays the names of criteria   │    │
│  │ used to determine the time interval or call  │    │
│  │ interval. Included in the list of possible   │    │
│  │ criteria are time units and call units.      │    │
│  │                                              │    │
│  │ To select a time interval, choose a criteria │    │
│  │ of "hours", "minutes", or "seconds". To do   │    │
│  │ this, click and hold down the left mouse      │    │
│  │ button while the cursor is positioned over   │    │
│  │ the criteria column in the row you wish to   │    │
│  │ change. A pop-up menu appears. Highlight     │    │
│  │ "hours", "minutes", or "seconds", and        │    │
│  │ release the button.                          │    │
│  │                                              │    │
│  │ To select a call interval, click and hold    │    │
│  │ down the left mouse button while the cursor  │    │
│  │ is positioned over the criteria column in    │    │
│  │ the row you wish to change. A pop-up menu    │    │
│  │ appears. Along with the "hours", "minutes",  │    │
│  │ and "seconds" criteria, a list of OM         │    │
│  │ equation names is present in the menu. Move  │    │
│  │ to the one you wish to select. As you move   │    │
│  │ through the list, you will see a description │    │
│  │ of each equation presented as a sub-menu of  │    │
│  │ the currently selected equation. To select  │    │
│  │ an equation, highlight the equation          │    │
│  │ description and release the button.          │    │
│  │                                              │ ▽  │
│  └──────────────────────────────────────────────┘    │
└─────────────────────────────────────────────────────┘
```

You can display help for almost all the screen elements. For example, buttons, status fields, entry fields, and the main table all support context-sensitive help. To get general help, click anywhere else on the window.

The On Help... menu option displays a dialog displaying instructions on how to use help. The On-line help dialog is similar to the dialog used for context-sensitive help.

Status fields

Below the parameter table are five status fields. These describe the current status of log parameters being edited. They are as follows:

- View - This field indicates what the current view is. Possible values are By Office, By Log, and Default File.

- Total - This field indicates how many log parameters are being edited.

- Viewing - This field indicates what logs are being viewed. Possible values are all, nothing, or a set of enabled, disabled, and unavailable. For example, Viewing: enabled.

- Sorted by - This field indicates how the logs are sorted, for example, Sorted by Log Name.

- Changes - This field indicates whether or not changes are pending. Possible values are **changes pending** and **no changes**

Keyboard shortcuts

If you want to use the keyboard rather than the mouse, all menu options and buttons can be selected using the keyboard. To select a menu, hold down the Alt key and press the letter shown underlined in the menu or button. To select a menu option, after selecting the menu, either press the letter shown underlined for the option or use the arrow keys to move to the option and press Enter.

Using command menus

The Log Customization Utility commands are listed in menus that can be invoked from either the pull-down menu bar or in the case of Edit menu commands from pop-up menus.

From the menu bar

Use the following procedure to execute a menu command from the menu bar.

From the menu bar:

1   Activate the Log Customization Utility window.

2   With the left mouse button, click on the appropriate pull-down menu in the menu bar.

The menu commands are displayed. Executable commands are highlighted.

3   Position on the command you want to execute and click once.

4   You have completed the procedure.

From a pop-up menu

Use the following procedure to execute Edit menu commands from a pop-up menu.

From a pop-up menu:

1   Activate the Log Customization Utility window.

2   Using the mouse, position the cursor anywhere in the parameter table.

3   Press and hold down the right mouse button.

The Edit menu commands are displayed. Executable commands are highlighted.

> **4**   Keep the right mouse button pressed and drag the cursor to the command you want to execute.
>
> **5**   Release the mouse button to execute the command.
>
> **6**   You have completed the procedure.

Changing entries in the table

You can change the entries in the parameter table using the mouse buttons to select the rows and fields, and the keyboard and mouse to insert or select new values. Selected rows and fields are highlighted. You can also change all values in a column of fields to a single value.

Selecting rows in the table

You can select a single, several, or all rows in the table:

- To select a single row, click on the name field of that row.

- To select several rows, press and hold the Shift key, while clicking on the rows.

- To select all rows in the table, click on Select All in the Edit menu.

Selecting and editing fields in the parameter table

To edit a field in the log parameter table, first select the row.

Select numerical fields (System, Compon., in every, and Number) by double-clicking on the value. Once the value is separately highlighted, type the new value and press Enter.

Edit the Criteria and Severity fields by moving the cursor over the field. Then, press and hold down the left mouse button. A list of possible values is shown. Move the cursor to the desired value and release the mouse button.

When editing the Criteria column, a menu lists the time units and OM equations available. Each OM equation contains a submenu that describes the equation. When selecting an OM equation, move the cursor to the OM equation name, then to the submenu, before releasing the mouse button.

Edit the Tracking fields by single clicking on the field. If no check mark appeared before, a check mark is inserted. If a check mark appeared before, the check mark is removed.

Note that since category 0 log parameters do not contain a component threshold, the Threshold Settings--Compon. and Tracking--C fields cannot be edited for these logs.

Editing columns in the table

To change all values in a column to a single value, first highlight the column by clicking on the title row of the column. To change a numerical field column,

choose the Change Column menu option from the edit menu. All values are cleared on the screen except for the first row. The cursor appears in edit mode in the first row. Type a new value and press Enter. The new value is set in each row.

To change either the Criteria or Severity column, first highlight the column by clicking on the title row of the column, then choose the Change Column menu option from the edit menu. When editing these columns, the change column option has a submenu, which is the menu that appears when doing normal editing operations. Move the cursor to this submenu and select the desired entry.

To change one of the Tracking columns, choose either the Enable or Disable menu option from the Edit menu. Tracking in all fields in the column is set on or off, respectively.

Accessing help

Use the Help utility to obtain information on Log Customization Utility features or on the Help utility itself. Use the following procedure to access the help utility.
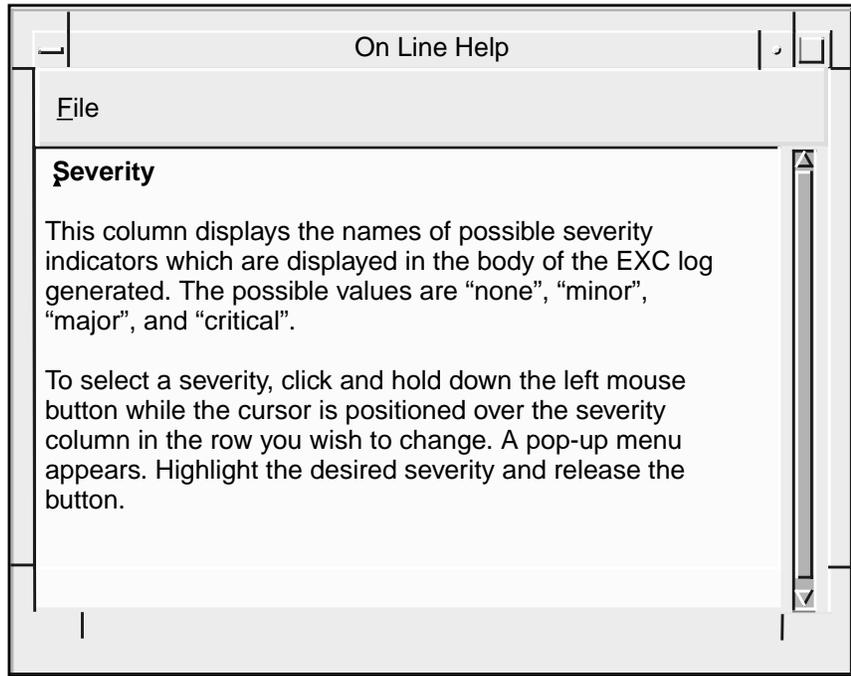
At a workstation:

1   Activate the Log Customization Utility window.

2   Click on Help in the menu bar.

3   For information about the Help utility, select On Help... from the Help menu.

4   For context-sensitive help, select On Context....

         The cursor changes to a large question mark.

5   Move the question mark to any area in the window for which you want information, and click on that area.

         Help information, similar to the following dialog, appears.

Figure 4-11 On-line help

On Line Help

<u>F</u>ile

<u>S</u>everity

This column displays the names of possible severity indicators which are displayed in the body of the EXC log generated. The possible values are "none", "minor", "major", and "critical".

To select a severity, click and hold down the left mouse button while the cursor is positioned over the severity column in the row you wish to change. A pop-up menu appears. Highlight the desired severity and release the button.

6   Use the scroll bar to navigate through the help text.

7   When you finish using help, you can leave the help window open and return to the Log Customization Utility window. To close the help window, select Exit from the File menu in the help window.

8   You have completed this procedure.

Logging out

To log out of the Log Customization Utility, select Exit from the File menu.

5 Threshold management

This chapter describes how to use the Log Customization Utility to manage the threshold values, which define the rules for the DMS SuperNode Data Manager (SDM) Exception Reporting application. The chapter includes individual procedures to change the various fields in the table, as they appear from left to right.

Selecting menu items

This chapter often instructs you to select a menu item. How you select a menu item differs depending on your workstation. Use the following guide to select a menu item:

- Press the right mouse button if you are using a SUN workstation.

- Press the left mouse button if you are using a Hewlett Packard or RS6000 workstation.
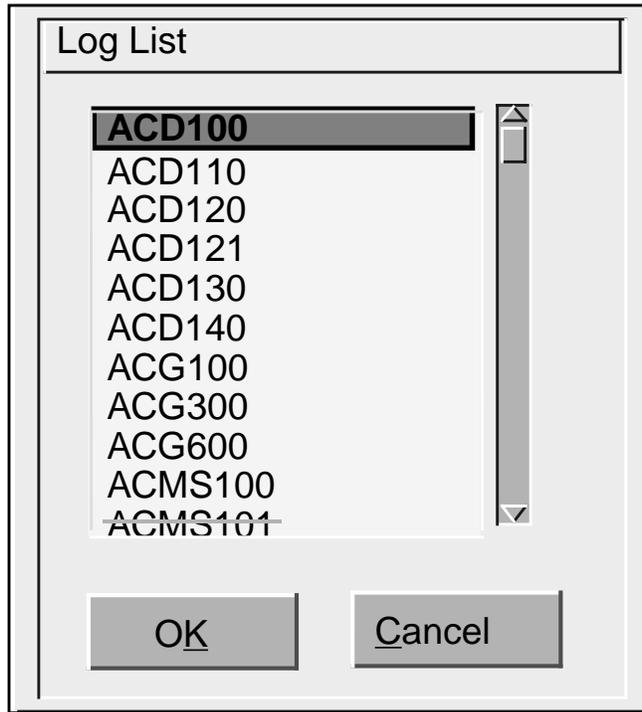
   Note: This guide may vary depending on how you have configured your mouse button.

Adding category 0 logs

The utility provides the ability to add new category 0 logs to the list of logs being tracked. Category 1 and 1P logs cannot be added.
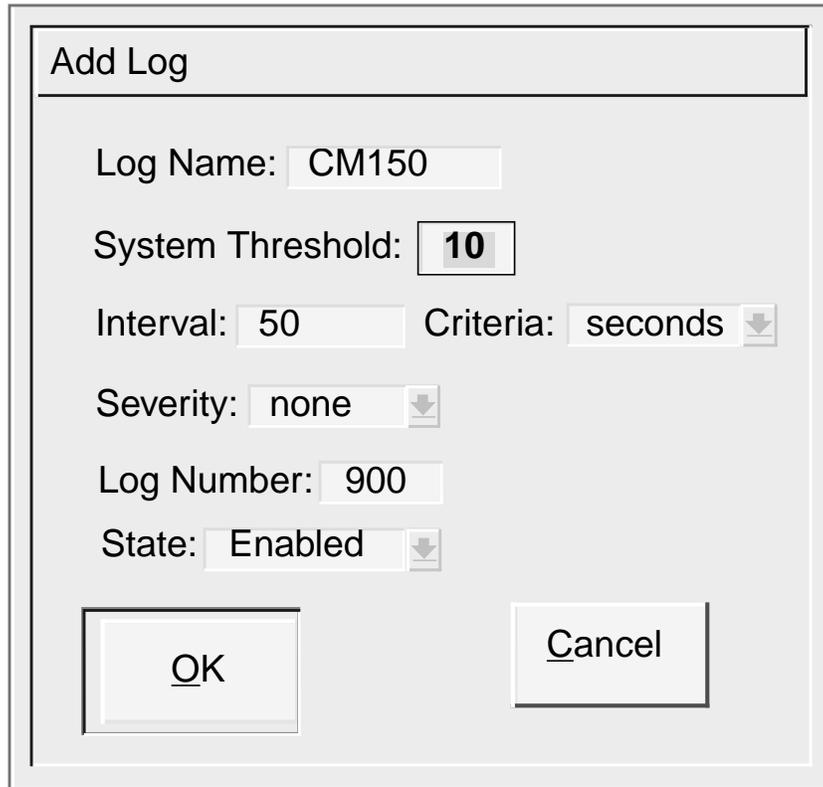
To add a new category 0 log, select the Add Log menu option from the Edit menu. A dialog that contains a list of all log types that can be chosen is displayed (see example that follows). Choose a log type and press the OK button.

Figure 5-1 Log list

```
Log List

  ┌─────────────────────┐ ▲
  │ ACD100              │ ▒
    ACD110               ▒
    ACD120               ▒
    ACD121               ▒
    ACD130               ▒
    ACD140               ▒
    ACG100               ▒
    ACG300               ▒
    ACG600               ▒
    ACMS100              ▒
    ACMS101              ▼

       OK            Cancel
```

When a log type is chosen, the Add Log dialog is displayed, as shown in the following figure.

Figure 5-2 Add log

```
┌─────────────────────────────────────────────┐
│  ┌─────────────────────────────────────────┐ │
│  │ Add Log                                 │ │
│  └─────────────────────────────────────────┘ │
│                                               │
│     Log Name:  CM150                          │
│                                               │
│     System Threshold:  10                     │
│                                               │
│     Interval:  50     Criteria:  seconds ▼    │
│                                               │
│     Severity:  none        ▼                  │
│                                               │
│     Log Number:  900                          │
│                                               │
│     State:  Enabled    ▼                      │
│                                               │
│     ┌──────────────┐    ┌──────────────┐      │
│     │              │    │   Cancel     │      │
│     │     OK       │    │              │      │
│     └──────────────┘    └──────────────┘      │
│                                               │
└─────────────────────────────────────────────┘
```

The Add Log dialog contains default data for the added log. Change the data as desired and press the OK button. The new log is added to the current log parameter list (a change flag is displayed as a reminder that there are pending changes that need to be applied).

Deleting category 0 logs

The utility provides the ability to delete category 0 logs from the list of logs being tracked.

To delete a category 0 log, select the log from the parameter table, then select the Delete Log menu option from the Edit menu. The log is removed from the table.

Setting system and component thresholds

Category 0 logs allow problems to be tracked on a system level, and category 1 and 1P logs allow tracking of problems from both the system and component levels.

The steps required for changing system threshold settings or component threshold settings are the same.

Use the following procedure to change the system or component thresholds in any of the views.

In the Log Customization Utility:

1   Select the row of log parameters.

2   Double click in the threshold field to be changed.

The value in the field is highlighted.

3   Type the new value and press Enter.

If the new value is within the allowed range of values, it appears in the field. If the value is not within range, you are shown the range and prompted to reenter.

4   You have completed this procedure.

Setting the threshold interval

The interval field ("in every") in the parameter table specifies the time-based or call-based interval during which logs are tracked to determine if an exception exists. If a certain number of log types are received within the defined interval, an exception report log is generated.

The time-based interval can be defined in seconds, minutes, or hours. The call-based interval uses whole numbers without spaces or commas.

As with the threshold settings, you can do the following:

•   set the interval separately for each log type and each system

•   set the interval for each log for all logs or all systems at once

Use the following procedure to change the interval value.

In the Log Customization Utility:

1   Select the row or rows of log parameters.

2   Double click in the "in every" field to be changed.

The value is highlighted and moves to the left end of the field.

Figure 5-3 Log Customization Utility

	Threshold Settings				Exception Log		Tracking	
Office Name: OTWAON10FCC ▼ Apply...								
Log Name	System	Compon.	in every	Criteria	Severity	Number	S	C
AUDT201	**15**	**5**	**1**	**hours**	**minor**	**100**	√	√
C7UP100	20	5	300	CMCalls	minor	900	√	√

3   Type the value for either the time-based or the call-based interval, and press Enter.

If the new value is within the range of allowed values, it appears in the field. If the value is not within range, you are prompted to reenter and shown the range.

4   You have completed this procedure.

Selecting the threshold criteria

Time-based criteria are expressed as seconds, minutes, or hours. Call-based criteria use OM equations (based on CM calls, line calls, trunk calls, CCS7 messages, CCS7 calls, and PM calls).

Use the following procedure to set the threshold criteria for one or more systems from any view.

In the Log Customization Utility:

1   Select the row or rows of log parameters.

2   Position the cursor on the field under the Criteria header that corresponds to the appropriate row.

3   Click and hold in the field.

The criteria pop-up menu appears, listing the time-based and call-based criteria. The call-based criteria menu items support submenus of OM equations.

Figure 5-4 Log Customization Utility

C7UP111		3	2	1	hours	none	900	✓	✓
C7UP112		2	2	10000	CMCalls	minor	910	✓	✓
CCS154		**8**	**2**	seconds		**minor**	**900**	✓	✓
CCS167		8	2	minutes		minor	900	✓	✓
CCS168		8	2	hours		minor	901	✓	✓
CCS204		8	2	CMCalls →				✓	✓
CM115		2		LineCalls →	OFZ:NIN + NORIG				
CM116		2		critical	900			✓	
CM120		2		6: TrkCalls →	critical	900		✓	
CM122		2		9: CCS7Msgs →	major	900		✓	
CM134		2		CCS7Calls →	minor	900		✓	
CM141		2		PMCalls →	none	900			

View: By Office	Total: 37	Viewing: all	Sorted by "Log Name"	changes pending...

4 Drag to the new value and release.

The value in the field changes to the selected value.

5 You have completed this procedure.

Selecting the exception log severity

When an exception report is generated, the EXC log indicates the relative severity of the log. There are four severity levels: none, minor, major, and critical.

Use the following procedure to set the severity thresholds for one or more systems from any view.

In the Log Customization Utility:

1 Select the row or rows of log parameters.

2 Position the cursor on the field under the Severity header that corresponds to the appropriate row.

3 Click and hold in the field.

The severity pop-up menu appears (none, minor, major, or critical)

Figure 5-5 Log Customization Utility

Settings		Exception Log		Tracking	
every	Criteria	Severity	Number	S	C
1	**hours**	none	**900**	✓	✓
300	CMCalls		900	✓	✓
1	hours	minor	900	✓	✓
2	minutes	major	900	✓	✓
65000	CMCalls	critical	900	✓	✓
1000	LineCalls		900	✓	✓

4   Drag to the new value and release.

The value in the field changes to the selected value.

5   You have completed this procedure.

Setting the exception log number

Use the following procedure to set the exception log number in any of the views.

In the Log Customization Utility:

1   Select the row or rows of log parameters.

2   Double click in the field to be changed.

The value in the field is highlighted.

3   Type the new value and press Enter.

If the new value is within the allowable range of values (900 to 999), it appears in the field. If the value is not within range, you are shown the range and prompted to reenter.

4   You have completed this procedure.

Enabling and disabling tracking

You can specify which logs you want to track for exception reports by enabling the Tracking fields. When tracking is on, the logs are correlated according to their threshold settings, and exception reports can be generated. When tracking is off, logs are not correlated and exception reports cannot be generated. A check mark indicates that tracking is enabled.

Use the following procedure to enable and disable tracking.

In the Log Customization Utility:

1 Select the row or rows of log parameters.

2 To enable tracking at the system and component level for all the selected rows, choose Enable from the Edit menu.

All appropriate tracking is enabled, indicated by check marks in the S and C fields.

3 To disable tracking at the system and component level for all the selected rows, choose Disable from the Edit menu.

All appropriate tracking is disabled, indicated by no check marks in the S and C fields.

4 To manually enable or disable system (S) or component (C) tracking, click on the fields under the respective Tracking header so that the check mark appears or disappears.

5 You have completed this procedure.

Applying changes

Changes to log parameters while in the By Office or By Log view only affect data within the utility. To have the changes take effect, they must be applied.

To apply changes, press the Apply button or select the Apply menu option from the Action menu. These options are only available when at least one change is pending. You are prompted to confirm the application of changes.
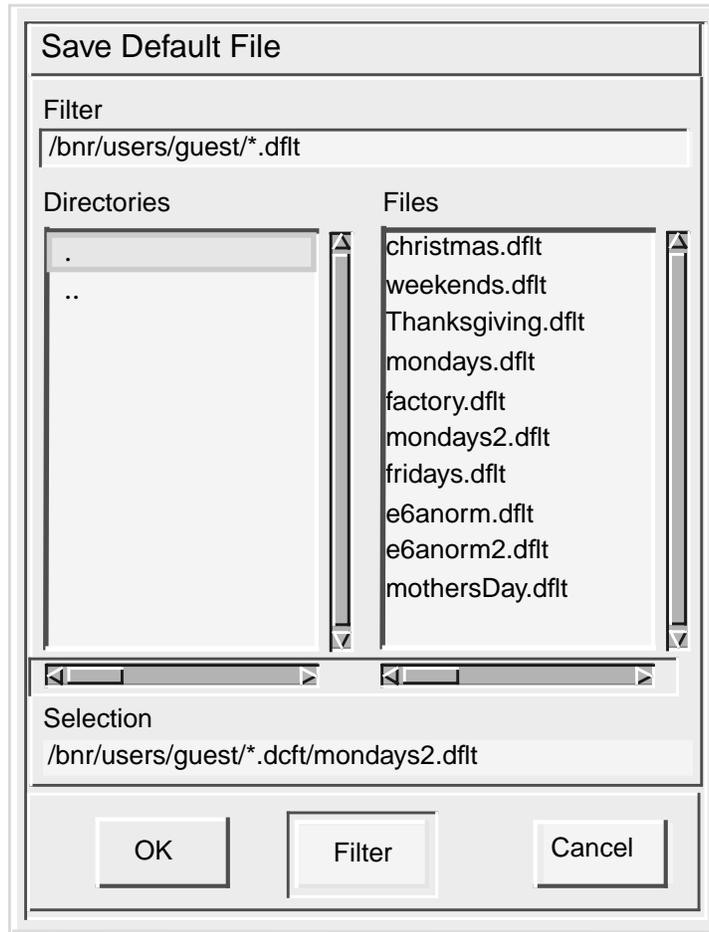
Saving log parameters

Log parameters may be saved to a file in the By Office or Default File view by selecting the Save Defaults As... menu option from the File menu.

This option can be used to make a backup copy of the current threshold data for a system. Select the default file you want to save the log parameters to from the Files list menu. To save the file, click on the OK button.

The Save Default File dialog box is shown in the following figure.

Figure 5-6 Save Default File dialog box

```
┌─────────────────────────────────────────────┐
│ Save Default File                            │
├─────────────────────────────────────────────┤
│ Filter                                       │
│ /bnr/users/guest/*.dflt                      │
│                                              │
│ Directories              Files              │
│ ┌─────────────────┐▲  ┌──────────────────┐▲ │
│ │.                │   │christmas.dflt    │  │
│ │..               │   │weekends.dflt     │  │
│ │                 │   │Thanksgiving.dflt │  │
│ │                 │   │mondays.dflt      │  │
│ │                 │   │factory.dflt      │  │
│ │                 │   │mondays2.dflt     │  │
│ │                 │   │fridays.dflt      │  │
│ │                 │   │e6anorm.dflt      │  │
│ │                 │   │e6anorm2.dflt     │  │
│ │                 │▼  │mothersDay.dflt   │▼ │
│ └─────────────────┘   └──────────────────┘  │
│ ◄──────────►          ◄──────────►          │
│ Selection                                    │
│ /bnr/users/guest/*.dcft/mondays2.dflt        │
│                                              │
│   ┌──────┐    ┌──────┐    ┌──────┐          │
│   │  OK  │    │Filter│    │Cancel│          │
│   └──────┘    └──────┘    └──────┘          │
└─────────────────────────────────────────────┘
```

If overwriting an existing file, a dialog is displayed warning that an existing file is about to be overwritten.

Loading default values

The Log Customization Utility allows you to load previously saved default values for all logs. Loading the defaults automatically sets the interval value, the threshold values, and enables tracking.

Loading, saving, save default as (save as), and deleting default values are actions available from the Default File view. Save default as and deleting default values are also available from the By Office view.
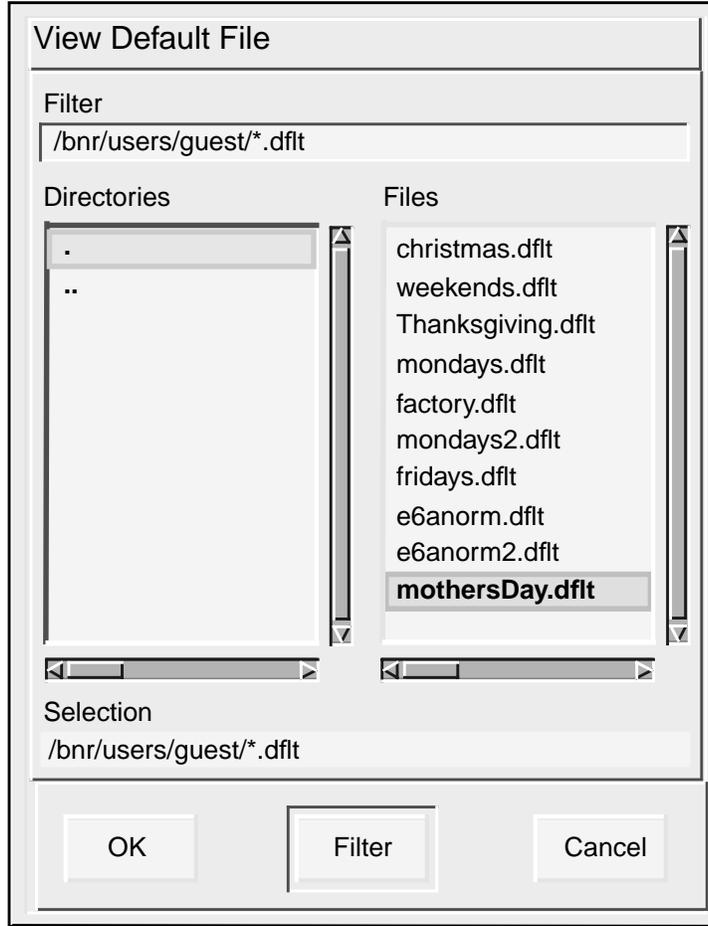
Use the following procedure to load defaults from the Default File view.

In the Log Customization Utility:

1   From the View menu, select Default File.

The View Default File dialog box appears.

Figure 5-7 View Default File dialog box

```
┌────────────────────────────────────────────────┐
│ View Default File                               │
├────────────────────────────────────────────────┤
│ Filter                                          │
│ /bnr/users/guest/*.dflt                         │
│                                                 │
│ Directories              Files                  │
│ ┌──────────────────┐     ┌──────────────────┐   │
│ │ .                │     │ christmas.dflt   │   │
│ │ ..               │     │ weekends.dflt    │   │
│ │                  │     │ Thanksgiving.dflt│   │
│ │                  │     │ mondays.dflt     │   │
│ │                  │     │ factory.dflt     │   │
│ │                  │     │ mondays2.dflt    │   │
│ │                  │     │ fridays.dflt     │   │
│ │                  │     │ e6anorm.dflt     │   │
│ │                  │     │ e6anorm2.dflt    │   │
│ │                  │     │ mothersDay.dflt  │   │
│ └──────────────────┘     └──────────────────┘   │
│ Selection                                       │
│ /bnr/users/guest/*.dflt                         │
│                                                 │
│   OK          Filter          Cancel            │
└────────────────────────────────────────────────┘
```

2   From the dialog, select the appropriate file and click on OK.

The Default File view for that file appears.

3   You have completed this procedure.

Broadcasting log parameters

Log parameters can be broadcast to many offices at once by pressing the Broadcast... button in the main window or selecting the Broadcast... menu option from the Action menu. When this operation is chosen, a broadcast dialog is displayed.

Figure 5-8 Log Customization Utility - Broadcast dialog box
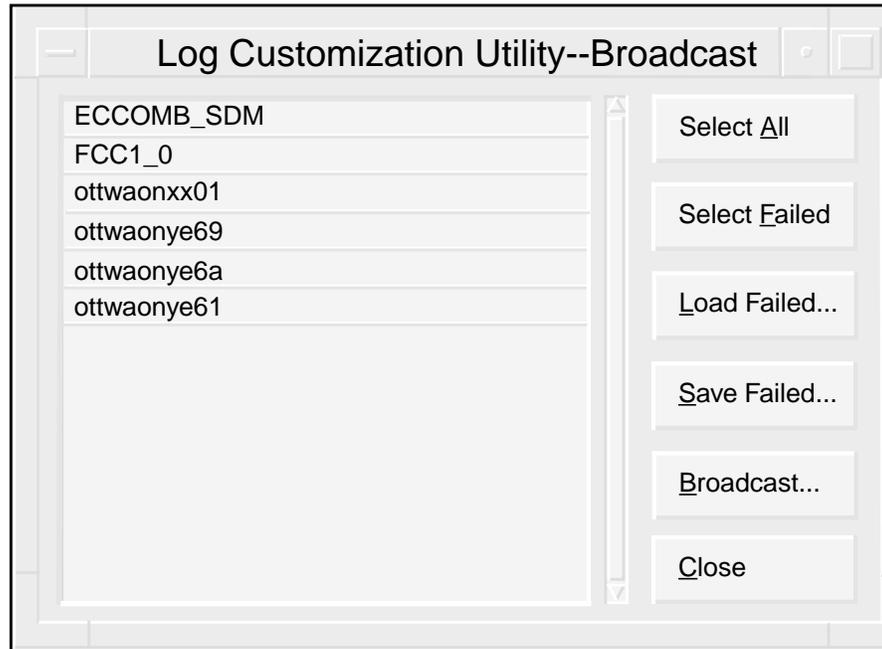
This dialog box is displayed as long as you stay in the Default File view. From this dialog, to broadcast log parameters, first highlight the offices where the parameters should be sent. All offices may be selected by pressing the "Select All" button.

If communication errors occur, events are logged to the event logger. As well, a communication trouble icon is displayed next to each office experiencing communication trouble. If a broadcast failure occurs, you are prompted to click on the Save Failed... button.

To save a failure status to a file, press the Save Failed... button. All log parameters, as well as a status record indicating to which offices the utility failed to broadcast, are saved in a file.

The Save Default Failure File dialog is shown in the following figure.

Figure 5-9 Save Default Failure File dialog box
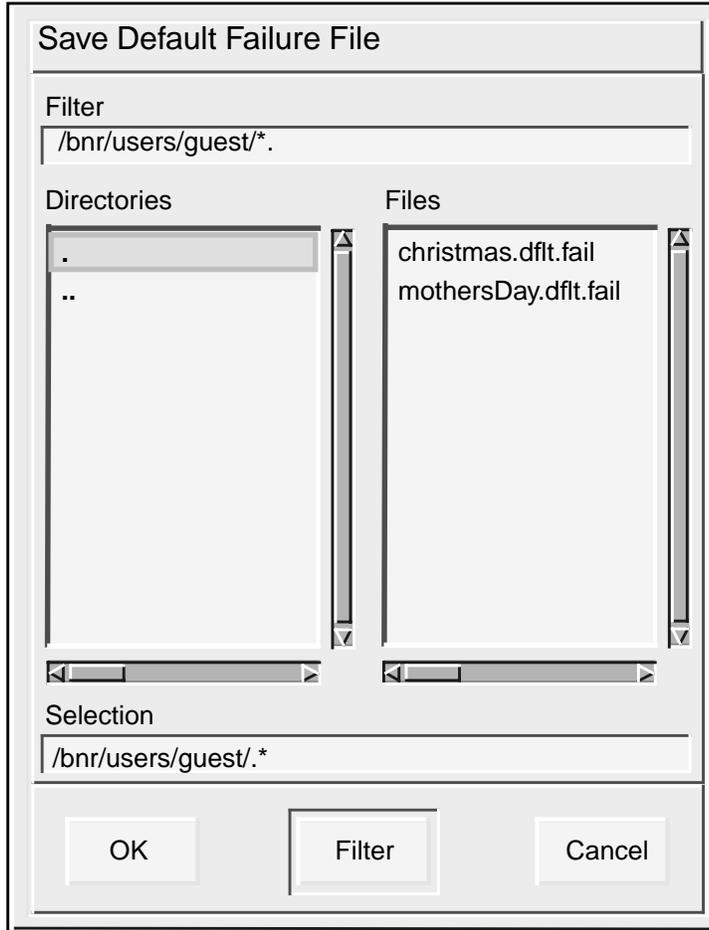
The default name for the failure file is <default file>.fail. However, any name can be used.

Later, to retry a failed broadcast operation, press the Load Failed... button. Note that this need not be in the same session. The utility can be exited and reentered before performing this operation.

A load failure dialog is displayed. The Load Default Failure File dialog is shown in the following figure.

Figure 5-10 Load Default Failure File

Load Default Failure File

Filter

/bnr/users/guest/*.

Directories

.
..

Files

christmas.dflt.fail
mothersDay.dflt.fail

Selection

/bnr/users/guest/*.

OK   Filter   Cancel
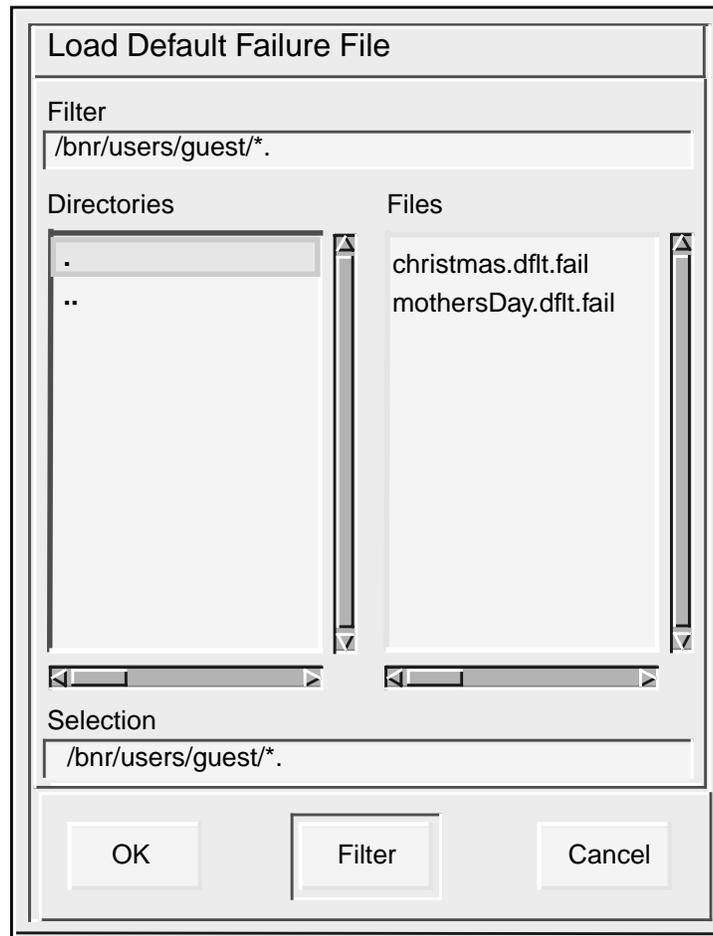
All failure files are listed. When a failure file is selected, log parameters in the file overwrite current log parameters. Before overwriting current parameters, a dialog is presented warning that parameters will be overwritten. As well, each office that had failed previously is indicated by a communications trouble icon next to the office. As well, the failed offices are highlighted. Press the Broadcast... button to broadcast to these offices.

6 Log reports

This chapter describes the log reports that are generated by the DMS
SuperNode Data Manager (SDM) Exception Reporting application.

Log categories (0, 1, and 1P) for the source logs are listed in "Category 0 and
1 logs" in Chapter 1.

Log EXC900

Explanation

The Exception Reporting application correlates computing module (CM) and SDM logs and generates this report whenever customer specified threshold values are met or exceeded. All exception report logs have the same log name (EXC) and default number (900), regardless of the originating log name and number. You can assign other log numbers, in the range 900–999.

Formats

The formats for log report EXC900 follow:

Format 1

<switch_name> ** EXCnnn mmmdd hh:mm:ss <sequence_number> EXC
Switch Threshold Exceeded
Component: ALL
Event: <event_id>
Info: <description>
Correlation ID: <correlation_id>

Format 2

<switch_name> ** EXCnnn mmmdd hh:mm:ss <sequence_number> EXC
Component Threshold Exceeded
Component: <component_id>
Event: <event_id>
Info: <description>
Correlation ID: <correlation_id>

Example

Examples of log report EXC900 follow:

```
FCC1 ** EXC900 JAN15 13:05:04 1234 EXC Component
Threshold Exceeded
Component: OCONNO3781TI 2
Event: Threshold Exceeded
Info: 2 C7UP112 messages in last 2 hours
Correlation ID: c7up112oconno3781ti_2.4

FCC1 * EXC900 JAN15 13:05:04 1234 EXC Component
Threshold Exceeded
Component: ALL
Event: Repeat Notification
Info: 7 PM106 messages in last 1 hours
Correlation ID: pm106.66
```

Field descriptions

The header of the EXC900 log report includes the following variable fields, from left to right:

- switch name

- severity indicator, as follows:

    — no asterisk indicates a severity of "none"

    — one asterisk indicates a severity of "minor"

    — two asterisks indicate a severity of "major"

    — three asterisks indicate a severity of "critical"

- log number, immediately following "EXC"

- month and day date

- time

- sequence number, which is inherited

The following table explains the variable fields in the body of the log report.

Table 6-1 Variable fields

Field	Value	Description
component_id	"ALL" (for format 1) Alphanumeric string up to 64 characters (for format 2)	This field represents the identifier from the originating logs that is used to generate the exception report. This is a mandatory field.
event_id	"Threshold Exceeded" or "Repeat Notification"	This field identifies the event that generated the exception log. The message "Threshold Exceeded" appears when the threshold has been crossed. The message "Repeat Notification" appears when the interval has expired and the problem still exists. This is a mandatory field.
description	character string	This field describes how many logs were received within the interval, what the interval was, and what the log type was. The range for the message count and the interval is 1–99 or "100+".
		The unit for the time-based interval is one of seconds, minutes, or hours. The unit for the call-based interval is "call", based on CMCall, LineCall, TrunkCall, CCS7Message, CCS7Call, or PMCall.
		This is a mandatory field.
correlation_id	text string, up to 80 characters	This field contains a unique identifier that can be used to link repeat notifications. This is a mandatory field.

Action

There is no required action for an EXC900 log report. To analyze the output of the report, refer to the originating log name and number. Table 5-1 lists the originating logs alphabetically, and provides a brief description of what the logs mean. For more information about the originating log and action to be taken, see the *DMS-100 Logs Report Reference Manual.*

Log SDM615

Explanation

The Exception Reporting application generates a daily warning/information report at 8:00 a.m. (local time). The report indicates which logs have been generated with a threshold indication within the surveillance period. Those logs can cause a conflict with the Exception Reporting application. This conflict can be either of the following:

- the number of logs received by the expert system will be inaccurate, potentially affecting system-level counts

- component information in the body of all threshold reports is lost, potentially affecting component-level counts for category 1 and category 1P logs

Format

The format for log report SDM615 follows:

<switch_name>   SDM615 mmmdd hh:mm:ss <sequence_number> INFO Threshold Conflict
Event: Log Thresholding In Effect For Logs Managed By Exception Reporting Application – Exception Reports May Be Inaccurate
Action: Disable Thresholding Via LOGUTIL For The Following Reports:
<Thresholded Log>

In the body of the log, the <Thresholded Log> field is repeated up to seven times on a line, up to eight lines (to a maximum of 56 entries in a report), depending on the number of logs that have been thresholded.

If more than 56 logs are known to have been thresholded, additional SDM615 logs are generated.

Example

An example of log report SDM615 follows:

```
FCC1    SDM615 DEC03 10:53:35 1234 INFO Threshold
Conflict
Event: Log Thresholding In Effect For Logs Managed By
Exception Reporting Application – Exception Reports
May Be Inaccurate
```

```
Action: Disable Thresholding Via LOGUTIL For
Following Reports:
```

Table 6-2

AUDT201	C7UP100	C7UP101	C7UP102	C7UP107	C7UP111	C7UP112
CCS154	CCS167	CCS168	CCS204	ENET111	ENET203	ENET205
ENET211	LINE100	MS303	MS304	MS306	MS307	PM100
PM101	PM102	PM103	PM104	PM105	PM106	PM107
PM108	PM109	PM110	PM111	PM112	PM113	PM114
PM115	PM116	PM117	PM118	PM119	PM120	PM121
PM122	PM123	PM124	PM125	PM126	PM127	PM128
PM129	PM130	PM131	PM132	PM133	PM134	PM135

Field description

The header of the SDM615 log report includes the following variable fields, from left to right:

- switch name
- month and day date
- time
- sequence number, which is inherited

The following table explains the variable field in the body of the log report.

Table 6-3

Field	Value	Description
Thresholded Log	Alphanumeric string up to 8 characters	This field contains the log identifier for the originating log thresholded via LOGUTIL and received by the Exception Reporting application. This is a mandatory field.

Action

The recommended action is to remove the threshold or ensure that threshold criteria have been correctly established, based on the system threshold.

To analyze the output of the report, refer to the thresholded log names and numbers.

Appendix A ER status messages

This chapter describes the Exception Reporting (ER) status messages.

ER status messages

This section describes the ER status messages and what actions you must take to resolve a trouble message.

The state of the ER application appears as InSv (in service) during operation.

The ER application appears ISTb (in–service trouble) during the initialization of the operational measurements application.

During the in-service trouble state, call-based thresholding is not functional. All other aspects of the application remain in operation. If the in-service trouble state persists for more than 10 min., it may be necessary to manually busy (ManB) and return to service (RTS) the ER application.

> *Note:* To busy an application you must access the application (Appl) menu level of the SDM remote maintenance interface (RMI). For more information, refer to the *DMS-100 Family SuperNode Data Manager Fault-tolerant User Guide*, 297-5061-906.

If the application fails to go in-service 10 min. after busying it and returning it to service, contact your next level of support.

DMS-100 Family

SuperNode Data Manager Exception Reporting

User Guide

NØRTEL
NETWORKS™

How the world shares ideas.