STRICTLY CONFIDENTIAL

IMS User Manual

Document **LZBP 101 289 Rev X**

The information in this document may be changed without prior notice and does not represent a commitment on the part of Ericsson.

Ericsson assumes no legal responsibility for any error or damage resulting from the use of this manual.

Ericsson AsiaPacificLab Australia Pty Ltd acknowledges that any Trade Name or Trade Mark or Registered Name used in this manual is the sole property of its legal owner.

Contents

STRICTLY CONFIDENTIAL

Chapter 2 Installing and Configuring IMS

Chapter 4 Administering the IMS Database

STRICTLY CONFIDENTIAL

STRICTLY CONFIDENTIAL

Chapter 9 IMS Alarm-Log Printout Descriptions

STRICTLY CONFIDENTIAL

STRICTLY CONFIDENTIAL

STRICTLY CONFIDENTIAL

1 Functional Specification of IMS

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	1/155 17-CNAP 102 11 Uen
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-03-14
		Revision	T
		Pages	22

A description of the functions of the Interception Management System and its administrative and operational features

In this chapter

This chapter details the functions implemented in the Interception Management System (IMS).

These are implemented for the management of interception functionality in switches known as network elements (NE).

Prerequisites

The NE needs to be connected to the IMS via the MTP or Corba (G10) protocol and Law Enforcement Monitoring Facilities (LEMF) via one of the available protocols.

The operator must be an XMATE system administrator or operator with the appropriate NE and MML command-access authority.

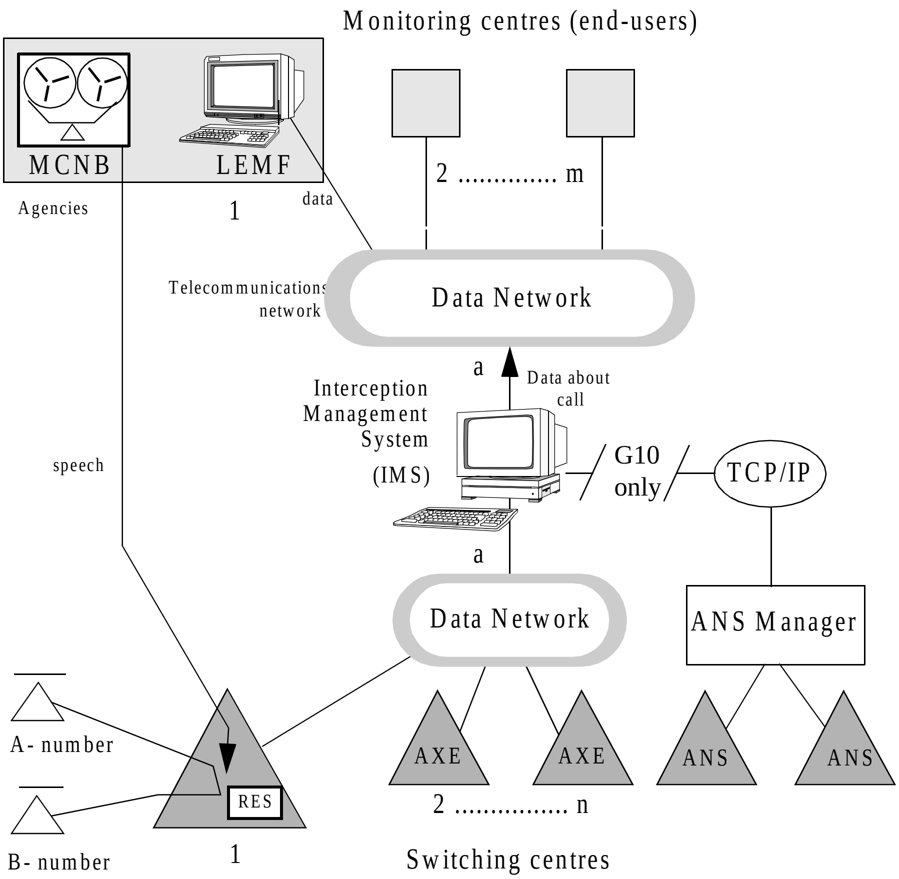
Overview

The Remote-control Equipment Subsystem (RES) [1,2] function of an AXE (domestic) or ANS (G10) monitors calls on switched connections and services. The content of the call can be speech or data.

Both calls to and from a target subscriber can be monitored. The monitored calls are treated as a normal call. The connections used for transferring the call content to the LEMF are set up in parallel with the monitored calls.

Data about the call is gathered and transmitted at the connection and disconnection of each monitored call to the LEMF by IMS, which provides data routing and management of the interception service (Figure 1.1 on page 1-4).

Figure 1.1 Telecommunication interception model



Applicability

IMS supports all network technologies where the RES function is applicable. This document deals with its implementation in:

- Analog Mobile (CMS 88), for monitoring voice calls,
- Digital Mobile (CME 20), for monitoring voice, data and SMS calls,
- PSDN/ISDN, for monitoring voice and data calls, and
- ANS switch, for monitoring voice and data calls (G10).

IMS provides the network operator with the possibility to setup the management system exclusively for one of these network technologies or a centralised system managing a combination.

IMS provides initiation of subscriber interception and the routing of the data product to a number of LEMF.

IMS initiates the monitoring of a subscriber's calls in the NE to which the subscriber is connected. In the case of mobile networks, the system initiates the monitoring in all mobile NE.

The routing of the data product is based on routing criteria stored in the IMS database. The database provides association between the target subscriber's number (monitored network number or MNN/IMEI/IMSI) and the LEMF where the data product is to be received.

The X.25 communication network provides the data transfer between the NE and IMS. The data about the monitored call arrives in the form of a file output. Ericsson's message transfer protocol (MTP) is used as the transport and upper layer protocol.

The data products can be transmitted to a LEMF via any of the communication protocols supported by the computer and application platform. In the current system release the following protocols are supported:

- X.25 PLP
- X.29
- FTAM

Implementation

The relations between the REDRB functions and the other system components are shown in Figure 1.2 on page 1-7.

The IMS functions are implemented as a function block (REDRB) on the XMATE system application platform.[4]

Communication with the external systems is provided via the data communication block (DCB) which allows the applications running on the UNIX system to communicate with the applications running in the NE. The DCB provides a gateway function between the internal network based on TCP/IP protocol and the external communication networks based on the X.25 protocol. For G10, communication with the ANS switch is provided by the ANM server of the XMATE platform and the ANS server is implemented to communicate with the ANS Manager.

A collection and delivery server (**CTB**) is responsible for receiving data products (DPs), and transmission to LEMF. Data product adaption and conversion functionality will be available in a form of a shared-library module (.so), linked by the collection and delivery server.

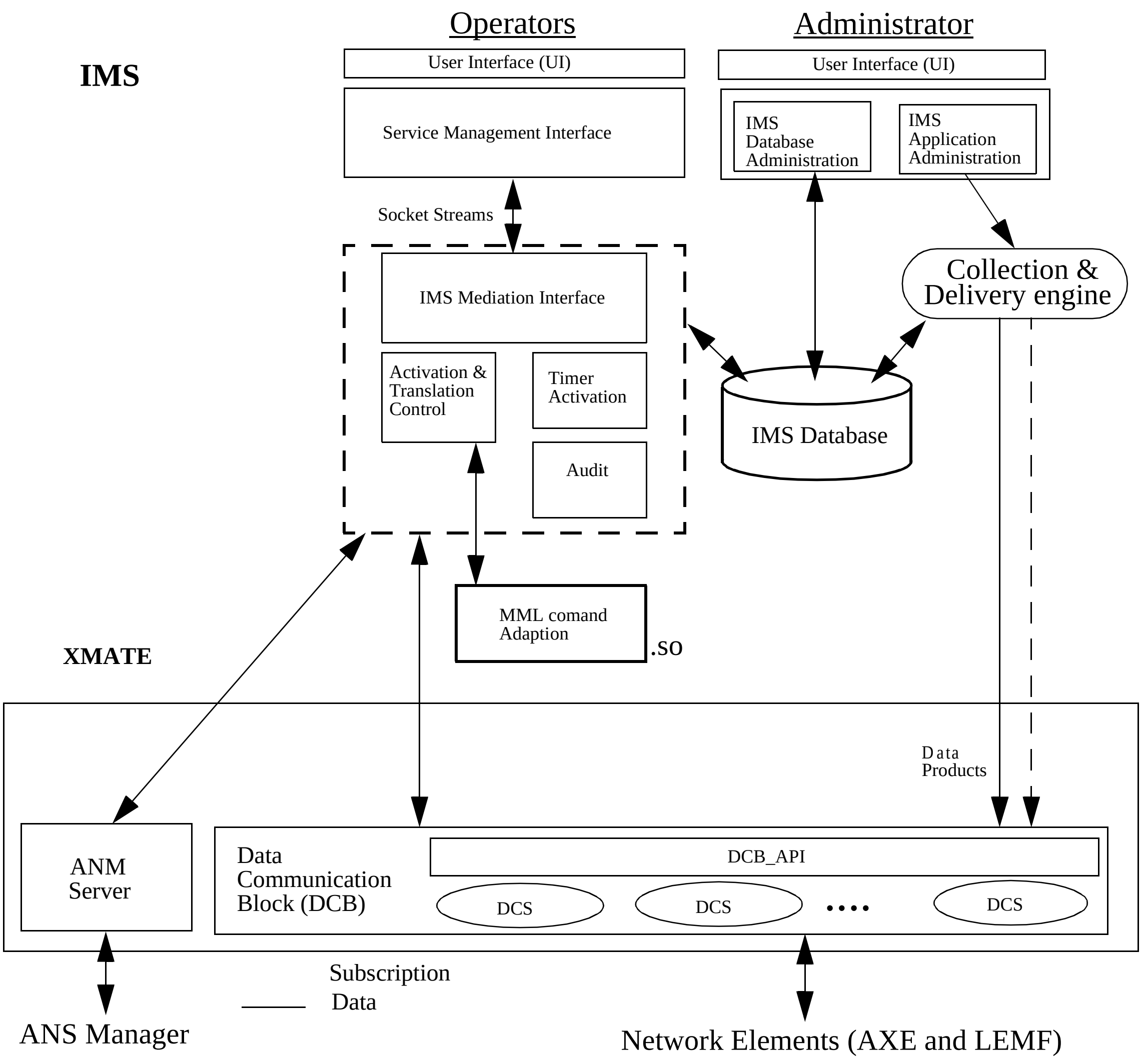
The IMS mediation interface serves as a glue between various IMS modules. It has the following core functionality:

- Provision of a standardised (socket-based) interface to the service management layer.
- As a ‘go-between’, managing warrant activation and scheduling.
- Verifying authorisation and general IMS database access.

This functionality is the responsibility of the mediation and activation server (**imas**). Activation control provides functionality for invoking and monitoring of activation tasks (activating, terminating and auditing). This module manages activation tasks by keeping track of and limiting concurrent session usage, immediate connection retries (including back-off delays or delayed activation), translation of requests into man-machine language (MML) scripts and interpretation of the responses.

The service management layer relies upon a consistent socket-based interface with the core IMS platform, but by construction and the platform environment, it offers a flexible base for the development of customised user interfaces and service management offerings.

Figure 1.2 IMS system concept



General functions

The IMS application functions are categorised into three groups:

Function	*Description*
Server functions	The functions that are related to analysis of the data products collected from NE and its transmission to the LEMF according to the routing criteria.
Operational functions	The group of the functions that have been given to an IMS operator to perform the management of the interception service.
Administration functions	The functions that allow the system administrator to configure and maintain the application.

Server functions

Figure 1.3 summarises the server functions of IMS, which consists of

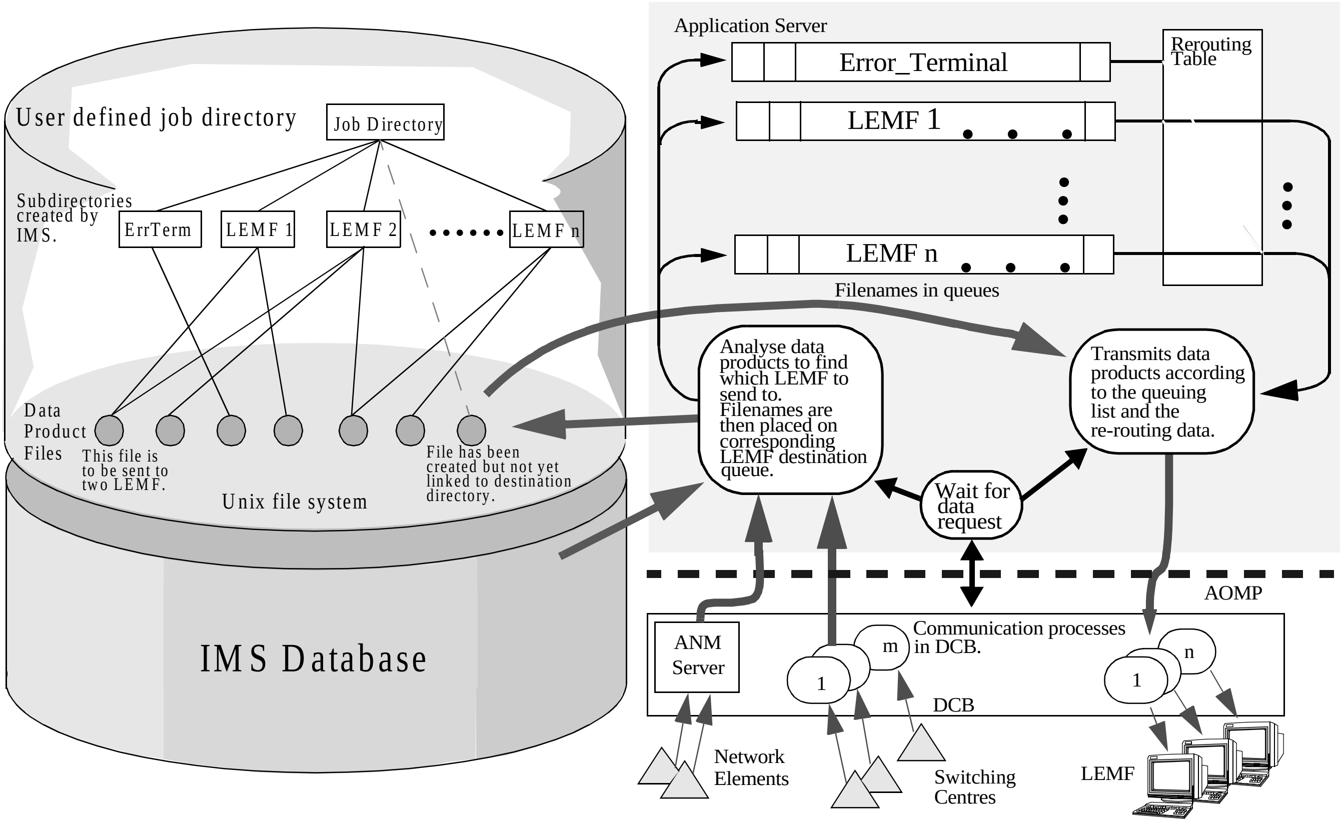
- Collecting data,
- Counting traffic, page 1-11,
- Restarting routing analysis, page 1-11,
- Transmitting data products to end-users, page 1-11, and
- Interworking with LEMF, page 1-12.

Collecting data

A data product from the AXE is sent to the IMS as a spontaneous (direct) file output session within the MTP and, for G10, the ANS switch comes as a CAD (Call Associated Data) file.

Each data product is stored as a data file in the UNIX file system. The file name is defined by the routing analysis function.

Figure 1.3 Server functions implementation model


User defined job directory
Job Directory
Subdirectories created by IMS.
ErrTerm
LEMF 1
LEMF 2
LEMF n
Data Product Files
This file is to be sent to two LEMF.
File has been created but not yet linked to destination directory.
Unix file system
IMS Database
Application Server
Error_Terminal
LEMF 1
LEMF n
Rerouting Table
Filenames in queues
Analyse data products to find which LEMF to send to. Filenames are then placed on corresponding LEMF destination queue.
Transmits data products according to the queuing list and the re-routing data.
Wait for data request
AOMP
ANM Server
Communication processes in DCB.
m
1
n
1
DCB
Network Elements
Switching Centres
LEMF

Two parameters within the data product are relevant for the analysis and the routing algorithm:

- Monitored Network Number (MNN/IMEI/IMSI) – the target subscriber number.
- MUID - monitoring user ID (if supported).

Note: The switch fault code is also analysed and an alarm raised if configured correctly.

Routing process

MNN/IMEI/IMSI is a generic name for the subscriber's number used in IMS for all the number types that are supported by the current system implementation. A MNN/IMEI/IMSI is mapped to the monitored subscriber number and, in the case of G10, it is mapped in a particular network technology via the network identifier (NI).

The relevant MNN/IMEI/IMSI number field of the file is taken as the routing key. If MUID is supported, it is used as a second routing key. The IMS database provides the association between a key and the LEMF to where the data product must be routed. A data product can be routed to one or two LEMF (LEMF-A and LEMF-B).

The routing analysis procedure is invoked by the collection and delivery server. It obtains the relevant key(s) from the data printout and consults the database to determine where the data product (file) is to be transmitted. The results of the routing analysis process are:

- *Data product file* The routing procedure generates one file per data product per destination (LEMF). For example, in the case where the data product needs to be sent to two LEMF, two data product files will be generated.
- *Transmission request list entry* This entry contains the data product file name.
- *Internal alarm message* This message is produced only when applicable.

Handling routing errors

If the routing process detects an error (for example, a MNN/IMEI/IMSI is not initiated within the database) the data product is routed to the Error_Terminal and the appropriate alarm message is generated. The Error_Terminal is the application internal destination where the data products with the unresolved routing cases are directed. The Error_Terminal can be rerouted to any active LEMF.

The routing process analyses the fault code which the data product may contain and generates an internal alarm message. The printout containing the RES fault code is routed to the appropriate LEMF and an alarm message is sent to the alarm block.

A special procedure is taken when the fault code 'Restart in the switch has taken place' occurs. The data product which contains this fault code does not contain any other information, so it cannot be routed to a LEMF. This fault code indicates that the reloading is taking place, so the table of monitored subscribers in the particular NE must be checked. The routing analysis process sends the warning to the system operator by storing appropriate alarm messages in the alarm block. The data product is then deleted.

Counting traffic

In order to keep track of the number of data products received from NE, two traffic counters are implemented in the database for each monitored subscriber. The counters are incremented for each received data output for the life of the warrant. The following counters are defined:

WDPC Warrant Data Product Counter provides information on the number of data products received per monitored subscriber since the monitoring started. The operator/system administrator cannot change the counter.

MDPC Measurement Data Product Counter provides information on the number of data products received per monitored subscriber since the measurements started i.e. when the counter was last reset. The system administrator can reset the counter at any time. The time when the counter has been reset is automatically captured in the database.

Restarting routing analysis

The restart routing analysis procedure is invoked by the application start procedure. Its task is to recreate the transmission request list for the data product files remaining in the system since the last shut-down.

The procedure analyses the directory where the data product files are stored. It takes the file generation time as the argument to create an entry in the appropriate transmission queue in chronological order.

Transmitting data products to end-users

This function initiates the transmission of the data products to a LEMF based on the information stored in the transmission queue. Each LEMF destination has its own transmission queue which contains the data product file names that have to be transmitted to the particular LEMF. The elements in the list are sorted in chronological order where the generation time of the data product file is taken as the argument.

Transmission states

The transmission queue can be in one of the following states:

- *Active*. The LEMF where the data products are to be transmitted is indicated as an active (‘working’) destination.
- *Blocked*. The LEMF where the data products are to be transmitted is blocked.
- *Blocked/Rerouted*. The LEMF where the data product(s) is to be transmitted is blocked and the output of the blocked transmission queue is redirected to the input of an active transmission queue.

Transmission processes

The IMS transmission process opens communication to an active LEMF if the LEMF transmission queue or the transmission queues that have been routed to the LEMF contain entries. All data products queued in the system for the opened destination will be transmitted via the same logical channel. After the successful transmission of a data product, the file name entry is removed from the queue and the data product file is deleted.When all data products are successfully transmitted, the connection to the LEMF is closed.

The connection to the LEMF will be closed according to the value of the Inactivity Timer. The Inactivity Timer defines the time delayed in seconds in which the connection to the LEMF will still be open after the transmission of the data products. By setting the Inactivity Timer value, the system operator can optimise the usage of the data network resources according to the traffic expectation.

Multiple transmissions

A number of connections to different LEMF can be opened simultaneously. The number of simultaneous connections depends on the number of available logical channels in the communication network. If the transmission process cannot send the data product to the LEMF the following actions are taken:

- *Retransmission*. The transmission process tries to send the data *n* times, where *n* is a parameter which defines the number of consecutive call attempts.
- *Delay retries*. If the data product has not been transmitted after *n* call attempts, the same number of call attempts is re-issued after the time delay *Td*, until the data product is successfully transmitted to the LEMF or is rerouted to another LEMF.
- *Alarm*. The system administrator specifies the number of unsuccessful call attempts which can occur before the transmission process generates an alarm to an operator. If the alarm status has been detected, an alarm ceasing message is generated after the successful transmission of data products to a LEMF.

Interworking with LEMF

Data products can be transmitted to a LEMF via any of the communication protocols supported by the XMATE application platform. It can be sent as a:

- *Data message*. The content of the data product file is initiated for the transmission via D-Data request primitive of the applied data-communication protocol.
- *File*. The data product file is initiated for the transmission via F-File request primitive of the applied file-transfer protocol.

Currently the transmission process uses the following communication protocols:

X.25 PLP and X.29	For transmission of the data product as a data message.
FTAM	For transmission of the data product as a file.

Operational functions

The operator functions are grouped in a user-interface panel which can be selected from the operator root menu. Each operator function shows on the panel as an icon.

The operator can activate a function by clicking the appropriate icon. An additional panel appears asking the operator to enter the required data.

Note that you cannot open multiple windows in ims_app. Any open dialog boxes must therefore be closed before another can be opened.

Activation of monitoring (Init icon [Dom]/Create Warrant icon [G10])

The initiation of subscriber monitoring function sends the MML command for activation of monitoring of a particular MNN+MUID or IMEI+MUID to the NE (single or group) associated with the warrant as shown in the following table:

	MNN	IMEI	IMSI	MUID (if supported)
TL3/L5	✔	N/A	N/A	✔
TL4/L6	✔	N/A	N/A	✔
GSM 7.0	✔	✔	N/A	✔
GSM 8.0	✔	✔	✔	✔

If the NE name selected is a group name, then the commands are broadcast to all NE in the group.

The initiation cannot be issued if the monitoring of a particular MNN+MUID or IMEI+MUID or IMSI+MUID is already initiated.

If a new MNN/IMEI/IMSI is entered and it is a partial match (the comparison is based on the shorter of the two starting at the first digit) or subset of an existing MNN/IMEI/IMSI, then the entry will be rejected e.g:

MNN=12345 (existing)	IMEI=12345 (existing)	IMSI=12345 (existing)
MNN=123 will be rejected	IMEI=123 will be rejected	IMSI=123 will be rejected
MNN=123456 will be rejected.	IMEI=123456 will be rejected.	IMSI=123456 will be rejected.
MNN=0123 will be accepted	IMEI=0123 will be accepted	IMSI=0123 will be accepted
MNN=0012 will be accepted	IMEI=0012 will be accepted	IMSI=0012 will be accepted

The system has retry functionality which is used when a command fails due to there being no active communication with the NE or when the NE is busy. This functionality defines the waiting period between successive attempts at communication with the NE and a limit on the number of attempts. Both the waiting period and the number of attempts are defined in the environment files and the operator can modify them as required.

Note: Each unsuccessful attempt to send commands to the NE will result in an alarm. An alarm will also indicate when the final attempt has been made and these alarms will all appear in the Alarm log.

If the limit on the number of attempts is set to 0 (zero), then retries are attempted indefinately.

The waiting period must be a positive number representing the number of minutes.

Changes to either of these parameters are recognised on the next attempt.

Note: While a command is being retried, the monitor status shows the warrant with a ’pending’ state.

Termination of monitoring (Stop icon- Domestic)

The termination of subscriber monitoring is similar to initiation except for the MML commands used. Broadcast of commands and the retry functionality are similar to that of initiation.

The termination cannot be issued if the monitoring of a particular MNN+MUID, IMEI+MUID or IMSI+MUID has not been initiated before.

Modify Warrant icon (G10)

This function is used to update information of a target subscriber in IMS. A warrant can be deleted if its current state is not activated.

NE audit (Audit icon)

The audit function provides a comparison between the list of monitored subscribers in an NE and the IMS. The difference between the lists may occur as a result of a restart in the NE. Some of the data (activation or termination of monitoring) may be lost if the restart occurred before they had been backed up.

The collected information is compared with the information stored in the IMS database, which is taken as the reference and the audit report is generated. The audit report is saved to a log file in the form of two lists:

- List of warrants to be terminated for monitoring in the selected NE.
- List of warrants to be activated for monitoring in the selected NE.

The operator can update the monitoring table in the NE by selecting the synchronise option which will perform the update automatically.

Note: While multiple audits can be run, individual users can only run the one audit at the one time.

The following table shows the support available using the audit function.

Info audited/ synched NE	MNN	IMEI	IMSI	MUID	MCNB
TL3/L6	Y	N/A	N/A	Y	N
TL4/L7	Y	N/A	N/A	Y	N
GSM 7.0	Y	Y	N/A	Y	Y
GSM 8.0	Y	Y	Y	Y	Y

Note: A manual audit can be done by issuing the appropriate MML commands via terminal emulation application (WiOZ) included in the XMATE platform.

Monitor status list (Monitor Status icon)

This function displays the list of NE from the database associated with the activation or termination status of the specified warrant.

In the case of the mobile network application the function displays the list of NE where the selected subscriber is successfully initiated for monitoring. The list also displays the list of NE where the subscriber is not initiated.

Transmission handling (Rerouting)

The LEMF terminal can be active or blocked for transmission of data products. The operator can block and deblock a LEMF.

The data products routed to the blocked LEMF can be rerouted to an active LEMF. The rerouting can not be initiated to a LEMF terminal which has already been rerouted to another one. The operator can initiate/terminate the rerouting for the selected LEMF. The commands for initiation and termination of the blocking and rerouting are logged into the AOMP command log file.

The following data is displayed for each destination in the list of active LEMF:

- Number of data products in the queue.
- Number of the consecutive call attempts.
- Alarm status (ALARM or blank).

The following data is displayed for each destination in the list of blocked LEMF:

- LEMF terminal name if rerouting is taking place.
- Number of data products in the queue.

Dynamic LEMF Administration (G10)

The system administrator as well as the operator can create a LEMF at the time of warrant creation. They can also delete an existing LEMF so long as it is not being used by a warrant, used for rerouting by another LEMF or DP's are currently being sent to it.

Administrative functions

The administration functions allow the system administrator to maintain the IMS application. These functions are implemented in two panels (IMS Administration and IMS-Parameter Setup) and via a command line application for the Intercept Billing System.

Database administration

The database administration functions allow the system administrator to set up and maintain the data relevant for the management of the interception service.

The database administration function allows the system operator to:

- search the database based on various user defined criteria,
- print the list obtained by the search criteria,
- add or delete MNN, IMEI or IMSI,
- add or delete NE and LEMF,
- create NE groups, and add NE to or delete them from these groups,
- reset the MDPC (which automatically updates the reset time),
- modify the characteristics of a NE after deactivating the **imas** and **CTB** servers,
- modify database record (G10).

The IMS database modifications are logged.

Note: The IMS uses the LEMF names as the Monitoring User Identifier (MUID), however, the switch limits this to 8 characters while the LEMF name is 20 characters. As such, an algorithm has been implemented that generates 8 character MUID from the LEMF names.

Application administration

The IMS application is designed on the XMATE platform which allows the application to run within a distributed computer environment. The application administration allows the system administrator to define the computer environment for the application. This includes:

- the application host name (IMS host),

- IHS server name which contains the information about the XMATE system domain,
- selecting the transmission mode (*Transmit* or *Receive Only).*The **CTB** server can be started in the mode of only receiving the data product from NE without transmitting it to the LEMF (*Receive Only*). That mode of operation is implemented for testing purposes,
- activating or deactivating the collection and delivery (**CTB**) server,
- activating or deactivating the mediation and activation (**imas**) server,
- defining the job directory where the data product files are stored,
- viewing the status of both servers mentioned above.

The collection and delivery server parameters are defined as variables in the application setup file. They include:

- the number of consecutive call attempts for re-transmission (n),
- the time delay between the series of re-transmission (Td),
- call attempts before issuing an alarm,
- an inactivity timer,
- a condition that allows the use of STX/ETX around X.29 data products.

They can be changed by the administrator while the server is running and come into effect immediately after the edited file is saved.

Intercept billing system administration

The **ibs** application allows the administrator to generate billing records which provide sufficient information for the billing of voice and data transfer.

Characteristics

There are a number of characteristics of IMS. They are described by the following headings:

- Capacity,
- Performance,
- Authorisation, page 1-19,
- Starting, stopping and restarting, page 1-19,
- Communication network interface, page 1-19, and
- Communication with NE, page 1-20.

Capacity

The REDRB block is designed to handle a maximum of 5000 monitored subscribers per monitored network. The subscribers can be initiated for voice and data monitoring. The maximum number of monitored subscribers is limited by the RES block in the NE.

- The maximum number of LEMF is 255.
- The maximum number of NE is 200.
- Up to 8 simultaneous monitorings on one MNN/IMEI/IMSI for MUID supporting NE.

The above listed capacity parameters in the release are related to the size of the IMS database. These parameters have been taken according to the typical deployment requirements. Those parameters are not limited by the capabilities of the application processing, the application, or computer platform.

Performance

Determination of performance and capacity figures is a complex problem owing to the variety of the possible system configurations and real testing environment. Therefore a number of simulators have been made during the development process to provide basic information related to the system performance and capacity.

Authorisation

The user access security in IMS is based on the security management function implemented in the application platform. The security management in XMATE operates at four levels:

- Access to the system.
- Access to the application.
- Access to the NE.
- Authorisation to issue individual commands.

The security access to the system level is controlled by UNIX authorisation features. The operating system used in the current release controls the access based on the user identification (or logon) and password.

Starting, stopping and restarting

The IMS operational and database administration functions are defined as user interface functions so they can be started and stopped by the operator and system administrator respectively. The functions are restarted manually after an XMATE system restart.

Starting and stopping the servers (**CTB** and **imas**) is provided by the IMS application administration user interface. They are restarted automatically after an XMATE system restart.

Once restarted, IMAS will run through the IMS database and send out the appropriate activation commands for any warrants that were entered by the IMS administrator in the IMS Administration window.

Communication network interface

The communication network for connection to the NE can be PSDN or leased lines. The network parameters need to be set-up according to the XMATE (DTE) communication parameters (with G10, the communication network for connection to the ANS NE can be CORBA over TCP IP).

Communication with NE

The IMS sends the administration commands to a NE and collects the data output from the RES subsystem. The file-oriented output is used by RES to collect the data in **RCEFILE** (AXE) and for G10, **CAD** (ANS).

To transfer the file output data to IMS, the direct file output has to be set up for **RCEFILE** via the communication port connected to IMS in the AXE.

At least two logical channels have to be allocated for the communication between a NE and IMS (one for the command handling and one for the data output) in the case of PSDN. In G10, for ANS, the IMS needs to subscribe CAD files to ANS Managers.

References

1 Remote Control Equipment,
1/155 17-ANT 233 01 Uen

2 Remote Control Equipment in CME20,
1/155 17-ANT 233 02 Uen

3 Remote Control Equipment (Local Exchanges),
1/155 17-ANT 233 03 Uen

4 AOMP Network Management System,
155 17-AOMP 102 01 Uen

2 Installing and Configuring IMS

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	1531 CNAP102 11 Uen	**Pages**	22
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-03-16	**Revision**	J

Installing the fileset and setting up the operating parameters of the Interception Management System

In this chapter

This chapter provides a guideline to the installation and configuration of IMS.

It addresses both the installation instructions and the practical aspects of the configuration possibilities so that the information presented is more as a reference guide than as a specific procedural document.

Installation and Configuration Information

The IMS functions are implemented as a function block (REDRB) on the XMATE (AOMP) system application platform [1]. Although logically the IMS application system resides on top of the XMATE platform, default installation will integrate the IMS related files into the existing XMATE system and directory hierarchy.

IMS therefore extends the functionality of the base Network Management platform of XMATE.

Following the package installation, a number of configuration items may be adjusted/fine-tuned to match local requirements and desired operation.

A number of third-party products and the relevant configuration are also discussed in this chapter for completeness.

Further detail on other available configuration parameters can be sourced directly from the product documentation set or on-line media if installed.

Additional configuration parameters are also available in Chapter 5 “Administration of the IMS Transmission Process” for run-time variables that affect the operation of CTB (Collection and Transmission Block).

For a description of the available alarms, refer to Chapter 9-IMS Alarm-Log Print-out Descriptions.

Installation of IMS

Prerequisites

The following must be completed before you begin the installation:

- Install XMATE according to the XMATE Installers & Administrators Manual B[2]. Use automounter to install XMATE under the $AOMPHOME path.
- Command logging should be enabled. To do this, set the environment variable LOG_COMMANDS to 1 in $AOMPHOME/setup/aomp.setup.
- Install Applix (tm) base and spread-sheet applications under /home/applix (automounted) path.
- Install SunLink X.25, Solstice OSI and Solstice FTAM communication products as appropriate (depending on the protocol used for communication to AXE and LEMF).
- Install Java Runtime Environment (JRE). (G10 only)

Installing IMS

IMS is generally distributed on CD-ROM or on tape in `pkgadd` format. The UNIX pathname defining your CD-ROM or tape drive is represented below as *`device`* (for example, `/cdrom or /dev/rmt/0`).

To begin the installation of IMS type the command below. Note: You need to log in as root to run this command.

```
pkgadd -d device <Blockname(s)>
```

You will be presented with a series of prompts where you will need to either answer questions or enter path names. These prompts will look similar to the following:

Enter the hostname of the default IMS server

(Default: prsm05)

for Domestic, enter the applix path

(Default: /opt/applix)

APPLIX_PATH=*/opt/applix*

IMS_HOSTNAME=*prsm05*

for G10, enter the Java 2 Runtime Environment path

(Default: /opt/java2re)

JAVA_HOME=*/opt/java2re*

IMS_HOSTNAME=*prsm05*

Would you like to alter any of the above parameters?

Enter Y to alter or press RETURN if not:

Would you like to copy CDE Menu files to ~aomp?

Enter Y to copy or press RETURN if not:

Enter path to package base directory [?,q] /home/aomp

Using </home/aomp> as the package base directory.

To manually copy the CDE Menu files:

Obtain a recursive copy from the directory /home/aomp/install/sample_env/aompadm/.dt to the {home directory}/.dt of users in group aompadm.

Obtain a recursive copy from the directory /home/aomp/install/sample_env/aompusr/.dt to the {home directory}/.dt of users in group aompusr.

Installation of <REDRB> was successful.

The installation is now complete.

IMS Directory Structure

Root menu

The root menu will be modified automatically to include the IMS functions, as follows:

IMS Administrator root menu:

Server Administration	`$AOMPHOME/bin/admin/ims_run TR_PARAM`
Database Administration	`$AOMPHOME/bin/ims_run READM`
Rerouting	`$AOMPHOME/bin/ims_run RRS`

IMS Operator root menu:

IMS Application System	`$AOMPHOME/bin/ims_run ims_app`
Database Search	`$AOMPHOME/bin/ims_run READM`
Rerouting	`$AOMPHOME/bin/ims_run RRS`

IMS Operator and IMS Administrator root menus will be added to the XMATE user configuration automatically at the time of the installation (if selected by the installer).

Sample environment menus under `$AOMPHOME/install/sample_env` will also be updated for both administrators and operators. When creating users (administrators or operators), a recursive copy of the `sample_env/aompadm` or `aompusr` is all that is required to configure the menu system.

For example:

```
su - imsoper1
cp -r ~aomp/install/sample_env/aompusr/.
exit
```

Applications

The following describes the applications that belong to both the Administration and Operator groups.

$AOMPHOME/bin Directory

`READM`	Database admin/search application (user interface)
`RRS`	Rerouting application (user interface)

`irun`	Script used to start IMS applications
`irun_debug`	Debug version of the irun script
`ibs`	Application for IMS billing record generation
`legalbstat`	Application for Legal Basis counter statistics
`ims_run`	Script used to start IMS application on an executive server host.
`ims_app`	IMS Warrant Management (Operator) application (user interface)- startup script.

$AOMPHOME/bin/admin Directory

`TR_PARAM`	IMS Server Administrator and configuration application (user interface).
`CTB`	Collection and Transmission Server
`imas`	Monitoring and Activation Server
`DCFTAM`	FTAM Protocol module of DCS
cdstrigger	Application to manually trigger start and end data records - i.e. notification (dummy) data products of monitoring activation begin/end to the LEMF.

Other Directories

Below is a list of directories that IMS uses for various tasks.

`/etc/rc2.d/S97lmgrdapplix`

Automatic Applix licence startup script.

`/etc/rc2.d/[SK]98xmateims`

Automatic server startup scripts after server-host reboot.

`$AOMPHOME/axhome/macros`

Applix(tm) Macros and icons for IMS Warrant Management (Operator) user interface.

`$AOMPHOME/scripts/imsau.abo (dom)`

Applix(tm) IMS Warrant Management (Operator) user interface.

`$AOMPHOME/classes (G10)`

Java classes for the IMS Warrant Management (Operator) user interface (G10 version).

`$AOMPHOME/log`

Various debug log files

`$AOMPHOME/data/redrs/jobq`

Default placement of jobq and LEMF destination queues

`$AOMPHOME/data/redrs/billing`

Default placement of processed billing records

`$AOMPHOME/data/redrs/billing.err`

Default placement of erroneous billing records

`$AOMPHOME/setup/redrs`

IMS system configuration area and database.

`$AOMPHOME/doc`

Contains a pdf version of the IMS Operator and Administrator Manual.

IMS Configuration Files

All IMS configuration parameters are located under $AOMPHOME/setup/redrs directory. Their significance is explained below:

$AOMPHOME/setup/redrs Directory

`axegroups`	AXE Groups
`datemsk`	date mask file
`environment`	IMS Environment Variable configuration file
`imas.stat`	Temporary file used by TR_PARAM
`packet_format`	RES File specification information
`RTDS.REDRS`	IMS Database
run_variables	CTB Run-Time variables
`text`	IMS Mapping Tables
`trb`	Routing Tables

axegroups

This directory contains a list the Network Element (NE) Group files which contain a list of the NE belonging to each group. These NE group files are managed by the Edit NE Group window (READM function).

environment

Environment file contains defined paths of files used by the IMS system (composed during package installation). “irun” and “irun_debug” scripts will source this file prior to execution of any of the IMS programs. Changes made here will become available on the next invocation of an IMS application.

packet_format

Contains information about the RES file (data-packet) format. Field positions and offsets are specified here against the RES revision (application system version) and a record-type specification. The content of this file is closely linked with the internal IMS operation and therefore the file is NOT intended for general operational administration.

RTDS.REDRS

This is the main IMS database. It contains all information relevant for warrant processing, operation, and data product management. This file is the main run-time IMS configuration storage area (database), containing such things as IMS AXE, LEMF, all warrants and warrant related information, etc.

It is useful to back up this file on a regular basis as it constitutes all run-time knowledge of the IMS system (warrants, warrant related data and status).

run_variables

CTB run-time parameters. Changes made here will be dynamically propagated to CTB without the need for a server restart. The content of this file is listed and explained separately.

trb

This directory contains routing tables and some basic configuration parameters used by the CTB process. The parameters are editable through TR_PARAM user interface, and the routing table through the RRS program (user interface). Changes to routing tables will be taken into account dynamically without any need to restart servers. Basic configuration parameter changes require all IMS servers to be restarted.

$AOMPHOME/setup/redrs/text Directory

`IMSAttribute`	Main IMS Configuration file
`IMSRESID`	Mapping Table: RES Identifier
`IMSNETOPID (G10)`	Mapping Table: Network Operator Identifier
`IMSSUBOPID (G10)`	Mapping Table: Sub-Network Operator Identifier

IMSAttribute file

The `$AOMPHOME/setup/redrs/text/IMSAttribute` file contains various parameters controlling the behaviour of IMS, for example, time-out values and retry attempts. Changes in this file take effect when an administrator next launches the

IMS Administrator window (see Chapter 4, ‘Administering the IMS Database’) and restarts the IMS servers (Chapter 5, ‘Administering the IMS Transmission Process’). The contents of this file are self-documenting.

Mapping Tables

Mapping tables are text files, such as `$AOMPHOME/setup/redrs/text/IMSRESID`, used during conversion of RES output (RCEFILE) and data product specification. The conversion itself is performed by the CTB process (Collection and Transmission Block).

The files are very specific to the current RES application system implementation and can be updated as needed to reflect any changes or updates in RES.

Further discussion and comments on the mapping tables can be found within the files themselves (comment lines) and for G10, in Chapter 12, ‘IMS Data-Product Specifications’.

Any updates of the mapping tables will become visible to the IMS system after the first subsequent administrator invocation of the READM (Database Modify) user interface. There is no need to restart any of the IMS servers or applications.

run_variables

consec_call_att 5

When routing output data products to LEMF ‘n’ (5) consecutive call attempts will be made before a delay.

time_del_call_att 30

Time delay in seconds between consecutive call attempt blocks.

alarm_call_att 10

Number of data product delivery call attempts before raising an internal system alarm.

time_del_close_conn 2

Connection idle time-out value (seconds) before a LEMF channel release. Time delay an open connection with a LEMF will be maintained after a delivery of the last data product.

x29lemf_use_stx_etx 1

If set to 1, an (STX STX STX), for Start of Transmission, is prepended (prefixed) and (ETX ETX ETX), for End of Transmission, is postfixed to every outgoing data product in case of X29 delivery protocol. Setting 0 disables this action. Not relevant for any other LEMF protocols.

IMSAttributes

The following is a list of used and configurable IMS Attributes. Other parameters which may be found in the IMSAttributes file (briefly commented within), are currently unused, non-changeable, or otherwise irrelevant for the IMS administration tasks as per the current IMS system release - they must NOT be changed and hence they have not been described in any more detail in the section below.

max_pra 240 (G10)

Specifies maximum number of PRA (PRimary Access) devices allowed for RES monitoring (ie per AXE). Note that a single Primary Rate Access Interface uses 30 PRA devices/channels. Therefore default of 240 devices is equivalent to 8 PRA interfaces.

This parameter is used during an automatic MNN verification procedure at warrant initiation to prevent exceeding number of PRA devices that can be monitored in one AXE.

cds_delete_dps yes

Setting this to’no’ will prevent the CTB server from deleting the intermediary files in the jobq directory during reception and conversion of data products. This configuration is only to be used for testing purposes.

Upon reception, the original RCE files are stored by default in the top-level jobq directory, converted into the appropriate format (.cv filename extension), and then linked into the appropriate LEMF queues. If this option is set to yes (default), the original RCE file and the converted output file (*.cv) are removed from the top level jobq directory.

Disabling this deletion will allow observation of the original data products and their corresponding converted outputs (ie format debug analysis).

mas_max_conc_conn 6

Specifies the maximum number of concurrent activation/termination sessions to be permitted. This parameter will restrict command handling activities of the Monitoring and Activation Server (MAS) in order to prevent flooding (ie over-consumption) of available logical channels and communication resources.

For example, when a total of 15 logical channels are available, setting mas_max_conc_conn to 6 will permit up to 12 logical channels to be consumed for command handling activities at peak-time (activation/termination/auditing). This will maintain the availability of the remaining 3 logical channels for incoming data products or other XMATE applications.

Note that MNN Verification procedure (conducted during warrant initiation) is not restricted in this respect since typically this is a one-to-one limited activity.

g10_printout_identification AA (G10)

Two character identifier used in G.10 field 2 (Data Record Identification)

g10_printout_filename AA (G10)

Two character identifier used in filename creation of data products for delivery to LEMF.

res4act_misc (G10)

Market specific MISC argument for RES command RCSUI (Subscriber Monitoring Initiate). Default is commented out (ie undefined).

res4act_pass_cugni yes (G10)

Optionally pass CUG and NI parameters in the RCSUI command when activating warrants. Setting this configuration parameter to no, will result in ignoring CUG and NI value settings that are associated with a warrant.

res4actterm1_waiting_period 1 (G10)

Specifies period in minutes of automatic retry of warrant activation/termination upon certain kinds of failures. Failure in parameter values or command formats will not result in repeated attempts to activate/terminate a warrant. When set to 0, no retry attempt will be made.

res4actterm1_number_of_attempts 5 (G10)

Specifies an expiry counter (infinity, if the value is set to 0) of a number of retry attempts for activation/termination upon certain kinds of failures.

MAXCALLS 10 (G10)

Specifies the maximum number of calls. 10 is the default value.

Whatever the default value is set to in this file, then this will automatically be displayed in the Create Warrant window when initially opened.

LEGAL_BASIS G10 (G10)

Default value for the Legal Basis.

Whatever the default value is set to in this file, then this will automatically be displayed in the Create Warrant window when initially opened.

MNN_ACC_twice Yes

Setting this attribute to ‘No’ will force the MNN input from the IMS Warrant Management Operator user interface to be verified only once.

LEMF_PASSWD_twice Yes (G10)

Setting this attribute to ‘No’ will force the LEMF Password input from the IMS Warrant Management Operator user interface to be verified only once.

START_TIME_twice Yes (G10)

Setting this attribute to ‘No’ will force the Start Time/Date input from the IMS Warrant Management Operator user interface to be verified only once.

MCN_ACC_twice Yes (Dom)

Setting this attribute to **No** will force the MCNB input from the IMS Warrant Management Operator window to be verified only once.

MOBILE_NE Yes (Dom)

Seting this attribute to **No** will display the windows (Admin and Operator) with some disable features to suit the Fixed Network environment.

END_TIME_twice Yes (G10)

Setting this attribute to ‘No’ will force the Stop Time/Date input from the IMS Warrant Management Operator user interface to be verified only once.

res3actterm1_waiting_period 15

Specifies period in minutes of automatic retry of warrant activation/termination upon certain kinds of failures. Failure in parameter values or command formats will not result in repeated attempts to activate/terminate a warrant. When set to 0, no retry attempt will be made.

The retry period is set as default to 15 minutes in order to minimise the AXE going beyond a small restart.
This applies to Local 5 switches only.

res9actterm1_waiting_period 15

Specifies period in minutes of automatic retry of warrant activation/termination upon certain kinds of failures. Failure in parameter values or command formats will not result in repeated attempts to activate/terminate a warrant. When set to 0, no retry attempt will be made.

The retry period is set as default to 15 minutes in order to minimise the AXE going beyond a small restart.
This applies to Local 7 switches only.

res3actterm1_number_of_attempts 3

Specifies an expiry counter (infinity, if the value is set to 0) of a number of retry attempts for activation/termination upon certain kinds of failures.

The expiry counter has been set to 3 in order to minimise the AXE going beyond a small restart.

This applies to Local 5 switches only.

res9actterm1_number_of_attempts 3

Specifies an expiry counter (infinity, if the value is set to 0) of a number of retry attempts for activation/termination upon certain kinds of failures.

The expiry counter has been set to 3 in order to minimise the AXE going beyond a small restart.

This applies to Local 7 switches only.

aomp.setup

This is an XMATE platform configuration file and is located in $AOMPHOME/ setup directory. The following XMATE platform parameters are of relevance when configuring the IMS system:

log_ne_dcs_alarms

This variable in the aomp.setup file affects operation of the IHS and DCS servers. Default value is *yes* meaning, the IHS will subscribe to all DCS's for reception of NE alarms.

In a configuration system where two XMATE platforms are used e.g., one for the regular Operation and Maintenance work, and the other being the IMS (base platform), and if the Data Communication Servers (DCS) are shared between the two systems, this variable can be used to disable IMS IHS from "stealing" alarms already collected by the O&M IHS (ie the XMATE O&M system).

Hence, if the IMS system shares a data communication server (gateway) with an existing XMATE element management system, set this variable to *no* in order to disable subscription of IMS IHS to DCS for alarm collection.

AOMP_TRANSMIT_SHORT EnvVar

Defining this variable (e.g.: `setenv AOMP_TRANSMIT_SHORT` in the $AOMPHOME/setup/environment file) will cause CTB to transmit only ONE data product to LEMF per X.25 session. That is, each data product will open and use a separate session ("call request", "data product", "clear request") even if destined for the same LEMF.

This will typically be used for debugging purposes.

X.25 setup

Log in as root and set up X.25 links to all MSCs and LEMF as described in the *XMATE Installation and Administration Manual B*[*3*].

For LEMF using the PLP protocol, the frame size (K) and window size (W) of the X.25 network should both be set to 1.

Note: X.25 configuration using the x25tool from /opt/SUNWconn/bin configures local physical ports, addresses, and links only. X.25 network parameters of course must be compatible with the PSDN (X.25) network and remote hosts.

Log Files

When IMS servers/applications are activated for the first time, log files are created to record all trace messages being generated by system usage.

These log files are:

- IMSMASErrorLog - generated by the imas server
- IMSMiscErrorLog - generated by the billing system
- IMSCDSErrorLog - generated by the CTB server
- IMSREADMErrorLog - generated by READM process

These log files and their parameters are detailed in the environment file $AOMPHOME/setup/redrs/environment.

Note: There should be no more than two instances of these log files on the system at any one time. The filename suffix ranges from 00 to 99. When 99 is reached, the number then restarts at 00.
After the initial startup, new log files are created once the user definable log file size limit is reached. This is set using the parameter MAX_LOG_LENGTH found in the environment file. The new log file will then replace the oldest existing instance found on the system.

Setup of IMS

Creating LEMF

Before any setting up is carried out on the other NE, LEMF entries must be added first. Prior to adding in new LEMF, remove all existing LEMF entries in NE Setup and entire entries in the dcs_passwds text file.

One of the mandatory constraints is that the Password ID of the newly created LEMF, using the NE Setup program, must match the Password ID in the dcs_passwds file as indicated in the two tables shown below. The password ID must also have the same name as the LEMF NE. It is also recommended that all NE names and addresses be numbered in numerical order, e.g. LEMF1, LEMF2. The LEMF itself, however, can be specified to use X.29 or PLP protocol depending on the LEMF requirements.

For each LEMF NE created, specify the network type to be a LEMF. The address field for FTAM type LEMF must contain an alias name previously defined in the FTAM remote hosts database. The address field for FTP type LEMF can either be an IP address or a name previously defined in the /etc/hosts file. The password will therefore reference the dcs_passwds text file which must contain actual account login details.

The following steps are required to create new LEMF and set up the necessary NE.

Note: The creation of new LEMF will be limited by the number of existing licenses.

- Open the dcs_passwds text file in $AOMPHOME/setup/dcs and add in the new LEMF entries. The new LEMF entries must be inserted before all other existing entries in the file.
- Run the NE Setup program (under the XMATE Administrator root menu) according to the instructions in the *XMATE Installation and Administration Manual B* [4].and create the new LEMF. After adding the new LEMF, click on the File menu and select “Generate DCS File” to record the changes.

Setup from user interface

Start up the IMS Transmission process window. For ‘Job Directory’ use the full path of `jobq` created in step 2 of section 4.3. For IHS Host use the IHS host of the platform. The IMS host is usually the file server.

Once all the parameters have been specified in the IMS Transmission process window press Apply, but do not Activate the process yet.

Define every NE (for example, mobile switching centres – MSC) on the network to IMS by following the procedures in ‘Adding, deleting, or modifying intercepting NE’ on page 4-4.

Define every NE group on the network to IMS by following the procedures in ‘Adding, editing, or deleting NE groups’ on page 4-9.

Define every LEMF on the network to IMS by following the procedures in ‘Adding, deleting, or updating law enforcement monitoring facilities’ on page 4-12.

The transmission process can now be activated by following the procedures in Chapter 5, ‘Administering the IMS Transmission Process’.

Automatic start facility

CTB (Collection and Transmission Server) and imas (Monitoring and Activation Server) will be started automatically upon executive host restart (for High Availability support) by the `/etc/rc2.d/[SK]98xmateims` startup scripts.

Example AXE Configuration for RCEFILE DFO

Direct file output setup

Using WIOZ, connect to each AXE in the network and perform the following steps.

Step 1: Define a device

Type in the following MML commands.

1 **>IMLCT:SPG=0;**

2 **:ILNAP;**

This lists out all ports and their names. The name for the port being used is needed.

3 **:ILDFP;**

This lists out all I/O devices currently defined.

4 **:ILDFI: IO=io,PROT=MTP,NAME=name;**

where **name** is the name found in 2 above, and **io** is a new device name, e.g., DL-1.

5 **:END;**

Step 2: Define a device file

Type in the following MML commands.

1 **>INMCT:SPG=0;**

2 **:INFII:FILE=RCEFILE, RLENGTH=256, BLK=64, SIZE=1, EXP=10, TYPE=SEQ, FCLASS=DEV, IO=io, NODE=A;**

where **io** is the I/O device defined in ‘Step 1: Define a device’ above.

3 **:END;**

STRICTLY CONFIDENTIAL

References

1 AOMP – Network Management System,
1551-AOMP 102 01 Uen

2 XMATE Installation Instruction in *XMATE Installation and Administration Manual B*, 3/1531-AOMP 102 01

3 X.25 Link Administration in *XMATE Installation and Administration Manual B*, 1/198 17-CNAP 102 01

4 Information Model Administration in *XMATE Installation and Administration Manual B*, 2/198 17-CNAP 102 07

STRICTLY CONFIDENTIAL

3 IMS Function Verification

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	1/15321-CNAP 102 11		
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-04-30	**Revision** H	**Pages** 28

ERICSSON

Procedures for verifying that all IMS functions perform correctly after installation

In this chapter

This chapter describes the function verification process otherwise known as the Acceptance Test for the Interception Management System.

Application

This chapter is to be used in the process of function verifying IMS. The function verification is to be carried out by qualified and experienced personnel with the support of Ericsson staff.

Scope

This chapter doesn't include the following IMS system function:

- XMATE platform functions which are covered by the XMATE Function Verification document (included in the XMATE B documentation module).

Getting started

The test cases are written in the same order as the recommended work flow for the function test execution. This is to optimise the verification process.

Verifying administrative functions

You need to create an administrator account so you can test all the functions available to administrators.

Create an IMS Administrator

1 Create an IMS administrator within the Administration group using **admintool**.

2 Copy the desktop environment *$AOMPHOME/install/sample_env/aompadm/* to the newly created administrator's home directory.

3 Go to the .dt directory and move dtwmrc.imsadm to dtwmrc.

4 Log out then log in as an IMS administrator at the initial XMATE startup screen. Click on the workspace menu and check the privileges provided to an administrator.

There should be XMATE administrator and IMS administrator selection facilities in the menu.

5 Select ***IMS Administrator>Database Admin*** from the workspace menu.

The IMS Administration GUI should start up. It should now be possible to create or delete any warrant using the GUI.

6 From the main menu select ***File***.

Setup *should be highlighted.*

7 Select ***IMS Operator>IMS Application System***.

The IMS-Remote Equipment Data Routing System GUI should appear on the screen. The features appearing on the screen vary according to market requirements.

Perform the administrative verification tests

1 Log on to the XMATE system at the initial Welcome screen.

2 Type your administrator's user id and press Return.

The password screen appears.

3 Type your administrator's password and press Return.

After a short wait the desktop appears with the Front Panel at the foot of the display.

4 Right-click the desktop and from the workspace menu select ***IMS Administrator***.

The IMS Administrator menu appears. This is the main menu from which you access all administrator functions.

5 Perform all test cases.

Verifying operational functions

You need to create an operator's account so you can verify functions available only to operators.

Create an IMS Operator

1 Create an IMS operator within the Operator group, aompusr, using **admintool.**

2 Create the directory, */usr/<operator>*.

3 Copy the desktop environment *$AOMPHOME/install/sample_env/aompusr* to the newly created operator's home directory.

4 Copy the *$AOMPHOME/axhome/macros* directory to the */home/<operator>/axhome/macros* directory.

5 Go to the .dt directory and move dtwmrc.imsop to dtwmrc.

6 Log out then log in as an IMS operator at the initial XMATE startup screen. Click on the workspace menu and check the privileges provided to an operator.

There should be no XMATE administrator or IMS administrator selection facilities in the menu.

7 Select ***IMS Operator>Database Search...*** from the workspace menu.

The IMS Administration GUI should start up. It should not be possible to create or delete any warrants using the GUI.

8 From the main menu select ***File***.

Setup *should not be highlighted.*

9 Select ***IMS Operator>IMS Application System***.

The IMS-Remote Equipment Data Routing System GUI should appear on the screen. The features appearing on the screen varies according to market requirements.

Perform the operations verification tests

1 Log on to the XMATE system at the initial Welcome screen.

2 Type your operator's user ID and press Return.

The password screen appears.

3 Type your operator’s password and press Return.

After a short wait the desktop appears with the Front Panel at the foot of the display.

4 Right-click the desktop and from the workspace menu select ***IMS Operator***.

The IMS Operator menu appears showing the following icons:

For Domestic:

- *Init (Domestic)*
- *Stop (Domestic)*
- *Audit*
- *Monitor Status*

For G10:

- *Select New Host*
- *Connect to Server*
- *Create New Warrant*
- *Modify Warrant*
- *Audit Network*
- *Monitor Status*
- *Help*

5 Perform the following specific test cases:

- Test case 5: Activate and monitor the status of a warrant, page 3-10
- Test case 6: Re-transmission during link failure, page 3-11
- Test case 7: Multiple operator support (G10), page 3-12
- Test case 9: Audit Warrants, page 3-14
- Test case 10: LEMF connected, page 3-16
- Test case 12: DP Delivery with a warrant on the same MNN/IMEI/IMSI but with a different MUID, page 3-18
- Test case 13: DP Delivery with Notify Record Sent, page 3-18
- Test case 14: LEMF not connected, page 3-18
- Test case 18: Terminate a warrant (Domestic), page 3-21
- Test case 20: Delete a warrant (G10), page 3-21
- Test case 30: Display on-line help, page 3-26

Definition of NE/LEMF

Test case 1 Define NE/LEMF

1 Use the Network Element (NE) Setup GUI to define a number of NE/LEMF which will be used for testing and check the NE List.

Note: The naming convention in IMS for LEMF should all be in uppercase.

The NE/LEMF are now defined.

2 Define the time scheduled polling mechanism for the network link supervision.

3 Add NE/LEMF into the IMS database by using the IMS Administration GUI.

NE/LEMF defined.

Test case 2 Delete NE/LEMF

1 From the IMS Administration GUI, delete NE/LEMF as follows:

- Use the NE List GUI to delete NE.
- Use the Law Enforcement Monitoring Facility GUI to delete LEMF.

2 Check the NE list.

The selected NE should have been deleted from the IMS database.

3 Check the Law Enforcement Monitoring Facility list.

The selected LEMF should have been deleted from the IMS database.

Test case 3 Defining an NE Group

1 Select the ***Edit NE Group*** menu option from the ***Database Admin*** GUI.

2 Create 3 new NE Groups from the ***Edit NE Group*** panel.

The new groups will be displayed in the ***Edit NE Group*** *panel.*

3 Check that the group file is now stored in the `/home/aomp/setup/redrs/axegroups` directory.

IMS Servers activation

Test case 4 Start IMS servers

1 Ensure that the XMATE servers (FTS, IHS, DCS) are running.

2 Start ***Server Admin*** from the ***IMS Administration Workspace*** menu.

3 Click on *Activate* for the IMS Activation Process and check the status by clicking on *Status*.

The status field should show that the imas server is in an 'Active' state.

4 Click on *Activate* for the IMS Transmission Process and check the status by clicking on *Status.*

The status field should show that the CTB server is in an 'Active, Transmit and Receive' state.

Warrant activation

Test case 5 Activate and monitor the status of a warrant

1 Click on the ***Init*** (domestic) or ***Create Warrant*** (G10) icon in the ***IMS Operator>IMS Application System*** window.

The appropriate window is displayed.

2 Fill in the information. Select Data Monitoring Only for the warrant. Press *Apply.*

Double-click on the newly created warrant in the Database administration window and verify that all warrant information previously entered is accurately displayed.

3 Check the XMATE command log.

*The command **WRCRI,RCSUI,RCMUI** should be listed. Click on each command entry to verify whether the parameters transferred with them are correctly sent in the order as determined by each POD.*

Note: The RCMUI command is forwarded only in case a warrant is raised on an MUID supporting NE.

4 Click on the ***Monitor Status*** icon in the IMS Application System Window. Enter the MNN, IMEI or IMSI number on the Monitor Status Dialog then click Apply.

The Activation State of the Warrant should be Activated, the Monitor Status should be Monitored and the NE name should be the same as the NE in which the warrant was raised.

5 Send the RCSUP command via WiOZ to verify activation.

The output window on WiOZ should provide the printout indicating the warrant is active on the NE.

6 Create a warrant with ‘Data Monitoring Only’ not selected. Fill in the numbers depending on whether the network is fixed or mobile as follows:

Fixed: The MCMCNB number and up to five SCMCNB numbers.

Mobile: Up to ten SCMCNB numbers (if more than one SCMCNB number, then the RCMCC command must be activated).

Once entered, click Apply.

7 Check XMATE Transaction Log and **Retrieve all** commands which are logged.

The following commands are sent: WRCRI, RCSUI, RCMUI, RCMCI (mobile), RCSTC (fixed) and RCMCC (mobile). Click on each command entry to verify whether the parameters to be transferred with them are correctly sent in the order determined by each POD.

8 Make a call from the target subscriber whose warrant has been registered and verify whether the call content is getting transferred to the MCMCNB (fixed) and SCMCNB numbers.

The call should have been transferred to the Monitoring call numbers (MCMCNB [fixed] and SCMCNB).

9 Repeat steps 1 to 7, replacing the MNN with an IMEI and with the SF flag set.

10 Repeat steps 1 to 7 using IMSI with the SF flag set and DT entered.

Test case 6 Re-transmission during link failure

1 Disconnect the link to the NE by pulling the cable. Open the Graphical Alarm User Presentation window.

The internal alarm icon of XMATE should flash up after the scheduled polling interval. The transaction log should have raised an alarm.

2 Create a warrant using the IMS Operator system. Open the Monitor Status window and monitor the warrant.

Check the status using Monitor Status:

Activate State = Activation Failed
Monitor Status = Not Monitored

Note: The mediation and activation server will try reconnecting to the NE after a specified interval of time. The attribute which defines this time is <resid>actterm1_waiting_period and is in the `$AOMPHOME/setup/redrs/text/IMSAttribute` file. Also another attribute in the same file, <resid>actterm1_number_of_attempts, defines the maximum number of times the imas tries to connect to the NE.

The default number of attempts is 3 and the default waiting period is 15 minutes.

3 Reconnect the link after the first alarm appears.

IMS should attempt to re-activate existing warrants.
Target numbers should have been Activated and Monitored in the NE.

Use WiOZ to verify the success of warrant initiation.

Note: The target number can be either a MNN, IMEI or an IMSI number.

Supporting multiple operators (G10)

Test case 7 Multiple operator support (G10)

1 Add entries to the IMS network operator ID and sub-network operator ID files, files *“IMSNETOPID”* and *“IMSSUBOPID”* respectively. The files are located in `/home/aomp/setup/redrs/text`.

2 From the Database Administration GUI, verify in the ***File>Add* Target No** window that the identifiers are defined.

The correct operator information will be displayed in pop-up windows.

Test case 8 Modify a warrant (G10)

1 Click the Modify Warrant icon in the IMS Operator>IMS Application system window and enter the target number to modify (Not Activated state).

All existing warrant information associated with the target number should be displayed.

2 Change the selected warrant activation/deactivation time.

3 View the warrant status in the Database Admin GUI.

XMATE internal icon should be flashing and an acoustic alarm should sound.

4 Read the Transaction Log.

The WRCRC command should have been registered.

Auditing the network

Test case 9 Audit Warrants

Scenario 1: Warrant active in IMS but not in NE.

1 Use Audit in the IMS Application System to check the warrant list in an NE.

The Audit report should be empty.

2 Delete one warrant in an NE using the RCSUE command in WiOZ. Use the RCSUP command to verify.

The warrant is deleted in NE.

3 Use Audit to check the warrant list in the NE with the Synchronise option selected to ’Yes’.

The Audit Report lists the warrant that exists only in IMS and not in the NE. The RCSUI command should have been initiated to the AXE for the warrant in IMS database only.

4 Use Audit to check the warrant list in the NE again but with the Synchronise option selected to ’No’.

The Audit report should be empty.

5 Print a list of warrants in the NE using the RCSUP command in WiOZ.

The NE list matches the list in the IMS database.

6 Read the Transaction Log.

Check that all commands sent to the NE are logged.

Scenario 2: Warrant active in NE but not in IMS.

1 Use Audit in IMS Application System to check the warrant list in an NE.

The Audit report should be empty.

2 Delete one warrant in IMS using the Database Admin Operator GUI.

The warrant is deleted in IMS.

3 Use Audit to check the warrant list in the NE with the Synchronise option selected to ’Yes’.

The Audit report lists the warrant that exists only in the NE and not in IMS.
IMS sends the RCSUE command to terminate the warrants.

4 Use Audit to check the warrant list in the NE again but with the Synchronise option selected to ’No’.

The Audit report should be empty.

5 Print a list of warrants in the NE using the RCSUP command in WiOZ.

The warrant would have been deleted from the NE, thereby matching the IMS database.

6 Read the Transaction Log.

Check that the RCSUE command sent to the NE is logged.

Transmission Handling: Data Product Conversion and Delivery to LEMF

Test case 10 LEMF connected

1. Ensure that CTB is running and Transmission control is set to Transmit and Receive mode.
2. Create a warrant. Make calls from, or call the targeted number.
3. Check the data product counters in the IMS Admin GUI.

   The WDPC and MDPC counters should have been incremented by one.
4. Check the data product to verify its format and contents.

   The IMS should have processed the received RCEFILE and transmitted the resultant converted Data product to FTAM target accounts (LEMF). The format of the received file name should be:

   (domestic) AAAACCCCYYYYMMDDHHMMSS.NNN where:

AAAA	The short name of the switching centre (First four characters) where data product was originated.
CCCC	WDPC value from IMS database. Error_Terminal packets use number stored in ".fileno" file.
YYYY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
NNN	The hexadecimal representation of XWID.

   (G10) **`ddeejjmmtthhllssrr`** where :

`dd`	Network OpID
`ee`	SubNetwork OpID
`jj`	Year
`mm`	Month
`tt`	Day

`dd`	Network OpID
`hh`	Hour
`ll`	Minute
`ss`	Seconds
`rr`	Sequence #

Note: For every call made from or received by the target number, there should be two DPs (one is called Call Data and the other is called Call Completion) on the FTAM target account directory.

Test case 11 Case of no LEMF connected (POD)

1 Ensure that CTB is running and Transmission control is set to Transmit and Receive mode.

2 Create a warrant. Make calls from, or call the targeted number.

3 Check the data product counters in the IMS Admin GUI.

The WDPC and MDPC counters should have been incremented by one.

4 Check the data product to verify its format and contents.

The IMS should have processed the received RCEFILE and stored the resulting converted data product relative to the LEMF name. The format of the received data product file should be *`target_no_yyyymmddhhmmss_csn where :`*

target_no	Target number used to generate the warrant
`yyyy`	Year
`mm`	Month
`dd`	Day
`hh`	Hour
`mm`	Minute
`ss`	Seconds
`csn`	Call sequence #

Test case 12 DP Delivery with a warrant on the same MNN/IMEI/IMSI but with a different MUID

1. Create warrants for the same MNN with different LEMF selected (Maximum 8). Call from the MNN telephone.

   The DP file will be created and routed to the specified LEMF home directory.
2. Repeat, replacing the MNN with an IMEI and with the SF flag set.
3. Repeat step1 using an IMSI target number.

Test case 13 DP Delivery with Notify Record Sent

1. Create new warrants for the target number connected to the Model exchange or use the warrants created in previous tests. Make a call from the target number. Create Restart on exchange before the call is ended.

   There will be only Call Data (Record Type 1) sent to the LEMF target directory.
2. Open XMATE Transaction Log and Retrieve the Alarms.

   A Fault Code 6 should have been logged in the alarm list.

Test case 14 LEMF not connected

1. Change the password in dcs_passwds to simulate a non-connected LEMF. Create a warrant and make calls to the target number. Use rerouting GUI to verify number of data products on queue, number of consecutive call attempts and alarm status.

   The re-routing window status should show the alarm has been raised.
2. Correct the password in the dcs_passwds file.
3. Use File Manager to verify that data products are routed to a specific LEMF.
4. Use the re-routing dialog to read the number of data products in the queue, the number of call attempts and the alarm status.
5. Use Graphical Alarm Presentation to view the ALARM CEASING.
6. Acknowledge the alarm.

   The ALARM CEASING should have been raised.

Recreating transmission request list after restart

Test case 15 Recreate transmission request list

1. Activate CTB in IMS Parameter Setup.
2. Check the CTB server status.

   CTB server is activated. Make certain it is in RECEIVE ONLY mode.
3. Make calls to generate data products.
4. Use the Re-routing window to verify the number of data products waiting for transmission increases.
5. Use File Manager to check if data products are arriving.
6. Use File Manager to check that no data products are being routed to the LEMF.
7. Set CTB into TRANSMIT AND RECEIVE mode.
8. Update the status of the Re-routing window to verify that the number of data products waiting for transmission decreases as the data products are routed to the corresponding LEMF.
9. Use File Manager to check that data products are being routed to the LEMF.

Warrant database administration and re-routing

Test case 16 Handling non-existent warrants

1. Use the IMS Administration GUI to delete a warrant.
2. Make a call from the target number previously removed from the IMS database.

   An alarm is recorded in the IMS system ("MNN/IMEI/IMSI not in Routing Terminal") and the data product is routed to the ERROR_TERMINAL.
3. Acknowledge the alarm.

   The alarm is acknowledged.
4. Use re-routing to read the number of the data product in the queue for the ERROR_TERMINAL.
5. Use File Manager to view the data product in the ERROR_TERMINAL queue.

   Data Records in the ERROR_TERMINAL queue.

Test case 17 Activate a warrant in the database

1. Delete a warrant in the IMS Administration GUI.
2. Use the IMS Administration Operator GUI to activate a warrant with the same information as the one just deleted.
3. Check the Transaction Log.

   Check if the initiation of the warrant has been recorded.

   Check in the Monitor Status window that the warrant is Activated.
4. Make a call from the target number re-initiated in the IMS database.
5. Use the re-routing tool to read the Data Product queue.

   The data product is routed to the defined LEMF in the warrant.

Termination Handling

Test case 18 Terminate a warrant (Domestic)

1 From the **IMS Operator>IMS Application System** dialog box, click on the **Stop** icon.

2 View the warrant status using Monitor Status.

Target number is terminated and no longer monitored.

3 Send the RCSUP command via WiOZ.

Target number should not be the NE database.

4 Read the Transaction Log.

The RCSUE and RCSUP commands should be logged.

5 View the warrant status using IMS Administration GUI.

*The warrant's state should be **TERM**.*

Note: For G10, warrants terminate automatically based on the Stop Time

Test case 19 Delete a warrant (Domestic)

1 Start the IMS Administration.

2 Highlight a warrant with the status **TERM**.

3 With the cursor anywhere inside the IMS Administration dialog box, click the right mouse button.

4 From the displayed menu, select **Delete Warrant**.

The warrant should have been removed from the IMS database.

Test case 20 Delete a warrant (G10)

1 From the **IMS Operator>IMS Application System** dialog box, click on the **Modify Warrant** icon and enter the number to be deleted (must show the state as **Not Activated**).

All existing warrant information associated with the target number should be displayed.

2 Click on the Delete button.

3 View the warrant status using **Monitor Status**.

The target number has been deleted from the database.

Test case 21 Check Billing

Note: Set the transmission process to Transmit and Receive Mode when performing this test.

1 Create a warrant for each LEMF with the same target number.

2 Send RCEFILE for each warrant.

Billing records will be generated in the Billing file.

3 Start the interception billing process from the UNIX command line by typing `irun ibs $AOMPHOME/data/redrs/jobq/BILLING`.

4 Use File Manager to check the billing file generation.

The billing file is generated in the pre-defined directory and the file name contains the billing process activation date and time. Results will be stored in the directory as set in the IMS attribute file for `ibs_result_dest`*. The name of the billing record file produced is TT-YYYYMMDDHHmm, e.g. TT-199802141230.*

5 View (open) the billing file job queue directory and check the billing record structure.

The billing file contains the billing records for the calls generated during the function verification test. The structure is according to the specification. Also the billing records for different MUID should be separate.

High Availability - Data Communication Network Supervision

Note: Test only if redundant links to NFS are available. In such a scenario, if the primary link on the executive server is faulty, then a secondary link on the standby is used automatically. This implies that a second DCS is running on the standby.

Availability is subject to customer requirements.

Test case 22 Check automatic restart

1 Restart the executive server.

The following servers start automatically:

- Data Communication Server (DCS)
- Information Handling Server (IHS)
- File Transfer Server (FTS)
- Mediation & Activation Server (imas)
- Collection & Transmission Server (CTB)

2 Restart the standby server (if redundant links are available).

DCS starts automatically.

Test case 23 Force fallback to standby server

1 Shut down the executive server and perform the fallback procedure as described in the XMATE Installation and Administration Manual.

The standby server takes over the executive server role. The interception management function is fully restored.

Test case 24 Standby host link failure and re-link

1 Disconnect the link on the stand-by machine.

2 Wait for the link supervision alarm according to the time scheduled polling interval supervision setup.

Graphical and acoustic alarm notification on the Graphical alarm presentation window.

3 Acknowledge the alarm

Alarm acknowledged.

4 Re-connect the link.

5 Wait for the link supervision alarm ceasing according to the time scheduled polling interval supervision setup.

Graphical and acoustic alarm notification on the Graphical alarm presentation window.

6 Acknowledge the alarm

Alarm acknowledged.

Test case 25 Executive host link failure and re-link

1 Disconnect the link on the executive machine.

2 Wait for the link supervision alarm according to the time scheduled polling interval supervision setup.

Graphical and acoustic alarm notification on the Graphical alarm presentation window.

3 Acknowledge the alarm.

The alarm should be acknowledged.

4 Initiate/activate a new warrant.

The warrant is activated via the data link on the standby server.

5 Make a call from the monitored subscriber line.

The Transmission alarm, Data Record cannot be transmitted to LEMF. Graphical and acoustic alarm should be present on the Graphical alarm presentation window.

6 Acknowledge the alarm.

Alarm acknowledged.

7 Re-connect the link.

Data Record(s) are now sent to the LEMF.

The Transmission alarm should have ceased. Graphical and acoustic alarm notification on Graphical alarm presentation window.

8 Wait for the link supervision alarm to cease according to the time scheduled polling interval supervision setup.

Graphical and acoustic alarm notification on the Graphical alarm presentation window.

9 Acknowledge the alarm.

Alarm acknowledged.

Test case 26 Resetting the legal base statistical counters (G10)

1 Type the command `irun_debug legalbstat reset legal_base` from the UNIX command tool.

The counter’s value is 0.

Searching the Database

Test case 27 Search the database

1 Select the ***Define Criteria*** menu option from the Search menu and define the search criteria in the database.

*The correct summary warrant list is displayed in the **Search Result Window** according to the defined search criteria.*

LEMF licensing support

Test case 28 Check LEMF licensing limit

1 Check the current license feature for the number of LEMF allowed.

2 Verify LEMF licensing support by adding one more LEMF than the LEMF license limit allows.

A pop-up error window will indicate that the limit has been reached.

Test case 29 Dynamic LEMF creation (G10)

1 Add and delete entries from the LEMF table via READM and the application interface in the warrant create panels.

2 Verify that LEMF information can be added and deleted.

The LEMF list window and the LEMF selection window will show the correct information.

3 Verify that the “in Use” flag works by attempting to delete a LEMF that is “In Use”.

A pop-up error window will indicate that the limit has been reached.

Help function

Test case 30 Display on-line help

1 Select Help from the Help Menu Option in the IMS Administration GUI, IMS Parameter Setup GUI, re-routing GUI and the IMS Application System GUI.

Help information displayed is valid and correct. Also the user can customize the display format and print the document.

References

1 Administering the IMS Database
3/198 17 CNAP 102 11,

2 Functional Description of IMS.
1/15517 CNAP 102 11

3 IMS Installation Instruction.
1531 CNAP 102 11

4 Administering the IMS Database

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	3/198 17-CNAP 102 11 Uen
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-03-14
		Revision	V
		Pages	54

In this chapter

Before you can monitor a target subscriber’s calls, the IMS database must be set up. You must set up the NE that are to perform the interception and also designate the law enforcement monitoring facility (LEMF), specified by the monitoring agency, to which the call data are to be sent.

This chapter describes the procedures for administering the database.

Prerequisites

It is assumed that the user is familiar with a UNIX based workstation and with the manipulation of windows and associated menus.

Getting started

The database administration tasks that the system administrator can perform are accessed from the IMS Administration main window.

To launch the IMS Administration window

1 Log on to the XMATE system at the initial Welcome screen.

a Type your system administrator's user id and press Return.

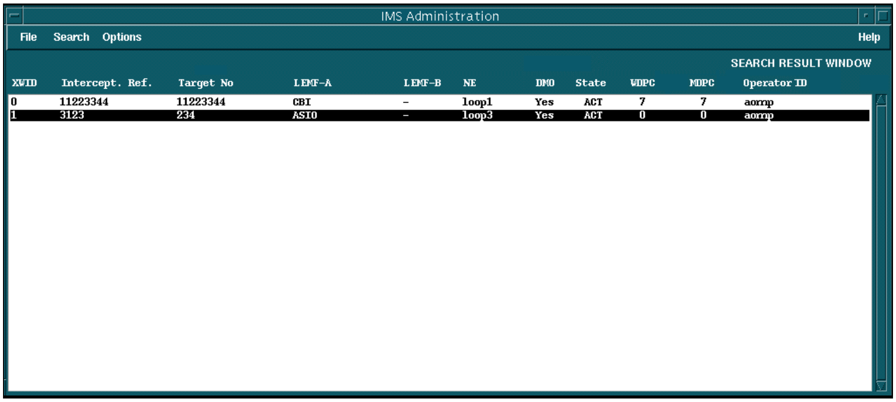
The password screen appears.

b Type your administrator password and press Return.

After a short wait the desktop appears with the Front Panel at the foot of the display.

2 Right-click the desktop and choose the Workspace Menu > IMS Administrator > Database Admin menu option.

The IMS Administration window displays and you can then access all database administration functions.



XWID	Intercept. Ref.	Target No	LEMF-A	LEMF-B	NE	DMO	State	WDPC	MDPC	Operator ID
0	11223344	11223344	CBI	-	loop1	Yes	ACT	7	7	aomp
1	3123	234	ASIO	-	loop3	Yes	ACT	0	0	aomp

Figure 4.1 IMS Administration Window

To quit the IMS Administration window

- Choose the File > Exit menu option in the IMS Administration window.

STRICTLY CONFIDENTIAL

Managing intercepting elements and monitoring centres

Before IMS can be used, the NE and LEMF to be connected to IMS must be set up. This section describes the major task areas of:

- Adding, deleting, or modifying intercepting NE
- Adding, editing, or deleting NE groups, page 4-9
- Adding, deleting, or updating law enforcement monitoring facilities, page 4-12

Adding, deleting, or modifying intercepting NE

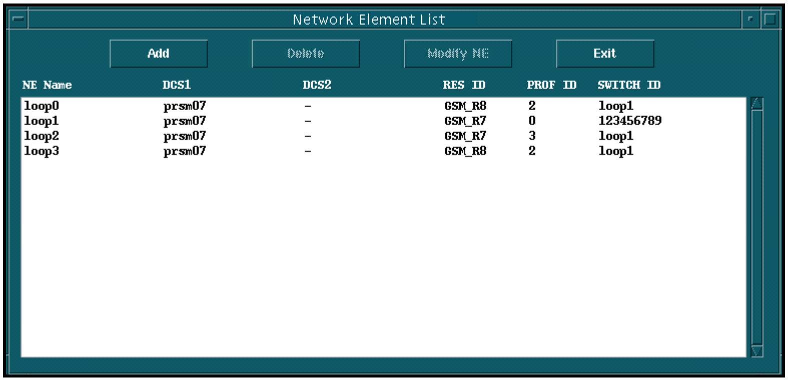
This section shows how

- To add a NE to the database
- To delete a NE from the database, page 4-7
- To modify a NE in the database, page 4-8

To add a NE to the database

1 Choose the File > Setup > Network Element List menu option in the IMS Administration window.

The Network Element List dialog box displays any NE that are currently defined.



NE Name	DCS1	DCS2	RES ID	PROF ID	SWITCH ID
loop0	prsm07	-	GSM_R8	2	loop1
loop1	prsm07	-	GSM_R7	0	123456789
loop2	prsm07	-	GSM_R7	3	loop1
loop3	prsm07	-	GSM_R8	2	loop1

Figure 4.2 Network Element List Dialog box

2 Click on the Add button in the Network Element List dialog box.

The Add NE Record dialog box displays.

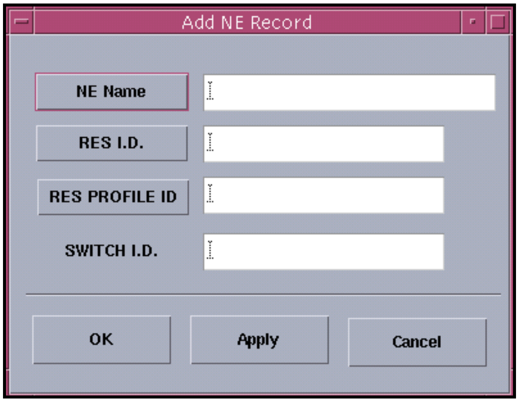


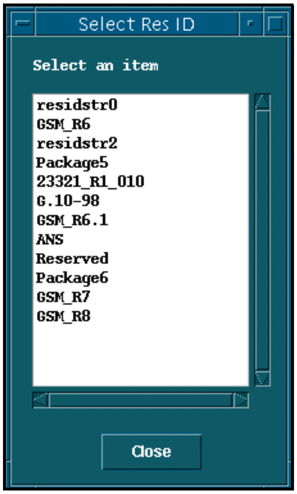
Figure 4.3 Add NE Record Dialog Box

a Click on the NE Name button and select a NE from the Network Element Selection dialog box that appears (Figure 4.6).

b Select the NE to which a target subscriber is connected and click on OK.

Note: This list of NE was previously defined using NE Setup.

c Click on the RES ID button and select a RES identifier from the Select Res Profile dialog box that displays then click on the Close button.



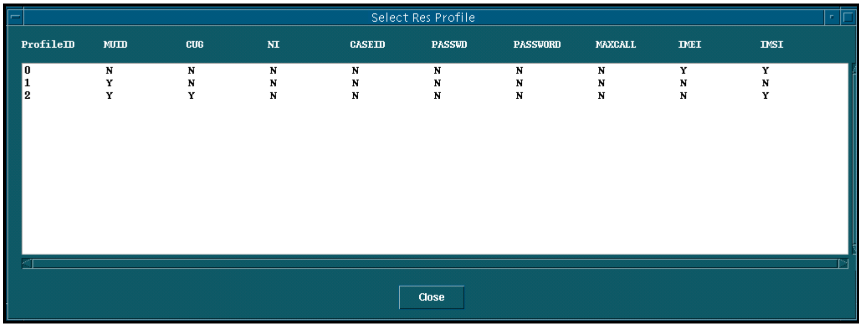
```
residstr0
GSM_R6
residstr2
Package5
23321_R1_010
G.10-98
GSM_R6.1
ANS
Reserved
Package6
GSM_R7
GSM_R8
```

Figure 4.4 Select ResID Dialog Box (I.D. list)

The RES facility in a NE is the function that actually carries out interceptions. The RED ID is used to indicate the version of the RES block in the NE.

d Click on the RES PROFILE ID to display the Select RES Profile dialog box.

The RES Profile defines the availability of specific characteristics of the RES functionality. For example, it indicates whether simultaneous monitoring is active or not.



Select Res Profile

ProfileID	MUID	CUG	NI	CASEID	PASSWD	PASSWORD	MAXCALL	IMEI	IMSI
0	N	N	N	N	N	N	N	Y	Y
1	Y	N	N	N	N	N	N	N	N
2	Y	Y	N	N	N	N	N	N	Y

Figure 4.5 Select Res Profile Dialog Box

e Select a RES Profile then click Close.

f Click in the SWITCH ID field of the Add NE Record dialog box and enter the required value.

It must be the same as the Switch Identifier in the CLI of the Cell Content Call. Each network (and possibly each NE within the network) will generate its own call sequence number since, in general, there is no way to coordinate them. Thus it is necessary to receive the Network Identifier and the NE in addition to the Call Sequence Number in order to unambiguously associate call content with call associated data.

g Click on the Apply and Okay buttons to close the Add NE Record dialog box.

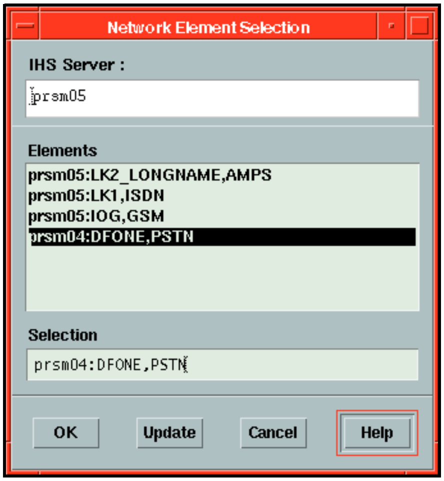
IMS adds the NE and RES identifier to the list of NE that can be requested to monitor target subscriber’s calls.

Note: Updating RES identifiers and profiles:
The list of RES identifiers is stored in the *`$AOMPHOME/setup/redrs/text/IMSRESID`* file. Edit this file to add, modify, or delete RES identifiers (RESID). Repeat

from Step 2 to associate RES identifiers to other NE. Please consult Ericsson before editing this file.

The list of RES Profiles is stored in the `$AOMPHOME/setup/redrs/text/resid.n/IMSProfile`. The ‘n’ value can be found in the IMSRESID file. Edit this file to add RES Profiles. Repeat from step 2 to associate RES Profiles to other NE. Please consult Ericsson before editing these files.

3 Click on the Exit button to close the Network Element List dialog box.



Network Element Selection

IHS Server : prsm05

Elements
prsm05:LK2_LONGNAME,AMPS
prsm05:LK1,ISDN
prsm05:IOG,GSM
prsm04:DFONE,PSTN

Selection: prsm04:DFONE,PSTN

Figure 4.6 Network Element Selection Dialog Box – MNN, IMEI or IMSI monitoring

To delete a NE from the database

1 Choose the File > Setup > Network Element List menu option in the IMS Administration window.

The Network Element List dialog box displays any NE that are currently defined.

2 Click on one NE and then click on the Delete button.

IMS removes the selected entry from the Network Element List dialog box and the database.

CAUTION: You cannot delete a NE that is still intercepting a target subscriber’s calls.

To modify a NE in the database

1. Deactivate both imas and CTB servers using Server Admin.
2. Choose the File > Setup > Network Element List menu option in the IMS Administration window.

   The Network Element List dialog box displays any NE that are currently defined.
3. Highlight the NE that needs to be Modified.

   Note: The modify button will now be enabled.
4. Click on the Modify NE button in the Network Element List dialog box.

   Note: If the activation server (imas) or transmission server are active, an error message will display.

   The Modify NE Record dialog box displays.

   a. Click on the new RES ID button and select a RES identifier from the Select RES Id dialog box that appears. The one chosen will replace the existing RES ID in the NE.
   b. Click on the RES PROFILE ID button and select a new RES Profile from the Select RES Profile dialog box that displays then click on the Close button.
   c. Click on the Apply and OK buttons to close the Modify NE Record dialog box.
   d. Reactivate both imas and CTB servers using Server Admin.
5. Click on the Exit button to close the Network Element List dialog box (Figure 4.2).

Adding, editing, or deleting NE groups

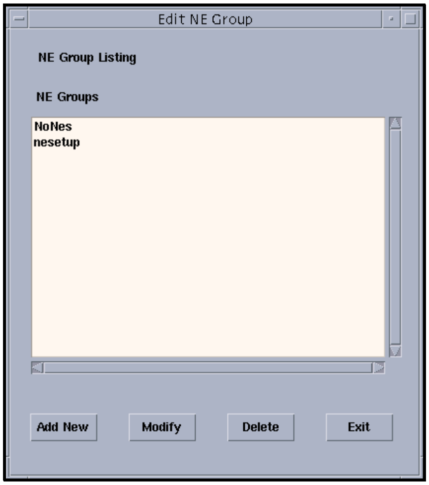
The NE Group facility can be used to broadcast warrant details to all NE at once. There are three operations associated with the NE Group that a user can perform:

- To add a new network-element group
- To edit the details of a network-element group, page 4-11
- To delete an NE group from the NE group list, page 4-12

To add a new network-element group

1 Choose the File > Edit NE Group option in the IMS Administration window.

The Edit NE Group dialog box is displayed.



Edit NE Group

NE Group Listing

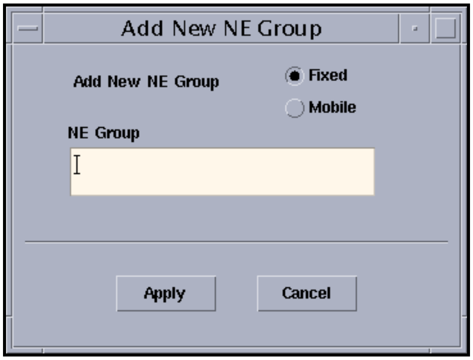
NE Groups

NoNes
nesetup

Figure 4.7 The Edit NE Group dialog box

2 Click on the Add New button.

The Add New NE Group dialog box is displayed.



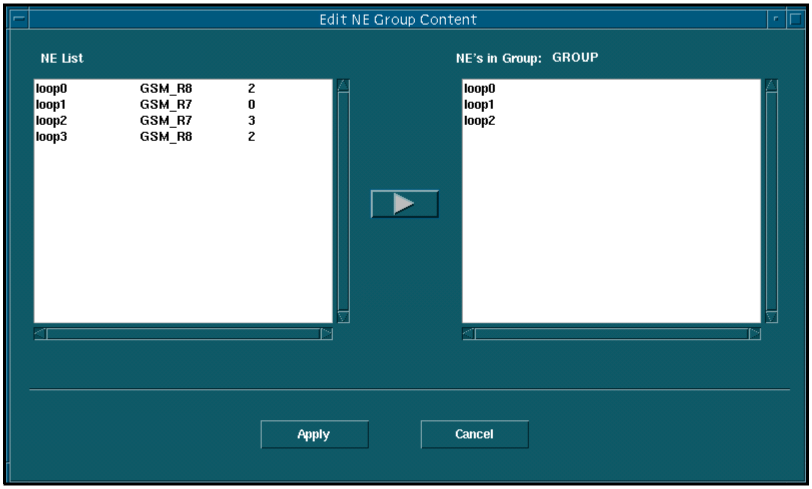
● Fixed
○ Mobile

Figure 4.8 The Add New NE Group dialog box

3 Enter the name of the new NE Group.

4 Choose the name of the new NE Group (fixed or mobile) and click on the Apply button.

The Edit NE Group Details dialog box is displayed. The left pane displays all NE available in IMS. The right pane lists all NE associated with the group.



NE List

```
loop0     GSM_R8     2
loop1     GSM_R7     0
loop2     GSM_R7     3
loop3     GSM_R8     2
```

NE's in Group: GROUP

```
loop0
loop1
loop2
```

Figure 4.9 The Edit NE Group Details dialog box

5 Add the required NE to the new network-element group.

a Click on a required NE in the NE List pane.

b Click on the right-pointing arrow between the two panes.

c Repeat to add more NE.

d Click on the Apply button.

The Edit NE Group dialog box is displayed.

6 Click on the Exit button to return to the main IMS Administration window.

To edit the details of a network-element group

1 Select the File > Edit NE Group option in the IMS Administration window.

The Edit NE Group dialog box is displayed (Figure 4.7).

2 Select the NE Group to be edited and click on the Modify button.

The Edit NE Group Details dialog box is displayed (Figure 4.9).

3 Add more NE to the network-element group.

a Click on a required NE in the NE List pane.

b Click on the right-pointing arrow between the two panes.

c Repeat to add more NE.

4 Remove unwanted NE from the network-element group.

a Click on an unwanted NE in the NE in Group pane.

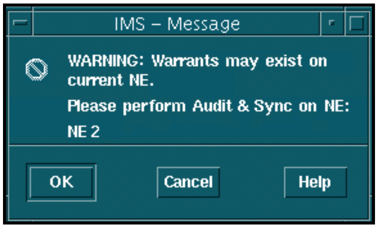
b Click on the left-pointing arrow between the two panes.

c Repeat to remove more NE.

5 Click on the Apply button.

The Edit NE Group dialog box is displayed (Figure 4.7).

Note: When you remove a NE from a network-element group, a warning message asks you to perform an warrant audit and sync on the NE.



IMS – Message

WARNING: Warrants may exist on current NE.

Please perform Audit & Sync on NE:

NE 2

Figure 4.10 IMS Message dialog box when removing a NE from a NE Group

6 Click on the Cancel/OK button to return to the main IMS Administration window.

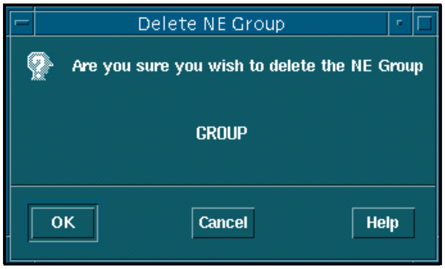
To delete an NE group from the NE group list

1 Choose the File > Edit NE Group option in the IMS Administration window.

The Edit NE Group dialog box is displayed (Figure 4.7).

2 Click the NE Group to be deleted and click on the Delete button.

The Delete NE Group dialog box is displayed.



Delete NE Group

Are you sure you wish to delete the NE Group

GROUP

Figure 4.11 The Delete NE Group dialog box

3 Click on the OK button to confirm the deletion.

The Edit NE Group dialog box is displayed (Figure 4.7).

4 Click on the Cancel button to return to the main IMS Administration window.

Adding, deleting, or updating law enforcement monitoring facilities

This section shows how

- To add a LEMF to the database (Dom)
- To add a LEMF to the database (G10), page 4-13
- To delete a LEMF from the database (Dom), page 4-17
- To delete a LEMF from the database (G10), page 4-17
- To update NE and LEMF in the database, page 4-19

To add a LEMF to the database (Dom)

1 Choose the File > Setup > LEMF List menu option in the IMS Administration window.

The Law Enforcement Monitoring Facilities dialog box displays any law enforcement monitoring facilities (LEMF) that are currently defined.

2 Click on the Add button in the Law Enforcement Monitoring Facilities dialog box.

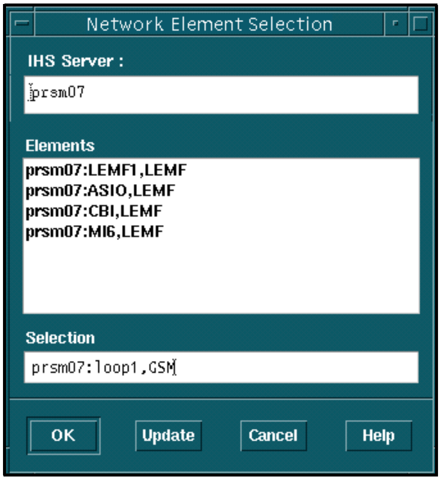
The Add LEMF Record dialog box appears.

a Click on the LEMF Name button and select a LEMF from the Network Element Selection dialog box that displays (Figure 4.12).

b Click on the Apply and OK buttons to close the Add LEMF Record dialog box.

IMS adds the LEMF to the table of LEMF to which data products containing information from call interceptions can be sent.

3 Click on the Exit button to close the Law Enforcement Monitoring Facilities dialog box.



IHS Server : prsm07

Elements
prsm07:LEMF1,LEMF
prsm07:ASIO,LEMF
prsm07:CBI,LEMF
prsm07:MI6,LEMF

Selection prsm07:loop1,GSM

Figure 4.12 Network Element Selection Dialog Box – LEMF selection

To add a LEMF to the database (G10)

1 Check IHSUP for the maximum permitted number of LEMF you can add to IMS.

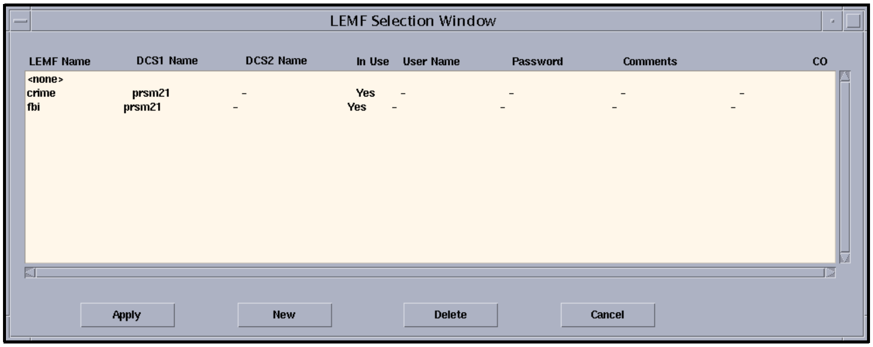
You cannot exceed the maximum permitted number.

2 Open the Add MNN/IMEI/IMSI or Modify MNN/IMEI/IMSI dialog box.

See ‘To add a target subscriber’s number to the database’ on page 4-25.

3 Click on either the LEMF-A or LEMF-B button in the Add MNN/IMEI or Modify MNN/IMEI/IMSI dialog box.

The LEMF Selection window displays any LEMF which have been defined previously.



LEMF Selection Window

LEMF Name	DCS1 Name	DCS2 Name	In Use	User Name	Password	Comments	CO
<none>							
crime	prsm21	-	Yes	-	-	-	-
fbi	prsm21	-	Yes	-	-	-	-

Figure 4.13 LEMF Selection Window dialog box

4 Click on the New button in the LEMF Selection window.

The Add LEMF Record dialog box is displayed.

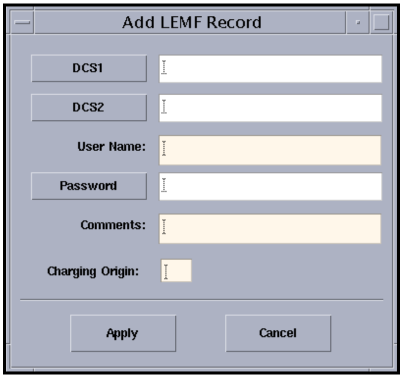


Figure 4.14 Add LEMF Record dialog box

5 Click on the DCS1 button.

The Select DCS dialog box is displayed (Figure 4.15).

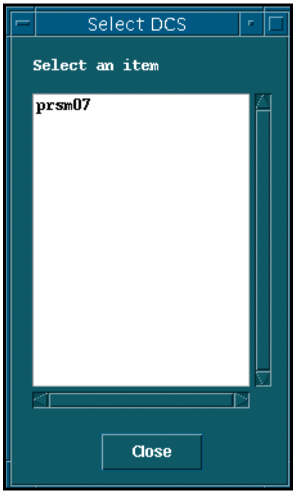


Figure 4.15 Select DCS

6 Click on the appropriate DCS (mandatory field).

7 Click on the Close button.

You are returned to the Add LEMF Record dialog box.

8 Repeat from Step 5 for DCS2 only if required (optional field).

9 Enter up to 20 characters for the User Name in the Add LEMF Record dialog box.

10 Enter the password (mandatory field).

a Click the Password button.

The Enter Data dialog box is displayed.

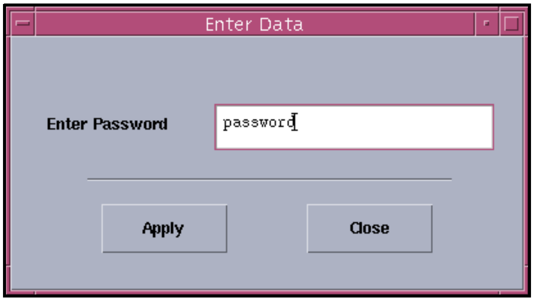
b Type a password of up to 20 characters and click on the Apply button.

The Enter Data dialog box is displayed for you to re-enter the password.

c Re-enter the password and click on the Apply button.

The Add LEMF Record dialog box is displayed.

Note: If you re-entered the password incorrectly, the Error - Password Confirmation dialog box will be displayed and you will be returned to the Add LEMF Record dialog box with the password field left empty. You will have to repeat the process of entering the password.



Enter Password password

Figure 4.16 Enter Data dialog box

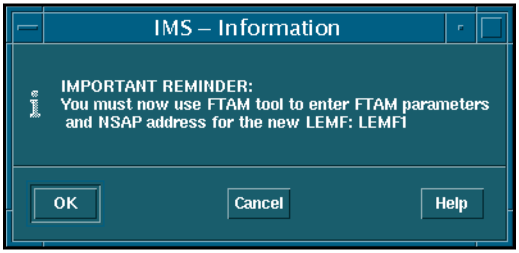
11 Enter up to 30 characters in the Comments field (optional field).

12 Enter the CO value (between 0 and 127).

13 Click on the Apply button in the Add LEMF Record dialog box.

The creation of a new LEMF will proceed and, if successful, an IMS Information window will be displayed informing the user that the LEMF has been created. The newly created LEMF will be displayed in the LEMF Selection dialog box.

Note: Another IMS Information dialog box is displayed reminding you that the actual warrant will not be initiated unless you update the record for the just created LEMF using the FTAMTOOL. This is only valid for FTAM protocol LEMF. For other LEMF types this message should be ignored.



IMPORTANT REMINDER:
You must now use FTAM tool to enter FTAM parameters
and NSAP address for the new LEMF: LEMF1

Figure 4.17 IMS Information dialog box

To delete a LEMF from the database (Dom)

1. Choose the File > Setup > LEMF List menu option in the IMS Administration window.

   The Law Enforcement Monitoring Facilities dialog box displays any law enforcement monitoring facilities (LEMF) that are currently defined.

2. Click on one LEMF and then click on the Delete button.

   IMS removes the selected entry from the Law Enforcement Monitoring Facilities dialog box and the database.

CAUTION: You cannot delete a LEMF that is still receiving data products from IMS, that is, one or more subscribers are still using it as either their primary (LEMF-A) or secondary (LEMF-B).

The circumstances preventing a LEMF from being deleted are when:

- another LEMF is re-routed to the LEMF to be deleted,
- there is an active warrant against the LEMF to be deleted, or
- the LEMF to be deleted has entries in its queue even if the warrant is in the TERMINATE state.

If this situation occurs, the system will flag the discrepancy and the text ERROR TERMINAL is displayed instead of the original LEMF name in the Search Result dialog box. This indicates to the user that the LEMF needs updating. To do this use the Modify Selected MNN/IMEI option from the popup menu. It is possible to temporarily route all data which has been sent to the ERROR TERMINAL to another destination.

To delete a LEMF from the database (G10)

You can only delete a LEMF if

- it is not being used by any warrant by any subscribers who have selected it as either their LEMF-A or LEMF-B (an error dialog box warns you and the name ERROR TERMINAL replaces the original LEMF name in the IMS Administration window – Search Result Window),
- it is not being used as an alternative route by LEMF re-routing program, and
- there are no data products due to be sent to this LEMF.

Note: When ERROR TERMINAL replaces the original LEMF name it indicates to the user that the LEMF needs updating using the Modify Selected MNN/IMEI option from the pop-up menu. It is also possible to temporarily route all data sent to the ERROR TERMINAL to another destination.

1 Open either the Add Target No or Modify Target No dialog box.

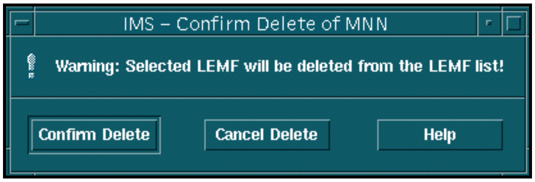
See ‘To add a target subscriber’s number to the database’ on page 4-25 or ‘To modify a target subscriber’s MNN entry in the database (G10)’ on page 4-33.

2 Click either the LEMF-A or LEMF-B button in the Add MNN/IMEI/IMSI or Modify MNN/IMEI/IMSI dialog box.

The LEMF Selection Window dialog box (Figure 4.13 on page 4-14) shows any LEMF which have been defined previously.

3 Click on the LEMF to be deleted and click on the Delete button.

The IMS – Confirm Delete of MNN/IMEI/IMSI dialog box (Figure 4.18) is displayed.



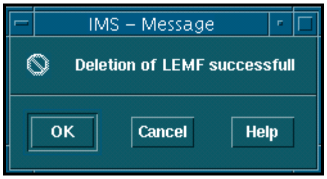
IMS – Confirm Delete of MNN

Warning: Selected LEMF will be deleted from the LEMF list!

Figure 4.18 IMS – Confirm Delete of MNN/IMEI/IMSI (LEMF) Dialog Box

4 Click on the Confirm Delete button.

The IMS – Message dialog box (Figure 4.19) confirms a successful deletion.



IMS – Message

Deletion of LEMF successfull

Figure 4.19 IMS – Message Dialog Box, LEMF deleted

5 Click on OK.

The LEMF Selection Window dialog box displays an updated list of LEMF.

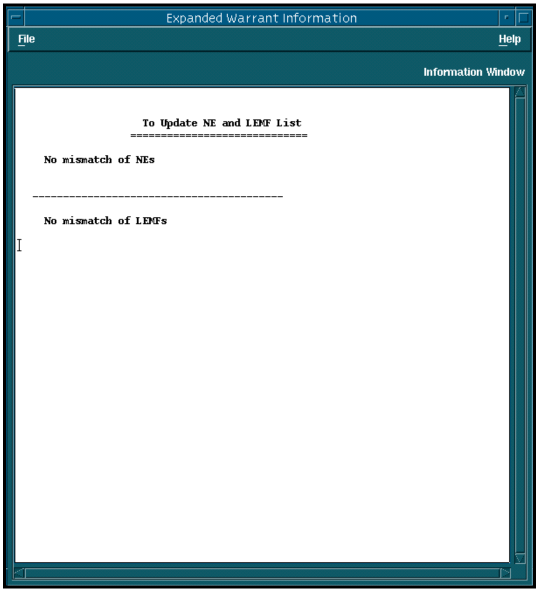
To update NE and LEMF in the database

This procedure reconciles both the NE and LEMF against those stored in the network gateway host, that is, those created using NE Setup.

1 Choose the Options > Update Network Element/LEMF menu option.

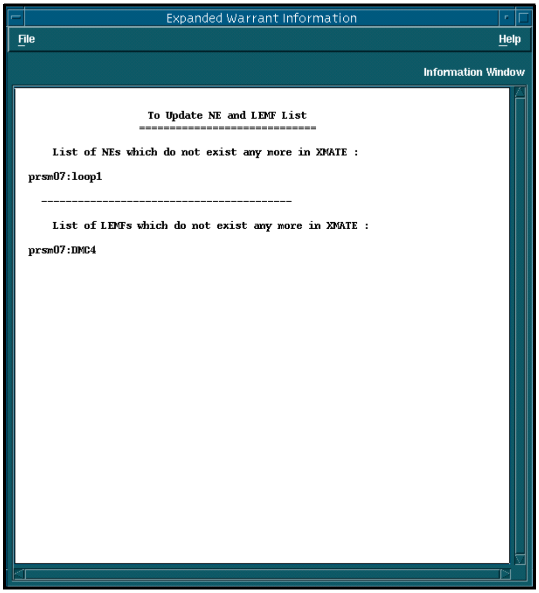
The Expanded MNN/IMEI/IMSI Information dialog box reports whether there is any mismatch between the NE and LEMF lists in the database and the gateway.

Figure 4.20 and Figure 4.21 show the Expanded MNN/IMEI/IMSI Information dialog box displaying reports with and without mismatches.



```
                    To Update NE and LEMF List
                  ==============================

   No mismatch of NEs

 -------------------------------------------

   No mismatch of LEMFs
```

Figure 4.20 Expanded MNN/IMEI/IMSI Information Dialog Box – database matches



```
                 To Update NE and LEMF List
                ===============================

    List of NEs which do not exist any more in XMATE :

prsm07:loop1

  --------------------------------------------

    List of LEMFs which do not exist any more in XMATE :

prsm07:DMC4
```

Figure 4.21 Expanded MNN/IMEI/IMSI Information Dialog Box – database mismatches

2 Update any mismatched NE if necessary.

Follow the procedure in ‘To add a NE to the database’ on page 4-4.

3 Update any mismatched LEMF if necessary.

Follow the procedure in ‘To add a LEMF to the database (Dom)’ on page 4-13.

Managing the database

Normally IMS maintains and updates the database automatically. But you may need to edit the database manually when faults occur in the network. This section describes the major task areas of:

- Viewing and printing target subscriber details
- Adding, editing, and deleting target subscriber entries, page 4-25
- Viewing and resetting the legal bases of warrants (G10), page 4-35

Viewing and printing target subscriber details

This section describes how

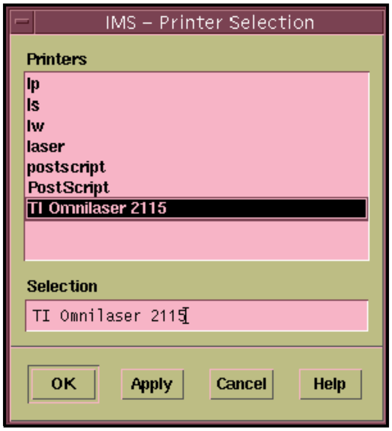
- To specify the destination printer
- To view or print the details of a single entry, page 4-22
- To print database entries, page 4-23

To specify the destination printer

1 Choose the Options > Print > Printer Setup menu option.

The IMS - Printer Selection dialog box is displayed (Figure 4.22) with the current print device listed in the Selection text box.

2 Click on another printer name in the Printers list and click on the OK button.



Selection
TI Omnilaser 2115

Figure 4.22 IMS – Printer Selection dialog box

To view or print the details of a single entry

You first have to search for entries to fill the IMS Administration window – see the section ‘Searching the database (Dom)’ on page 4-36.

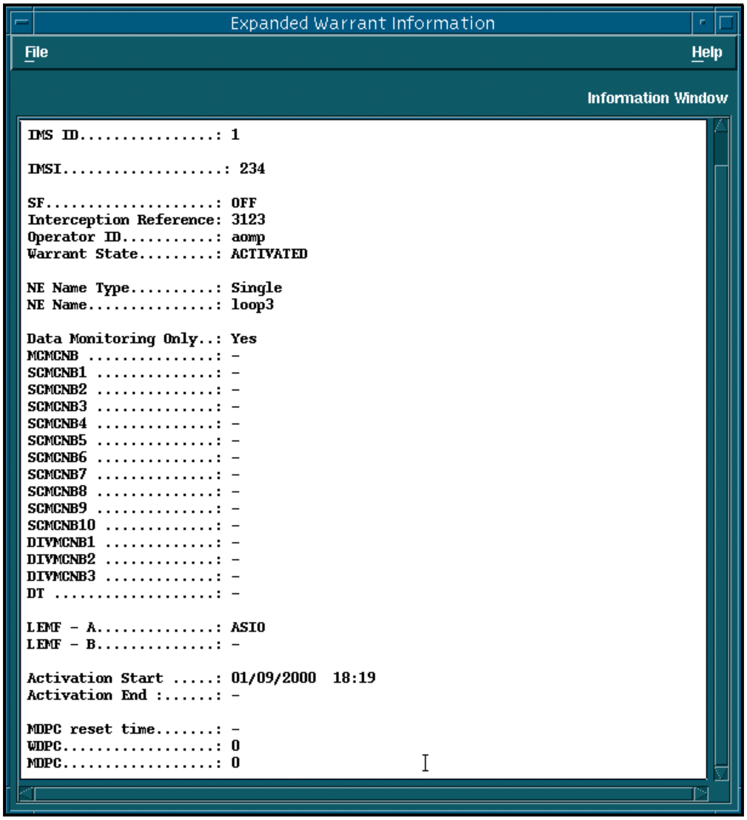
1 Double-click on an entry in the IMS Administration window.

The Expanded MNN/IMEI/IMSI Information dialog box appears (Figure 4.23).

2 Choose the File > Printer Setup menu option and a destination printer from the IMS – Printer Selection dialog box.

3 Choose the File > Print All menu option.

IMS prints the contents of the Expanded MNN/IMEI/IMSI Information dialog box.



```
IMS ID...............: 1

IMSI..................: 234

SF...................: OFF
Interception Reference: 3123
Operator ID...........: aomp
Warrant State.........: ACTIVATED

NE Name Type..........: Single
NE Name...............: loop3

Data Monitoring Only..: Yes
MCMCNB ...............: -
SCMCNB1 ..............: -
SCMCNB2 ..............: -
SCMCNB3 ..............: -
SCMCNB4 ..............: -
SCMCNB5 ..............: -
SCMCNB6 ..............: -
SCMCNB7 ..............: -
SCMCNB8 ..............: -
SCMCNB9 ..............: -
SCMCNB10 .............: -
DIVMCNB1 .............: -
DIVMCNB2 .............: -
DIVMCNB3 .............: -
DT ...................: -

LEMF - A..............: ASIO
LEMF - B..............: -

Activation Start .....: 01/09/2000  18:19
Activation End :......: -

MDPC reset time.......: -
WDPC..................: 0
MDPC..................: 0
```

Figure 4.23 Expanded Warrant Information Dialog Box

To print database entries

You must first search for the target subscribers’ entries and display them in the IMS Administration window – see the section ‘Searching the database (Dom)’ on page 4-36.

1 Choose the Options > Print > Printer Setup menu option in the IMS Administration window.

The IMS-Printer Selection dialog box lists printers available to the computer.

2. Click on the destination printer.
3. Click one or more entries in the IMS Administration window if you do not want to print all entries.
4. Choose the Options > Print > Print Selected menu option to print only the highlighted entries

   or

   Right-click in the window and choose the Print Selected menu option to print only the highlighted entries

   or

   Choose the Options > Print > Print All menu option to print all entries, whether selected or not.

Adding, editing, and deleting target subscriber entries

This section describes how

- To add a target subscriber's number to the database
- To delete a subscriber's entry from the database, page 4-32
- To reset the measurements data-product counter (MDPC), page 4-32

To add a target subscriber's number to the database

1 Choose the File > Add Target No menu option in the IMS Administration window.

- For Domestic, the Add New Warrant Record dialog box displays (Figure 4.24 on page 4-30).
- For G10, the Create Warrant Prologue dialog box displays (Figure 4.26 on page 4-31).

For G10 only:

a Choose the Network Element (NE) type (Fixed or Mobile).

b Choose Single or Group type.

c Click on the Network Element button, choose the NE from the list showing, then click on the Close button.

d Click on the Apply button. This displays the Add New Warrant Record dialod box (Figure 4.27 on page 4-32)

2 Complete the information requested in the dialog box.

Item	Procedure
MNN/IMEI/IMSI	This is the telephone number of the target subscriber whose incoming and outgoing calls are to be intercepted. **Note:** With G10, MNN, IMEI or IMSI cannot be subsequently modified in the Modify MNN/IMEI/IMSI dialog box. 1. Click the MNN, IMEI or IMSI option menu to indicate whether a subscriber’s telephone number, equipment identifier or subscriber number is to be entered. 2. Type the target subscriber’s telephone number or equipment identifier in the MNN, IMEI or IMSI dialog box when it appears. 3. Retype the target subscriber’s telephone number or equipment identifier when the MNN, IMEI or IMSI dialog box reappears to double-check that you typed the number correctly.
SF	This is a special monitoring feature that allows the generation of data products whenever the subscriber (or phone) moves from one cell to another.
Network ID (G10)	The Network ID list can be modified in the `/home/aomp/setup/redrs/text/resid.x/IMSNETOPID` file.
Subnet ID (G10)	The Subnet ID list can be modified in the `/home/aomp/setup/redrs/text/resid.x/IMSSUBOPID` file.
Network Element (Domestic)	Normally you choose the NE or NE group to which the target subscriber’s telephone or other service is connected. 1. Click on either the Single NE or Group NE choice button. 2. Click on the Network Element button. 3. Select either a single NE or group of NE from the LEMF Network Element List dialog box (Figure 4.2).
LEMF-A	You *must* select a primary LEMF. Make sure that the LEMF is the correct centre for the requesting agency. • Click on the LEMF-A button and select the LEMF from the LEMF Network Elements List dialog box.

Item	Procedure
LEMF-B	The secondary LEMF is optional but must be different from the LEMF-A if added. • Click on the LEMF-B button and select the optional secondary LEMF.
Suppress MNN/ IMEI/IMSI (Transmission) (G10)	1. Click on the Suppress MNN/IMEI/IMSI checkbox to include the target subscriber's number in the IMS data product (DP). 2. Clear the Suppress MNN/IMEI/IMSI checkbox to exclude the subscriber's number.
Begin (G10)	This is the date and time the interception is to begin. • Type the date in dd/mm/yyyy format and the time in 24-hour hh:mm format.
End (G10)	This is the date and time the interception is to end. • Type the date in dd/mm/yyyy format and the time in 24-hour hh:mm format.
Agency Information (G10)	• Enter the agency information: • Interception Reference, • Internal Reference, • Agency Name, and • Agency Contact Details.
NOTES (G10)	• Type any reminders, memos, or other notes here.
Legal Basis (G10)	• Select the legal basis appropriate to this interception: • STPO, • AWG, • G10, or • TEST.

Item **Procedure**

DT

The DT (delivery type) field specifies which data channels are to be sent to the LEMF and whether one or two trunk lines are to be used.

1. Click the DT radio button.
2. Click check boxes in the Enter DT dialog box to activate the delivery of the required channels.

   VCE Voice data

   UDI Unrestricted digital information

   F31 3.1 kHz Audio or data

   AVF Alternate voice or facimile

   DFA Data or facsimile
3. Click a radio button for each activated channel to set the number of trunk lines to be used.
   - Both data transmitted from and received by the monitored number is sent to the LEMF via a single trunk line.
   - Data transmitted from the monitored number is sent to the LEMF via one trunk line and date received via another trunk line.
4. Click Apply.

Interception Reference/CID

This is the code of the agency and it is used as an extra key to initiate the warrant where the MNN/IMEI/IMSI and MUID has been set up already. This is a manditory, alphanumeric field that holds up to 25 characters.

Data Monitoring Only

This option does not capture the voice content of a call, but only data associated with a call.

- Click on the Data Monitoring Only check box to retrieve only information about monitored calls, not their contents

  or
- Clear the check box to capture all interception data, including the voice and data content of monitored calls.

Item	Procedure
MCMCNB, SCMCNB-1 to SCMCNB-10, DIVMCNB1 to DIVMCNB3	These monitoring diversion numbers can consist of up to 28 digits. **Note:** SCMCNB applies to GSMR8, GSMR7, TL3/L5 and TL4/L6 NE. MCMCNB is applicable only to TL4/L6 NE. 1. Uncheck the Data Monitoring Only check box. 2. Type the appropriate telephone numbers into the SCMCNB and DIVMCNB fields. SCMCNB-1 is the primary diversion number supplied by the monitoring agency. SCMCNB-2 to SCMCNB-10 are optional secondary diversion numbers. DIVMCNB1 to DIVMCNB3 are the diverted monitoring centre numbers accepted by the called line verification function.
MAXCALLS (G10)	Type the maximun number of monitoring calls from one MNN/IMEI/IMSI.
Closed User Group (G10)	1. Clear the Data Monitoring Only check box. 2. Enter the numberic code corresponding to the user group.
Network Identifier (G10)	1. Clear the Data Monitoring Only check box. 2. Enter the type of network, for example, ISDN or PSDN.

3 Click on the Add New Record button.

A confirmatory alert appears when the target subscriber’s number (MNN), the equipment identity number)IMEI) or the subscriber identity number (IMSI), is successfully added to the database.

The IMS Administration window displays the new entry.

4 Activate the newly added warrant.

Inactivate and re-activate the IMS Mediation and Activation server in order for it to activate the monitoring of the newly created warrants in the NE.

5 Check whether the warrant activated successfully.

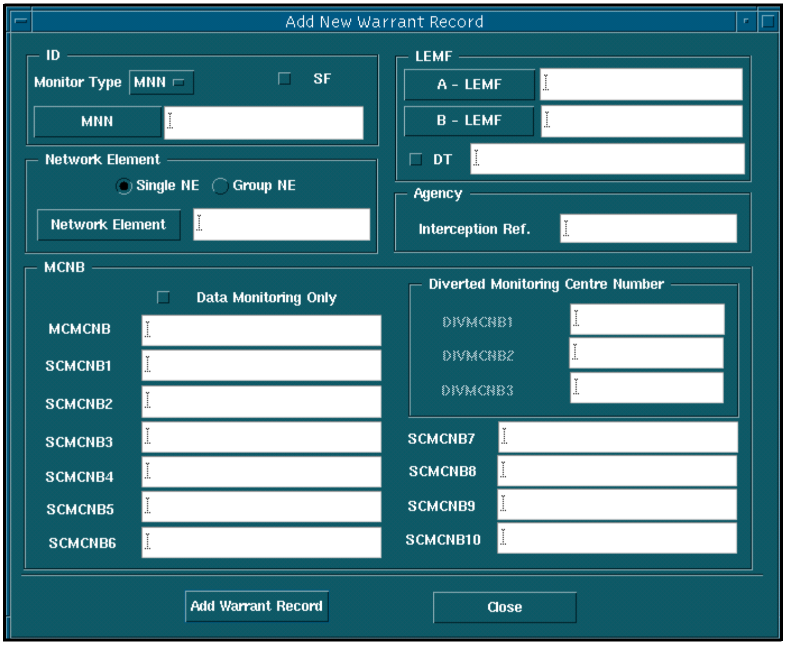


Figure 4.24 Add New Warrant Record Dialog Box (Dom)

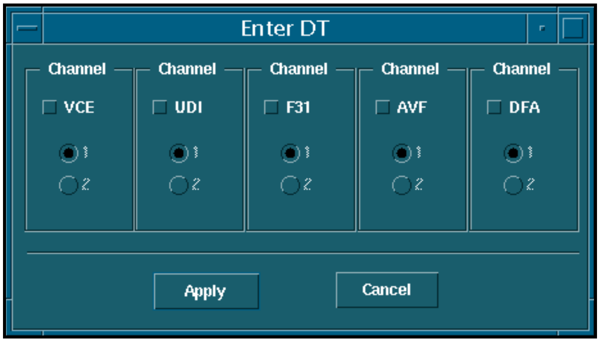
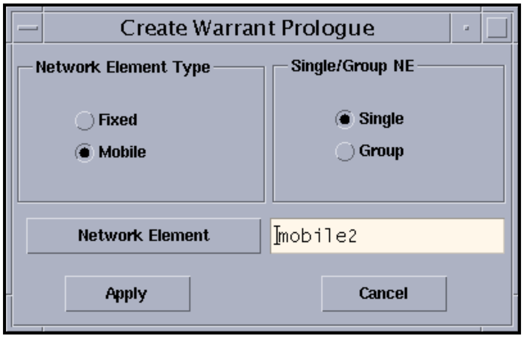


Figure 4.25 Enter DT Dialog Box



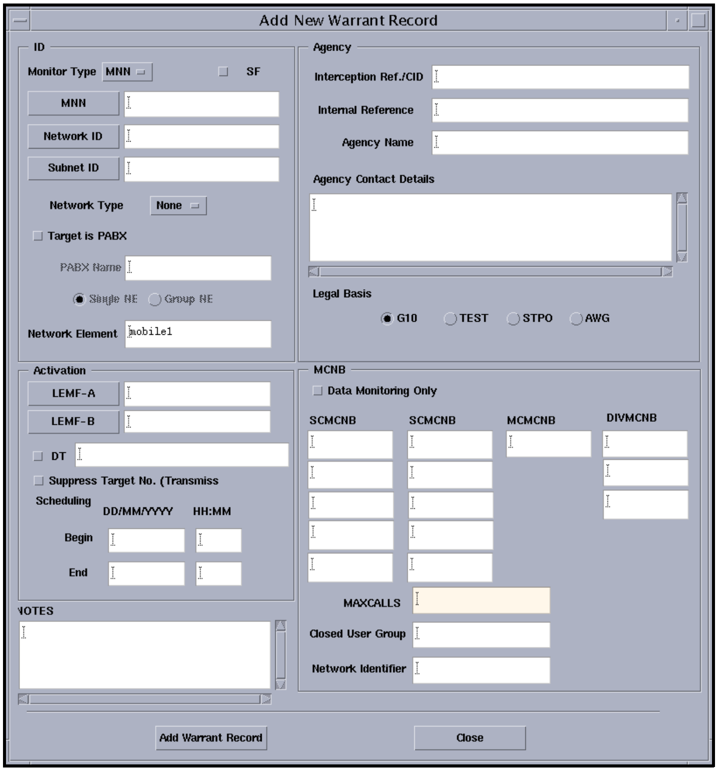
Create Warrant Prologue

Network Element Type: ○ Fixed ● Mobile

Single/Group NE: ● Single ○ Group

Network Element: mobile2

Figure 4.26 Create Warrant Prologue Dialog Box



Add New Warrant Record

ID

Monitor Type: MNN □ SF

Network Type: None

□ Target is PABX

● Single NE ○ Group NE

Network Element: mobile1

Agency

Legal Basis: ● G10 ○ TEST ○ STPO ○ AWG

Activation

□ DT

□ Suppress Target No. (Transmiss

MCNB

□ Data Monitoring Only

Figure 4.27 Add New Warrant Record Dialog Box (G10)

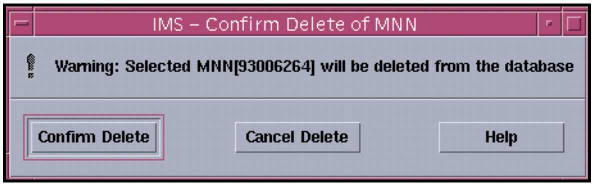
To delete a subscriber’s entry from the database

You must first search for the target subscriber’s number (monitored network number – MNN/IMEI/IMSI) or equipment identifier (IMEI or IMSI) and display it in the IMS Administration window – see the section ‘Searching the database (Dom)’ on page 4-36.

1. Click on the entry in the IMS Administration window to be deleted.
2. Right-click in the IMS Administration window and choose the MNN Admin > Delete Selected Target No menu option.

   The IMS – Confirm Delete of MNN/IMEI/IMSI dialog box appears (see below).
3. Click on the Confirm Delete button.

   IMS removes the target subscriber’s number or equipment identifier from the database and the IMS Administration window.



Warning: Selected MNN[93006264] will be deleted from the database

Figure 4.28 IMS – Confirm Delete of MNN/IMEI/IMSI Dialog Box

To reset the measurements data-product counter (MDPC)

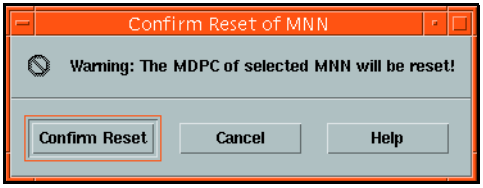
You must first search for the target subscriber’s number (MNN), equipment identifier (IMEI) or subscriber identifier (IMSI) and display it in the IMS Administration window – see the section ‘Searching the database (Dom)’ on page 4-36.

1. Click on the entry in the IMS Administration window whose MDPC is to be reset.
2. Right-click in the IMS Administration window and choose the MNN Admin > Reset MDPC menu option.

The IMS – Confirm Reset of MNN/IMEI/IMSI dialog box appears (see below).

3 Click on the Confirm Reset button.

IMS resets the measurements data-product counter (MDPC) to 0 (zero), and the Date and Time to the current date and time.



Warning: The MDPC of selected MNN will be reset!

Figure 4.29 IMS – Confirm Reset of MNN/IMEI/IMSI Dialog Box

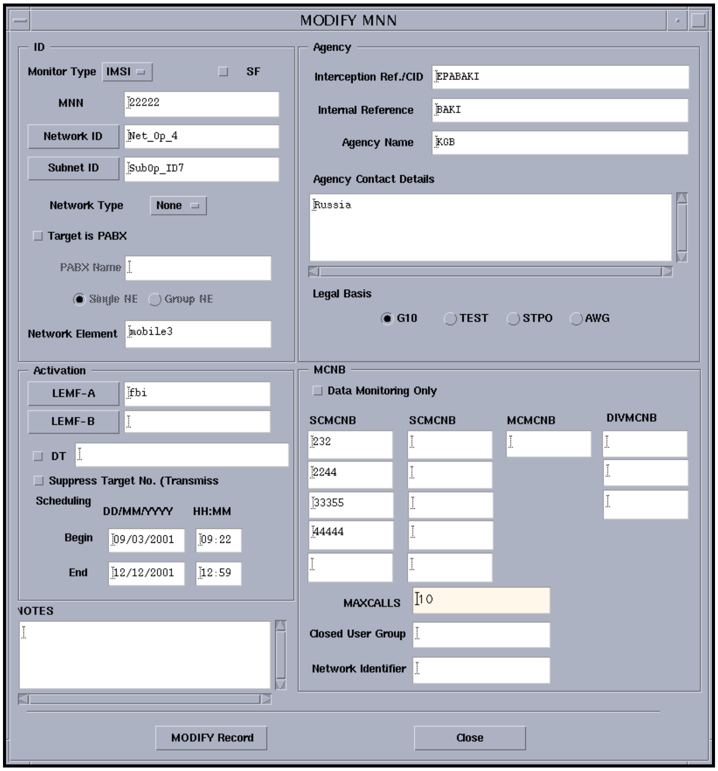
To modify a target subscriber's MNN entry in the database (G10)

You must first search for the target subscriber's number (MNN), equipment identifier (IMEI) or subscriber identifier (IMSI) and display it in the IMS Administration window – see the section 'Searching the database (Dom)' on page 4-36.

1 Click on an entry in the IMS Administration window (Figure 4.1 on page 4-3).

2 Right-click in the IMS Administration window and choose the MNN Admin > Modify Selected Target No option.

The Modify Target No dialog box is displayed.



MODIFY MNN

ID

Monitor Type: IMSI

□ SF

MNN: 22222

Network ID: Net_Op_4

Subnet ID: SubOp_ID7

Network Type: None

□ Target is PABX

PABX Name:

● Single NE ○ Group NE

Network Element: mobile3

Agency

Interception Ref./CID: EPABAKI

Internal Reference: BAKI

Agency Name: KGB

Agency Contact Details: Russia

Legal Basis: ● G10 ○ TEST ○ STPO ○ AWG

Activation

LEMF-A: fbi

LEMF-B:

□ DT

□ Suppress Target No. (Transmiss

Scheduling

	DD/MM/YYYY	HH:MM
Begin	09/03/2001	09:22
End	12/12/2001	12:59

NOTES

MCNB

□ Data Monitoring Only

SCMCNB	SCMCNB	MCMCNB	DIVMCNB
232			
2244			
33355			
44444			

MAXCALLS: 10

Closed User Group:

Network Identifier:

Figure 4.30 Modify Target No dialog box (G10)

3 Click in each field to be modified and edit their values as required.

Note:

- There are some fields that cannot be modified:
  - MNN, IMEI or IMSI box
  - Network Type
  - Network Element
- The values of LEMF-A and LEMF-B must not be identical
- SCMCNB fields can be modified only if the NE type is GSM-R7 or GSM-R8 and if DMO is un-set.

4 Click on the Modify Record button to accept the new parameters.

The Modify Target No dialog box closes and the IMS Administration window reflects the changes.

Viewing and resetting the legal bases of warrants (G10)

You can request a report listing the number of warrants currently issued against each of the legal bases for interceptions. The report is written to the console by the legalbstat command.

To see the parameters of the legalbstat command

- Type

  ```
  irun legalbstat -h
  ```

  at the command prompt.

  This summary of the command options is written to the console:

  ```
  legalbstat [-h|show|reset [STPO|AWG|G10|TEST|ALL]]
  ```

  To view the number of warrants per legal basis

- Type the following at the command prompt:

  ```
  irun legalbstat -show
  ```

  A report similar to that below is written to the console:

  ```
  Legal BasisNumber of Warrants
  STPO2
  AWG0
  G100
  TEST0
  ```

```
Time of Last Reset      = Fri Jan  9 15:47:24 1998
Time of Database Create = Tue Jan  6 15:43:34 1998
```

To reset the number of warrants for a legal basis

1. Type

   ```
   irun legalbstat -reset legalBasis
   ```

   at the command prompt, where legalBasis is one of STPO, AWG, G10, or TEST.

   The Number of Warrants column is reset to 0 for the relevant legal basis and the Time of Last Reset is the time the reset occurred. The Time of Database Create never changes after the initial set-up.

2. Check the results of the reset by typing

   ```
   irun legalbstat show
   ```

   at the command prompt.

   A report similar to that below is written to the console:

   ```
   Legal Basis      Number of Warrants
   STPO             0
   AWG              0
   G10              0
   TEST             0

   Time of Last Reset      = Mon Mar 28 17:36:51 2000
   Time of Database Create = Tue Jan  6 15:43:34 1998
   ```

Searching the database (Dom)

You must find a target subscriber's details before you can update them in the database. IMS search capabilities allows these details to be found using different searching criteria.

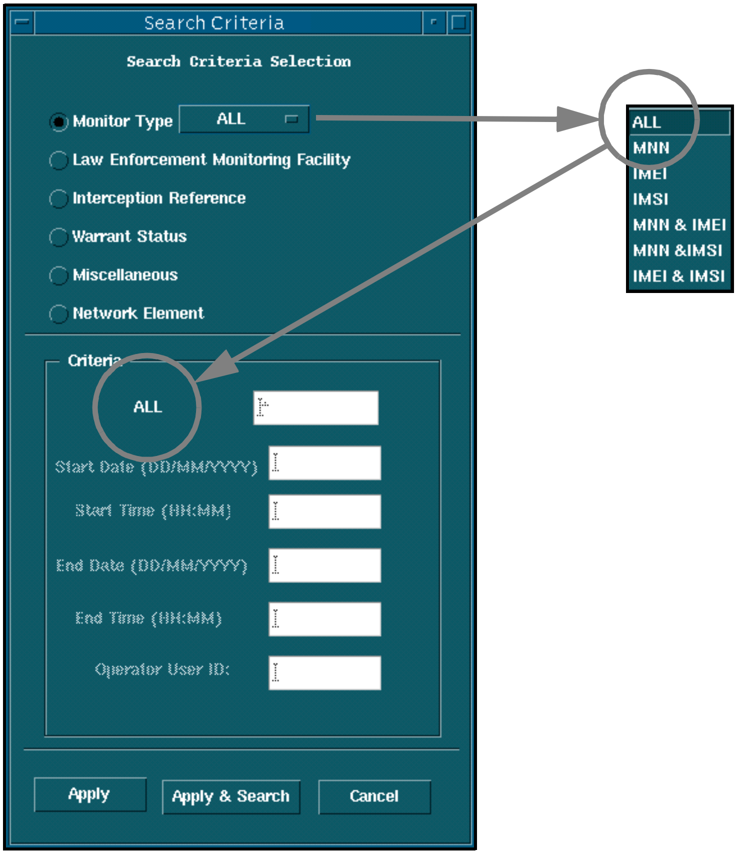
To specify search criteria

1. Choose the Search > Define Criteria menu option in the IMS Administration window.

   The Search Criteria dialog box appears (Figure 4.31).

2. Click on the All button or,click on the Law Enforcement Monitoring Facility, Interception Reference Number, Warrant Status, Miscellaneous, or Network Element choice button.

- MNN permits searches only on target subscriber’s numbers (monitored network numbers – MNN).
- IMEI permits searches only on target equipment identifiers (international mobile equipment identifier – IMEI).
- IMSI permits searches only on target equipment identifiers (international mobile subscriber identifier–IMSI).
- MNN & IMEI displays all MNN and IMEI warrants.
- MNN & IMSI displays all MNN and IMSI warrants.
- IMEI & IMSI displays all IMEI and IMSI warrants.
- All displays all warrants.
- Law Enforcement Monitoring Facility permits searches on LEMF and secondary keys as well.
- Interception Reference permits searches only on Interception Reference codes.
- Warrant Status permits searches only on the target warrant’s status.
- Miscellaneous permits searches on any secondary keys.
- Network Element permits searches only on the target NE name.



Search Criteria

Search Criteria Selection

● Monitor Type ALL
○ Law Enforcement Monitoring Facility
○ Interception Reference
○ Warrant Status
○ Miscellaneous
○ Network Element

Criteria

Figure 4.31 Search Criteria Dialog Box (Dom)

If Monitor Type is selected, clicking on the All button will open a drop-down menu where you can further define the basis of the search.

You can select from:

- IMNN
- IMEI
- IMSI
- MNN & IMEI
- MNN & IMSI
- IMEI & IMSI

3 Complete the Search Criteria dialog box.

Item	MNN	IMEI	MNN & IMEI	IMSI	MNN & IMSI	IMEI & IMSI	All	LEMF	IRN	WS	Misc	NE	Procedure
MNN	4	—	—	—	—	—	—	—	—	—	—	—	• Type the subscriber’s number. Type the * wildcard to select all subscribers’ numbers. • Type part of a number, for example, the area code and part of the local code, plus the * wildcard to select a range of related subscribers’ numbers: eg, 0398* .
IMEI	—	4	—	—	—	—	—	—	—	—	—	—	• Type the equipment identifier. Type the * wildcard to select all equipment. • Type part of an equipment identifier plus the * wildcard to select a range of related equipment identifiers .
MNN & IMEI	—	—	4	—	—	—	—	—	—	—	—	—	• Type an equipment identifier or subscriber’s number. Type the * wildcard to select all subscribers and equipment. • Type a number plus the * wildcard to select subscribers’ numbers or equipment identifiers containing the number .

Item	MNN	IMEI	MNN & IMEI	IMSI	MNN & IMSI	IMEI & IMSI	All	LEMF	IRN	WS	Misc	NE	Procedure
IMSI	—	—	—	4	—	—	—	—	—	—	—	—	• Type the subscriber identifier. Type the * wildcard to select all subscribers. • Type part of a subscriber identifier plus the * wildcard to select a range of related subscriber identifiers .
MNN & IMSI	—	—	—	—	4	—	—	—	—	—	—	—	• Type a subscriber's number or identifier. Type the * wildcard to select all subscribers. • Type a number plus the * wildcard to select subscribers' numbers or identifiers containing the number .
IMEI & IMSI	—	—	—	—	—	4	—	—	—	—	—	—	• Type an equipment identifier or subscriber's identifier. Type the * wildcard to select all subscribers and equipment. • Type a number plus the * wildcard to select subscribers' identifier or equipment identifiers containing the number .
All	—	—	—	—	—	—	4	—	—	—	—	—	
LEMF	—	—	—	—	—	—	—	4	—	—	—	—	Click on the LEMF button to choose from the Select LEMF dialog box.
Intercept Ref	—	—	—	—	—	—	—	—	4	—	—	—	Enter in the Interception Reference code to search on.

Item	**MNN**	**IMEI**	**MNN & IMEI**	**IMSI**	**MNN & IMSI**	**IMEI & IMSI**	**All**	**LEMF**	**IRN**	**WS**	**Misc**	**NE**	**Procedure**
Warrant Status	—	—	—	—	—	—	—	—	—	4	—	—	Select the warrant state to search on. The available states are Activated, Terminated and Not Activated.
NE name	—	—	—	—	—	—	—	—	—	—	—	4	Enter the name of the NE required.
Start Date	—	—	—	—	—	—	—	4	—	—	4	—	The starting date of an interception in dd/mm/yyyy format.
Start Time	—	—	—	—	—	—	—	4	—	—	4	—	The starting time of an interception in 24-hour hh:mm format.
End Date	—	—	—	—	—	—	—	4	—	—	4	—	The ending date of an interception in dd/mm/yyyy format.
End Time	—	—	—	—	—	—	—	4	—	—	4	—	The ending time of an interception in 24-hour hh:mm format.
Operator User ID	—	—	—	—	—	—	—	4	—	—	4	—	The operator’s user identifier (logon).

4 Click on the Apply button.

Now continue with ‘To search for database entries’ below.

Note: Your custom search criteria are retained over sessions. Once the criteria have been specified, they will be stored and used for subsequent searches.

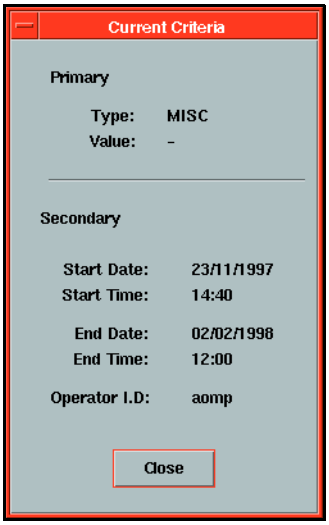
To search for database entries

IMS initially searches the database for all entries unless you have defined specific search criteria.

The initial default criterion is to search on all target subscriber's numbers (MNN), equipment identifier (IMEI) or subscriber identifier (IMSI) with a value of * as a primary key, where * is a wildcard that means to find all items – see Figure 4.31 on page 4-38. No secondary keys are defined.

1 Choose the Search > View Criteria menu option in the IMS Administration window to check the currently active criteria.

The Current Criteria dialog box (see below) displays the values for which a search looks.



Current Criteria

Primary

Type: MISC
Value: -

Secondary

Start Date: 23/11/1997
Start Time: 14:40

End Date: 02/02/1998
End Time: 12:00

Operator I.D: aomp

Figure 4.32 Current Criteria Dialog Box (Dom)

2 Click on the Apply & Search button in the Search Criteria dialog box.

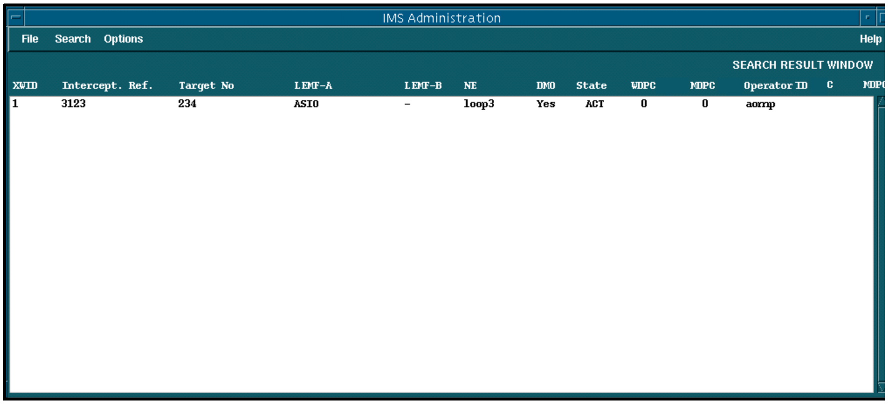
or

Choose the Search > Initiate Search menu option in the IMS Administration window.

or

Right-click in the IMS Administration window and choose the Update Window menu option.

Database entries matching the current search criteria appear in the IMS Administration window (see below). An alert notifies you when there are no matching entries. For an explanation of the data in the columns, see ‘Features of the IMS Administration window’ on page 4-49.



SEARCH RESULT WINDOW

XWID	Intercept. Ref.	Target No	LEMF-A	LEMF-B	NE	DMO	State	WDPC	MDPC	Operator ID	C	MDP
1	3123	234	ASIO	–	loop3	Yes	ACT	0	0	aornp		

Figure 4.33 IMS Administration window – after successful search (Dom)

Searching the database (G10)

You must find a target subscriber’s details before you can modify them in or delete them from the database, or reset the measurements data-product counter (MDPC). You can use different combinations of search criteria to locate these details.

To specify search criteria

1 Choose the Search > Define Criteria option in the IMS Administration window (Figure 4.1 on page 4-3).

The Search Title (Search Criteria Selection) dialog box is displayed (Figure 4.34 on page 4-46). All fields initially match all the possible values in the database: text fields display the wildcard value * and drop-down lists are set to Any. Clicking the Apply button without changing any fields fills the IMS Administration window with all entries in the database.

Note: You type either a specific value or the * (asterisk) wildcard value in the fields of the Search Title dialog box. For example, because the MNN field is initially set to *, on its own it would find all target subscribers' numbers but a value of 1234 would only find warrants for the MNN 1234. The following instructions only apply to finding specific values.

2 Complete the Search Title dialog box.

Group	Item	Procedure	
MNN ID	MNN	1	Click on the All option or on the MNN & IMSI, IMEI & IMSI, MNN & IMEI, MNN, IMEI or IMSI option menu. The label of the text box changes to the corresponding type of warrants selected.
		2	Type a number into the Target No box.
	Network Type	•	Select any one of the available list options from the Network Type list.
	Internal Reference	•	Type a complete code.
Network Element	Network Element	1	Click either the Single NE or Group NE radio button.
		2	Click on the Network Element button (Single NE chosen) to open the Select Network Element dialog box. or Click the Group NE button (Group NE chosen) to open the Select NE Group dialog box.
		3	Click an entry in the Select Network Element dialog box (Single NE chosen) or Select NE Group dialog box (Group NE chosen), and click the Close button.
Activation	Begin	1	Type the starting date of a warrant in DD/MM/YYYY format.
		2	Type the starting time of a warrant in HH:MM format.

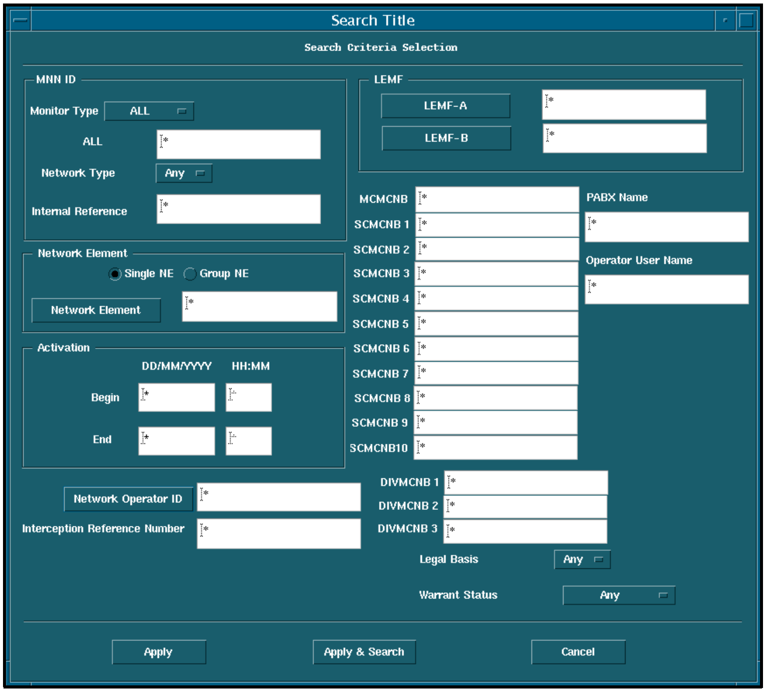
Group	Item	Procedure
	End	1 Type the end date of a warrant in DD/MM/YYYY format.
		2 Type the end time of a warrant in HH:MM format.
Network Operator ID	—	1 Click on the Network Operator ID button to open the Select Network Operator dialog box.
		2 Click an entry and click the Close button.
Interception Ref.	—	• Type the reference number authorising the interception.
LEMF	LEMF-A LEMF-B	1 Click on either the LEMF-A button or the LEMF-B button to open the Select LEMF dialog box.
		2 Click an entry in the Select LEMF dialog box and click Close.
MCMCNB SCMCNB DIVMCNB	—	• Type the destination telephone numbers for interceptions – some types of field can contain the wildcard * and others can have specific numbers.
		• One MCMCNB (Multiple Call Monitoring Number)
		• Four SCMCNBs (Single Call Monitoring Number)
		• Three DIVMCNB (Diverted Monitoring Centre Number)
PABX Name	—	• Type the name of a PABX.
Operator User Name	—	• Type the operator’s user name (log-on account name).
Legal Basis	—	• Choose a legal basis from the list.
Warrant Status	—	• Select the warrant state to search on. The available states are Activated, Terminated and Not Activated.

3 Save the criteria for the search.

- Click Apply to just save the search criteria, ready to start a search.
- Click Apply and Search to save the criteria and run a search.

The IMS Administration window displays the results of the search.

Note: The saved criteria are retained for the duration of the current session but are lost when you exit the IMS Administration window. That is, you can run a search in the current session many times with the same criteria until you specifically change them.



Monitor Type: ALL
ALL: *
Network Type: Any
Internal Reference: *
● Single NE ○ Group NE
Network Element: *
LEMF-A: *
LEMF-B: *
MCMCNB: *
SCMCNB 1: *
SCMCNB 2: *
SCMCNB 3: *
SCMCNB 4: *
SCMCNB 5: *
SCMCNB 6: *
SCMCNB 7: *
SCMCNB 8: *
SCMCNB 9: *
SCMCNB10: *
PABX Name: *
Operator User Name: *
DIVMCNB 1: *
DIVMCNB 2: *
DIVMCNB 3: *
Network Operator ID: *
Interception Reference Number: *
Legal Basis: Any
Warrant Status: Any

Figure 4.34 The Search Title (Search Criteria Selection) dialog box (G10)

To search for database entries

IMS initially searches the database for all entries unless you have defined specific search criteria. Once a set of criteria has been specified, you can search using those criteria.

1 Choose the Search > View Criteria option to open the Current Criteria message so you can check what criteria will be applied.

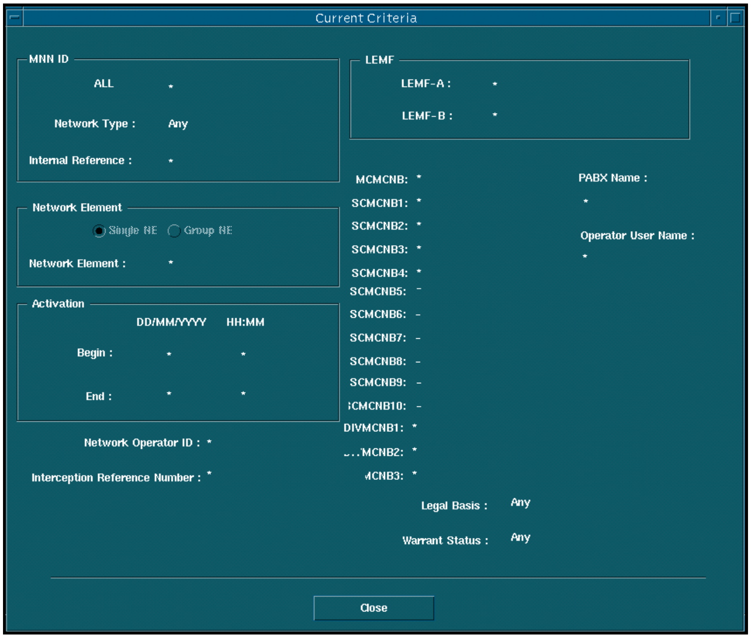
2 Specify new search criteria if necessary.

3 Right-click the IMS Administration window (Figure 4.1 on page 4-3) and choose Clear Window to erase the results of the previous search if desired.

4 Search using the current criteria.

- In the Search Title dialog box, click the Apply & Search button after specifying the criteria.
- In the IMS Administration window, choose the Search > Initiate Search option.
- In the IMS Administration window, right-click and choose the Update > Update Window option.

In each case, the results are displayed in the IMS Administration window (Figure 4.36 on page 4-48). When no entries match the specified criteria, the IMS Message alert (Figure 4.37 on page 4-48) informs you.



Current Criteria

MNN ID
ALL *
Network Type : Any
Internal Reference : *

Network Element
● Single NE ○ Group NE
Network Element : *

Activation
DD/MM/YYYY HH:MM
Begin : * *
End : * *

Network Operator ID : *
Interception Reference Number : *

LEMF
LEMF-A : *
LEMF-B : *

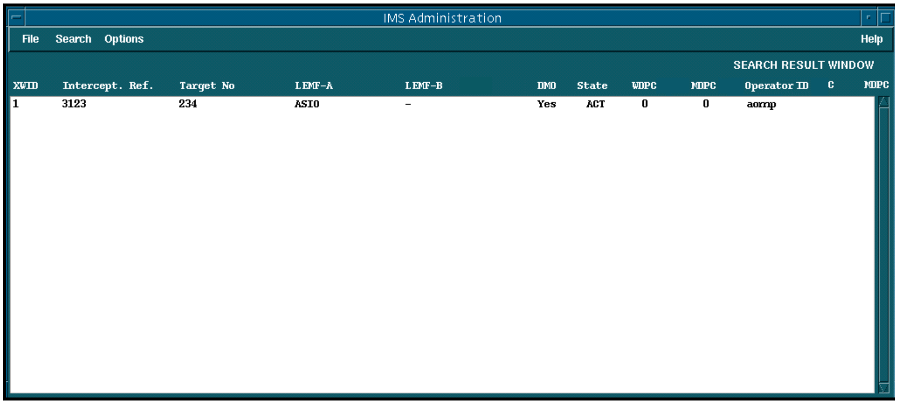
MCMCNB: *
SCMCNB1: *
SCMCNB2: *
SCMCNB3: *
SCMCNB4: *
SCMCNB5: -
SCMCNB6: -
SCMCNB7: -
SCMCNB8: -
SCMCNB9: -
;CMCNB10: -
DIVMCNB1: *
...'MCNB2: *
ICNB3: *

PABX Name :
*
Operator User Name :
*

Legal Basis : Any
Warrant Status : Any

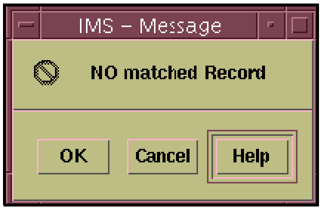
Figure 4.35 Current Criteria Dialog Box (G10)

STRICTLY CONFIDENTIAL



XWID	Intercept. Ref.	Target No	LEMF-A	LEMF-B	DMO	State	WDPC	MDPC	Operator ID	C	MDPC
1	3123	234	ASIO	–	Yes	ACT	0	0	aomp		

Figure 4.36 IMS Administration window – after successful search (G10)



NO matched Record

Figure 4.37 IMS – Message dialog box (G10)

IMS administration reference

This section describes the components of the IMS Administration window as follows:

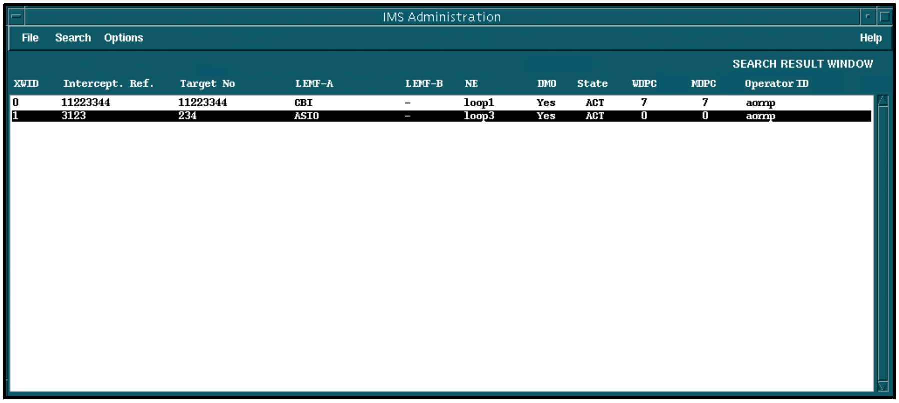
- Features of the IMS Administration window
- IMS Administration menus

Features of the IMS Administration window

The IMS Administration window displays information about current interceptions entered into the IMS database (Figure 4.38). These interceptions can either be activated, or terminated. The columns in the window display the following data:

Column	Description
XWID	Internal reference number.
Intercept Ref (G10)	A reference to the document or other authorisation for the interception.
MNN	Monitored network number, that is, the target subscriber's number.
IMEI	International mobile equipment identifier, that is, the unique serial number of the equipment.
IMSI	International mobile subscriber identifier.
LEMF-A	The primary law enforcement monitoring facility to which call data is to be sent.
LEMF-B	The secondary law enforcement monitoring facility.
NE (Dom)	Name of NE against which the warrant is activated.
DMO	Data monitoring only.
State	Activation state in NE. Either Activated or Terminated
WDPC	Warrant data-product counter, which indicates the number of data products transmitted to the LEMF by IMS for that warrant.

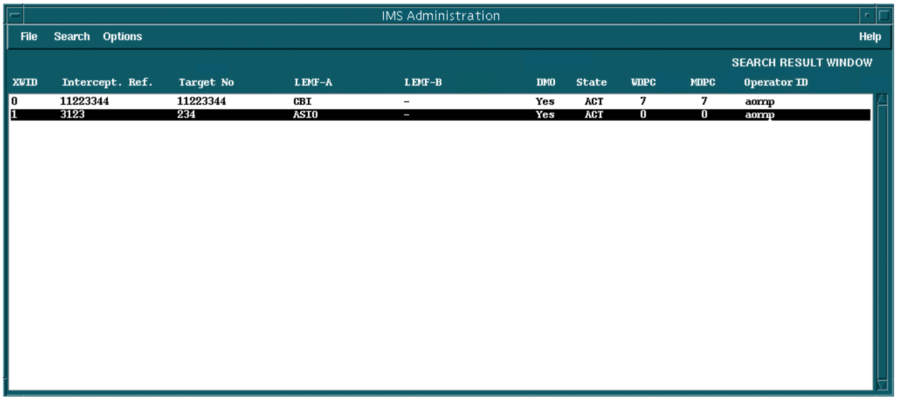
Column	Description
MDPC	Measurements data-product counter, which indicates the number of data products transmitted to the LEMF by IMS, that is, the same as WDPC, but it can be reset by the user.
Operator ID	The user identifier (or logon) of the operator who created the warrant.



SEARCH RESULT WINDOW

XWID	Intercept. Ref.	Target No	LEMF-A	LEMF-B	NE	DMO	State	WDPC	MDPC	Operator ID
0	11223344	11223344	CBI	–	loop1	Yes	ACT	7	7	aornp
1	3123	234	ASIO	–	loop3	Yes	ACT	0	0	aornp

Figure 4.38 IMS Administration window – features (Dom)



SEARCH RESULT WINDOW

XWID	Intercept. Ref.	Target No	LEMF-A	LEMF-B	DMO	State	WDPC	MDPC	Operator ID
0	11223344	11223344	CBI	–	Yes	ACT	7	7	aornp
1	3123	234	ASIO	–	Yes	ACT	0	0	aornp

Figure 4.39 IMS Administration window - features (G10)

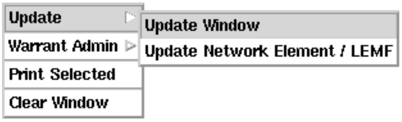
IMS Administration Menus

This section briefly looks at the following menus available through the IMS Administration window:

- Pop-up menu
- File menu, page 4-52
- Search menu, page 4-53
- Options menu, page 4-54
- Help menu, page 4-54

Pop-up menu

Right-clicking in the IMS Administration window pops up a menu which gives immediate access to updating and management dialog boxes as follows:

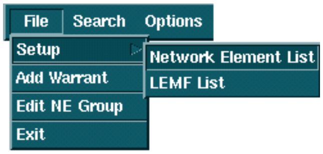


Menu option	Action
Update	• Update Window Searches all entries in the database that satisfy the criteria specified in the Search Criteria dialog box. This menu option is the same as the Search > Initiate Search menu option. • Update Network Element / LEMF Reconciles the NE list and LEMF list with those of the gateway host. This menu option is the same as the Options > Update Network Element / LEMF menu option.
MNN Admin	• Delete Selected MNN Deletes the target subscriber’s number (MNN), equipment identifier (IMEI) or subscriber identifier (IMSI) highlighted in the IMS Administration window.

Menu option	Action
	• Modify selected MNN (G10) Opens the Modify MNN, IMEI or IMSI dialog box so that you can alter the details of an interception. • Reset MDPC Resets the measurements data-product counter (MDPC) to 0 and resets Time and Date to the time and date of the reset for the highlighted MNN, IMEI or IMSI.
Print Selected	Prints the details of the target subscriber's number (MNN), equipment identifier (IMEI) or subscriber identifier (IMSI) highlighted in the IMS Administration window.
Clear Window	Clears all entries in the IMS Administration window.

File menu

The File menu lets you set up the IMS database with the details of NE, LEMF and target subscribers' numbers (MNN), equipment identifiers (IMEI) or subscriber identifiers (IMSI).



Menu option	Action
Setup	• Network Element List Opens the Network Element List dialog box so that you can add NE to, or delete them from, the list of NE available to IMS. • LEMF List Opens the Law Enforcement Monitoring Facilities dialog box so that you can add LEMF to or delete them from those available to IMS.
Add Target No	Opens the Add New Warrant Record dialog box so that you an add a new MNN, IMEI or IMSI to the database.

Menu option	**Action**
Edit NE Group	Opens the Edit NE Group dialog box which enables you to add, modify or delete NE groups.
Exit	Quits the IMS Administration window.

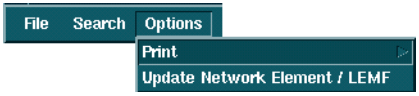
Search menu

The Search menu lets you define the criteria for searching the IMS database, then search for items matching those criteria.

Menu option	**Action**
Initiate Search	Initiates a search of the database using the criteria defined using the Search > Define Criteria menu option.
Define Criteria	Opens the Search Criteria dialog box so that you can define a set of criteria to be used when selecting entries from the database. Searches can be for target subscribers' numbers (MNN), equipment identifiers (IMEI), subscriber identifiers (IMSI), law enforcement monitoring facilities (LEMF), interception reference number, warrant status, NE, or miscellaneous entries.
View Criteria	Opens the Current Criteria dialog box so that you can see what the current search criteria are.

Options menu

The Options menu lets you print details of selected entries in the IMS Administration window and update the database with NE and LEMF data.



Menu option	Action
Print	• Printer Setup Opens the IMS – Printer Selection dialog box so you can choose the printer to which reports are to be sent. • Print Selected Prints the details of target subscribers’ numbers (MNN), equipment identifiers (IMEI) or subscriber identifiers (IMSI) highlighted in the IMS - Administration window. • Print All Prints the details of all MNN or IMEI in the window.
Update Network Element/ LEMF	Performs a consistency check of the NE and LEMF lists. This menu option is the same as right-clicking in the IMS Administration window and choosing the Update Network Element / LEMF menu option.

Help menu

The Help menu launches Acrobat Reader, which opens an on-line, hyperlinked version of the IMS User Manual. You can view the chapter on-line and navigate through it by clicking on entries in the chapter summary and on cross-references, and print out selected pages.

The on-line help supplied with Acrobat Reader gives more hints on navigating, finding topics, and printing.

5 Administering the IMS Transmission Process

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	1/198 17-CNAP 102 11 Uen		
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-03-15	**Revision** M	**Pages** 16

Procedures for managing the transmission process in the Interception Management System

In this chapter

This chapter describes how to set up the parameters used by the IMS transmission process, and how to start and stop both the transmission and activation processes.

Scope

The transmission process (CTB) provides a collection of data products from NE and transmission of the data products to LEMF. This window is used to activate and deactivate the transmission process and to enter the parameters needed by that process.

The IMS activation process (**imas**) provides:

- the provision of standardised (socket-based) interface to the service management layer
- an activation module go-between that also manages the activation initiation and scheduling.

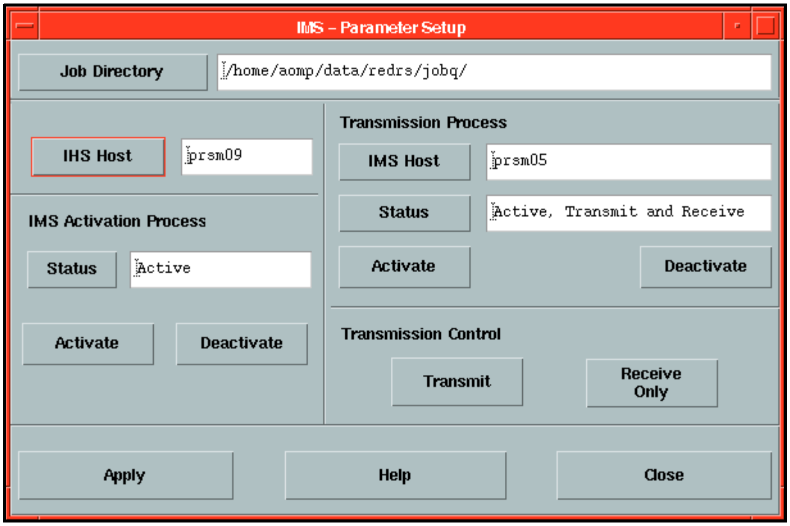
This window is also used to activate and deactivate the **imas** activation process.

Parameters

Eight parameters are required by the transmission process. Three are specified in the main window and five are located in the file `$AOMPHOME/setup/redrs/text/IMSAttribute`.

Main Window

Figure 5.1 IMS - Parameter Setup Dialog Box



Job Directory: /home/aomp/data/redrs/jobq/

IHS Host: prsm09

Status: Active

IMS Host: prsm05

Status: Active, Transmit and Receive

The main window has a number of functions:

- Specifying the directory where data products are stored (Job Directory).
- Specifying system hosts for the XMATE platform (IHS host) and hostname of the machine running the IMS servers (IMS host).
- Displaying the status of both servers (Status).
- Changing the mode of operation of the transmission process (Receive Only / Transmit).
- Starting and stopping both servers.(Activate/Deactivate).
- Saving changes (Apply).
- Displaying help documentation (Help).
- Exiting the application (Close).

The three parameters in the main window do not update immediately. The transmission process should be deactivated using **Deactivate** before these variables are changed.

After entering or modifying the parameters, click on **Apply** to save them, then **Activate** to restart the transmission process.

Job Directory

This directory is a working directory used by the transmission process to store incoming data products before they are transmitted[1].

Clicking on the **Job Directory** button will place a file selection window onto the screen, allowing the user to select the directory name.

IMS Host

This is the host where the transmission process will run. Clicking on the **IMS Host** button will place the host selection dialog box onto the screen, from which a host can be chosen. In the case of a single machine, the host name will be that of the host where IMS is installed.

IHS Host

This is the host where the IHS server is running. Clicking on the **IHS Host** button will place the host selection dialog box onto the screen, from which a host can be chosen. Check the monitor to find out which host this is. In the case of a single machine, the host name will be that of the host where AOMP (XMATE) is installed.

Parameter Files

The variables required for both servers are contained in the files `$AOMPHOME/setup/redrs/run_variables` and `$AOMPHOME/setup/redrs/text/IMSAttribute`. They can be changed while both the transmission and activation processes and `imas` are running and come into effect immediately the edited file is saved.

The files consist of the variable names followed by the appropriate value.

When IMS is installed, these variables have default values assigned.

Transmission Process Variables

The variables in the file `$AOMPHOME/setup/redrs/run_variables` are:

1. *consec_call_att*
2. *time_del_call_att*
3. *alarm_call_att*
4. *time_del_close_conn*
5. *x29lemf_use_stx_etx*

Example 5.1 Sample parameter file

```
# These variables are used while the transmission process is running.

# Number of consecutive call attempts before delay
consec_call_att 5

# Time delay after previous call attempts
time_del_call_att 30

# Number of call attempts before alarm is raised
alarm_call_att 10

# Time delay before connection to LEMF is closed
time_del_close_conn 2

# Prepend (STX STX STX) , Append (ETX ETX ETX) to all X29 LEMF
x29lemf_use_stx_etx 1
```

Transmission Process Variable Definitions

Consecutive Call Attempts

The variable *consec_call_att* is used to specify this value.

If the transmission process cannot send a data product, it retries **n** times before waiting for a given time delay and trying again. The **n** is specified as a number after the variable name in the file, e.g.

consec_call_att 5

Time Delay after Previous Call Attempts

The variable *time_del_call_att* is used to specify this value.

If the data product has not been transmitted after **n** call attempts, the same number of call attempts will be issued after time delay **Td**, until the data product is successfully transmitted. The **Td** is measured in seconds and specified as a number after the variable name in the file, e.g.

time_del_call_att 30

Call Attempts before an Alarm is Raised

The variable *alarm_call_att* is used to specify this value.

This is the number of unsuccessful attempts to transmit the data product that will be made before an alarm is issued. It is specified as a number after the variable name in the file, e.g.

alarm_call_att 10

Time Delay before Connection Closed

The variable *time_del_close_conn* is used to specify this value.

This variable specifies a time delay in seconds before a connection to a LEMF is closed. After a data product has been transmitted, the transmission process will keep the connection open for this amount of time in case another data product arrives. This prevents the repeated opening and closing of connections. If this feature is not desirable, then the variable can be set to 0 and the connection will be closed immediately.

The value is specified as a number (in seconds) after the variable name in the file, e.g.

time_del_close_conn 60

Header for X29

The variable x29lemf_use_stx_etx is used to specify whether the header is used or not.

This variable has the values 0 or 1. If it is set, CTB will append three STX and prepend three ETX to the message before sending to the LEMF using X29. The hex values are *STX-0x02 ETX-0x03*.

Activation Process Variables

The variables in the file `$AOMPHOME/setup/redrs/text/IMSAttribute` are:

1. *`mas_socksvr_port`*
2. *`mas_socksvr_range`*

Example 5.2 Sample Parameter File for the Activation Process

```
# These variables are used while the activation process is running.

# Imas to client TCP socket server port
mas_socksvr_port 30000

# Imas TCP socket server port range
mas_socksvr_range 0
```

Activation Process Variable Definitions

Socket server port number.

The variable `mas_socksvr_port` is used to specify the port number.

This is the TCP socket for the imas server to attach itself to clients. The default port is 30000, e.g.

`mas_socksvr_port 30000`

Socket server port number range

The variable `mas_socksvr_range` is used to specify the TCP socket imas server port range.

The default try-range is 0, e.g.

`mas_socksvr_range 0`

Starting and Stopping the Transmission Process

To start the transmission process, click on the **Activate** button on the main window. If it is not possible to start the process, a warning will be displayed in the warning window. If the transmission process starts but terminates shortly afterwards, errors will be displayed in the console. These errors are listed in 'Errors' on page 5-13. When the transmission process is activated, it will be able to both transmit and receive data products. It is also possible to block the transmission, see 'Blocking Transmission' on page 5-11.

To stop the transmission process, click on the **Deactivate** button on the main window. If the transmission process is stopped, the collection of data products also stops.

The current status of the process can be displayed at any time by clicking on the **Status** button on the main window. The status will be one of 'Inactive', 'Active, Receive Only', or 'Active, Transmit and Receive'.

If the DCS server is stopped and restarted, then the transmission process will also need to be stopped and restarted to regenerate the listen request.

Starting and Stopping the Activation Process

To start the **imas** server, click on the **Activate** button. The current status of the server can be displayed at any time by clicking on the **Status** button.

To stop the **imas** server, click on the **Deactivate** button.

Re-activating the IMS Server

If the IMS server (imas) needs to be re-activated and does not restart immediately, change the sockets in the `$AOMPHOME/setup/redrs/text/IMSAttribute` files by changing the following parameters to the same number:

File	***Parameter***
`$AOMPHOME/setup/redrs/environment`	`IMS_CMDSOCKET`
`$AOMPHOME/setup/redrs/text/IMSAttribute`	`mas_socksvr_port`

Blocking Transmission

It is possible to collect data files only, without transmitting them to LEMF. To do this click on the **Receive Only** button (if the button is not sensitive, the transmission process is already in this mode).

To transmit data products as well as receive them, click on the **Transmit** button (if the button is not sensitive, the transmission process is already in this mode).

The **Transmit** and **Receive Only** buttons can only be clicked on while the transmission process is active.

Corrupt Data Products

When data products are collected, the transmission process analyses them in an attempt to determine if the packet has been corrupted. If corruption is detected, the data product will be stores in `$AOMPHOME/<job directory>/ERROR_TERMINAL` and an alarm will be generated.

Errors

Transmission Process Errors

The following errors are produced by the transmission process if the process is able to start but exits before it starts transmitting data products. These errors are printed to the console.

DCS Error

```
IMS : CTB - COULD NOT CONTACT DCS SERVER <host>
```

The DCS on <host> must be running while the transmission process is active.

Use the XMATE Monitor Application to start DCS.

Parameter File Error

```
IMS : Parameter file <filename> is invalid.
```

You must enter some parameters (see ‘Parameters’ on page 5-4) and click on **Apply**, before clicking on the **Activate** button. If this fails, then check the filename mentioned in the error message. It should exist and be accessible by the user **aomp**.

IMS Database Error

```
CTB : Could not locate database.
```

The database could not be found or read successfully. Run IMS administration first.

LEMF Setup Error

```
IMS Transmission Process cannot start: LEMF is not delivered in
database.
```

Run **DataBase Admin** to create LEMF.

Usage errors

These errors can occur when the **Apply** button has been clicked on and parameters were incorrect or could not be saved.

Not all fields are filled in

```
Apply failed.
Not all fields are filled in.
```

There must be data entered in all fields (except the status field) on the main window.

Invalid Job Directory

```
Apply failed.
Invalid job directory.
```

Make sure the directory that has been entered exists.

Couldn’t save parameters

```
Apply failed.
Couldn’t save parameters in file.
```

The application is trying to save parameters in the file `$AOMPHOME/setup/redrs/trb/params`.

Make sure the directory exists and that if the file `params` exists that the user has write permission to it.

References

1 Chapter 2, ‘Installing and Configuring IMS’,
1531-CNAP 102 11

6 Operating the IMS

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	2/198 17-CNAP 102 11 Uen		
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-04-20	**Revision** U	**Pages** 26

Procedures used by operators to initiate and manage interceptions

In this chapter

This chapter describes how to initiate, modify, stop and check the status of interceptions.

Getting started

The tasks the operator can perform are accessed from the **IMS – Remote Equipment Data Routing System** window by clicking on icons. This window is also referred to as the IMS operator's window.

To launch the IMS operator's window

1. Log on to the XMATE system at the initial Welcome screen.

   a. Type your operator's user id and press **Return**.

      The password screen appears.

   b. Type your operator's password and press **Return**.

      After a short wait the desktop appears with the Front Panel at the foot of the display.

2. Right-click the desktop and choose **Workspace Menu** > **IMS Operator**.

   The IMS – Remote Equipment Data Routing System window appears (see Figure 6.1 for Dom or Figure 6.2 for G10)). This is the main window from which you access all operator functions.

3. Launch an operations dialog box by clicking an icon.

To quit the IMS operator's window

- For Domestic, select **Options** > **Quit** in the IMS – Remote Equipment Data Routing System window.
- For G10, select **File** > **Exit.**

STRICTLY CONFIDENTIAL

Figure 6.1 Main window of Interception Management System (Dom)

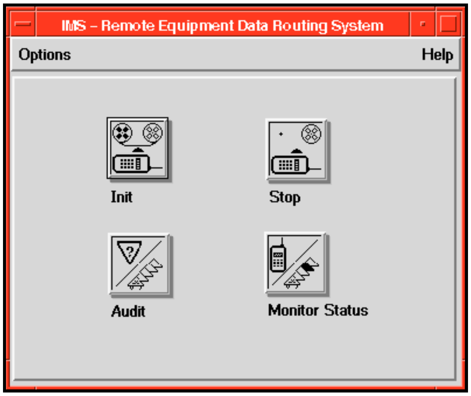
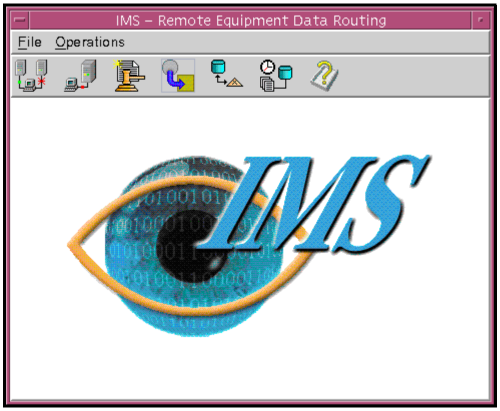


Figure 6.2 Main window of Interception Management System (G10)



Initialising a warrant (Dom) or Creating a warrant (G10)

This section shows you how to set up the IMS database for interceptions. After you type in and send all the data required for the interception, the relevant NE begin the interception immediately. Data about calls made to and from the target subscriber’s number are sent to a specified law enforcement monitoring facility (LEMF), together with the voice or data contents of those calls if requested.

To initialise (Dom) or create (G10) a warrant

1. Click the Init (Dom) or Create Warrant (G10) icon in the IMS – Remote Equipment Data Routing System window.
   - For Domestic, the Init dialog box displays (Figure 6.3 on page 6-11).
   - For G10, the Select Network Elements dialog box displays (Figure 6.5 on page 6-12) before the Create Warrant dialog box is displayed (Figure 6.6 on page 6-12).
2. Complete the Init dialog box.

Item — *Procedure*

MNN — Monitored Network Number (MNN) is the number of the target subscriber whose incoming and outgoing calls are to be intercepted.

1. Click the **MNN** choice button.
2. Type the target subscriber’s number in the **MNN** dialog box when it appears.
3. Retype the target subscriber’s number when the **MNN** dialog box reappears to double-check that you typed the number correctly.

IMEI — International Mobile Equipment Identifier (IMEI) is the equipment identifier of the target subscriber’s mobile or cell telephone whose incoming and outgoing calls are to be intercepted.

1. Click the **IMEI** choice button.
2. Type the target subscriber’s equipment identifier in the **IMEI** dialog box when it appears.
3. Retype the target subscriber’s number when the **IMEI** dialog box reappears to double-check that you typed the number correctly.

Item — *Procedure*

IMSI

International Mobile Subscriber Identifier (IMSI) is the subscriber identifier of the target subscriber’s mobile or cell telephone whose incoming and outgoing calls are to be intercepted.

1. Click the **IMSI** choice button.
2. Type the target subscriber’s identifier in the **IMSI** dialog box when it appears.
3. Retype the target subscriber’s number when the **IMSI** dialog box reappears to double-check that you typed the number correctly.

SF

Click this to generate a data product whenever the subscriber’s mobile or cell telephone moves from one cell to another.

Network ID (G10)

- Click the button and select the network operator ID.

Subnet ID (G10)

- Click the button and select the subnet operator ID.

MNN is PABX Number (G10)

- Click the check box to enable the PABX Name entry field.

PABX Name (G10)

- Type the optional name of a PABX if the subscriber’s number is an extension connected to a PABX.

Interception Reference

This is the number of the agency used as an extra key to initiate a warrant that has the MNN or IMEI and MUID set up already.

Note: This can be used to initiate another interception on the same MNN by entering a different reference number. However, the earlier warrant for the same MNN (with a different interception reference) must have been terminated.

Network Element/Group

(Domestic)

Normally a NE or NE group is chosen for connection to a target subscriber’s telephone or other service.

1. Select either the **Single NE** or **Group NE** choice button.
2. Click the **Network Element/Group** button.
3. Select either a single NE or group of NE from the **Network Element List** dialog box.

Note: For G10, this step occurs prior to the Create Warrant dialog box displaying. As a result, the Network Elements are not editable from here.

Item *Procedure*

DT

The DT (delivery type) field specifies which data channels are to be sent to the LEMF and whether one or two trunk lines are to be used.

Note: DT can only be used when DMO (data monitoring only) is off.

1. Click the DT radio button.
2. Click check boxes in the Enter DT dialog box to activate the delivery of the required channels (Figure 6.4 on page 6-11).

   VCE Voice data

   UDI Unrestricted digital information

   F31 3.1 kHz audio or data

   AVF Alternate voice or facsimile

   DFA Data or facsimile
3. Click a radio button for each activated channel to set the number of trunk lines to be used.

   1 Both data transmitted from and received by the monitored number is sent to the LEMF via a single trunk line.

   2 Data transmitted from the monitored number is sent to the LEMF via one trunk line and date received via another trunk line.
4. Click Apply.

LEMF-A

A primary law enforcement monitoring facility (LEMF) must be selected. Make sure that the LEMF is the correct centre for the requesting agency.

- Click the LEMF-A button and select the LEMF from the **LEMF Network Elements List** dialog box.

LEMF-B

The secondary LEMF is optional but must be different from the LEMF-A if added.

- Click the LEMF-B button and select the optional secondary LEMF.

Suppress MNN? (G10)

- Select No to include the target subscriber’s number in the IMS data product (DP).
  or
  Select Yes to exclude the subscriber’s number.

Item	*Procedure*
Start Time (G10)	This is the date and time the interception is to begin. 1 Click the button and type the date in `dd/mm/yyyy` format and the time in 24-hour `hh:mm` format when the **Start Time** dialog box appears. 2 Retype the date and time when the **Confirm Start Time** dialog box appears to double-check that you have typed these correctly. You can configure the confirmation as explained in Chapter 2. **Note:** Step 2 is only applicable if the IMSAttributes file is configured to request the Start Time twice.
Stop Time (G10)	This is the date and time the interception is to end. 1 Click the button and type the date in `dd/mm/yyyy` format and the time in 24-hour `hh:mm` format when the **Stop Time** dialog box appears. 2 Retype the date and time when the **Confirm Stop Time** dialog box appears to double-check that you have typed these correctly. You can configure the confirmation as explained in Chapter 2. **Note:** Step 2 is only applicable if the IMSAttributes file is configured to request the Stop Time twice.
Interception Reference (G10)	Number or other reference on the agency document authorising the current interception.
Internal Reference (G10)	• Type the monitoring agency's code for this interception.
Agency Name (G10)	The name of the authority that requested the current interception, for example, the police.
Agency Contact Details (G10)	Name, address, telephone number and other contact information for the authorising agency.
Legal Basis (G10)	The statute, regulation, or act of parliament that permits the current interception.
Closed User Group (G10)	You can only type in this text box when the Data Monitoring Only check box is cleared. • Type the numeric code corresponding to the closed user group.

Item *Procedure*

Network Identifier (G10)

- You can only type in this text box when the Data Monitoring Only check box is cleared.
- Type the type of network, for example, `ISDN` or `PSDN`.

Notes (G10)

Additional details about the interception that do not fit into the other fields of this dialog box.

Data Monitoring Only

A warrant with this option does not capture the voice content of calls for LEMF, only information *about* calls, such as called parties' numbers, calling parties' numbers, times and duration of calls, successful connections, unsuccessful connections, hang-ups before connection, and other similar data.

- Click the **Data Monitoring Only** check box to retrieve only information *about* monitored calls, not their contents, as required by agencies.

  or

- Clear the **Data Monitoring Only** check box to capture all interception data, including the voice and data content of monitored calls. This will cause all the monitoring centre number buttons to be selectable (MCMCNB, SCMCNBI, SCMCNB2, etc.).

MCMCNB

Multiple Call Monitoring Centre Number (MCMCNB) is a number used for the transfer of speech content. Note that it is the last resort used when all the single-call monitoring centre numbers (SCMCNB) are busy.

The MCMCNB field must always contain a number for Package 6 but must always be *blank* for Package 5 or Cellnet. The number can consist of up to 28 digits.

1. Type the MCMCNB in the MCNB dialog box when it shows.
2. Re-type the MCMCNB when the MCNB dialog box redisplays to double-check that you have typed the number correctly.

Item	*Procedure*
SCMCNB1 *to* SCMCNB10	Single Call Monitoring Centre Numbers (SCMCNB) are used to transfer the speech content of a single subscriber-to-subscriber connection. If a call involves many such connections, each will be assigned its own SCMCNB until none remain. These numbers can consist of up to 28 digits. SMNCNB1 is the first secondary diversion number supplied by the monitoring agency to which voice or data content of monitored calls is to be diverted. SMNCNB2 to SMNCNB10 are optional secondary diversion numbers. 1 Type the SCMCNB in the MCNB dialog box when it shows. 2 Re-type the SCMCNB when the MCNB dialog box re-displays to double-check that you have typed the number correctly.

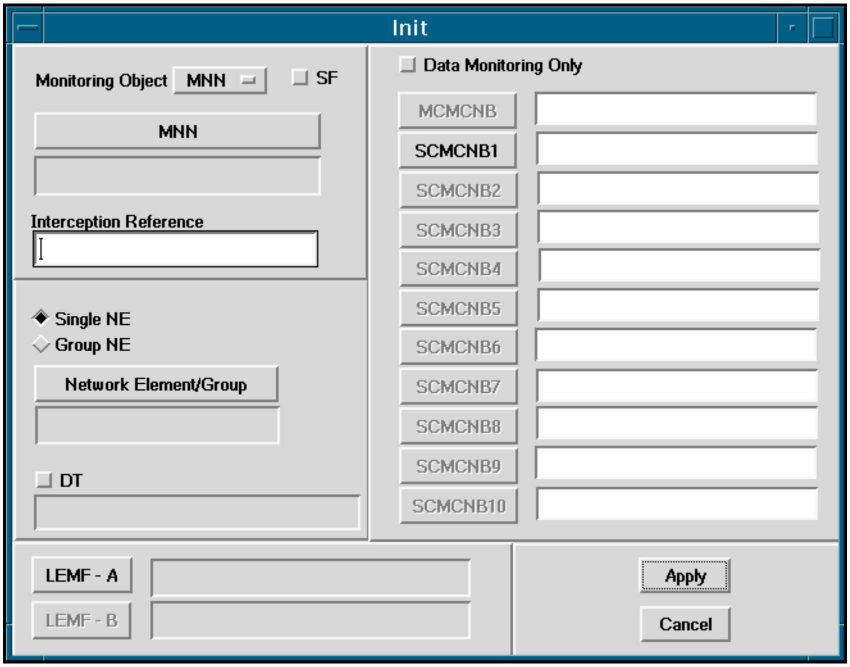
3. Click on the **Apply** button.

   The details of the warrant are added to the IMS database and the instructions are sent to activate the warrant in the NE or elements.

4. Check whether the warrant activated successfully.

   For the procedure, see ‘Monitoring warrant status’ on page 6-23.

Figure 6.3 Init Dialog Box (Dom)



Monitoring Object MNN

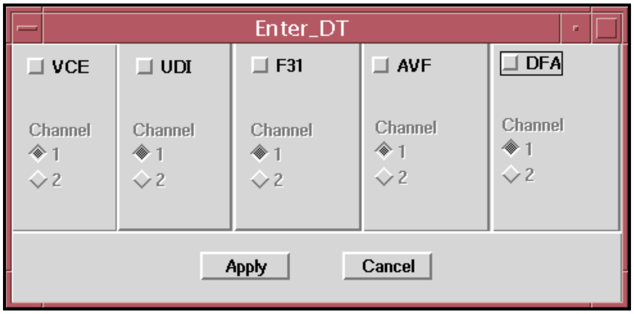
□ SF

◆ Single NE
◇ Group NE

□ DT

□ Data Monitoring Only

Figure 6.4 Enter DT Dialog Box



□ VCE Channel ◆ 1 ◇ 2

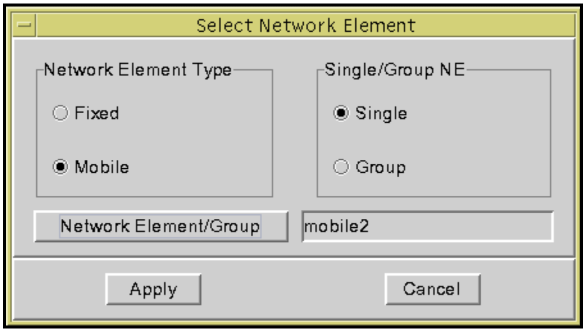
□ UDI Channel ◆ 1 ◇ 2

□ F31 Channel ◆ 1 ◇ 2

□ AVF Channel ◆ 1 ◇ 2

□ DFA Channel ◆ 1 ◇ 2

Figure 6.5 Select Network Element Dialog Box



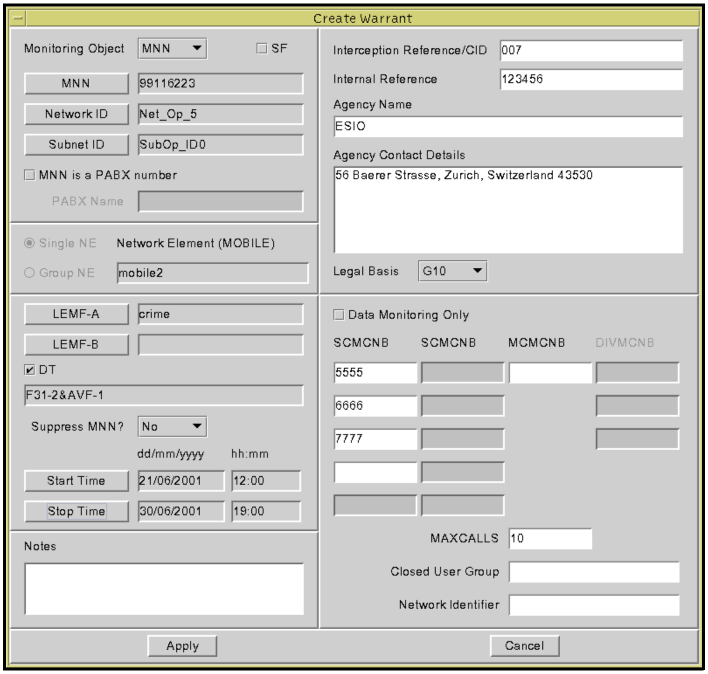
Select Network Element

Network Element Type
○ Fixed
● Mobile

Single/Group NE
● Single
○ Group

Network Element/Group: mobile2

Figure 6.6 Create Warrant Dialog Box (G10)



Create Warrant

Monitoring Object: MNN
□ SF
MNN: 99116223
Network ID: Net_Op_5
Subnet ID: SubOp_ID0
□ MNN is a PABX number
PABX Name:

● Single NE
○ Group NE
Network Element (MOBILE): mobile2

LEMF-A: crime
LEMF-B:
☑ DT
F31-2&AVF-1
Suppress MNN?: No

	dd/mm/yyyy	hh:mm
Start Time	21/06/2001	12:00
Stop Time	30/06/2001	19:00

Notes:

Interception Reference/CID: 007
Internal Reference: 123456
Agency Name: ESIO
Agency Contact Details: 56 Baerer Strasse, Zurich, Switzerland 43530
Legal Basis: G10

□ Data Monitoring Only

SCMCNB	SCMCNB	MCMCNB	DIVMCNB
5555			
6666			
7777			

MAXCALLS: 10
Closed User Group:
Network Identifier:

Stopping a warrant (Dom)

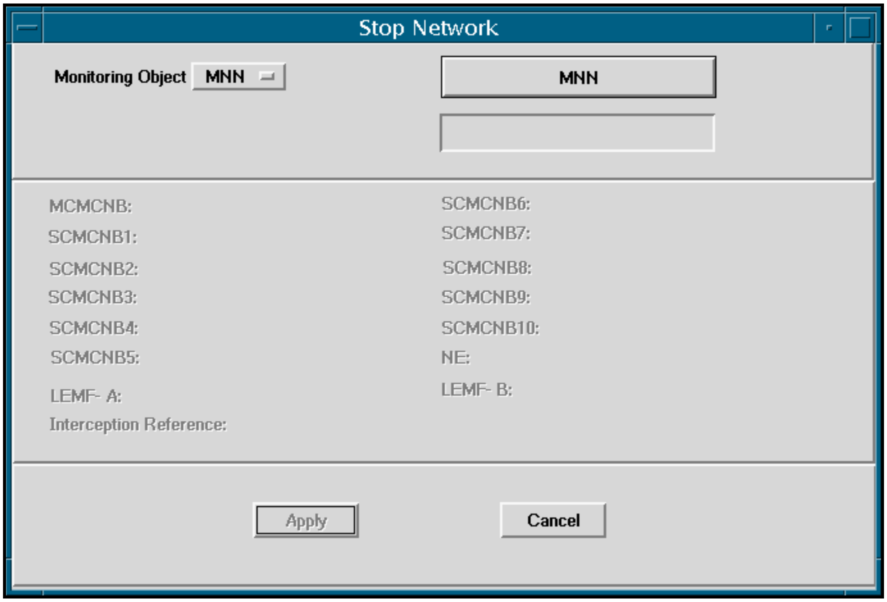
After you initially enter the details of a new interception into IMS, the monitoring authority may request changes. For example, they may want to end an interception.

To stop a warrant

1 Click the **Stop** icon in the **IMS – Remote Equipment Data Routing System** window.

The **Stop Network** dialog box appears (Figure 6.7 below).

Figure 6.7 Stop Network Dialog Box (Dom)



Monitoring Object MNN

2 Complete the Stop Network dialog box.

a Click on the Monitoring Object button (MNN shows by default) and select MNN, IMEI or IMSI from the drop-down menu to change the button label and also the name of the field button to the right of the screen.

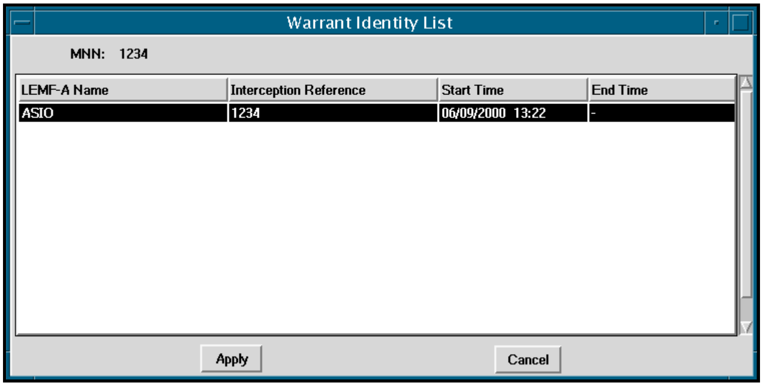
b Click on the MNN, IMEI or IMSI button to open the appropriate dialog box.

c Type the number or identifier then click on the Apply button.

d Retype the number to confirm that you have typed it correctly, then click on the Apply button.

This displays the Warrant Identity List dialog box (Figure 6.8 below) showing details of the warrants for the selected MNN, IMEI or IMSI that appear in the Stop Network dialog box.

Figure 6.8 Warrant Identity List Dialog Box



MNN: 1234

LEMF-A Name	Interception Reference	Start Time	End Time
ASIO	1234	06/09/2000 13:22	-

3 Select from the list the warrants required to be deleted.

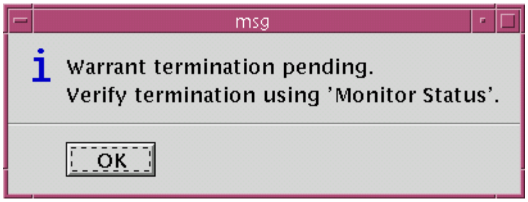
4 Click the **Apply** button on the **Warrant Identity List** dialog box.

The **Stop Network** dialog box shows details of the warrant selected for termination.

5 Click the **Apply** button on the **Stop Network** dialog box.

The **msg** dialog box displays.

Figure 6.9 msg Dialog Box



Warrant termination pending.
Verify termination using 'Monitor Status'.

6 Click on the **OK** button.

Commands to terminate the warrant should now have been sent to the appropriate NE and the IMS Administration Database should show a **TERM** state on the warrant.

Modifying a warrant (G10)

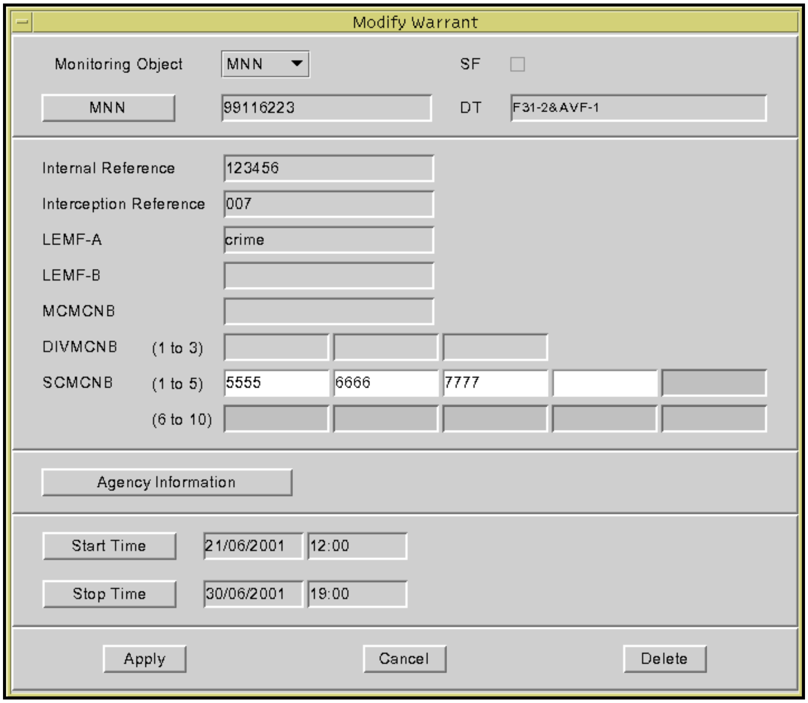
After you initially enter the details of a new interception (the warrant) into the IMS database, the monitoring authority may request changes. For example, they may want to end an interception, or extend or shorten the period of an interception.

To modify a warrant

1 Click the Modify Warrant icon in the IMS – Remote Equipment Data Routing System window.

The Modify Warrant dialog box appears (Figure 6.10).

Figure 6.10 Modify Warrant Dialog Box (G10)



Monitoring Object: MNN
SF ☐
MNN: 99116223
DT: F31-2&AVF-1
Internal Reference: 123456
Interception Reference: 007
LEMF-A: crime
LEMF-B:
MCMCNB:
DIVMCNB (1 to 3):
SCMCNB (1 to 5): 5555 6666 7777
(6 to 10):
Start Time: 21/06/2001 12:00
Stop Time: 30/06/2001 19:00

2 Complete the Modify Warrant dialog box.

a Select MNN, IMEI or IMSI from the drop-down list or choice buttons as required.

The label of the button below changes appropriately.

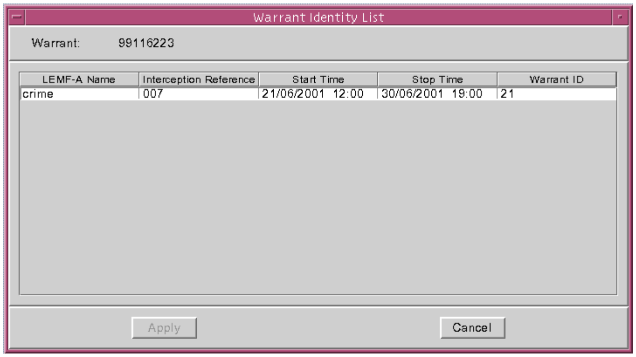
b Click on the button.

c Type the target subscriber’s MNN, IMEI or IMSI number in the Number dialog box when it appears, and click on the Apply button.

d If your configuration file requires it, retype the target number when the Number dialog box reappears to confirm that you have typed the correct number then click on the Apply button.

The Warrant Identity List dialog box appears (Figure 6.11).

Figure 6.11 Warrant Identity List Dialog Box (G10)



Warrant: 99116223

LEMF-A Name	Interception Reference	Start Time	Stop Time	Warrant ID
crime	007	21/06/2001 12:00	30/06/2001 19:00	21

e Select the appropriate LEMF for the chosen target number and click the Apply button.

The details of the interception appear in the Modify Warrant dialog box.

3 Click the Delete button if the interception warrant is to be removed.

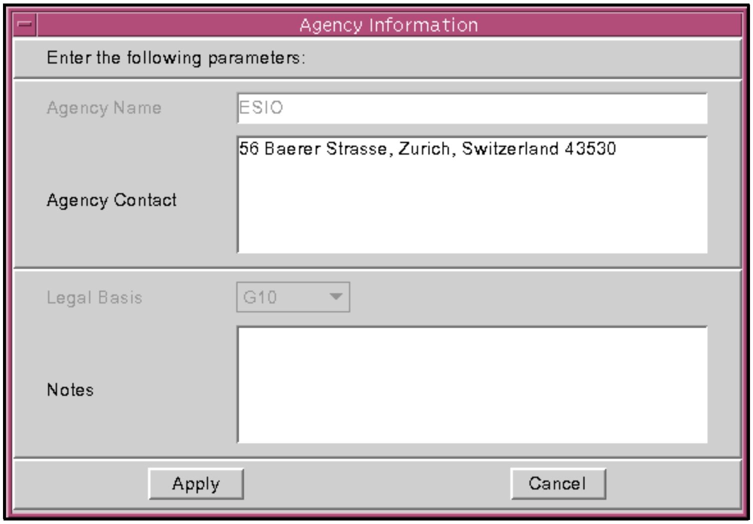
Note: This can only be done for warrants that are not currently ACTIVATED.

4 Click the Agency Information button if the agency details are to be changed.

Note: This can only be done if the warrant has not TERMINATED.

The Agency Information dialog box then displays.

Figure 6.12 Agency Information Dialog Box



Agency Information

Enter the following parameters:

Agency Name: ESIO

Agency Contact: 56 Baerer Strasse, Zurich, Switzerland 43530

Legal Basis: G10

Notes:

Update the details as required. For entry details, see Step **2 on page 6-5**

5 Click the Start Time button and type a new date and time the interception is to begin, if required.

a Type the date in dd/mm/yyyy format and the time in 24-hour hh:mm format when the Start Time dialog box appears.

b Retype the date and time when the Confirm Start Time dialog box appears to confirm that you have typed these correctly. You can configure the confirmation, as explained in Chapter 2.

Note: This can only be performed if the Start Time has not expired.

6 Click the Stop Time button and type a new date and time the interception is to end, if required.

a Type the date in dd/mm/yyyy format and the time in 24-hour hh:mm format when the Stop Time dialog box appears.

b Retype the date and time when the Confirm Stop Time dialog box appears to confirm that you have typed these correctly. You can configure the confirmation, as explained in Chapter 2.

Note: This can only be performed if the Stop Time has not expired.

7 Editing SCMCNB fields.

If a warrant is allowed to have its SCMCNB fields edited, you can add, remove or edit existing SCMCNB numbers.

Caution: Removal of a SCMCNB number will also remove all numbers following for example: if there are 7 numbers, removing number 3 will also remove numbers 4, 5, 6 and 7.

8 Click the Apply button.

The Modify Warrant dialog box updates the IMS database with the changed details of the interception warrant and then closes.

Note: Warrants can only be modified if they are not TERMINATED.

Auditing the network

You may need to check what interceptions have been initiated for a particular NE or group of NE. You may also need to know which NE or groups of NE are actively intercepting calls and which subscribers are the targets of interceptions.

The audit function can be used to obtain these details. Audit also has the facility to synchronise the IMS and NE databases. Synchronising forces the specified NE to be updated based on the audit report contents.

Note: The IMS Database is assumed to be correct, hence all activations in the NE are synchronised to be consistent with the IMS Database.

To audit the network

1. Click the **Audit** icon in the **IMS – Remote Equipment Data Routing System** window.
   - For Domestic, the **Audit** dialog box appears (Figure 6.13 on page 6-20).
   - For G10, the Select Network Element dialog box displays first (Figure 6.5 on page 6-12).
2. Click either the **Single NE** or **Group NE** choice button on which an audit has to be performed, then click the **Network Element/Group** button.

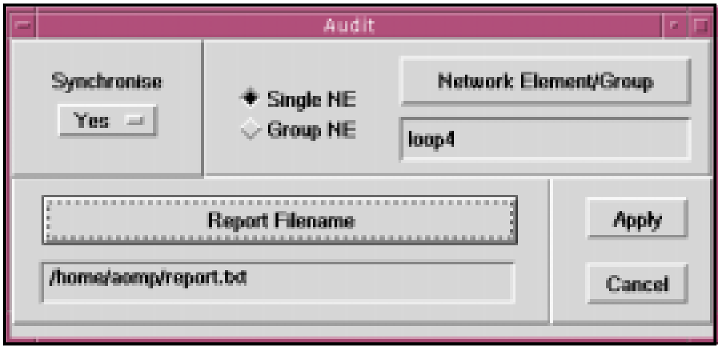
   The **LEMF Network Element List** dialog box lists either individual NE if you clicked **Single NE** or groups of NE if you clicked **Group NE**.
3. Click a single element or group from the list as appropriate.
4. Select **Synchronise** > **Yes** to force the specified NE to be updated based on the audit report file contents.

   or

   Select **Synchronise > No** to only check any discrepancy between IMS and NE databases, i.e. this will only report the differences without correcting the discrepancies.

Note: The Synchronise facility is available only when the Single NE option is selected.

Figure 6.13 Audit dialog box - Domestic



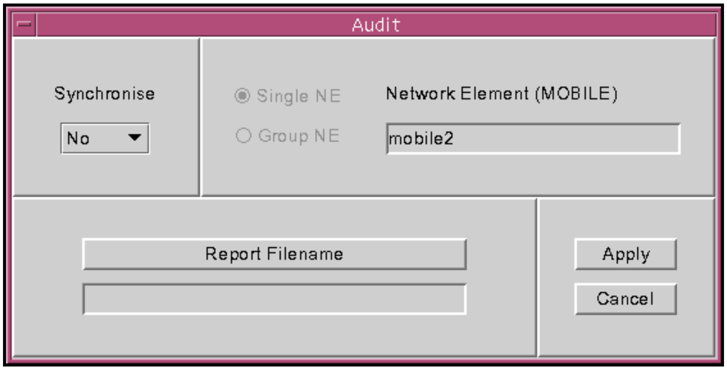
Synchronise: Yes

◆ Single NE
◇ Group NE

loop4

/home/aomp/report.txt

Figure 6.14 Audit dialog box - G10



Synchronise: No

● Single NE
○ Group NE

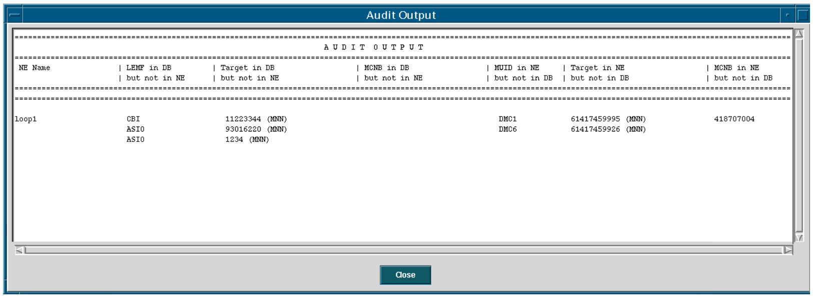
Network Element (MOBILE): mobile2

5 Click the **Report Filename** button and specify the directory and the name of the report file to be generated.

6 Click the **Apply** button to create the audit report file.

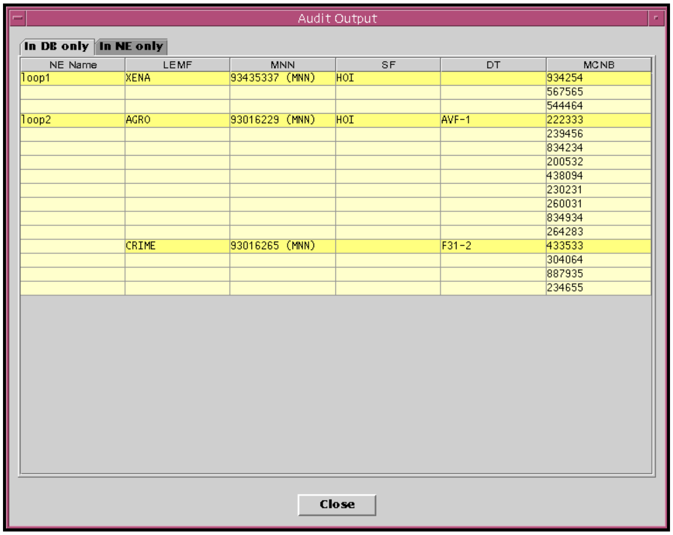
The **Audit Output** dialog box (Figure 6.15) displays the contents of the report file.

Figure 6.15 The Audit Output dialog box - Domestic



```
===========================================================================================================================================================================
                                                                      A U D I T   O U T P U T
===========================================================================================================================================================================
 NE Name               | LEMF in DB       | Target in DB                | MCNB in DB                  | MUID in NE     | Target in NE                | MCNB in NE
                       | but not in NE    | but not in NE               | but not in NE               | but not in DB  | but not in DB               | but not in DB
===========================================================================================================================================================================
===========================================================================================================================================================================

loop1                    CBI                 11223344  (MNN)                                             DMC1             61417459995  (MNN)            418707004
                         ASIO                93016220  (MNN)                                             DMC6             61417459926  (MNN)
                         ASIO                1234  (MNN)
```

Figure 6.16 The Audit Output dialog box - G10



NE Name	LEMF	MNN	SF	DT	MCNB
loop1	XENA	93435337 (MNN)	HOI		934254
					567565
					544464
loop2	AGRO	93016229 (MNN)	HOI	AVF-1	222333
					239456
					834234
					200532
					438094
					230231
					260031
					834934
					264283
	CRIME	93016265 (MNN)		F31-2	433533
					304064
					887935
					234655

Explanation of Audit Output dialog box

The audit report file records the results of the performed audit. The **Audit Output** dialog box is interpreted as follows:

Column	*Explanation*
NE Name	Lists NE selected earlier, either singly or in a group.
LEMF	Law enforcement monitoring facility requesting the interception.
Target in DB but not in NE	Lists all MNN/IMEI/IMSI that are only registered in the IMS Database but are not activated in the NE.
MCNB in DB but not in NE	Shows the complete lists all MCNB discrepancies and the associated warrant the MCNB belongs to that are only registered in the IMS Database but are not activated in the NE.
MUID	Monitoring user ID for the interception.
Target in NE but not in DB	Lists all MNN/IMEI/IMSI that are not registered in the IMS Database but are activated in the NE.
MCNB in NE but not in DB	Shows the complete lists all MCNB discrepancies and the associated warrant the MCNB belongs to that are not registered in the IMS Database but are activated in the NE.

Note: The audit report will be empty if the two databases are synchronised. This means all the warrants in the IMS database are identical with those in the NE database.

Monitoring warrant status

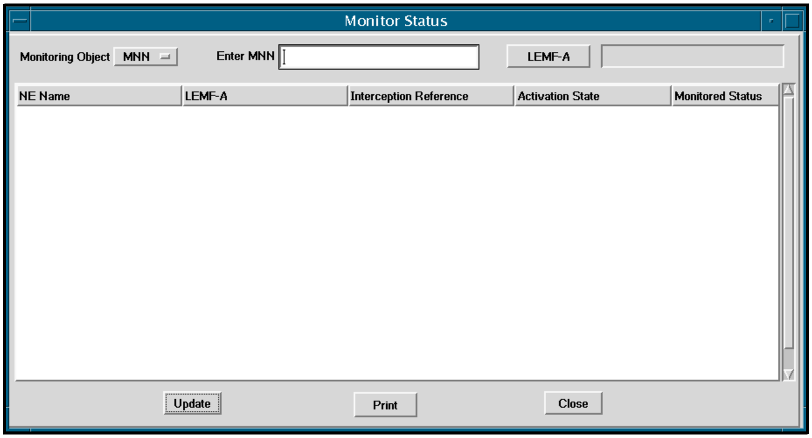
This function checks whether a given subscriber's number (monitored network number – MNN) is being monitored currently by particular NE. It should be used to check whether a warrant activated immediately after attempting an activation.

To monitor the status of warrants

1 Click the **Monitor Status** icon in the **IMS – Remote Equipment Data Routing System** window.

The **Monitor Status** dialog box appears (Figure 6.17 below).

Figure 6.17 Monitor Status Dialog Box



2 Click the MNN, IMEI or IMSI option as required.

3 Type the target number/identifier (MNN, IMEI or IMSI) into the **Enter MNN** field. Optionally, click on the **LEMF-A** button to specify the LEMF, and click the **Updat**e button.

The **Monitor Status** dialog box shows which NE are monitoring the target subscriber's number (*see* 'Explanation of Monitor Status dialog box' on page 6-24).

4 Initiate, extend, or delete a warrant if necessary.

- To cause a NE to begin monitoring, see 'Initialising a warrant (Dom) or Creating a warrant (G10)' on page 6-5.
- To stop a NE from monitoring, see 'Stopping a warrant (Dom)' on page 6-13.

- To activate a NOT_ACTIVATED warrant (G10), see ‘Modifying a warrant (G10)’ on page 6-15

Explanation of Monitor Status dialog box

You interpret the values in the columns of the **Monitor Status** dialog box as follows:

Column	*Explanation*
NE Name	Lists all NE capable of monitoring the target subscriber’s number.
LEMF-A	Lists all or selected primary LEMF to which data is routed for the specified warrant.
Interception Reference	Reference of the agency if IMS successfully activated the warrant in NE.
Activation State	- `NOT USED` – A warrant is initialised with a NE that has just been created. - `ACTIVATION FAILED` – Warrant activation has failed for any of several reasons; see ‘Warrant activation-failure’ below. - `ACTIVATED` – The warrant’s starting time has occurred and the NE is monitoring the subscriber’s number. - `ACTIVATE PENDING` – A warrant has been activated but the process is pending. - `NOT ACTIVATED` – A warrant has been initialised but the starting time has not occurred yet. - `TERMINATED`– The warrant’s stopping time has occurred and the NE is no longer monitoring the subscriber’s number. - `TERMINATED PENDING` – A warrant has been terminated but the process is pending. - `TERMINATED FAIL` – A warrant has been terminated but the process has failed.
Monitored Status	- `UNKNOWN` – A warrant is initialised but the processing for monitoring that warrant is still not complete. - `MONITORED` – IMS successfully initiated the warrant in the NE. - `NOT MONITORED` – IMS has not initiated the warrant in the NE.

The following table shows this in brief:

	Monitor State		
Activation State	UNKNOWN	NOT_MONITORED	MONITORED
NOT USED			
NOT_ACTIVATED	New warrant		
ACTIVATE_PENDING		Running and retrying	
ACTIVATE_FAILED		Finished and failed (including partial failure[*])	
ACTIVATED			Success
TERMINATE_PENDING			Running and retrying
TERMINATE_FAILED			Finished and failed (including partial failure[*])
TERMINATE		Success	

[*] Partial failure refers to the situation where only a subset of the commands are sent because the next command failed.

Warrant activation-failure A warrant can fail to activate for several reasons:

- The NE may be busy and unable to process the activation commands.
- The X25 link is down.
- The NE in not operating, for example, a switch may be restarting.

Activation failure records alarms in the alarm-log file, which can be examined in the Transaction Log window – see the *XMATE Operator Manual*, LZBP 101 294. The warrant activation process retries a number of times at specified intervals which are set up during installation in the IMS configuration files – see Chapter 2, ‘Installing and Configuring IMS’.

To print or save the status of warrants (Dom)

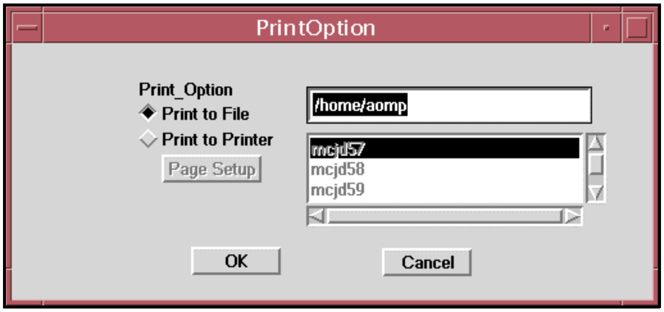
1 Click the **Print** button in the **Monitor Status** dialog box.

The **Print Option** dialog box appears (Figure 6.18).

2 Save the warrant activation status list to a file or print it out.

- Click the **Print to File** button, type a path and file name, and click **OK**.
- Click the **Print to Printer** button, click on a printer name, click on **Page Setup** and edit the dialog box, and click **OK**.

Figure 6.18 Print Dialog Box



PrintOption

Print_Option
◆ Print to File
◇ Print to Printer

/home/aomp

mcjd57
mcjd58
mcjd59

7 File Navigator

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	5/19817-CNAP 10211 Uen		
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2001-01-11	**Revision** A	**Pages** 10

Utility to search files

In this chapter

The File Navigation feature allows you to search for output files in IMS. This chapter looks at using this feature.

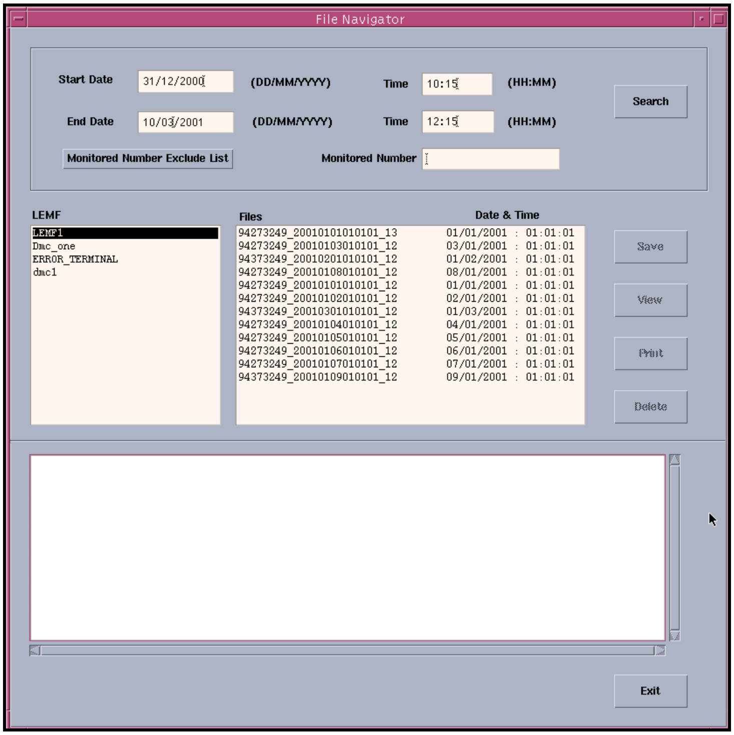
Introduction

Up to three Printout Description (POD) output files are generated each time a call is monitored using IMS.

The File Navigator utility allows you to search for each of these files based on their Date, Time and the Target No (inclusive and exclusive) and only these files are displayed. File Navigator also allows the ongoing maintenance of these files.

Accessing the File Navigator

Right-click on your desktop and select IMS Operator then File Navigator. This displays the File Navigator window as follows:



Start Date 31/12/2000 (DD/MM/YYYY) Time 10:15 (HH:MM)

End Date 10/03/2001 (DD/MM/YYYY) Time 12:15 (HH:MM)

Monitored Number Exclude List

Monitored Number

LEMF

LEMF1
Dmc_one
ERROR_TERMINAL
dmc1

Files	Date & Time
94273249_20010101010101_13	01/01/2001 : 01:01:01
94273249_20010103010101_12	03/01/2001 : 01:01:01
94373249_20010201010101_12	01/02/2001 : 01:01:01
94273249_20010108010101_12	08/01/2001 : 01:01:01
94273249_20010101010101_12	01/01/2001 : 01:01:01
94273249_20010102010101_12	02/01/2001 : 01:01:01
94373249_20010301010101_12	01/03/2001 : 01:01:01
94273249_20010104010101_12	04/01/2001 : 01:01:01
94273249_20010105010101_12	05/01/2001 : 01:01:01
94273249_20010106010101_12	06/01/2001 : 01:01:01
94273249_20010107010101_12	07/01/2001 : 01:01:01
94373249_20010109010101_12	09/01/2001 : 01:01:01

Figure 7.1 File Navigator Window

Using File Navigator

Files Navigator allows you to search for files based on a number of options. These are:

- All numbers
- Date
- Date and time
- Individual monitored number
- All number except for those selected
- A combination of options

Once the search results are known you can then perform the following maintenance options:

- View
- Save
- Print
- Delete

Searching

All numbers

This lets you access the files for all monitored numbers.

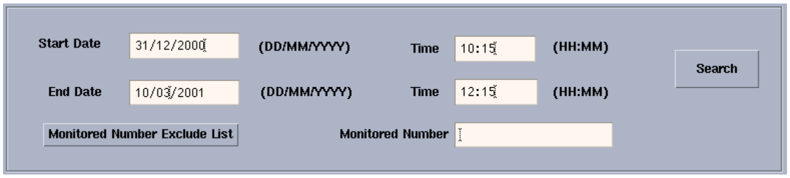
The steps are as follows:

1. Make certain all fields are empty of data.
2. Click on the **Search** button shown in Figure 7.2 below.

   This will display all LEMF.
3. Click on the required LEMF.

   All files for that LEMF will be displayed.

The following fields are used when searching on specific data:



Start Date 31/12/2000 (DD/MM/YYYY) Time 10:15 (HH:MM)

End Date 10/03/2001 (DD/MM/YYYY) Time 12:15 (HH:MM)

Monitored Number

Figure 7.2 Search Fields

Date

This lets you access files based on a particular date range.

Note: While you can stipulate a start and end date, you can also have just a start date or an end date for the search. If you only enter in a start date, all files since that date will be listed. If you only enter an end date, all files up to that date will be listed.

The steps are as follows:

1 Enter data in the **Start Date** and **End Date** fields.

2 Click on the **Search** button.

This will display all LEMF with files created within the date range.

3 Click on the required LEMF.

All files for the LEMF that meet the search criteria will be displayed.

Date and time

This lets you access files based not only on the date they were created but also based on the time.

Note: While you can stipulate a start and end date, you can also have just a start date or an end date for the search. If you only enter in a start date, all files since that date will be listed. If you only enter an end date, all files up to that date will be listed.

The Time fields are associated with the corresponding date field and if no dates have been chosen, the date for the search will be the current date.

The steps are as follows:

1 Enter in the required date (see ‘Date’ above).

2 Enter in the time(s) as required.

3 Click on the **Search** button.

This will display all LEMF with files meeting the search criteria.

4 Click on the required LEMF.

All files for the LEMF that meet the search criteria will be displayed.

Individual monitored number

This lets you access the files for a particular monitored number.

The steps are as follows:

1 Enter the required number in the **Monitored Number** field.

2 Click on the **Search** button.

This will display all files associated with that number.

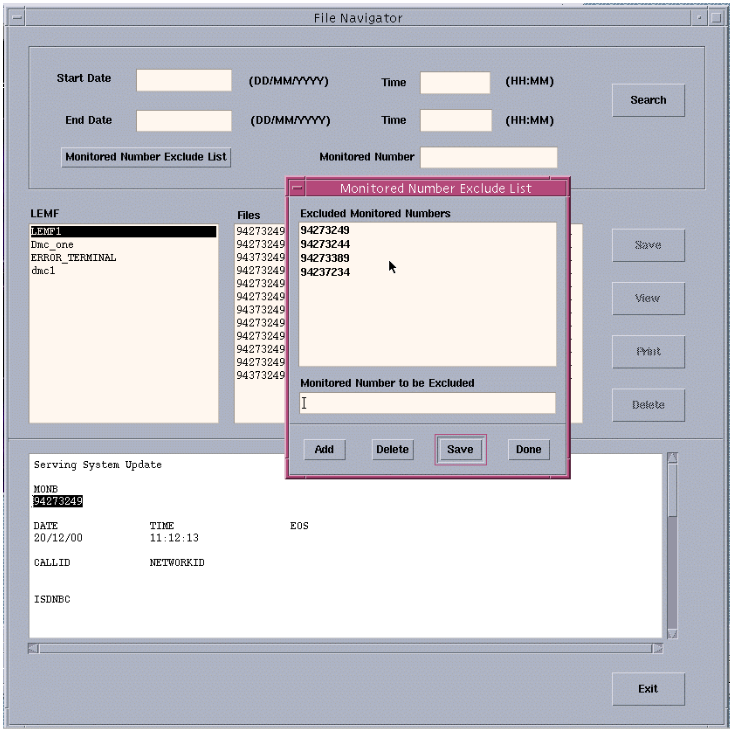
All numbers except for those selected

This lets you access the files for all numbers except those you select.

The steps are as follows:

1. Click on the **Monitored Number Exclude List** button.

   This displays the following dialog box:



LEMF:

```
LEMF1
Dmc_one
ERROR_TERMINAL
dmc1
```

Files:

```
94273249
94273249
94373249
94273249
94273249
94273249
94373249
94273249
94273249
94273249
94273249
94373249
```

Excluded Monitored Numbers:

```
94273249
94273244
94273389
94237234
```

```
Serving System Update

MONB
94273249

DATE                TIME                    EOS
20/12/00            11:12:13

CALLID              NETWORKID


ISDNBC
```

Figure 7.3 Monitored Number Exclude List Dialog Box

2. Enter the numbers to be **excluded** in the **Monitored Data to be Excluded** field then click on the **Add** button.

   This will add the number to the list above.

3. At this point you can either save the list by clicking on the **Save** button (see ‘Save’ below) or you can continue by clicking on the **Done** button.

4 Click on the **Search** button.

5 This will display the LEMF **not** associated with numbers in the exclusion list.

6 Click on the required LEMF.

All files for the LEMF that meet the search criteria will be displayed.

A combination of options

You can also enter a number of different options at the same time by entering in dates, times, a monitored number or any combination of these items.

Once the data is entered, click on the **Search** button and results appropriate to your selection will display.

Maintenance

There are a number of file maintenance options available after a search has been performed. They are:

- View
- Save
- Print
- Delete

View

This lets you view the contents of a file.

1 Click on the LEMF required then click on the file.

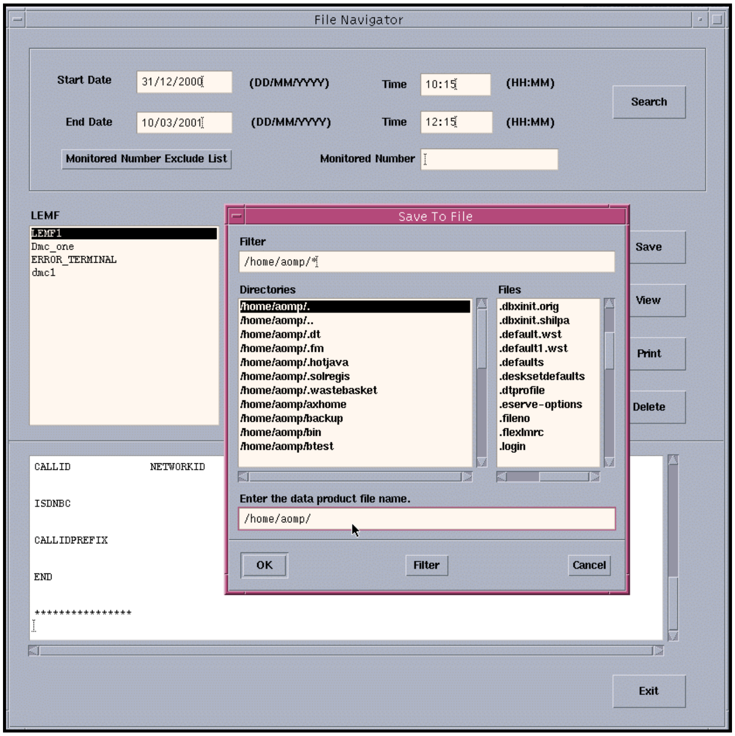
2 Click on the **View** button.

This displays the data in the file.

Save

This allows you to save the data displayed.

1 After you have found a file you are searching for (see previous options), click on the **Save** button to display the following dialog box:



Start Date 31/12/2000 (DD/MM/YYYY) Time 10:15 (HH:MM)
End Date 10/03/2001 (DD/MM/YYYY) Time 12:15 (HH:MM)
Monitored Number

LEMF
LEMF1
Dmc_one
ERROR_TERMINAL
dmc1

```
CALLID                NETWORKID

ISDNBC

CALLIDPREFIX

END

****************
```

Filter
/home/aomp/*

Directories	Files
/home/aomp/.	.dbxinit.orig
/home/aomp/..	.dbxinit.shilpa
/home/aomp/.dt	.default.wst
/home/aomp/.fm	.default1.wst
/home/aomp/.hotjava	.defaults
/home/aomp/.solregis	.desksetdefaults
/home/aomp/.wastebasket	.dtprofile
/home/aomp/axhome	.eserve-options
/home/aomp/backup	.fileno
/home/aomp/bin	.flexlmrc
/home/aomp/btest	.login

Enter the data product file name.
/home/aomp/

Figure 7.4 Save To File Dialog Box

2 Enter the path and file name, then click on the **OK** button.

The data is now saved to the required location.

Print

This option allows you to print out the file selected.

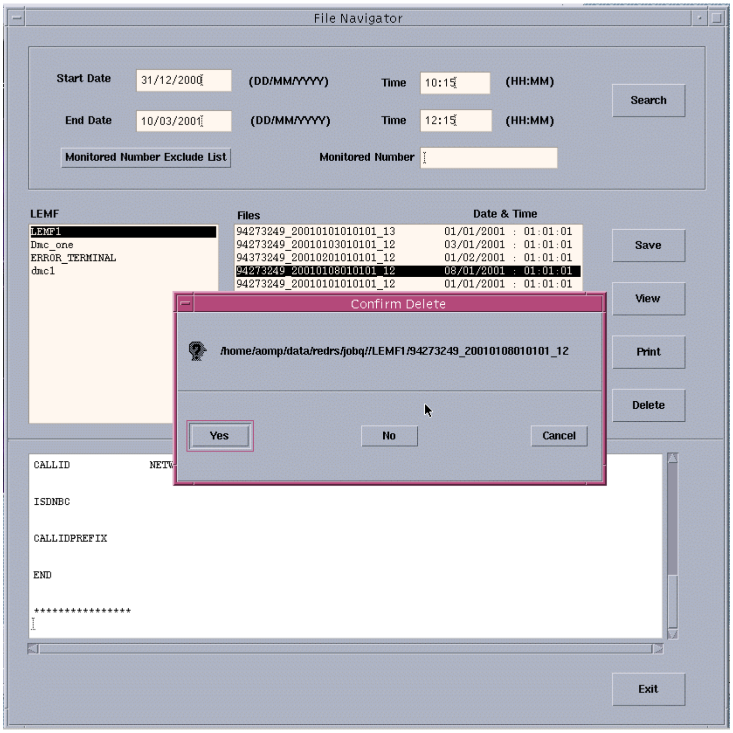
1 After you have found the file(s) you require (see previous options), click on the ones you want to print to highlight them.

2 Click on the **Print** button and the file(s) selected will be printed.

Delete

1 After you have located the file(s) required (see previous), highlight those to be deleted.

2 Click on the Delete button. This displays the following dialog box for you to confirm the deletion:



Start Date 31/12/2000 (DD/MM/YYYY) Time 10:15 (HH:MM)

End Date 10/03/2001 (DD/MM/YYYY) Time 12:15 (HH:MM)

Monitored Number

LEMF

```
LEMF1
Dmc_one
ERROR_TERMINAL
dmc1
```

```
Files                              Date & Time
94273249_20010101010101_13         01/01/2001 : 01:01:01
94273249_20010103010101_12         03/01/2001 : 01:01:01
94373249_20010201010101_12         01/02/2001 : 01:01:01
94273249_20010108010101_12         08/01/2001 : 01:01:01
94273249_20010101010101_12         01/01/2001 : 01:01:01
```

/home/aomp/data/redrs/jobq//LEMF1/94273249_20010108010101_12

```
CALLID              NETW

ISDNBC

CALLIDPREFIX

END

****************
```

Figure 7.5 Confirm Delete Dialog Box

3 Click on the **Yes** button to confirm.

STRICTLY CONFIDENTIAL

8 IMS Command-Log Printout Descriptions

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	1/190 83-CNAP 102 11 Uen
Approved by	EPA/D/N:(Peter Martiniello)	**Revision date**	2000-09-13
Revision	S	**Pages**	10

Introduction

This document contains the printout descriptions of the messages that are stored in the XMATE Transaction Log, **`acaui`**, as a result of an operator or system administrator action.

Warrant States in Alarm Log

When a command log entry is made, it may have one of two warrants as follows:

For WRCRI:

- NOT ACTIVATED
- ACTIVATED

For WRCRR:

- ACTIVATED
- TERMINATED

For WRBLI:

- ACTIVATED
- TERMINATED

The following is possible because the logging of the event and the sending of the commands are independent of each other.

For WRCRI e.g. if the sending of the commands is delayed and logging occurs first, then the warrant state will be NOT ACTIVATED.

If the commands are sent and the response is a success then the logging will indicate a warrant state of ACTIVATED.

Printout Messages

This document describes commands that IMS sends to the switch along with the internal messages IMS records in the command log.

AXE MML Commands

The following details the MML commands which are sent to the switch via IMS. The formats supported by IMS are listed along with each command.

For detailed information on these commands, refer to the appropriate command description.

RCMUI: Remote Control Equipment Monitoring User Initiate

Format: All formats are supported.[1]

RCMUE: Remote Control Equipment Monitoring User End

Format: All formats are supported.[2]

RCSUI: Remote Control Equipment Subscriber Initiate

Format: Local 7 - Only formats 2 and 3 are supported.[3]

Note: The MAXCALL parameter is not currently supported.

Format: Local 5 - Only format 2 is supported.[7]

Note: SUPPR, CUG and NI parameters are not currently supported.

RCSUE: Remote Control Equipment Subscriber End

Format: Local 7 - Only formats 1and 2 are supported.[4]

Format: Local 5 - All formats are supported.[9]

RCSTC: Remote Control Equipment Speech Transfer Change

Format: Only formats 1and 2 are supported.[5]

Note: The SUPPR, CUG and NI parameters are not currently supported.

RCSUP: Remote Control Equipment Subscriber Data Print

Format: Local 7- Only formats 1and 2 are supported.[6]

Format: Local 5 - All formats are supported.[8]

ANS Commands (G10)

RCSUI: Remote Control Equipment Subscriber Initiate

```
Parameters:MONB=monb, MUID=muid, CTYPE=ctype, MISC=misc,
           SUPPR=suppr, MAXCALL=maxcall, PASSWD=passwd,
           CUG=cug, NI=ni, MCNB=mcnb, SCMCNB1=scmcnb1,
           SCMCNB2=scmcnb2, SCMCNB3=scmcnb3, SCMCNB4=scmcnb4,
           DIVMCNB1=divmcnb1, DIVMCNB2=divmcnb2,
           DIVMCNB3=divmcnb3;
```

Parameter Definitions:

CUG=cug	Closed User Group number. This parameter is used to specify the closed user group which is to be used for speech transfer. The value can be NONE.
DIVMCNB=divmcnb	Diverted Monitoring Centre Number.
MONB=monb	Monitored network number. Up to 25 characters.
MUID=muid	Monitoring user ID. Up to 8 characters. MUID is only sent if simultaneous monitoring is activated in the exchange.
NI=ni	Network Identifier. The Network Identifier gives the network that is responsible for administration.
PASSWD=passwd	AXE security password.
SCMCNB=scmcnb	Single Call Monitoring Number.

RCSUE:Remote Control Equipment Subscriber End

```
Parameters:MONB=monb,MUID=muid;
```

RCSUP:Remote Control Equipment Subscriber Data Print

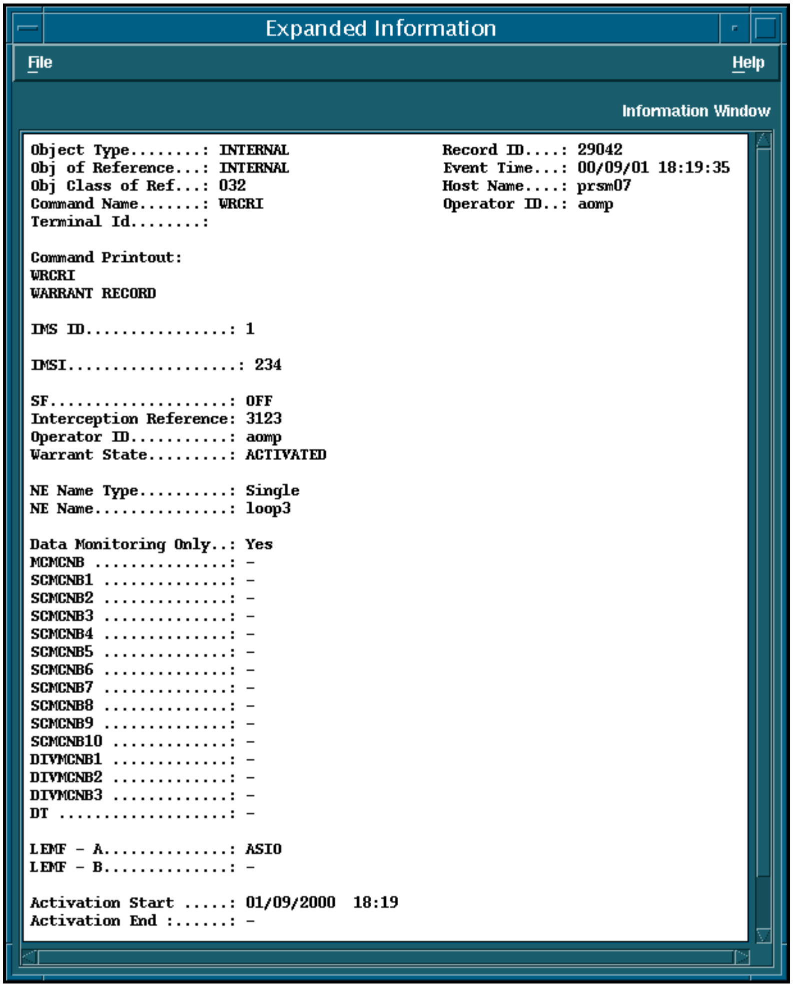
```
Parameters::[MONB=all, MUID=all];
```

IMS Internal Messages

Message WRCRI - Warrant Create Initiate

The following is an example of the message stored in the command log when the operator adds a new warrant record to the IMSDBIF database. This happens when the operator activates a warrant.

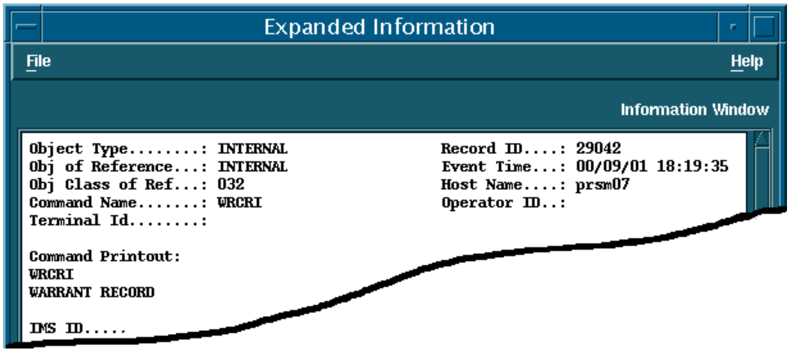
Figure 8.1 WRCRI Message



```
Object Type........: INTERNAL                    Record ID....: 29042
Obj of Reference...: INTERNAL                    Event Time...: 00/09/01 18:19:35
Obj Class of Ref...: 032                         Host Name....: prsm07
Command Name.......: WRCRI                       Operator ID..: aomp
Terminal Id........:

Command Printout:
WRCRI
WARRANT RECORD

IMS ID...............: 1

IMSI..................: 234

SF...................: OFF
Interception Reference: 3123
Operator ID..........: aomp
Warrant State........: ACTIVATED

NE Name Type.........: Single
NE Name..............: loop3

Data Monitoring Only..: Yes
MCMCNB ..............: -
SCMCNB1 .............: -
SCMCNB2 .............: -
SCMCNB3 .............: -
SCMCNB4 .............: -
SCMCNB5 .............: -
SCMCNB6 .............: -
SCMCNB7 .............: -
SCMCNB8 .............: -
SCMCNB9 .............: -
SCMCNB10 ............: -
DIVMCNB1 ............: -
DIVMCNB2 ............: -
DIVMCNB3 ............: -
DT ..................: -

LEMF - A.............: ASIO
LEMF - B.............: -

Activation Start .....: 01/09/2000  18:19
Activation End :......: -
```

The following is an example of the message stored in the command log when the NE is restarted and re-synchronised.

Figure 8.2 WRCRI Message after NE restart



```
Object Type........: INTERNAL                    Record ID....: 29042
Obj of Reference...: INTERNAL                    Event Time...: 00/09/01 18:19:35
Obj Class of Ref...: 032                         Host Name....: prsm07
Command Name.......: WRCRI                       Operator ID..:
Terminal Id........:

Command Printout:
WRCRI
WARRANT RECORD

IMS ID.....
```

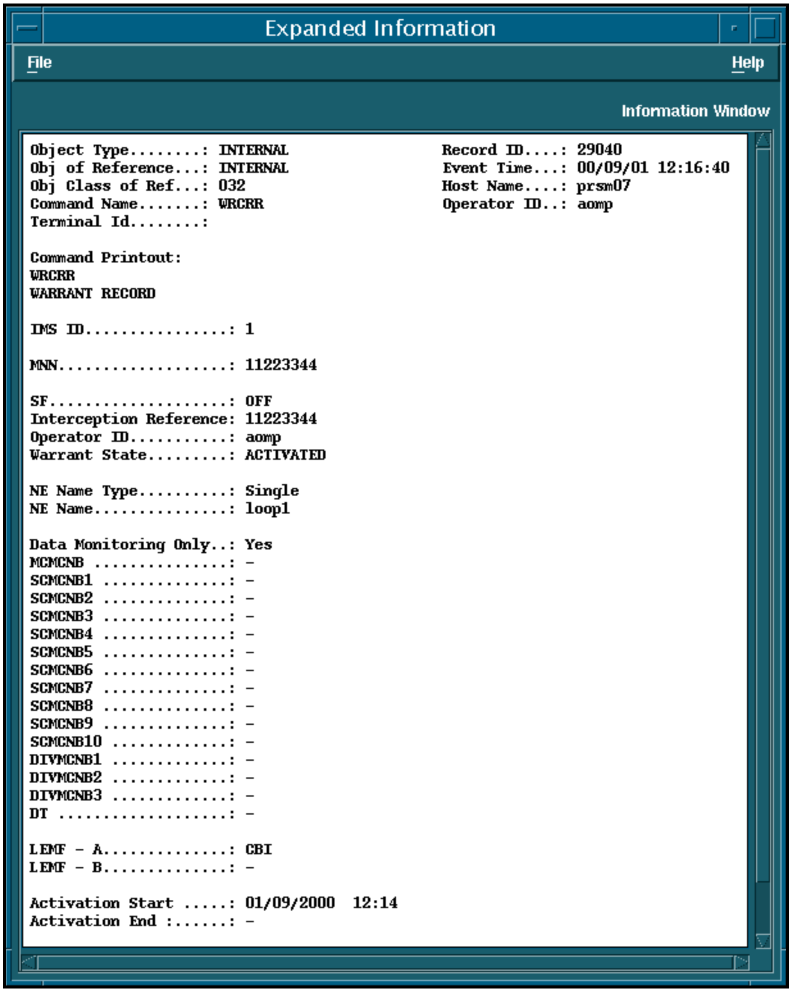
This occurs when a Restart fault code is received and the NE in question is re-synchronised, i.e., re-populated with the warrants it had.

Note that the header is the same as when a warrant was created except for the operator ID which is empty.

Message WRCRR - Warrant Create Remove

The following is an example of the message stored in the command log when the operator removes a warrant record from the IMSDBIF database.

Figure 8.3 WRCRR Message

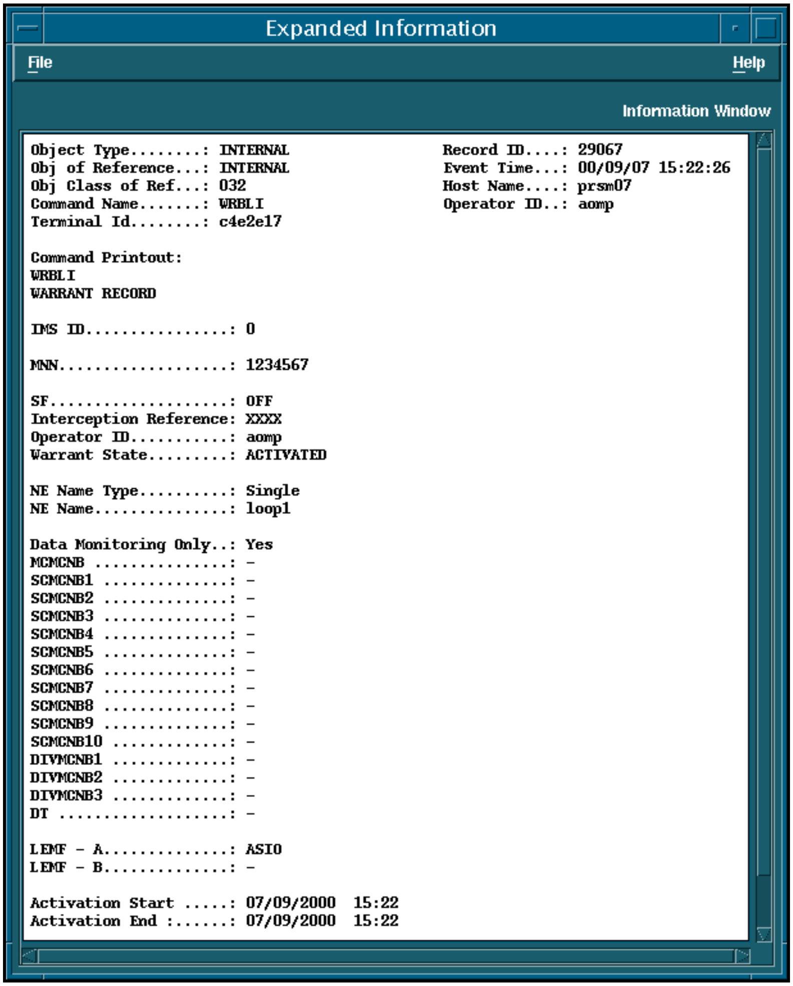


```
Object Type........: INTERNAL                   Record ID....: 29040
Obj of Reference...: INTERNAL                   Event Time...: 00/09/01 12:16:40
Obj Class of Ref...: 032                        Host Name....: prsm07
Command Name.......: WRCRR                      Operator ID..: aomp
Terminal Id........:

Command Printout:
WRCRR
WARRANT RECORD

IMS ID...............: 1

MNN..................: 11223344

SF...................: OFF
Interception Reference: 11223344
Operator ID..........: aomp
Warrant State........: ACTIVATED

NE Name Type.........: Single
NE Name..............: loop1

Data Monitoring Only..: Yes
MCMCNB ..............: -
SCMCNB1 .............: -
SCMCNB2 .............: -
SCMCNB3 .............: -
SCMCNB4 .............: -
SCMCNB5 .............: -
SCMCNB6 .............: -
SCMCNB7 .............: -
SCMCNB8 .............: -
SCMCNB9 .............: -
SCMCNB10 ............: -
DIVMCNB1 ............: -
DIVMCNB2 ............: -
DIVMCNB3 ............: -
DT ..................: -

LEMF - A.............: CBI
LEMF - B.............: -

Activation Start .....: 01/09/2000  12:14
Activation End :......: -
```

Message WRBLI - Warrant Block Initiate

The following message is stored in the command log when the operator terminates a warrant.

Figure 8.4 WRBLI Message

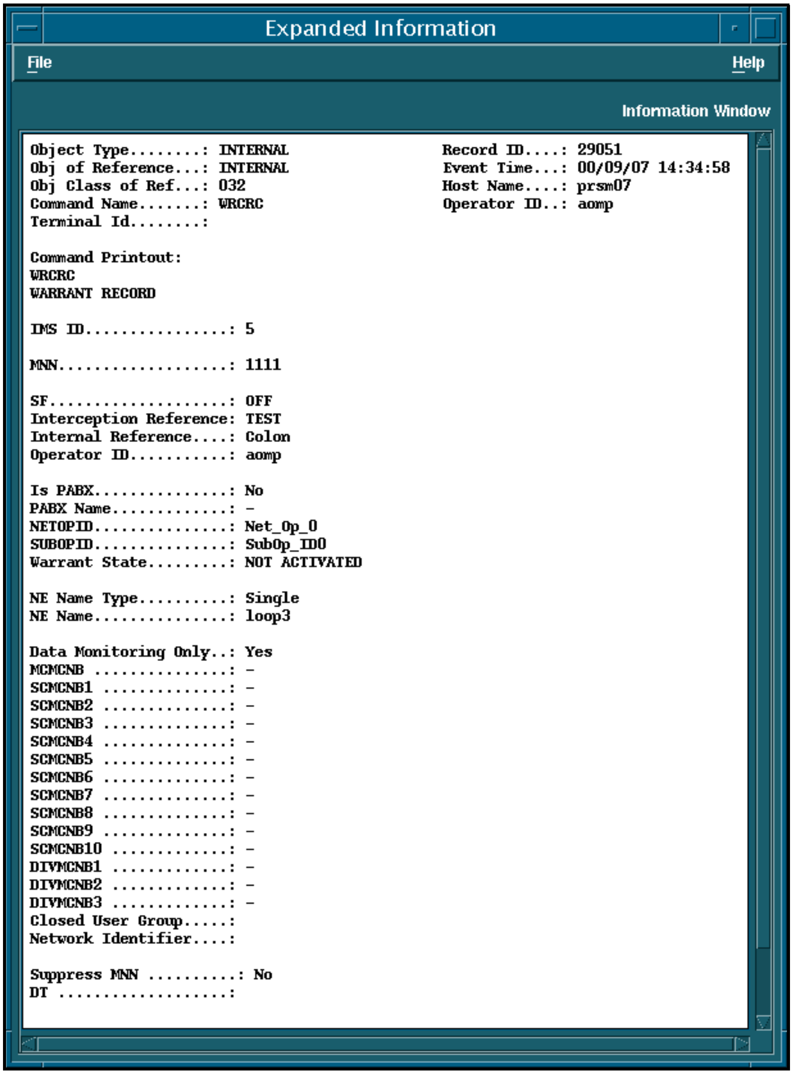


```
Object Type........: INTERNAL                    Record ID....: 29067
Obj of Reference...: INTERNAL                    Event Time...: 00/09/07 15:22:26
Obj Class of Ref...: 032                         Host Name....: prsm07
Command Name.......: WRBLI                       Operator ID..: aomp
Terminal Id........: c4e2e17

Command Printout:
WRBLI
WARRANT RECORD

IMS ID................: 0

MNN...................: 1234567

SF....................: OFF
Interception Reference: XXXX
Operator ID...........: aomp
Warrant State.........: ACTIVATED

NE Name Type..........: Single
NE Name...............: loop1

Data Monitoring Only..: Yes
MCMCNB ...............: -
SCMCNB1 ..............: -
SCMCNB2 ..............: -
SCMCNB3 ..............: -
SCMCNB4 ..............: -
SCMCNB5 ..............: -
SCMCNB6 ..............: -
SCMCNB7 ..............: -
SCMCNB8 ..............: -
SCMCNB9 ..............: -
SCMCNB10 .............: -
DIVMCNB1 .............: -
DIVMCNB2 .............: -
DIVMCNB3 .............: -
DT ...................: -

LEMF - A..............: ASIO
LEMF - B..............: -

Activation Start .....: 07/09/2000  15:22
Activation End :......: 07/09/2000  15:22
```

Message WRCRC (G10)

The following is an example of the message stored in the command log when the operator changes warrant details in the IMSDBIF database.

Figure 8.5 WRCRC Message.



```
Object Type........: INTERNAL                     Record ID....: 29051
Obj of Reference...: INTERNAL                     Event Time...: 00/09/07 14:34:58
Obj Class of Ref...: 032                          Host Name....: prsm07
Command Name.......: WRCRC                        Operator ID..: aomp
Terminal Id........:

Command Printout:
WRCRC
WARRANT RECORD

IMS ID...............: 5

MNN..................: 1111

SF...................: OFF
Interception Reference: TEST
Internal Reference....: Colon
Operator ID...........: aomp

Is PABX...............: No
PABX Name.............: -
NETOPID...............: Net_Op_0
SUBOPID...............: SubOp_ID0
Warrant State.........: NOT ACTIVATED

NE Name Type..........: Single
NE Name...............: loop3

Data Monitoring Only..: Yes
MCMCNB ...............: -
SCMCNB1 ..............: -
SCMCNB2 ..............: -
SCMCNB3 ..............: -
SCMCNB4 ..............: -
SCMCNB5 ..............: -
SCMCNB6 ..............: -
SCMCNB7 ..............: -
SCMCNB8 ..............: -
SCMCNB9 ..............: -
SCMCNB10 .............: -
DIVMCNB1 .............: -
DIVMCNB2 .............: -
DIVMCNB3 .............: -
Closed User Group.....:
Network Identifier....:

Suppress MNN ..........: No
DT ...................:
```

References

1 4/190 82-CNT 233 18 Rev B - RCMUI

2 6/190 82-CNT 233 18 Rev B - RCMUE

3 2/190 82-CNT 233 18 Rev B - RCSUI

4 1/190 82-CNT 233 18 Rev B - RCSUE

5 9/190 82-CNT 233 18 Rev B - RCSTC

6 3/190 82-CNT 233 18 Rev B - RCSUP

7 2/190 82-CNT 233 18/5 Rev B - RCSUI

8 3/190 82-CNT 233 18/5 Rev A - RCSUP

9 1/190 82-CNT 233 18/5 Rev A - RCSUE

9 IMS Alarm-Log Printout Descriptions

Prepared by	EPA/D/N: Bruce Ashley
Approved by	EPA/D/N: (Peter Martiniello)
Document no.	2/190 83-CNAP 102 11 Uen
Revision date	2000-09-13
Revision	S
Pages	28

STRICTLY CONFIDENTIAL

Introduction

This chapter lists examples of internal alarms which are forwarded to the XMATE IHS server to be stored in the alarms log. Each example is accompanied by an explanation of what the alarm means.

This alarm printout description is in line with general AXE printout standards.

Note: Not all alarms will be observed on any particular AXE system.

Alarm Printouts Examples

This section gives examples of alarm printouts from:

- Alarm printouts fixed network, page 9-4
- Mobile switching centre (MSC) alarms descriptions, page 9-14
- Access node switch (ANS) alarms descriptions (G10), page 9-16
- Internal IMS Alarms, page 9-19

Alarm printouts fixed network

Fault code 11: COF congestion

Indicates that a data product contains fault code 11. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 11: COF CONGESTION.
NE
ne
END
```

This alarm is applicable for the Local 5 market only.

Fault code 12: Fault or congestion at call setup to monitoring centre

Indicates that a data product contains fault code 12. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 12: FAULT OR CONGESTION AT CALL SETUP TO
MONITORING CENTER.
NE
ne
END
```

This alarm is applicable for the Local 5 market.

Fault code 13: Fault in CCD/DMJ or no free CCD/DMJ individual

Indicates that a data product contains fault code 13. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 13: FAULT IN CCD/DMJ OR NO FREE CCD/DMJ
INDIVIDUAL.
NE
ne
END
```

This alarm is applicable for the Local 5 market.

Fault code 14: Time release, no answer from monitoring centre

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 14: TIME RELEASE, NO ANSWER FROM MONITORING
CENTRE.
NE
ne
END
```

This alarm is applicable for the Local 5 and Local 7 markets only.

Fault code 16: AXE restart/reload has taken place

Indicates that a data product contains fault code 16. The data product will be deleted.

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 16: AXE RESTART/RELOAD HAS TAKEN PLACE.
NE
ne
END
```

This alarm is applicable for the Local 5 (reload) and Local 7 (restart) markets.

Fault code 17: Printout queue exceeded

Indicates that a data product contains fault code 17. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 17: PRINTOUT QUEUE EXCEEDED.
NE
ne
END
```

This alarm is applicable for the Local 5 and Local 7 markets.

Fault code 18: No completion printout due to disconnection of call before B-answer or due to lack of B-answer

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 18: NO COMPLETION PRINTOUT DUE TO DISCONNECTION
OF CALL BEFORE B-ANSWER OR DUE TO LACK OF B-ANSWER.
NE
ne
END
```

This alarm is no longer applicable to the Local 5 and Local 7 markets at the request of Telstra.

Fault code 19: Speech transferred to MCN not possible

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED
FAULT CODE 19: SPEECH TRANSFERRED TO MCN NOT POSSIBLE.
NE
ne
END
```

This alarm is applicable for the Local 5 and Local 7 markets.

Fault code 22: Log fault

Indicates that a data product contains fault code 22. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A3/RED “IMS “U 971201 0948
FAULT CODE 22: LOG FAULT
END
```

This alarm is applicable for the Local 5 and Local 7 markets.

Fault code 25: Congestion or fault outside RES, full monitoring aborted

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 25: CONGESTION OR FAULT OUTSIDE RES, FULL
MONITORING ABORTED.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 26: Congestion or fault outside RES, speech monitoring not possible

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 26: CONGESTION OR FAULT OUTSIDE RES, SPEECH
MONITORING NOT POSSIBLE.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 28: Congestion or fault within RES ceased to exist

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 28: CONGESTION OR FAULT WITHIN RES CEASED TO
EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 29: B-number is busy

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 29: NO CALL COMPLETION PRINTOUT WILL BE GENERATED
DUE TO DISCONNECTION OF MONITORED CALLS.
NE
ne
END
```

This alarm is no longer applicable to the Local 5 and Local 7 markets at the request of Telstra.

Fault code 35: Monitored number is disconnected from exchange, thus number removed

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 35: MONITORED NUMBER IS DISCONNECTED FROM
EXCHANGE, THUS NUMBER REMOVED.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 60: Unauthorised access: illegal password entered in command

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 60: UNAUTHORISED ACCESS: ILLEGAL PASSWORD ENTERED
IN COMMAND.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 62: Unauthorised access: attempt to use illegal terminal

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 62: UNAUTHORISED ACCESS: ATTEMPT TO USE ILLEGAL
TERMINAL.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 80: Congestion in UUIND (RCELINK)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 80: CONGESTION IN UUIND (RCELINK).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 81: Congestion in UUIND (RCELINK) has ceased to exist.

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 81: CONGESTION IN UUIND (RCELINK) HAS CEASED TO
EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 82: Congestion fault in temporary call set up file CALLREF (RCEECH)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 82: CONGESTION FAULT IN TEMPOARY CALL SET UP FILE
CALLREF (RCEECH).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 83: Congestion fault in temporary call set up file WFCONNECT (RCEA)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 83: CONGESTION FAULT IN TEMPOARY CALL SET UP FILE
WFCONNECT (RCEA).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 84: Congestion in RCEH

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 84: THE CALLING PARTY NUMBER ANB IS NOT
NECESSARILY THE CALLING PARTY NUMBER OF THE CALL.
WFCONNECT (RCEH).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 90: Congestion in RCEADATA (RCEA)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 90: CONGESTION IN RCEADATA (RCEA).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 91: Congestion in RCEADATA (RCEA) has ceased to exist

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 91: CONGESTION IN RCEADATA (RCEA) HAS CEASED TO
EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 92: Congestion in USERDATA (RCEA)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 92: CONGESTION IN USERDATA (RCEA).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 93: Congestion in RCEADATA (RCEA) has ceased to exist

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 93: CONGESTION IN USERDATA (RCEA) HAS CEASED TO
EXIST.
```

```
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 94: Congestion in LEGDATA (RCEA)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 94: CONGESTION IN LEGDATA (RCEA).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 95: Congestion in LEGDATA (RCEA) has ceased to exist

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 95: CONGESTION IN LEGDATA (RCEA) HAS CEASED TO
EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 96: Congestion in RCECHDATA (RCECH)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 96: CONGESTION IN RCECHDATA (RCECH).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 97: Congestion in RCECHDATA (RCECH) has ceased to exist

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 97: CONGESTION IN RCECHDATA (RCECH) HAS CEASED TO
EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 98: Congestion in RCELINKDATA (RCELINK)

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 98: CONGESTION IN RCELINKDATA (RCELINK).
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Fault code 99: Congestion in RCELINKDATA (RCELINK) has ceased to exist

```
NE = INTERNAL; CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX XX/RED “IMS “U 971201 0948
FAULT CODE 99: CONGESTION IN RCELINKDATA (RCELINK) HAS
CEASED TO EXIST.
NE
ne
END
```

This alarm is applicable for the Local 7 market.

Mobile switching centre (MSC) alarms descriptions

Fault code 1: COF congestion

Indicates that a data product contains fault code 11. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 11: COF CONGESTION.
NE
ne
END
```

Fault code 2: Fault or congestion at call setup to monitoring centre

Indicates that a data product contains fault code 12. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 12: FAULT OR CONGESTION AT CALL SETUP TO
MONITORING CENTER.
NE
ne
END
```

Fault code 3: Fault in CCD/DMJ or no free CCD/DMJ individual

Indicates that a data product contains fault code 13. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 13: FAULT IN CCD/DMJ OR NO FREE CCD/DMJ
INDIVIDUAL.
NE
ne
END
```

Fault code 4: Time release, no answer from LEMF

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 14: TIME RELEASE, NO ANSWER FROM MONITORING
CENTRE.
NE
ne
END
```

Fault code 6: AXE restart/reload has taken place

Indicates that a data product contains fault code 16. The data product will be deleted.

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 16: AXE RESTART/RELOAD HAS TAKEN PLACE.
NE
ne
END
```

Fault code 7: Printout queue exceeded

Indicates that a data product contains fault code 17. The data product will be sent to the appropriate LEMF.

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 17: PRINTOUT QUEUE EXCEEDED.
NE
ne
END
```

Fault code 8: No completion printout due to disconnection of call before call set-up to monitoring centre

```
NE = INTERNAL; CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 18: NO COMPLETION PRINTOUT DUE TO DISCONNECTION
OF CALL BEFORE CALL SETUP TO MONITORING CENTRE.
NE
ne
END
```

Access node switch (ANS) alarms descriptions (G10)

Fault code 16: ANS restart/reload has taken place

Indicates that a data product contains fault code 16.

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
FAULT CODE 16: ANS RESTART/RELOAD HAS TAKEN PLACE
NE
ne
END
```

Fault code 17: Printout queue exceeded

Indicates that a data product contains fault code 17.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 17: PRINTOUT QUEUE EXCEEDED
NE
ne
END
```

Fault code 18: State Event error

Indicates that a data product contains fault code 18.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 18: STATE EVENT ERROR
NE
ne
END
```

Fault code 19: Data Range error

Indicates that a data product contains fault code 19.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 19: DATA RANGE ERROR
```

```
NE
ne
END
```

Fault code 20: Parameter error

Indicates that a data product contains fault code 20.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 20: PARAMETER ERROR
NE
ne
END
```

Fault code 21: Timeout error

Indicates that a data product contains fault code 21.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 21: TIMEOUT ERROR.
NE
ne
END
```

Fault code 22: Subscriber PID not found

Indicates that a data product contains fault code 22.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 22: SUBSCRIBER PID NOT FOUND
NE
ne
END
```

Fault code 23: OamOdth process not started

Indicates that a data product contains fault code 23.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
```

```
FAULT CODE 23: OAMODTH PROCESS NOT STARTED
NE
ne
END
```

Fault code 24: Data Manager error

Indicates that a data product contains fault code 24.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 24: DATA MANAGER ERROR
NE
ne
END
```

Fault code 25: CC Circuit not started

Indicates that a data product contains fault code 25.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 25: CC CIRCUIT NOT STARTED
NE
ne
END
```

Fault code 26: Query not found

Indicates that a data product contains fault code 26.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 26: QUERY NOT FOUND
NE
ne
END
```

Fault code 97: Connection to an ANS is down

Indicates that a data product contains fault code 97.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 97: CONNECTION TO AN ANS IS DOWN
NE
ne
END
```

Fault code 98: Connection to an ANS is restored

Indicates that a data product contains fault code 98.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 98: CONNECTION TO AN ANS IS RESTORED
NE
ne
END
```

Fault code 99: RES application error

Indicates that a data product contains fault code 99.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE 99: RES APPLICATION ERROR
NE
ne
END
```

Internal IMS Alarms

ATC: Activation event for warrant MMN = XXX is delayed due to Communication Failure

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: Activation event for warrant MNN = 987 is delayed due
to Communication Failure.
END
```

ATC: Activation event for warrant MMN = XXX is delayed due to FUNCTION BUSY condition

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED "IMS "U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: ACTIVATION EVENT FOR WARRANT MNN=987 IS DELAYED DUE TO
FUNCTION BUSY CONDITION.
END
```

ATC: Cannot access database

Cannot access IMSDBIF database to activate/ terminate the warrant for the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
ATC: CANNOT ACCESS DATABASE
END
```

ATC: cannot activate warrant because it is in terminated state

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED "IMS "U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: CANNOT ACTIVATE WARRANT BECAUSE IT IS IN TERMINATED
STATE
END
```

ATC: Cannot find warrant record in database

Cannot find warrant record in database to activate/ terminate the warrant for the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: CANNOT FIND WARRANT RECORD IN DATABASE
WN
wn
END
```

ATC: Could not open connection to NE

Could not open connection to NE to activate/terminate a warrant.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: COULD NOT OPEN CONNECTION TO NE
NE
ne
END
```

ATC: Error obtaining the password for the res ID 1 and res profile number 2

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED "IMS "U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC:  PROFILE VALUE FOR PASSWORD, RES I.D. X, PROFILE NUMBER
Y, RETURNED ERROR.
END
```

ATC: Open Connection Failed

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: Open Connection Failed
     NE     DC3
     NE3    prsm20
END
```

ATC: Unable to access primary DCS; secondary DCS was used to activate/terminate the warrant

```
NE = INTERNAL; LASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED "IMS "U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION
```

```
ATC: PRIMARY DCS GATEWAY XXX FOR WARRANT MNN=XXX WAS NOT
ACCESSIBLE. WARRANT WAS ACTIVATED SUCCESSFULLY VIA SECONDARY
DCS YYY.
END
```

ATC: Unable to send command to activate warrant for NE

Could not send command to activate a warrant

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: UNABLE TO SEND COMMAND TO ACTIVATE WARRANT FOR NE
NE
ne
END
```

ATC: Unable to send command to terminate warrant for NE

Could not send command to activate a warrant

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: UNABLE TO SEND COMMAND TO TERMINATE WARRANT FOR NE
NE
ne
END
```

ATC: Warrant activation failed

Warrant activation failed on the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: WARRANT ACTIVATION FAILED
NE  MNN
ne  mnn
MAXIMUM NUMBER OF TRIES ATTEMPTED
END
```

ATC: Warrant audit printout failed

Warrant audit printout failed.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
ATC: WARRANT AUDIT PRINTOUT FAILED
END
```

ATC: Warrant termination failed

Warrant termination failed on the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: Cannot terminate Warrant MNN = XXX in NE = nename
because it was never activated
END
```

ATC: RCMCI failure

RCMCI failed on the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: RCMCI FAILED.
END
```

ATC: RCSUI failure

RCSUI failed on the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: RCSUI FAILED. Command will not be retried
END
```

ATC: Warrant never activated

The warrant was never activated in the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: Warrant XXX was never activated in this NE: nename
END
```

ATC: Termination event

Warrant termination on the NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: Termination event for Warrant MNN = XXX
END
```

ATC: RCMCI failure (no more retry)

RCMCI failed on the NE and will not be retried.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX 22/IMSEVENTLOG "IMS Alarm Event Log"U 1647
FAULT CODE DURING WARRANT DE/ACTIVATION

ATC: RCMCI FAILED. Command will not be retried
END
```

Corrupt data packet

A data product from the specified NE is corrupt.

```
NE = INTERNAL;CLASS = 01; CATEGORY = APPLICATION;

*** ALARM XXX 01/RED “IMS “U 971201 0948
DATA PACKET CORRUPT
NE
ne
END
```

Data product conversion: Cannot access database

Cannot make data product during conversion process as the database is inaccessible.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
DATA PRODUCT CONVERSION: CANNOT ACCESS DATABASE
END
```

LEMF communication alarm

This alarm is generated when a data product could not be sent to a LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
UNABLE TO CONTACT LEMF (OR COMMUNICATION FAILED)
LEMF       HOST
lemf       host
END
```

LEMF communication alarm cease

This is generated when communication has been re-established with a LEMF.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
ALARM CEASE: COMMUNICATION WITH LEMF ESTABLISHED.
LEMF       HOST
lemf       host
END
```

LEMF congestion alarm

This alarm is generated when communication to a LEMF is taking longer than usual due to congestion in the network.

```
NE = INTERNAL;CLASS = A3; CATEGORY = APPLICATION;

*** ALARM XXX A3/RED “IMS “U 971201 0948
TIMEOUT: CONGESTION IN NETWORK (WARNING).
LEMF       HOST
lemf       host
END
```

LEMF congestion alarm cease

This alarm is generated when communication to a LEMF has been re-established.

```
NE = INTERNAL;CLASS = A3; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A3/RED “IMS “U 971201 0948
ALARM CEASE: LEMF CONGESTION RESOLVED.
LEMF       HOST
lemf       host
END
```

Invalid LEMF

Indicates that a MNN has been routed to an invalid LEMF (this happens if a MNN has been routed to a LEMF, and the LEMF is later deleted.) The data product will be sent to ERROR_TERMINAL.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
MNN routed to invalid LEMF
Data product rerouted to ERROR_TERMINAL
MNN
mnn
END
```

Invalid MNN

Indicates that a data product has arrived containing a MNN that is not in the internal routing table. The data product will be rerouted to ERROR_TERMINAL.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;
```

```
*** ALARM XXX A2/RED “IMS “U 971201 0948
MNN not in internal routing table
Data product rerouted to ERROR_TERMINAL
MNN
mnn
END
```

Number of incoming sessions exceeded

The maximum number of incoming sessions that IMS can handle has been exceeded. The NE from which the call was rejected is specified.

```
NE = INTERNAL;CLASS = A1; CATEGORY = APPLICATION;

*** ALARM XXX A1/RED “IMS “U 971201 0948
Maximum number of incoming sessions exceeded.
NE
ne
END
```

Timeout

This message is generated when communication with a LEMF has been initiated, but no signals have been received from it for a given timeout.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “IMS “U 971201 0948
TIMEOUT: NO REPLY RECEIVED FROM LEMF.
LEMF       HOST
lemf       host
END
```

Timeout (ordering process)

This message is generated when the ordering process was unable to contact an NE.

```
NE = INTERNAL;CLASS = A2; CATEGORY = APPLICATION;

*** ALARM XXX A2/RED “ORDERING PROCESS “U 971201 0948
NE       HOST
ne       dcs host
Reason for failure
END
```

References

1 RCEFILE for Local 7,
1/190 83-CNT 233 21/6 Uen Rev B

2 1/190 83-CNT 233 21 Uen Rev G

3 RCEFILE for Local 5,
1/190 83-CNT 233 09 Uen Rev A

10 LEMF Rerouting and Status

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	9/198 17-CNAP 102 11 Uen				
Approved by	EPA/D/N: (Peter Martiniello)	**Revision date**	2000-09-13	**Revision**	H	**Pages**	8

STRICTLY CONFIDENTIAL

Blocking and rerouting law enforcement monitoring facilities (LEMF) and viewing their current status

In this chapter

This chapter details how to block and reroute law enforcement monitoring facilities.

Scope

This function is used to block and reroute law enforcement monitoring facilities and to display their current status.

The LEMF Rerouting/Status dialog box is accessed from the Workspace Menu.

1 Click the right mouse button.

Workspace Menu is displayed.

2 Click on the IMS Administrator (or IMS Operator) with the left mouse button.

IMS options are displayed.

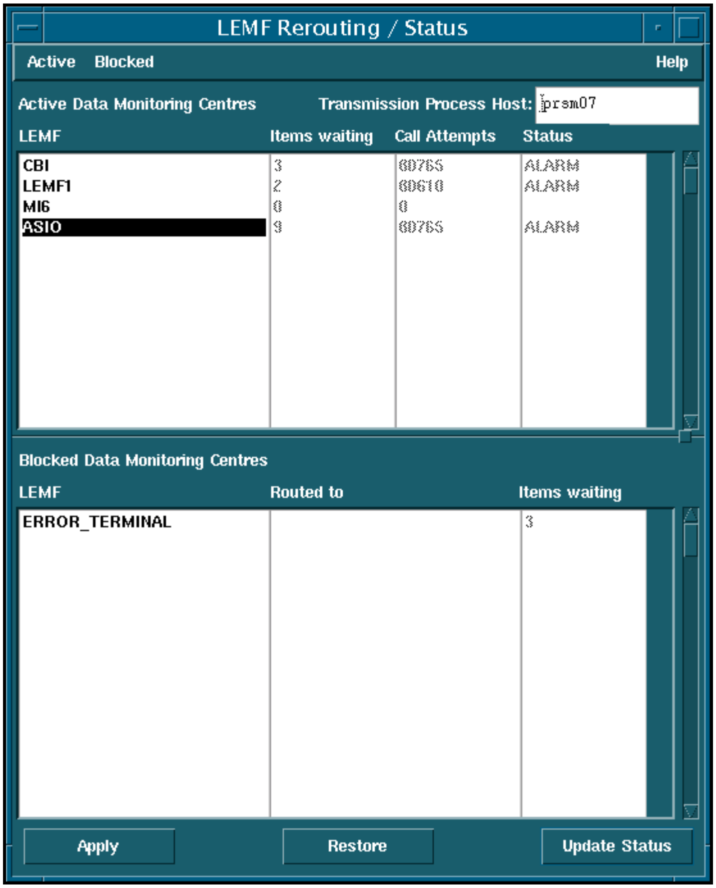
3 Click on the Rerouting option with the left mouse button.

The LEMF Rerouting/Status dialog box is displayed, Figure 10.1 overleaf.

The dialog box is in two parts, top part for active LEMF and the lower part for blocked LEMF.

4 Click on **Update Status** to view the current LEMF status.

Figure 10.1 LEMF Rerouting / Status dialog box



Active Data Monitoring Centres

Transmission Process Host: prsm07

LEMF	Items waiting	Call Attempts	Status
CBI	3	60765	ALARM
LEMF1	2	60610	ALARM
MI6	0	0	
ASIO	9	60765	ALARM

Blocked Data Monitoring Centres

LEMF	Routed to	Items waiting
ERROR_TERMINAL		3

For each active LEMF, the following information is displayed:

Items Waiting — The number of data products that have arrived in the system and are waiting to be transmitted to the LEMF. If -1 is displayed, the LEMF is invalid since this LEMF was deleted while active. Press Restore to remove it from the list.

Call Attempts — If transmission to a LEMF has been unsuccessful, this field shows the number of failed call attempts.

Status — This field will show ALARM if the LEMF is in an alarm state, or will be left blank if it is not. The LEMF will be in an alarm state if the number of unsuccessful call attempts have exceeded the predefined limit.

For each blocked LEMF, the following information is displayed:

Routed to — If the blocked LEMF has been rerouted to an active LEMF, this field will show the active LEMF. Otherwise, it will be blank.

Items Waiting — The number of data products that have arrived in the system and are waiting to be transmitted to the LEMF. If -1 is displayed, the LEMF is invalid since it was deleted while blocked. Press Restore to remove it from the list.

Blocking a LEMF

Blocking a LEMF means that all data products which are to be sent to that LEMF will be held in the system rather than be transmitted. They will be held until the LEMF is activated or rerouted.

To block a LEMF

1. Click on an active LEMF.
2. Choose the Block option from the Active drop-down menu.
3. Click the Apply button to complete the operation.

Activating a LEMF

Activating a LEMF means that data products held in the system for a particular LEMF will be sent to that LEMF.

To activate a LEMF

1. Click on a blocked LEMF.
2. Choose the Active option from the Blocked drop-down menu.
3. Click the Apply button to complete the operation.

NOTE **It is not possible to activate** the ERROR_TERMINAL or any LEMF that is rerouted.

Rerouting a LEMF

Rerouting a LEMF means that data products to be sent to that LEMF will be sent to another LEMF instead. It is only possible to reroute a blocked LEMF to an active LEMF. The ERROR_TERMINAL can be rerouted.

To reroute a LEMF

1. Block the LEMF if it is active, see 'To block a LEMF' on page 10-5.
2. Click on the blocked LEMF to reroute.
3. Click an active LEMF to reroute to.
4. Choose Add Route from the Blocked drop-down menu.
5. Click the Apply button to complete the operation.

End rerouting of a LEMF

To end rerouting of a LEMF means data products will no longer be sent to another LEMF.

To end rerouting of a LEMF

1. Click on the rerouted LEMF
2. Choose Drop Route from the Blocked drop-down menu.
3. Click the Apply button to complete the operation.

Status of LEMF

To display the status of all LEMF click on the Update Status button.

NOTE **It is only possible** to display the status if the transmission process is active.

Additional Features

Error Terminal

The error terminal is an internal destination that unresolved data products are sent to. It is always blocked.

Error Terminal can be rerouted to one of the non-blocked LEMF.

Apply & Restore

Any changes made to rerouting will not come into effect until the Apply button is clicked. A number of changes can be made, and then all applied at the same time.

If you make a mistake, click the Restore button to return the rerouting to the last applied state.

References

1 Chapter 4, ‘Administering the IMS Database’,
3/198 17-CNAP 102 11

2 WiOZ User Instruction,
1/198 17-CNAP 102 05

STRICTLY CONFIDENTIAL

11 IMS Billing Printout Descriptions

Prepared by	EPA/D/N: Bruce Ashley	**Document no.**	4/19817-CNAP 10211 Uen				
Approved by	EPA/D/N: (Elton Cross)	**Revision date**	2000-08-30	**Revision**	H	**Pages**	10

ERICSSON

STRICTLY CONFIDENTIAL

Procedures for billing monitored calls

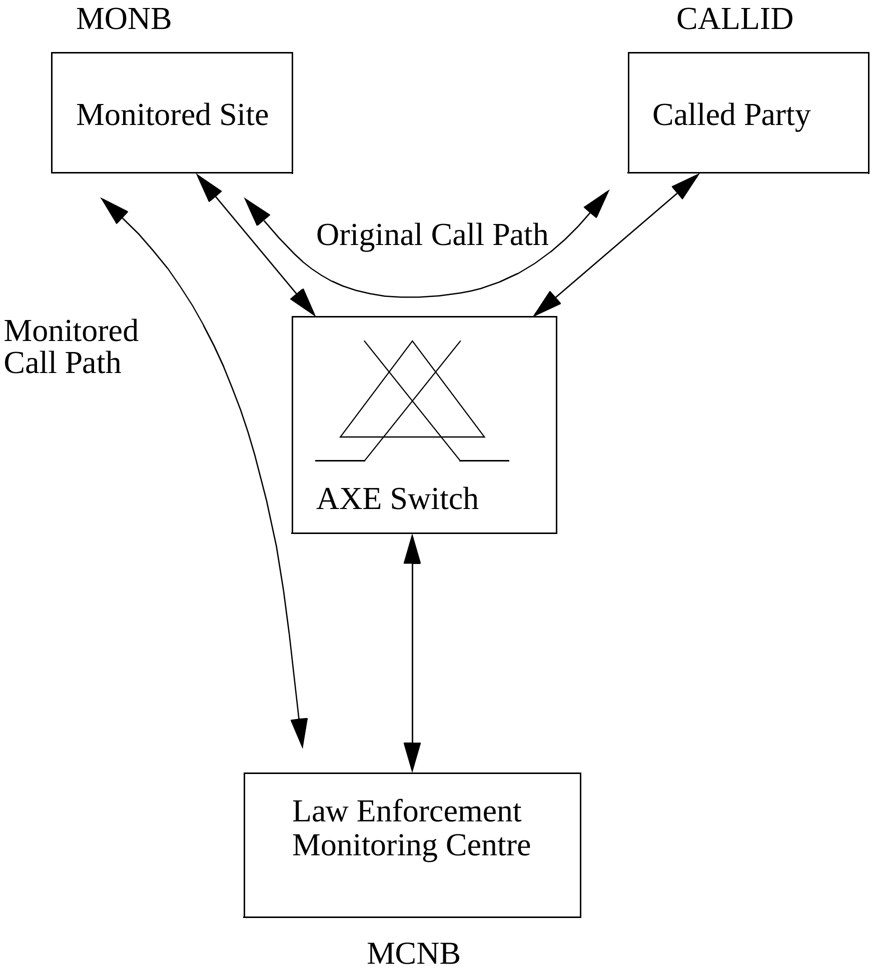
In this chapter

This chapter provides the specification for generation of billing records for monitored calls.

Scope

The Intercept Billing System exists as a single executable file, **ibs**. It is executed as a single process, with one command line argument.

Figure 11.1 Basic connections used in `ibs`



Administering IBS

Installation

The **ibs** file is installed and located in `$AOMPHOME/bin`.

Operation

To invoke **ibs** enter `irun ibs` *`<directory containing billing files>`* where the directory mentioned is `$AOMPHOME`/<*job directory*>/`BILLING`.

The job directory is the one specified in the IMS Administration GUI.

The results from running **ibs** are stored in `$AOMPHOME`/<*ibs_result_dest*>/, where `ibs_result_dest` is defined in the IMSAttribute file.

Billing files that contain errors or have wrong formats are moved to `$AOMPHOME`/ <*ibs_error_dest*>/<*time stamp*>, where `ibs_error_dest` is defined in the IMSAttribute file. The <*time stamp*> is the directory named after the time when **ibs** is run.

Errors in processing or problems in execution are notified by raising an external alarm (see Chapter 9, ‘IMS Alarm-Log Printout Descriptions’).

The billing record is required to provide sufficient information for the billing of voice and data transfer. Relevant data for creation of the billing record is taken from the **RCEFILE**.

Format

The Billing Record format is shown below.

Table 11.1 Billing Record Format (Dom)

Pos	Data	Bytes	Comments	AXE Local 7 Value Range	AXE Local 5 Value Range
0	Record type	1	1 if voice and data transmission charging (if MCNB is supplied) 2 if data transfer charging only (if MCNB is not supplied)	1 or 2	unchanged
1	MONB	28	Monitored number		unchanged
30	MUID	20	Monitored user ID		empty
51	EWID	25	Interception ID		empty
77	Switch ID	21	Switch identity		unchanged
99	CALLID	5	Id of called or calling party		unchanged
105 110 113 116 119 122	Year Month Day Hour Minute Second	4 2 2 2 2 2	Start time	1970-2036 1-12 1-31 00-23 00-59 00-59	unchanged
125	AXE FCODE	2	- Fault code - Supplied only in the **RCEFILE** record type 1	00 - 99	empty
128	Duration	10	- Duration of call in seconds.		unchanged

Pos	Data	Bytes	Comments	AXE Local 7 Value Range	AXE Local 5 Value Range
139	MCNB1	28	- Monitoring Centre Number. - Supplied only in the RCE-FILE record type 1 if transfer of speech is ordered. - Note Pkg5 will use the normal MCNB number. For Pkg6 the MCMCNB will be used to map to this field.		unchanged
Sum of bytes:		169	Includes new line characters.		

.

Table 11.2 Billing Record Format (G10)

Position	Data	Bytes	Comments	Value
0	Record type	1	• 1 if voice and data transmission charging (if MCNB1 is supplied) • 2 if data transfer charging only (if MCNB1 is not supplied)	1 or 2
1	Revision	20	The revision of Billing record Interface.	
21	Record Id	10	Switch (RES) A-number	
31	MONB	28	Monitored number, that is, the monitored network number (MNN).	
59	MUID	20	Monitored user ID	
79	EWID	25	Interception ID	
104	IWID	25	Internal reference number	

Table 11.2 Billing Record Format (G10)

Position	Data	Bytes	Comments	Value
129	Year Month Day Hour Minute Second	4 2 2 2 2 2	Start time	
143	AXE EOS	4	• End of selection code • Supplied only in the **RCE-FILE** record type 1	0 - 9999
147	AXE FCODE	2	• Fault code • Supplied only in the **RCE-FILE** record type 1	0 - 99
149	MCNB1	28	• Monitoring Centre Number • Supplied only in the **RCE-FILE** record type 1 if transfer of speech is ordered	
177	Year Month Day Hour Minute Second	4 2 2 2 2 2	• End time • Supplied only in the **RCE-FILE** record type 2	
191	no_mc_line	2	Number of MC connection	
193	REASON	1	• Reason for the call to Monitoring Centre release • Supplied only in the **RCE-FILE** record type 2	0 - 9
Sum of	bytes	194		

Billing file structure

The billing process creates a billing file which has, similar to AXE, date and time stamp in its name. For example:

```
TT-231119972300
```

The billing file contains a number of billing records which were generated within a billing period. The billing records are written to the billing file sequentially, with no separator character.

Collection of billing data

The Collection and Delivery Server (CTB) extracts the relevant billing data from the **RCEFILE** printout as a part of the printout analysis function.

The CTB:

- opens/creates the billing intermediate file
- appends the extracted information
- closes the intermediate file

Create billing record

In order to create the billing record the following information needs to be extracted from the **RCEFILE** and the database. All types need to be analysed.

- Record type
- Record ID (G10)
- MONB
- MUID (if applicable)
- EWID (if applicable)
- Date and time
- CALLID (if applicable)
- AXE FCODE (if applicable)
- MCNB1 (if applicable)
- REASON (if applicable) (G10)

The billing process is started manually or by time activation (UNIX cron job).

Voice records

If the file representation contains CALLID, the billing process finds the matching Call record and End record.

Before looking for the match, the billing process analyses the fault code associated with record type 1 (call record).

The search for the matching record type 2 (end) includes the following matching parameters:

For domestic:

- MONB
- CALLID
- MUID (if applicable)
- EWID (if applicable)

For G10:

- Record ID
- MONB
- CALLID
- MUID (if applicable)
- EWID (if applicable)
- IWID (if applicable).

If the match is found, the billing record type 1 is generated and both intermediate billing files are to be deleted (Call Record and End).

End record not found

In the IMSAttribute file, there is a variable called **Maximum_Call_Duration** and this, by default, is set to 168 hours (i.e. 7 days).

If a matching record cannot be found and the call record is less than that defined, this could imply that the matching record has not arrived yet. In this scenario, the billing intermediate file is left as is and it will be included the next time **ibs** is run.

The exchange sends notification records which indicate why the End record did not arrive. These notification records are categorised into four categories based on their FCODE. These are:

1. Exchange restart (no record expected).
2. MC exchange release (no record expected).
3. No end record.
4. Buffer overflow (end record is expected).

Categories 1, 2 and 4 are determined from the CTB by looking at the AXE FCODE of the **RCEFILE**.

For categories 1, 2 and 3 the time when the notification record was received will be used as the end time to complete the call. However, for category 4, if an End record arrives later, the time of its arrival will override the arrival time of the notification record time.

It is also possible that due to technical problems the matching End record or Call Record will never be received. To resolve this situation, the following measures are defined:

- If the matching record cannot be found and the call duration is longer than defined, the billing process creates the billing record type 2, data charging only, with the available information. The billing intermediate file is then deleted.
- If the `Maximum_Call_Duration` variable is not defined, a default of 7 days is used instead and the same action as mentioned above occurs.
- If all the above fail, an alarm will be raised to describe the error and the billing intermediate record in error will be moved to the billing error directory mentioned earlier.

12 IMS Data-Product Specifications

Prepared by EPA/D/N: Bruce Ashley	**Document no.** 3/190 83-CNAP 102 11 Uen		
Approved by EPA/D/N: (Elton Cross)	**Revision date** 2001-03-15	**Revision** G	**Pages** 40

STRICTLY CONFIDENTIAL

Specifications of IMS data products in the format specified by Bundesrepublik interception statute G10

In this chapter This chapter describes the format of the translated IMS data products (output files) as required by the G10 standard[1] and relates the fields to the source fields in the `RCEFILE` printout format.

NOTE **RCEFILE format not described** This chapter does not describe the format of the records in the `RCEFILE` printout from which the IMS data products are derived. You should refer to the Printout Description, RCEFILE, Rev. G,[2] for this specification.

Overview of call data processing

Process stages

When you initiate an interception, the following stages occur:

A Interception Management System (IMS) sends a data product to the LEMF advising of the commencement of the interception.

The LEMF usually belongs to a monitoring agency such as the police.

B The interception function in the network element sends data products in binary format to IMS whenever call events occur.

The RES interception facility in an AXE sends Data About Call data products, also known as `RCEFILE` printouts, to IMS as binary data. Depending on the type of call event, these data products are one of these types:

Type ID	RES-4	RES-5
1	Call record	Call data
2	Call completion	Call completion
3	User-to-user message	User-to-user message
4	Call related service activation	ISDN-E call related service data
5	Call unrelated service activation	ISDN-E call unrelated service data
6		PSTN call related service data
7		PSTN call unrelated service data
8		Notify

Note: Notify is not sent to the LEMF. It is used to notify IMS that a serious problem has occurred in the AXE.

C IMS converts each record in the received `RCEFILE` to a data product (DP) in text format, that is, ASCII.

The `RCEFILE` format[2] is unsuitable for processing by existing facilities. It is therefore converted to the ASCII format specified by the Telecommunications Traffic Interception Ordinance[1] of the Deutsch Bundesrepublik, usually referred to as G.10.

IMS converts the binary data in the fields of `RCEFILE` printouts into intelligible text strings by using look-up tables (see below) that can be edited by the system administrator if necessary.

D IMS sends the converted data product to LEMF in the G.10 format.

E IMS sends a final data product advising of the ending of an interception.

STRICTLY CONFIDENTIAL

Look-up tables

All IMS look-up tables are stored as text files in `$AOMPHOME/setup/redrs/text/` and `$AOMPHOME/setup/redrs/text/resid.x` where `x` represents the `resid` revision, for example, `resid.4`. To generate new tables, edit the relevant text files to include changes. The binary table stored in memory that corresponds to each of these text files is created automatically when the CTB server accesses any of the text files. Table 12.1 overleaf summarises these files and their functions.

Table 12.1 Summary of look-up tables

File	Type of mapping	Field	See page
IMSClearCause	EOS and MONCALL codes into standard notation*	[018: Clearing cause–target facility] field	12-31
IMSReason	Reason for call clearing*	[019: Clearing cause - interception link] field	12-38
IMSSupplementaryService	Supplementary services	[013: Supplementary service] field	12-20
IMSTMR	Transmission medium requirement	[012: Service] field	12-19
IMSISDNServices	Decoding Matrix for ISDN services	[013: Supplementary service] field	12-20
IMSISDNProcedures	Decoding Matrix for ISDN procedures	[013: Supplementary service] field	12-20
IMSISDNNotificationIndicators	Decoding Matrix for ISDN Notification Indicator	[013: Supplementary service] field	12-20
IMSPSTNServices	Decoding Matrix for PSTN services	[013: Supplementary service] field	12-20
IMSPSTNProcedures	Decoding Matrix for PSTN procedures	[013: Supplementary service] field	12-20
IMSTON	Type of number	[006: Address of the target facility] field [007: Address of the correspondent] field	12-12 12-17
IMSNAPI	Numbering Plan Identifier	[006: Address of the target facility] field [007: Address of the correspondent] field	12-12 12-17

* Notation specified in EIS 300 485/ITU-T Q.850.

IMS data-product structure

This section describes the structure of the ASCII data products that IMS generates and relates them to the different types of binary `RCEFILE` printouts (records) from which they are derived.

IMS data products (records) always have the same number of fields. But not all fields in every data product contain values. Table 12.2 overleaf shows which fields contain values for each of type of source `RCEFILE` printouts.

Each field begins with a *field tag* on a single line, for example, `[003: Data record type]`, to identify the field. The field tag is followed by a value consisting of one or more lines or subfields of data. Lines in the *field value* may have subfield tags appended to them to identify the subfield and the type of data.

When there is no corresponding data in the source `RCEFILE` printout, the field tag is still present but the field value may be missing or contain lines of null data. The section 'Field descriptions' on page 12-10 describes the differing structure of each field when data is present and absent.

The symbols in Table 12.2 have the following meanings:

Symbol	*Meaning*
m	Mandatory
c1	Conditional. The information may be suppressed at the request of the monitoring agency.
c2	Conditional. The information provided depends on the traffic case.
c3	Conditional. The information is not provided in the Data Monitoring Only mode of interception.
—	There is no data, the field is empty, or the field is not applicable to the PSTN/ISDN application.

Table 12.2 Summary of IMS data product record

Field tag* (number and name)	See page ...	Call record	Call completion	User-to-user message	Call related service activation	Call unrelated service activation	ISDN-E Call Related Service Data	ISDN-E Call Unrelated Service Data
[001: Version identification]	12-10	m	m	m	m	m	m	m
[002: Data record identification]	12-10	m	m	m	m	m	m	m
[003: Data record type]	12-11	begin	end	continue	continue	report	continue	report
[004: Reference number]	12-11	m	m	m	m	m	m	m
[005: Correlation number]	12-12	c3	c3	c3	c3	—	c3	—
[006: Address of the target facility]	12-12	c1	c1	c1	c1	c1	c1	c1
[007: Address of the correspondent]	12-17	m	m	m	m	—	m	—
[008: Begin]	12-18	m	—	m	m	m	m	m
[009: End]	12-18	—	m	—	—	—	—	—
[010: Duration]	—	—	—	—	—	—	—	—
[011: Direction]	12-18	m	m	m	m	m	m	m
[012: Service]	12-19	m	—	—	m	m	m	m
[013: Supplementary service]	12-20	c2	—	—	m	m	m	m
[014: User data]	12-30	—	—	m	—	—	—	—
[015: Cell identity]	—	—	—	—	—	—	—	—
[016: Paging area code]	—	—	—	—	—	—	—	—
[017: Paging message]	—	—	—	—	—	—	—	—
[018: Clearing cause - target facility]	12-31	c2	c2	—	—	—	—	—
[019: Clearing cause - interception link]	12-38	c2	c2	—	—	—	—	—

Table 12.2 Summary of IMS data product record

Field tag (number and name)*	*See page …*	*Call record*	*Call completion*	*User-to-user message*	*Call related service activation*	*Call unrelated service activation*	*ISDN-E Call Related Service Data*	*ISDN-E Call Unrelated Service Data*
`[020: Beginning of intercept]`	12-38	—	—	—	—	—	—	—
`[021: End of intercept]`	12-38	—	—	—	—	—	—	—

Table 12.3 Summary of IMS data product record (continued)

Field tag (number and name)*	*PSTN Call Related Service Data*	*PSTN Call Unrelated Service Data*	*Start of interception*	*End of interception*
[001: Version identification]	m	m	m	m
[002: Data record identification]	m	m	m	m
[003: Data record type]	continue	report	report	report
[004: Reference number]	m	m	m	m
[005: Correlation number]	c3	—	—	—
[006: Address of the target facility]	c1	c1	c1	c1
[007: Address of the correspondent]	m	—	—	—
[008: Begin]	m	m	—	—
[009: End]	—	—	—	—
[010: Duration]	—	—	—	—
[011: Direction]	m	m	—	—
[012: Service]	m	m	—	—
[013: Supplementary service]	m	m	—	—
[014: User data]	—	—	—	—
[015: Cell identity]	—	—	—	—
[016: Paging area code]	—	—	—	—
[017: Paging message]	—	—	—	—
[018: Clearing cause - target facility]	—	—	—	—
[019: Clearing cause - interception link]	—	—	—	—
[020: Beginning of intercept]	—	—	m	—
[021: End of intercept]	—	—	—	m

*All fields are present in all IMS data products. Each tag occupies a single line immediately before the lines of the field value.

Field descriptions

This section describes the data structure of each field present in an IMS data product. Each field description gives the field tag, a description of the field value when it contains data, and a description of the field value when no data is available.

[001: Version identification] field

For every network element (AXE) registered in the IMS database, the system administrator can define the text which is transmitted to monitoring agencies as the version identification information.

To define the version identification information, the system administrator must edit the `$AOMPHOME/setup/redrs/text/IMSRESID` file.

[002: Data record identification] field

This field identifies the network operator of the network from which interceptions are sent. The operator is defined when the warrant is created.

The second SupOpID field is optional and is part of the data record identification field. If it is not used, 20 ASCII characters are inserted instead.

The date and time are read from the UNIX system clock, which is synchronised with the DCF77 signal via external equipment.

Example 12.1 [002: Data record identification] field

```
OT #910# 27/11/97 14:17:20
```

[003: Data record type] field

The RES in the AXE supplies a number corresponding to the type of data in the `RCEFILE` printout. The system administrator can map these numbers to a suitable text description by editing the `$AOMPHOME/setup/redrs/text/IMSRecordType` file. Table 12.4 below defines the default mapping of RES record-type codes into the text descriptions specified in the Telecommunications Traffics Interception Ordinance.[1]

Table 12.4 Mapping RES record type codes to IMS descriptors

record type code	record type name for RES-4	record type name for RES-5	[003: Data record type] value
1	Call Data Format	Call Data Format	`begin`
2	Call Completion	Call Completion	`end`
3	User-to-user Message	User-to-user Message	`continue`
4	Call Related Service Activation	ISDN-E Call Related Service Data	`continue`
5	Call Unrelated Service Activation	ISDN-E Call Unrelated Service Data	`report`
6		PSTN Call Related Service Data	`continue`
7		PSTN Call Unrelated Service Data	`report`

[004: Reference number] field

This field contains the Interception Reference Number read from the IMS database. The operator enters this number when initiating the warrant.

[005: Correlation number] field

This field contains the `CALLID` parameter supplied either by RES-4 with `RCEFILE` printouts record types 1, 2, 3, and 4 or by RES-5 with RCEFILE printouts record types 1, 2, 3, 4, and 6 for voice and data interceptions. If an interception requires only delivery of Data About Call (data record), IMS does not supply `CALLID`.

Example 12.2 [005: Correlation number] field: CALLID number

```
[005: Correlation number]
54546
```

[006: Address of the target facility] field

This field contains the address data of the target subscriber. This is the target subscriber's number and other details. Example 12.3 defines the structure of the field value.

Example 12.3 [006: Address of the target facility] field:

General structure for RES-4:

```
[006: Address of the target facility]
number#NumberingPlanId#typeofNumber#ANB
number#ANB_U
SUB:subaddress
number#NumberingPlanId#typeofNumber#OCN
number#NumberingPlanId#typeofNumber#RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:subaddress
number#NumberingPlanId#typeofNumber#CPNR
```

General structure for RES-5:

```
[006: Address of the target facility]
number#NumberingPlanId#typeofNumber#ANB
number#ANB_U
SUB:subaddress
number#NumberingPlanId#typeofNumber#OCN
number#NumberingPlanId#typeofNumber#INB1
number#NumberingPlanId#typeofNumber#INB2
number#NumberingPlanId#typeofNumber#INB3
number#NumberingPlanId#typeofNumber#INB4
number#NumberingPlanId#typeofNumber#INB5
number#NumberingPlanId#typeofNumber#INB6
number#NumberingPlanId#typeofNumber#INB7
number#NumberingPlanId#typeofNumber#INB8
number#NumberingPlanId#typeofNumber#INB9
number#NumberingPlanId#typeofNumber#INB10
number#NumberingPlanId#typeofNumber#BNB
SUB:subaddress
number#NumberingPlanId#typeofNumber#CPNR
```

Notice that only valid INB numbers will appear in the printout. For example, if there are only two INB numbers in RCEFILE then only these two will appear in the G.10 printout.

Each line of the field value has a suffix which identifies the calling and called numbers as summarized in Table 12.5 below.

Table 12.5 Type of numbers supplied in RCEFILE printout

Matching RCEFILE field	Description	IMS line suffix
ANB	Calling Party Number	ANB
CGPNR	Calling Party Number – User-defined (Private)	ANB_U
OCN	Original Called Number	OCN
RDN*	Last Redirected Number	RDN
INB1**	The first leg redirected Number	INB1
INB2	The second leg redirected Number	INB2
INB3	The third leg redirected Number	INB3
INB4	The fourth leg redirected Number	INB4

Table 12.5 Type of numbers supplied in RCEFILE printout *(continued)*

INB5	The fifth leg redirected Number	INB5
INB6	The sixth leg redirected Number	INB6
INB7	The seventh leg redirected Number	INB7
INB8	The eight leg redirected Number	INB8
INB9	The ninth leg redirected Number	INB9
INB10	The tenth leg redirected Number	INB10
BNB	Called Party Number	BNB
CPNR	Call Pick-up Number	CPNR

[*] This field is only available in RES-4.

[**] The fields INB1 to INB10 are only available in RES-5.

The characteristics of the `RCEFILE` record structure presented above are as follows:

- All the line items are included in the field values whether or not the information is available. If this information is not available then a white space will be used in place of subscriber numbers/types of numbers/numbering Plan Ids.
- When one or more field values are not supplied in the `RCEFILE` printout, the corresponding fields in the `RCEFILE` printout are empty, that is, all characters are set to the space character (ASCII 20). The empty field value in the Address of Target Facility information object will be coded as one ASCII 20 character in the IMS data product.
- All possible types of numbers (ANB, CGPNR, OCN, RDN or INB1 to INB10, BNB, CPNR) are printed in all `RCEFILE` printouts. The information object Direction is used in order to define in which field the Address of the target facility is to be printed.
- The Monitored Subscriber Number (MNN) stored in the IMS database is printed as the *Address of the target facility* in the data products which indicate the beginning and ending of the interception – see '[020: Beginning of intercept] field' and '[021: End of intercept] field' on page 12-38.
- The subaddress information is provided only in the `RCEFILE` printout record type 1 (at the call set-up phase) in the fields `SUBADRINF CALLING` and `SUBADRINF CALLED`.

Examples from 11.4 to 11.12 are based on RES-4. For RES-5, the RDN printout line will be replaced by one or more INB lines (as in example 11.3) depending on how many valid INB numbers appear on the RCEFILE.

Example 12.4 [006: Address of the target facility] field: Outgoing call, PSTN or BRA

```
[006: Address of the target facility]
number#NumberingPlanId#typeofNumber#ANB
#ANB_U
SUB:subaddress(ANB)
 # # #OCN
 # # #RDN
 # # #BNB
SUB:
 # # #CPNR
```

Example 12.5 [006: Address of the target facility] field: Outgoing call, PABX, no validation

```
[006: Address of the target facility]
number#NumberingPlanId#typeofNumber#ANB
number#ANB_U
SUB:subaddress(ANB)
 # # #OCN
 # # #RDN
 # # #BNB
SUB:
 # # #CPNR
```

Example 12.6 [006: Address of the target facility] field: Incoming call

```
[006: Address of the target facility]
 # # #ANB
#ANB_U
SUB:
 # # #OCN
 # # #RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:subaddress(BNB)
 # # #CPNR
```

Example 12.7 [006: Address of the target facility] field: Incoming call, redirected, RES-4

```
[006: Address of the target facility]
 # # #ANB
```

```
#ANB_U
SUB:
number#NumberingPlanId#typeofNumber#OCN
number#NumberingPlanId#typeofNumber#RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:Subaddress(BNB)
 # # #CPNR
```

Example 12.8 [006: Address of the target facility] field: Incoming call, pick-up

```
[006: Address of the target facility]
 # # #ANB
#ANB_U
SUB:
 # # #OCN
 # # #RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:
number#NumberingPlanId#typeofNumber#CPNR
```

[007: Address of the correspondent] field

A correspondent is any subscriber who calls the target subscriber or is called by the target subscriber. This field value has the same structure and `RCEFILE` printout codes to IMS text descriptions as that described in ‘[006: Address of the target facility] field’ on page 12-12.

Example 12.9 [007: Address of the correspondent] field: Incoming call

```
[007: Address of the correspondent]
number#NumberingPlanId#typeofNumber#ANB
#ANB_U
SUB:subaddress(ANB)
 # # #OCN
 # # #RDN
 # # #BNB
SUB:
 # # #CPNR
```

Example 12.10 [007: Address of the correspondent] field: Outgoing call

```
[007: Address of the correspondent]
 # # #ANB
#ANB_U
SUB:
 # # #OCN
 # # #RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:Subaddress(BNB)
 # # #CPNR
```

Example 12.11 [007: Address of the correspondent] field: Outgoing call, redirected, RES-4

```
[007: Address of the correspondent]
 # # #ANB
#ANB_U
SUB:
number#NumberingPlanId#typeofNumber#OCN
number#NumberingPlanId#typeofNumber#RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:subaddress(BNB)
 # # #CPNR
```

Example 12.12 [007: Address of the correspondent] field: Outgoing call, pick-up

```
[007: Address of the correspondent]
 # # #ANB
#ANB_U
SUB:
 # # #OCN
 # # #RDN
number#NumberingPlanId#typeofNumber#BNB
SUB:
number#NumberingPlanId#typeofNumber#CPNR
```

[008: Begin] field

The RES interception facility in an AXE supplies the beginning date and time in this field within the RCEFILE printout, record types 1, 3, 4, 5, 6 and 7 (see Table 12.4 on page 12-11).

[009: End] field

The RES interception facility in an AXE supplies the ending date and time in this field within the RCEFILE printout, record type 2 (see Table 12.4 on page 12-11).

[010: Duration] field

Not described.

[011: Direction] field

The direction of the call is notified by the Monitored Party Identifier (MPI) parameter of data records of all types in the RCEFILE printout. If the content of MPI is zero (0), the call from the target subscriber is outgoing.[2] MPI is available for RES-4 only. For RES-5 the MONOBJ field is used. MONOBJ identifies the target.

In the case of the User-to-user message field (RCEFILE printout, record type 3), the MPI parameter identifies which of the supplied numbers is the Address of the target facility or the Correspondent number. The direction of the message is given in the Direction field of the Data Record.

[012: Service] field

The RCEFILE printout is converted by IMS as follows:

```
[012: Service]
BC: contents of Basic Service field
LLC: contents of Basic Service field
HLC: contents of Basic Service field
Textual interpretation of the Basic Service field
```

The characteristics of this field are as follows:

- All the RCEFILE printout elements are printed regardless of the available information.
- If one or more line items (BC, LLC, HLC) are not supplied in the RCEFILE printout, the corresponding fields in the IMS data product are set to 0. That is, there won't be any character printed in the corresponding field of the Service information object.

The TMR field supplied in the RCEFILE printout, record type 1, is converted into corresponding text descriptions in IMS using a Transmission Medium Requirement (TMR) table. The system administrator can edit the $AOMPHOME/setup/redrs/text/resid.4/IMSTMR and the $AOMPHOME/setup/redrs/text/resid.5/IMSTMR files to change these text descriptions. Table 12.6 opposite shows the default mappings of TMR codes to text descriptions.

Table 12.6 Transmission Medium Requirement (TMR) table

TMR in RCEFILE printout*	IMS data product†
0	Speech
1	UDI BS
2	Speech BS
3	3.1k audio
4	64 kb/s preferred
5	2x64k UDI BS
6	4x64k unrestricted
7	6x64k unrestricted
8	8x64k unrestricted
9	12x64k unrestricted
10	23x64k unrestricted
11	24x64k unrestricted
12	20x64k unrestricted
13-255	Spare

* Values range from 0 to 255.
† These descriptions are specified in the Telecommunications Traffic Interception Ordinance.[1]

[013: Supplementary service] field

Table 12.7 overleaf summarises supplementary services supported in IMS and defined in the `$AOMPHOME/setup/redrs/text/resid.4/IMSSupplementaryService`.

.

Table 12.7 Summary of supplementary services *(part 1 of 2)*

Type[*]	Field[†]	Supplementary service[‡]	RCEFILE value[§]	IMS data product[¶]
1	ENQ	Enquiry in PSTN	0 (No)	–
			1 (Yes)	ENQ
1	COLP	Connection Line Identification Presentation	0 (No)	–
			1 (Yes)	COLP
1	CUG	Closed User Group	0 (No)	–
			1 (Yes)	CUG
1	CF	Call Forwarding	0 (Not used)	–
			1 (Unknown)	–
			2 (User busy)	CFB
			3 (No reply)	CFNR
			4 (Unconditional)	CFU
			5 (Deflection during alerting)	CD During alerting
			6 (Deflection immediate response)	CD Immediate response
1	CCBS	Completion of Call to Busy Subscriber	0 (No)	–
			1 (Yes)	CCBS
1	CLIR	Calling Line Identification Restriction	0 (No)	–
			1 (Yes)	CLIR
1	CAW	Call Waiting	0 (No)	–
			1 (Yes)	CW
3	COLR	Connected Line Identification Restriction	0 (No)	–
			1 (Yes)	COLR

Table 12.7 Summary of supplementary services *(part 2 of 2)*

Type[*]	Field[†]	Supplementary service[‡]	RCEFILE value[§]	IMS data product[¶]
3	Hold/ Re	Hold/Retrieve	0 (Not used)	–
			1 (Calling Party on Hold)	HOLD Calling Party on hold
			2 (Called Party on Hold)	HOLD Called Party on Hold
			3 (Calling Party Retrieved)	HOLD Calling Part Retrieved
			4 (Called Party Retrieved)	HOLD Called Party Retrieved
3	TP	Suspend/Resume	0 (Not used)	–
			1 (Call suspended by calling party)	TP Call suspended by calling party
			2 (Call suspended by called party)	TP Call suspended by called party
			3 (Call resumed by called party)	TP Call resumed by called party
			4 (Call resumed by calling party)	TP Call resumed by calling party
3	ECT	Explicit Transfer	0 (Not used)	–
			1 (Call transfer by called party)	ECT Call transfer by called party
			2 (Call transfer by calling party)	ETC Call transfer by calling party

[*] RCEFILE printout record type number – see Table 12.4 on page 12-11.

[†] Name of the field in the RCEFILE printout that identifies the supplementary service.

[‡] Extended name of supplementary service.

[§] Numeric code in the RCEFILE printout identifying the type of event in the supplementary service, with explanation in parentheses.

[¶] Output generated by IMS formatted according to Annexure 4 of the Telecommunications Traffic Interception Ordinance.[1]

Tables 11.8 to 11.12

Tables 11.8 to 11.12 summarise RES-5 supplementary services supported in IMS and defined in the files listed below.

Table 11.8 summarises the PSTN services supported and information to be delivered in IMS and defined in the `$AOMPHOME/setup/redrs/text/resid.5/IM-SPSTNServices` file.

Table 12.8 PSTN Services

Service*	Service Code**	Extra Information***
ADI	09	EOS KEYPAD
ASU	12	EOS KEYPAD
ALS	6, 56, 57	EOS KEYPAD
CAB	164	EOS KEYPAD
CAMBC	170	EOS KEYPAD
CANR	168	EOS KEYPAD
CAU	169	EOS KEYPAD
CDP	102	EOS
CFB	5	EOS KEYPAD
CFFL	149	KEYPAD
CFNR	4	EOS KEYPAD
CFTU	144	EOS KEYPAD
CFU	3	EOS KEYPAD
SFCU	107	EOS KEYPAD
CR	105	EOS KEYPAD
KWC	58	EOS KEYPAD
CCBS	16	EOS KEYPAD
CCNR	71	EOS KEYPAD
DDB	13	EOS KEYPAD
FDC	10, 7	EOS KEYPAD
CAW	17	EOS KEYPAD
MCIDSC	172	EOS
MCIDA	172	EOS

Table 12.8 PSTN Services

Service*	Service Code**	Extra Information***
TPS		
GDSS	45	EOS KEYPAD
GISS	46	EOS KEYPAD
LNR	14	EOS KEYPAD
LHW	147	EOS KEYPAD
MWI	49	EOS
MSN	178	EOS
CCB	11	EOS KEYPAD
RCSS		
SCA	142	EOS KEYPAD
SCR	143	EOS KEYPAD
SR	106	EOS KEYPAD
QUE	44	EOS KEYPAD
VCI-A	145	EOS KEYPAD
VCI-B	146	EOS KEYPAD
CLIP	177	EOS
CLIR	55	EOS

*Abbreviated PSTN Service Name

**Value in `RCEFILE` being used to identify a PSTN service

***Fields in `RCEFILE` holding more information for a service

Table 11.9 summarises the PSTN procedures supported in the IMS and defined in the `$AOMPHOME/setup/redrs/text/resid.5/IMSPSTNProcedures` file.

Table 12.9 PSTN Procedure

Procedure*	**Procedure Code****
Innovation	8, 9, 16, 17, 18
Activation	2, 4
Deactivation	3, 5, 52
Interrogation	6
Registration	4
Erasure	5
Verification	7

*PSTN Procedures supported

**Values in `RCEFILE` being used to identify a procedure

Table 11.10 summarises the ISDN services supported and information to be delivered in IMS and defined in the `$AOMPHOME/setup/redrs/text/resid.5/IMSISDNServices` file.

Table 12.10 ISDN Service

Service*	**Service Code****	**Extra Info*****
AOC-S	117	
AOC-D	30	
AOC-E	28	
AOC-T	31	KEYPAD
ASICF	129	
ASICV	130	KEYPAD
MCT	174	
BSICF	127	
BSICV	128	KEYPAD
CAB	164	KEYPAD FACILITY
CAC	167	KEYPAD FACILITY
CANR	168	KEYPAD FACILITY
CAU	169	KEYPAD FACILITY
CCBS	16	FACILITY
CD	54	
CFU	3	KEYPAD FACILITY
CFNR	4	KEYPAD FACILITY
CFB	5	KEYPAD FACILITY
CW	17	KEYPAD
CLIP	118	
CLIR	55	

Table 12.10 ISDN Service

Service*	**Service Code****	**Extra Info*****
CKY	58	KEYPAD
CUG	121	
CONF	40	FACILITY
COLP	120	
EA	163	KEYPAD
ECT	150	
FDC	7	KEYPAD
HOLD	66	
ICI	156	
IS	140	
MCID	126	
MWIC	182	
MWIR		
OCBV	11	KEYPAD
RH	141	KEYPAD
Retrieve	66	
TP	122	
3PTY	115	
UUS2	124	
UUS2	125	FACILITY

*ISDN Abbreviated service name

**Values in `RCEFILE` being used to identify a ISDN service

***Fields in `RCEFILE` holding more information delivered by a service

Table 11.11 summarises the ISDN procedures supported in the IMS and defined in the `$AOMPHOME/setup/redrs/text/resid.5/IMSISDNProcedures` file.

Table 12.11 ISDN Procedure

Procedure*	**Procedure Code****
Invocation	2***, 16, 37, 38, 39, 40, 42, 43
Activation	2
Deactivation	3
Interrogation	6
Registration	4
Erasure	5
Verification	

*Activities supported by ISDN Services

**Values in `RCEFILE` representing a corresponding procedure

***2 represents the procedure Invocation only for the services AOC-S, AOC-D and AOC-E.

Table 11.12 summarises ISDN notification indicators supported in IMS and defines in the `$AOMPHOME/setup/redrs/text/resid.5/IMSISDNNotificationIndicators` file.

Table 12.12 ISDN Notification Indication

Indicator Code*	Description
0	user suspended
1	user resumed
2	bearer service change
3	discriminator for extension to ASN.1 encoded component
4	call completion delay
66	conference established
67	conference disconnected
68	other party added
69	isolated
70	reattached
71	other party isolated
72	other party reattached
73	other party split
74	other party disconnected
75	conference floating
96	call is a waiting call
104	diversion activated (used in 1)
105	call transfer, alerting
106	call transfer, active
121	remote hold
122	remote retrieval
123	call is diverting

*All other values are currently not used and are reserved for further extensions.

[014: User data] field

This field contains the *User-to-user message* which is sent in the `RCEFILE` printout, record type 3.The AXE system considers the *User-to-user message* as a transfer of binary information, so IMS encodes this binary data in the IMS data product in a hexadecimal representation.

Example 12.13 [014: User data] field

```
[014: User data]
02 3F 4D 76 3A …
```

[015: Cell identity] field

Not described.

[016: Paging area code] field

Not described.

[017: Paging message] field

Not described.

[018: Clearing cause–target facility] field

Table 12.13 overleaf maps EOS codes generated by an AXE, as well as Release cause `MON-CALL` information, into the notation specified by ETS 300 485/ITU-T Q.850. This table specifies only the mapping between different notations and does not specify an implementation in IMS.

The system administrator can edit the `$AOMPHOME/setup/redrs/text/resid.x/IMSClear-Cause` file to change the mappings for particular implementations or services.

Table 12.13 Clearing cause conversion table *(part 1 of 6)*

End Of Selection code, IMS (EOS IMS)[*]	CAU[†]	Value[‡]	Hex[§]	IMS data product[¶]
4, 25, 35, 100, 1608, 3183, 3551	1	1	81	Unallocated (unassigned) number
	104	2	82	No route to specified transit network
	58	3	83	No route to destination
32, 43, 230, 239, 665	2, 59	4	84	Send special information tone
	60	5	85	Misdialled trunk prefix
		6	86	Channel unacceptable
		7	87	Call awarded and being delivered in an established channel
	83	8	88	Preemption
	84	9	89	Preemption – circuit reserved for reuse
2440	3	16	90	Normal call clearing
24, 33, 367, 851, 1668, 2746	4	17	91	User busy
	5	18	92	No user responding
666	61	19	93	No answer from user (user alerted)

Table 12.13 Clearing cause conversion table *(part 2 of 6)*

End Of Selection code, IMS (EOS IMS)*	CAU†	Value‡	Hex§	IMS data product¶
	85	20	94	Subscriber absent
94, 501-503, 850, 1124, 2467, 2857, 2858, 2859	6	21	95	Call rejected
5, 41, 1468	7	22	96	Number changed
		26	9A	Non-selected user clearing
7, 8, 27, 28, 36, 38, 878, 1000, 1622	8	27	9B	Destination out of order
76, 77, 85, 504, 625, 3162	9, 10, 78	28	9C	Invalid number format (address incomplete)
668, 670, 671, 674, 1610, 1611, 1612, 3245	11	29	9D	Facility rejected
	12	30	9E	Response to STATUS ENQUIRY
1, 2, 85, 95, 99, 141, 167, 190, 324, 675, 801, 802, 858, 859, 860, 1458	13, 82	31	9F	Normal, unspecified
34, 50, 56, 90, 186, 191-205, 425, 468, 472, 473, 679, 800, 803-809, 2585	14	34	A2	No circuit/channel available
9, 77, 89, 160, 161, 698, 699	15	38	A6	Network out of order
		39	A7	Permanent frame mode connection out of service
		40	A8	Permanent frame mode connection operational

Table 12.13 Clearing cause conversion table *(part 3 of 6)*

End Of Selection code, IMS (EOS IMS)[*]	CAU[†]	Value[‡]	Hex[§]	IMS data product[¶]
10, 71, 92, 97, 168, 669, 676, 1657-1662	16, 65-75	41	A9	Temporary failure
53, 54, 61-64, 67, 68, 70, 79, 93, 96, 114, 142, 153, 667, 680, 681, 1197,1655, 2586	17, 77	42	AA	Switching equipment congestion
	18	43	AB	Access information discarded
	19	44	AC	Requested circuit/channel not available
	86	46	AE	Precedence call blocked
	20	47	AF	Resource unavailable, unspecified
		49	B1	Quality of service unavailable
1191, 1430	48	50	B2	Requested facility not subscribed
1432	50	53	B5	Outgoing calls barred within CUG
1435, 1436, 3751	52	55	B7	Incoming calls barred within CUG
1115	21	57	B9	Bearer capability not authorized
136	22	58	BA	Bearer capability not presently available
	87	62	BE	Inconsistency in designated outgoing access information and subscriber class

Table 12.13 Clearing cause conversion table *(part 4 of 6)*

End Of Selection code, IMS (EOS IMS)[*]	CAU[†]	Value[‡]	Hex[§]	IMS data product[¶]
	23	63	BF	Service or option not available, unspecified
91, 467, 2220	24, 79	65	C1	Bearer capability not implemented
	25	66	C2	Channel type not implemented
2804	53	69	C5	Requested facility not implemented
	26	70	C6	Only restricted digital information bearer capability is available
2468	27	79	CF	Service or option not implemented, unspecified
		81	D1	Invalid call reference value
	28, 29	82	D2	Identified channel does not exist
	30, 31	83	D3	A suspended call exists, but this call identity does not
	32	84	D4	Call identity in use
	33	85	D5	No call suspended
		86	D6	Call having the requested call identity has been cleared
1437, 1471, 3759	62	87	D7	User not member of CUG

Table 12.13 Clearing cause conversion table *(part 5 of 6)*

End Of Selection code, IMS (EOS IMS)[*]	CAU[†]	Value[‡]	Hex[§]	IMS data product[¶]
80, 120-135, 462, 1117, 1434, 1438, 1440, 1607	34	88	D8	Incompatible destination
	54	90	DA	Non-existent CUG
	88	91	D9	Invalid transit network selection
	35	95	DF	Invalid message, unspecified
	36	96	E0	Mandatory information element is missing
	37	97	D1	Message type non-existent or not implemented
	38	98	D2	Message not compatible with call state or message type non-existent or not implemented
	39, 40, 73	99	D3	Information element /parameter non-existent or not implemented
	41	100	D4	Invalid information element contents
	42	101	D5	Message not compatible with call state
84, 140, 206	44	102	D6	Recovery on timer expiry
	43	103	D7	Parameter non-existent or not implemented, passed on
	89	110	DD	Message with unrecognized parameter, discarded

Table 12.13 Clearing cause conversion table *(part 6 of 6)*

End Of Selection code, IMS (EOS IMS)[*]	CAU[†]	Value[‡]	Hex[§]	IMS data product[¶]
1656	45, 63, 64, 76, 80, 81	111	DF	Protocol error, unspecified
	46	127	FF	Interworking, unspecified
98, 1609, 238, 1437, 1471, 3759	47, 49, 51, 55, 56, 57, 90-103	-		

[*] List of EOS codes which are mapped into the ETS 300 485/ITU-T Q.850 codes for a particular AXE application. The EOSIMS codes listed in the table are those currently used in the Local 4. The list is not complete so the implementation should deal with the function which would allow an easy maintenance of the table.

[†] CAU is the AXE parameter which provides association between internal causes (EOS) and Cause values defined by ITU-T.

[‡] ‘Cause value’ is an ITU-T term. These values listed here are the first 7 bits of the Cause value octet in decimal notation.

[§] ‘Hex’ is the ‘Cause value’ given in hexadecimal notation.

[¶] Description of the clearing cause.

[019: Clearing cause - interception link] field

The REASON field in the `RCEFILE` printout, record type 2, provides release cause information. The field REASON contains the RES internal values of the release codes to the LEMF.

The internal value is mapped to the ETS 300 485/ITU-T Q.850 definition as follows and is defined in `$AOMPHOME/setup/redrs/text/resid.x/IMSReason`.

Table 12.14 REASON code table

REASON code*	RES definition	IMS data product†
0	Normal release from the original call	Normal call clearing
1	MC released the call	Normal call clearing
2	Fault from CCD	Temporary failure
3	Fault from GS	Temporary failure
4	Release order from CLCOF	Temporary failure

* These codes are generated in the RCEFILE printout.
† Conforms to the ETS 300 485 specification.

[020: Beginning of intercept] field

IMS fills this field after successfully activating an interception. IMS reads the date and time from the UNIX system clock, which is synchronised with the DCF77 signal via an external equipment.

[021: End of intercept] field

IMS fills this field after successfully terminating an interception. IMS reads the date and time from the UNIX system clock, which is synchronised with the DCF77 signal via an external equipment.

References

1 Technical Directives for Requirements as provided for §13 of the Telecommunications Traffic Interception Ordinance (TR FUV), Federal Ministry of Post and Telecommunications, Bonn, Version 2.0, April 1997.

2 1/190 83-CNT 233 21 Uen, Printout Description, RCEFILE, Rev. G, specifies the format of data records in RCEFILE printouts (Data About Call printouts) generated by the RES interception facility in AXE. This document specifies for each field in the byte stream its position, length in bytes, range of legal values, and standard name.

STRICTLY CONFIDENTIAL

Glossary

A

AMB Application Monitor Block.

ANS Access Node Switch.

AOMP *See* XMATE.

API Application Programming Interface.

ASN Abstract Syntax Notation.

AVF Alternate voice and facsimile channel.

AXE (automatic exchange equipment) This is an Ericsson term for a device that routes calls within a public switched telecommunications network (PSTN). Often called a switch, especially in USA telecommunications literature.

B

BER Basic Encoding Rules.

C

Carrier *See* TSP.

CCC Call Content Channel.

CDC Call Data Channel.

CME 20 Ericsson's implementation of GSM digital mobile telephony.

CMS 88 Ericsson's implementation of AMPS analogue mobile telephony.

CO Charging Origin

COD Command Description

CTB Collection Transmission Block is an IMS transmission process.

CUG Closed User Group.

D

data communications server (DCS) *See* DCS (data communications server).

data product (DP) (a) The `RCEFILE` printout generated by the RES subsystem in a network which contains data about the monitored call. (b) The record output by IMS after converting the binary data in the `RCEFILE` printout to ASCII text format. IMS sends the text data product to a specified LEMF.

Prepared by EPA/D/N:Bruce Ashley **Document no.** 19006-CNAP 10211 Uen

Approved by EPA/D/N:(Elton Cross) **Revision date** 2000-09-13 **Revision** H **Pages** 6

DCB (data communication block) A functional module in XMATE that handles communication with the managed network.

DCS (data communications server) A software application in XMATE that acts as a gateway for communications with remote network elements.

DFA Data and facsimile channel.

DMO Data Monitoring Only. An interception that sends all data except voice data to a LEMF.

DP *See* data product (DP).

DT (delivery type) The DT (delivery type) field specifies which data channels are to be sent to the LEMF and whether one or two trunk lines are to be used. The available channels are: VCE (voice data), UDI (unrestricted digital information), F31 (3.1 kHz audio or data), AVF (alternate voice or facsimile), DFA (data or facsimile).

DTE Data Terminal Equipment.

E

ERROR_TERMINAL The default destination to where IMS sends data products when it is unable to communicate with the specified LEMF.

EWID External Warrant Identifier. *See* Interception Reference.

F

F31 3.1 kHz audio and data channel.

FTAM File Transfer, Access, and Management (ISO 8571).

G

GMT Greenwich Mean Time. *See* UTC.

I

IAP Intercept Access Print.

IHS Information Handling Server.

IMAS Intercept Management Application Server.

IMEI International Mobile Equipment Identifier. A serial number that uniquely identifies each cellular (mobile) telephone and which is transmitted by the telephone to the base station.

IMS (Interception Management System) The Interception Management System installs and removes interceptions (electronic analogue or digital PSDN/ISDN phone taps or line taps), collects details of the connections, and copies call content (voice or data), known as *data product*, to a law enforcement monitoring facility (LEMF). IMS was previously known as Remote-control Equipment Data Routing System (REDRS).

IMSI International Mobile Subscriber Identifier. Similar to IMEI but for subscribers rather than equipment.

interception An electronic ‘phone tap’ of a particular subscriber’s incoming and outgoing calls of which the details and content are forwarded to an agency authorised to monitor the calls.

Interception Reference A code that identifies the legal instrument or other document that legally authorizes an interception.

IWID Internal Warrant Identifier. *See* Interception Reference.

L

LAESP Lawfully Authorised Electronic Surveillance Protocol.

LEA Law Enforcement Agency.

LEMF(law enforcement monitoring facility) A secure premise where the monitoring agent, such as the police, monitors data about calls (data products) and records the voice or data content of calls, both of which are sent there by IMS.

M

MC Monitoring Centre.

MCNB Monitoring Centre Number Block for voice and data calls.

MDPC Measurements Data Product Counter.

MDPC reset time The time at which MDPC is reset to 0.

message transfer protocol (MTP) *See* MTP (message transfer protocol).

MML (Man-Machine Language) A symbolic ‘assembler’ language for writing commands understood by network elements (NE) conforming to an ITU-T recommendation for a man-machine interface for operating and maintaining network elements. Different Ericsson NEs understand different MML commands and commands that perform the same action may differ from one NE to the next.

MNN (monitored network number) The number of the subscriber who is a target of an interception.

MONB (monitored number) The address of the target facility as defined in the RES interception subsystem in an AXE. *See also* MNN (monitored network number).

Monitor XMATE application, used to start and stop servers.

MSC (mobile switching centre) A network element that routes calls on digital (GSM) or analogue mobile telephone networks.

MSNB (mobile station number) The mobile number of the subscriber who is a target of an interception.

MTP (message transfer protocol) An Ericsson proprietary communications protocol based on X.25 approximating the OSI levels 4 to 6, for transporting messages to and from network elements (NE).

MUID Monitoring User Identification.

N

NE (network element) A device in a telecommunications network for routing calls, for example, an AXE, LEMF, or PABX. Can also include multiplexers, repeaters, and other devices but in XMATE refers mainly to automatic exchange equipment (AXE). A network element is connected to the IMS system via a PSDN or point-to-point connection.

NI Network Identifier.

network operator A telecommunications carrier that owns and manages a telecommunications network. *Compare with* operator.

O

operator A person able to configure and operate network elements in a network day-to-day within constraints imposed by the system administrator, such as only qualified access to IMS functions. *Compare with* system administrator; network operator.

OSI Open System Interconnection.

P

PLP *See* X.25 PLP.

POD Printout Description

PSDN Packet Switched Data Network.

PSTN Public Switched Telephone Network.

R

RCEFILE Output file generated by the RES interception subsystem in an AXE that contains the data about intercepted calls.

REDRB Remote-control Equipment Data Routing Block.

REDRS *See* IMS (Interception Management System).

RES (remote-control equipment subsystem) Interception subsystem within an network element (AXE or MSC). *See also* AXE (automatic exchange equipment); MSC (mobile switching centre).

routing table An table in the IMS Database containing mobile subscriber numbers, and the LEMF to which they are routed.

RPC Remote Procedure Call (RFC-1057).

S

SF Special [monitoring] Features.

SMS (short message service) The ability to send a short text message to a digital mobile telephone (CME 20).

SNB Subscriber Number.

switch An informal term for a network element that routes telecommunications calls. *See* AXE (automatic exchange equipment); MSC (mobile switching centre).

system administrator A person with superuser access to the hosts running network management applications who installs software, adds and deletes operator accounts, and sets the authorizations for operators to use particular IMS functions. The system administrator can access all IMS system functions. *Compare with* operator.

T

transmission process The part of IMS which provides the transmission and rerouting of data products to the end-user terminal.

TSP Telecommunications Service Provider. Also known as **carrier**.

U

UDI Unrestricted digital information channel.

UTC Universel Temps Coördinatée (Coordinated Universal Time). A universal time-reference standard equivalent to the local time at Greenwich, United Kingdom, formerly known as Greenwich Mean Time (GMT).

V

VCE Voice channel.

W

warrant A legal document issued by a monitoring authority, for example, the police, instructing and authorizing a telecommunications carrier to intercept the calls of particular subscribers for a particular period of time. In IMS, *warrant* also refers to the details of an interception entered into the IMS database.

WDPC Warrant Data Product Counter.

WiOZ Window based terminal emulation application in XMATE.

X

X.25 A communication protocol standardised according to the OSI levels 1 to 3 by the ITU-T.

X.25 PLP ITU-T X.25 Packet Level Protocol.

X.29 Defines the interface between pad and packet mode DTE.

XMATE E**x***chang*e **ma***nagement* **te***rminal. A* suite of applications developed by Ericsson Australia Pty Ltd.

XMATE IMS *See* IMS (Interception Management System).