

Interception Management System

CELLNET Drop 2

Course Objectives:

After this course, participants will be able to:

- Understand the Interception Concept
- Understand the Remote Control Equipment Subsystem functions
- Overview of XMATE Platform - WIOZ Tool and Transaction Log Tool
- Use the IMS platform functions to:
 - I. Initiate a warrant
 - II. Audit a warrant
 - III. Monitor a warrant
 - IV. Terminate a warrant

Course Objectives:

After this course, participants will be able to:

- To manage the directory structure and files
- To manage the security and access control / authorisation
- To have an overview of the Monitoring Tool
- To administer the IMS transmission process
- To administer the IMS database
- To manage the IMS backup and recovery
- To have an overview of system upgrade procedure
- To manage Third Party Software Components

Table of Contents

1. Overview	4
1.1 IMS General Functions	
1.2 Ericsson Interception Concept	5
1.3 IMS Architecture Platform	6
1.4 IMS Application and Relationship.....	7
2. Remote Control Equipment Subsystem.....	
2.1 Remote Control Equipment Subsystem Implementation ...	
3. Overview of XMATE Platform Functions	
4. IMS Operation	18
4.1 Network Interface Communication.....	19
4.2 Warrant handling	23
4.3 Audit process	29
4.4 Warrant Management Interface.....	30

Table of Contents

3. Administering IMS	10
3.1 IMS Directory Structure - \$AOMPHOME/bin directory	11
3.2 \$AOMPHOME/bin/admin directory..	23
3.3 Other directories	36
3.4 IMS Configuration Files - \$AOMPHOME/setup/redrs.....	39
3.5 IMS Configuration Files - \$AOMPHOME/setup/redrs/text....	61
3.6 IMS Configuration Files - CTB Run-Time Variables.....	62
3.7 Configurable IMS Attributes	65
3.8 \$AOMPHOME/setup - Parameters of Interest	
3.9 dcs_password Configuration	
4. Security and Access Control / Authorisation	
4.1 Security and Access Control / Authorisation	
4.2 Create new	

1. Overview

Module Objectives

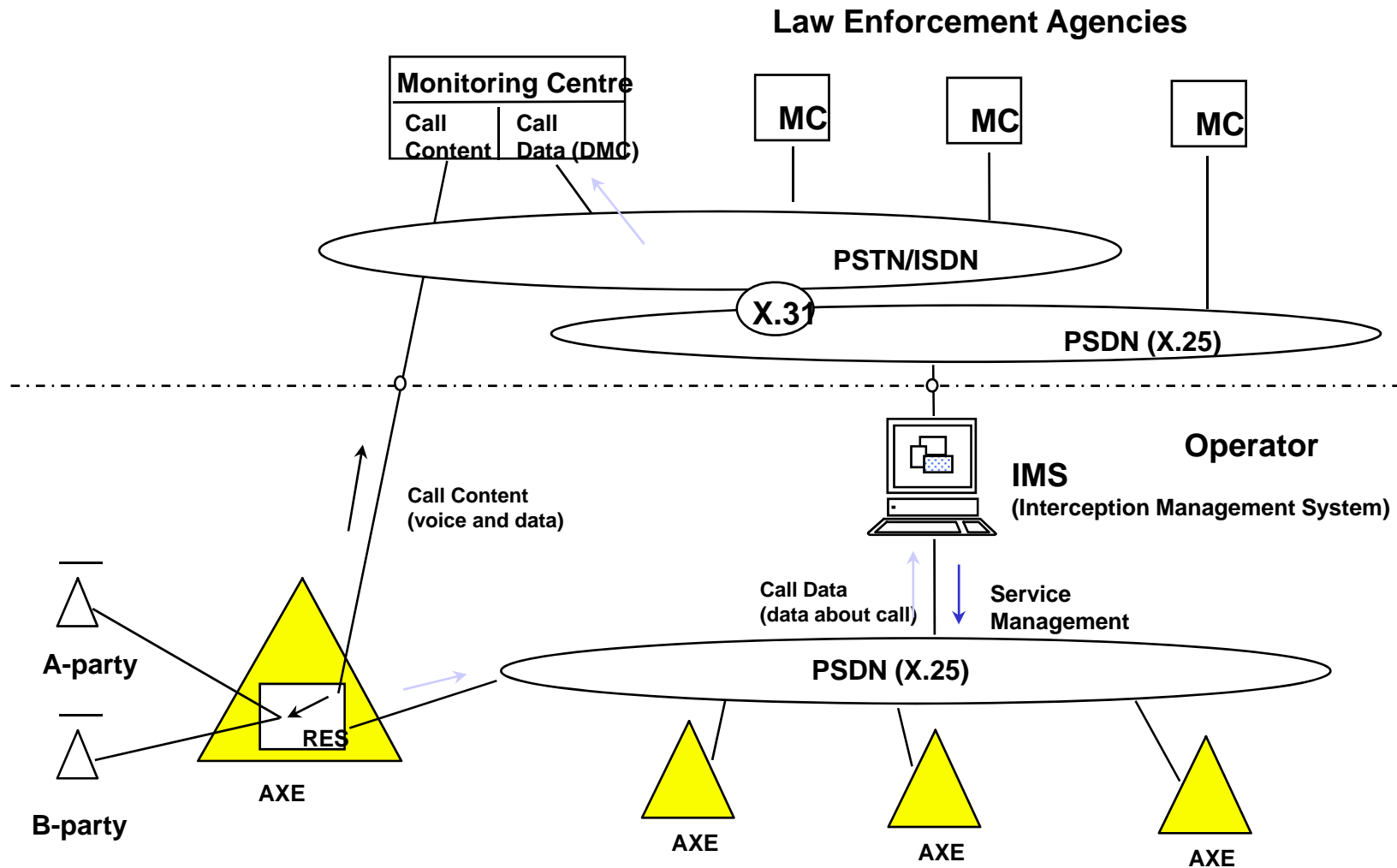
Be able to explain:

- Intercept Concept
- IMS Architecture Platform
- IMS Application and Relationship

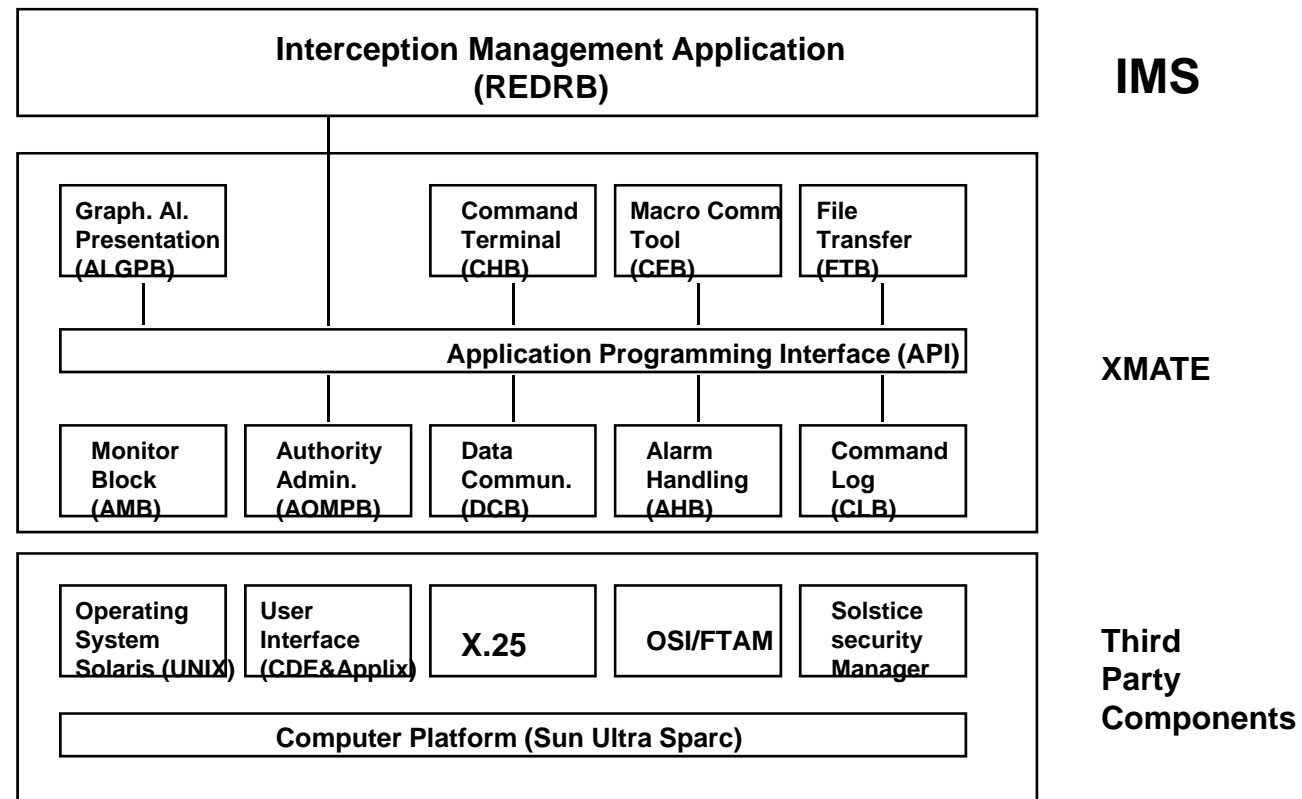
1.1 IMS General Functions

- **Server Functions**
Sending of commands to the Network Element
- **Operator Functions**
Management of the interception service performed by an IMS operator
- **Administration Functions**
Configure & maintain the application

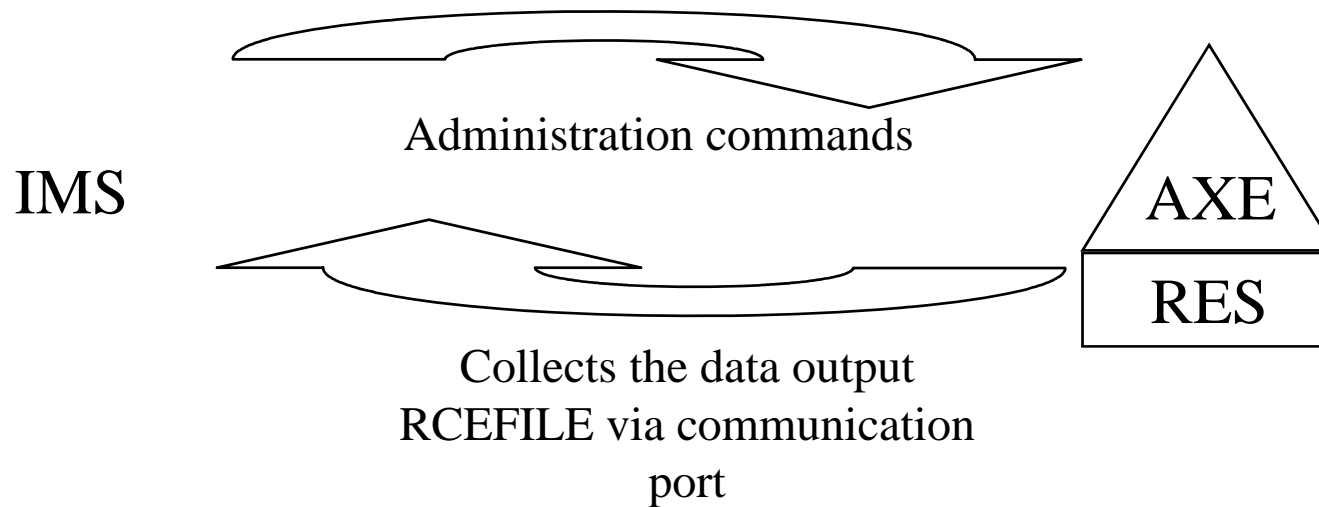
1.2 Interception Concept



1.3 IMS Architecture Platform



1.4 Network Interface Communication



1.5 Communication to AXE

Link supervision

OMC

Supervision based on the heart-beat reception from AXE
(1 min)

IMS

Supervision based on the time scheduled polling from IMS
(defined by Administrator, recommended 5-10 min)

Includes supervision of:

- Data Communication Server (DCS)
- Physical connection to the data network (IMS connection)
- Physical connection of AXE to the data network

1.6 Warrant Handling


Characteristics

- Warrant Activation/deactivation
- Warrant subscription monitoring (Audit, reload related update)
- Checking Monitoring number operational status
- Security access control
- Event logging
- Security input of the interception sensitive information

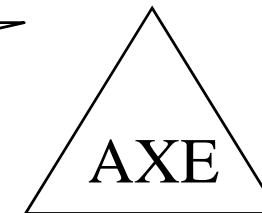
1.7 Broadcast Ordering

Activation

IMS




Sends the MML commands for
ordering of monitoring of an
warrant RCSUI

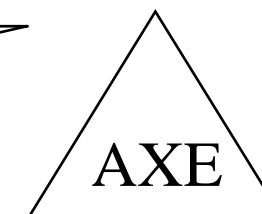


Deactivation

IMS

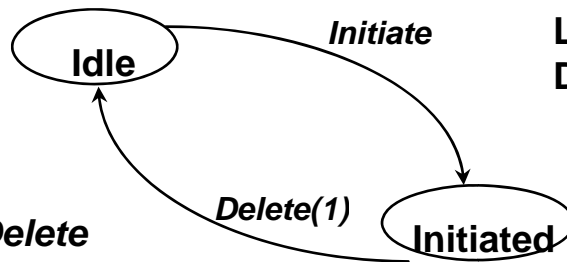


Sends the MML commands &
update the database
RCSUE



1.8 Warrant Handling

Initiate State machine model



Action: *Initiate*
Actor : Operator
Tool : Warrant Init.
Log : Yes
Descr. : Warrant initiated in the IMS DB but not in the network

Action: *Delete*
Actor : Administrator
Tool : DB Admin
Log : Yes
Descr. :

(1) Deletion of the warrant in the IMS DB.
No warrant in the network

1.8 Warrant Handling

Initiate State machine model

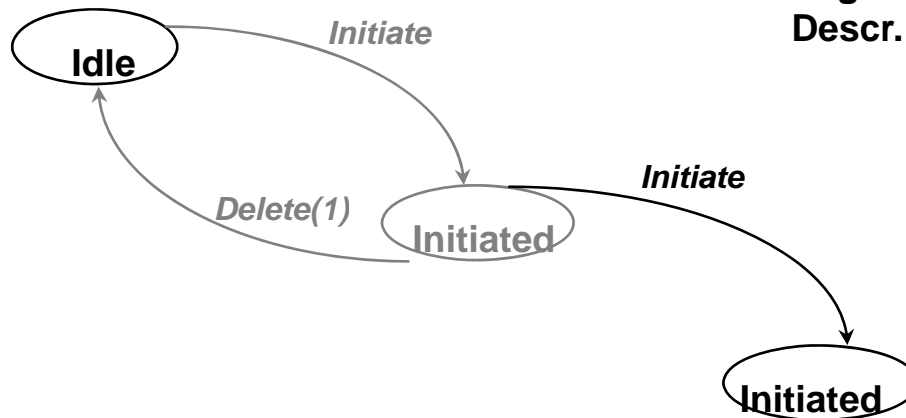
Action: *Initiate*

Actor : System (automatic)

Tool : n/a

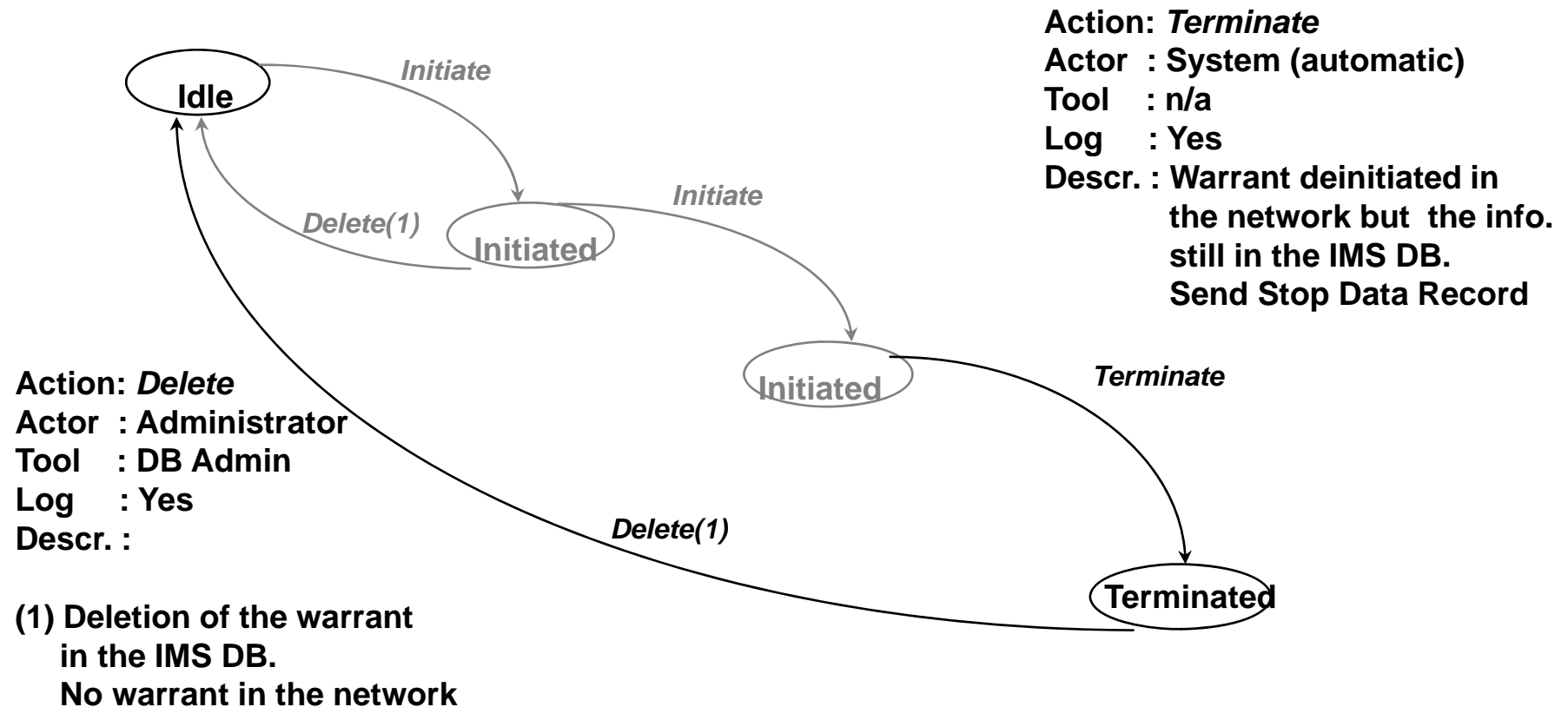
Log : Yes

Descr. : Warrant initiated in the IMS DB and in the network.
Send Start Data Record.
Increment respective warrant statistic counter



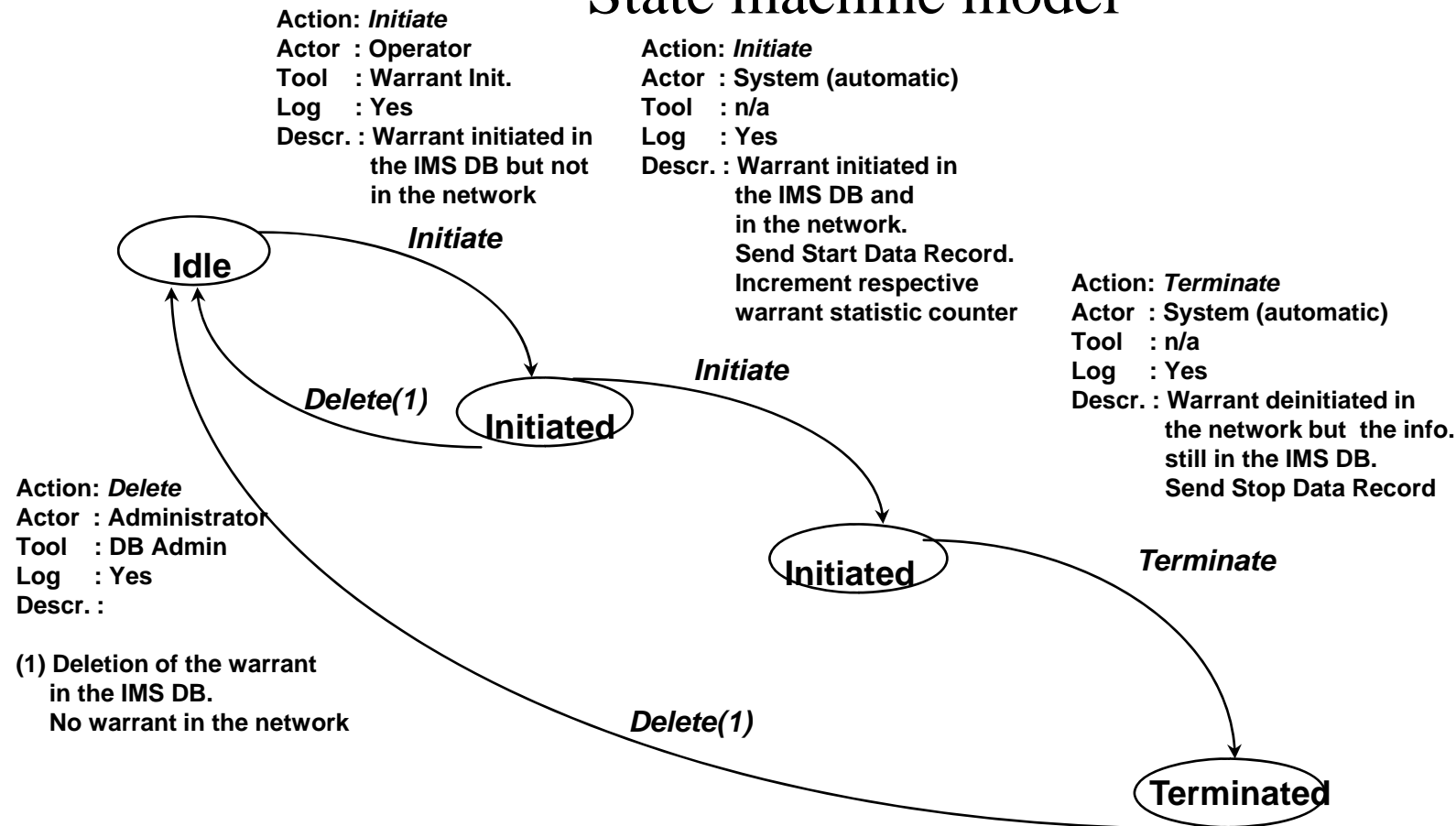
1.8 Warrant Handling

Terminate State machine model



1.8 Warrant Handling

State machine model



1.9 Grouping of Network Element

- NE can be grouped according to characteristics like location, and type of services
- A NE can be member of multiple groups
- Benefit of grouping NE:
 - time saving when updating, upgrading and maintaining
 - centralize the controlling function

2. Remote Control Equipment Subsystem Module Objectives

Be able to:

- Use the AXE MML commands

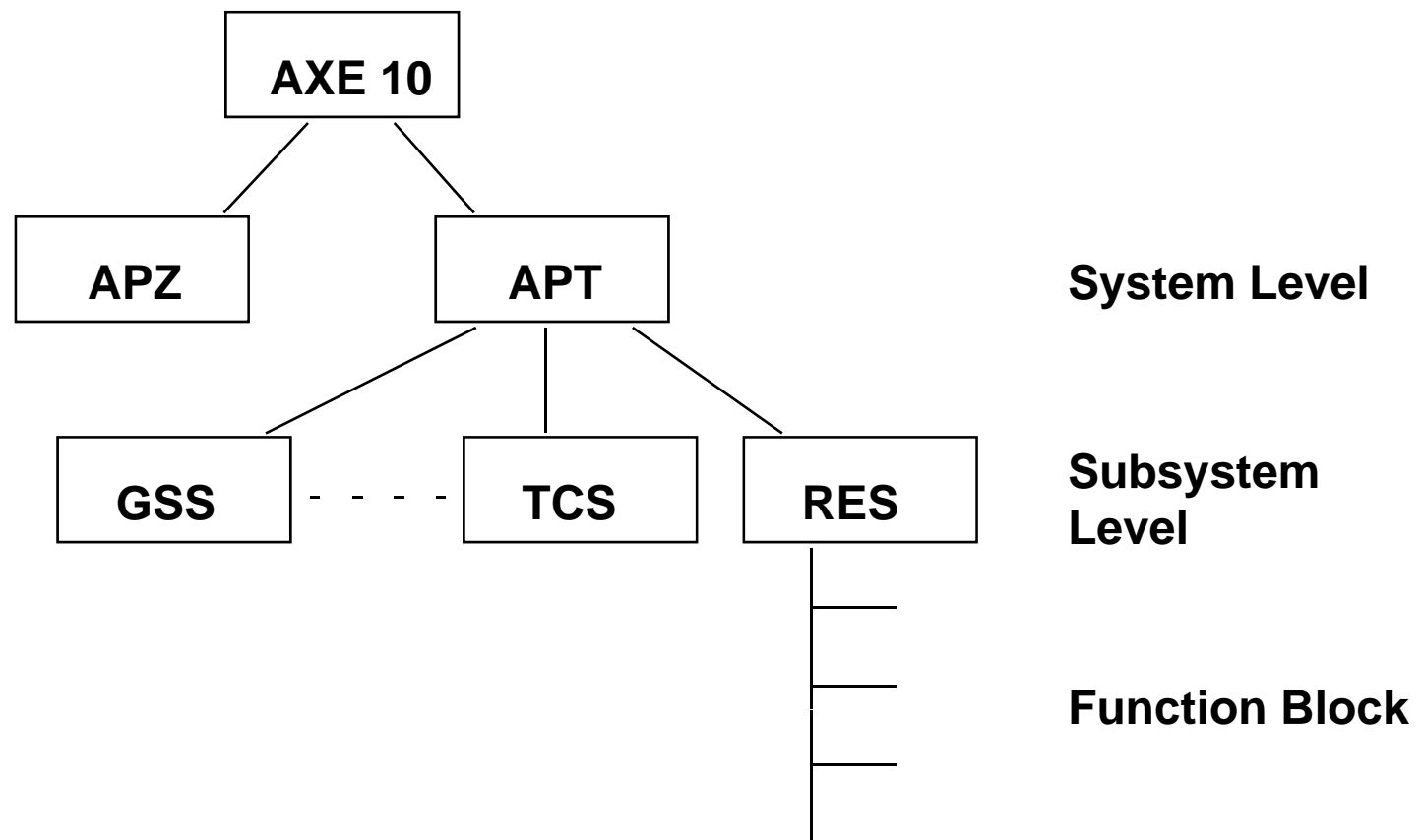
2.1 Remote Control Equipment Subsystem

- The content of the call can be speech or data
- Both calls to & from a target subscriber can be monitored

2.1 Remote Control Equipment Subsystem Implementation

- IMS functions are implemented as a function block (REDRB) on the XMATE system application platform.
- Communication with the external system is provided via DCB
- DCB provides a gateway function between the internal network based on TCP/IP protocol & external communication networks based on the X.25 protocol

2.2 Remote Control Equipment Subsystem



2.3 Useful RES Commands

Here are some sample RES commands:

- **RCSUI** for initiating of a monitoring
Parameters: **MONB, MCNB, CTYPE, RCE, CUG, NI, SUPPRESS** and **MUID**
- **RCSUE** for ending of a monitoring
Parameters: **MONB, MUID**
- **RCSUP** for printing defined data
Parameters: **MONB, MUID**

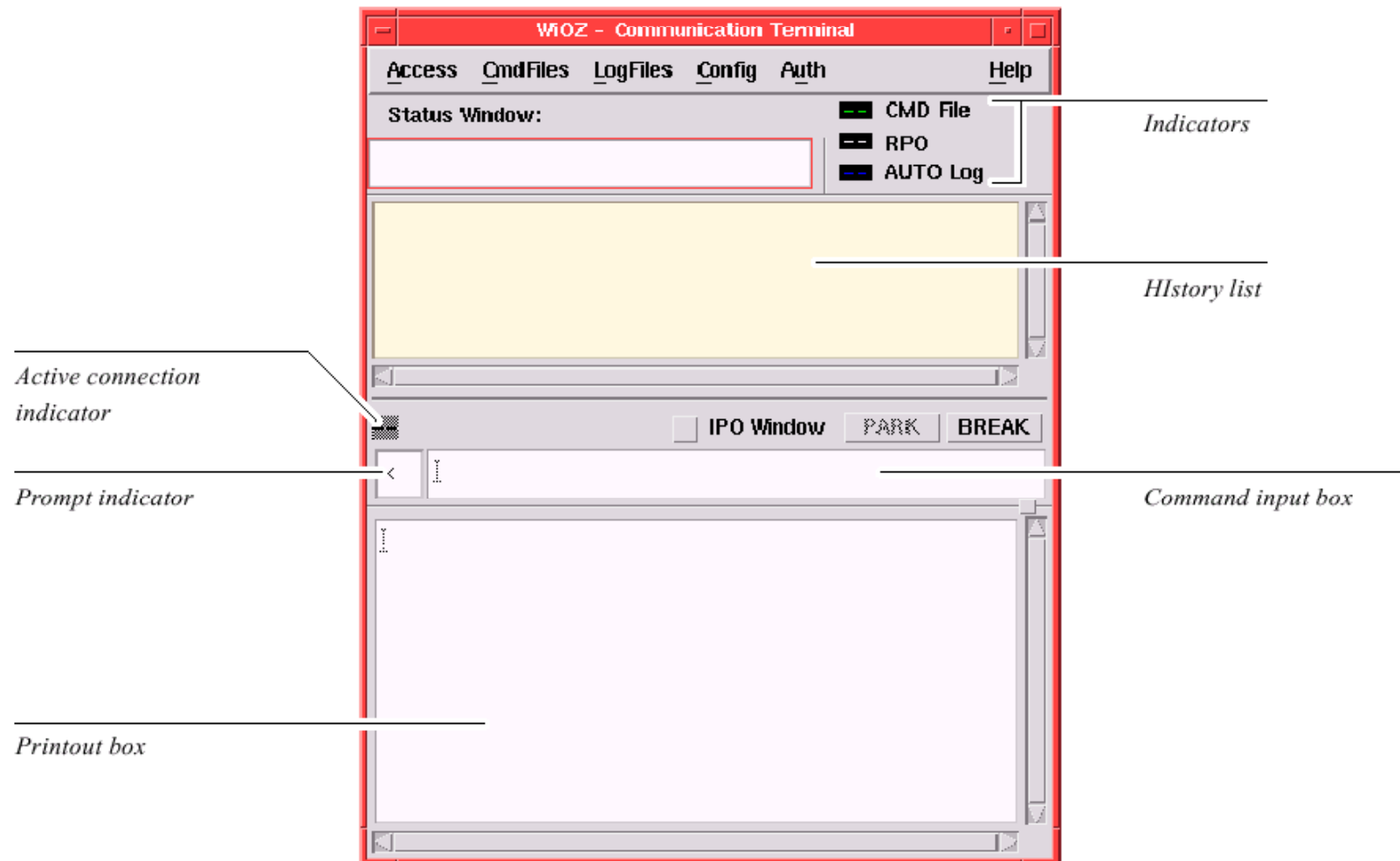
3. Overview of XMATE Platform

Module Objectives

Be able to operate:

- WIOZ Tool
Man Machine Language (MML) Command
Terminal Tool
- Transaction Log Tool

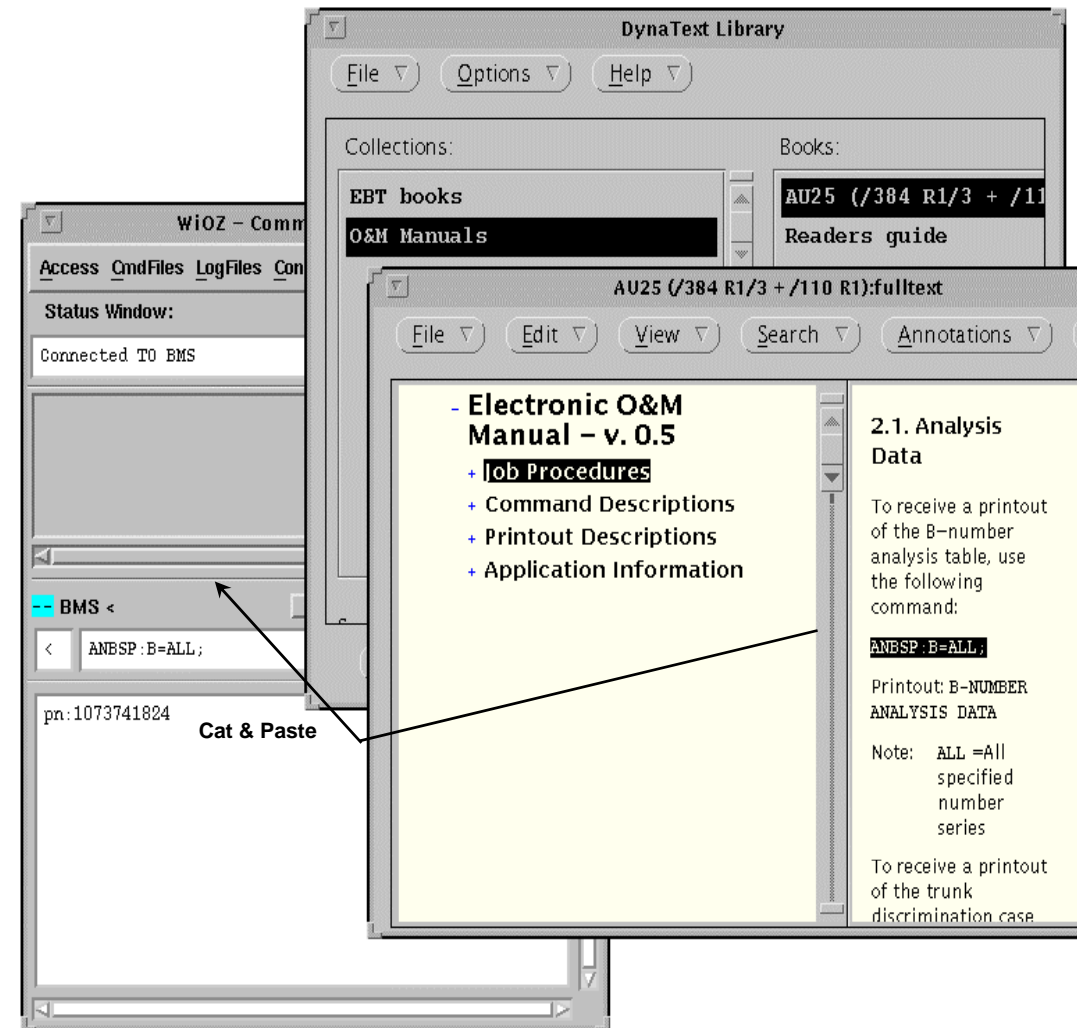
3.1 Man Machine Language Command (MML) Terminal Tool



3.2 MML Terminal Tool Interaction with the electronic manual

Supports:

- Automatic log of commands and responses (Autolog)
- Authority and access control
- Dangerous command notification
- Command log
- Support for the remote FC



3.3 Setting up user preferences

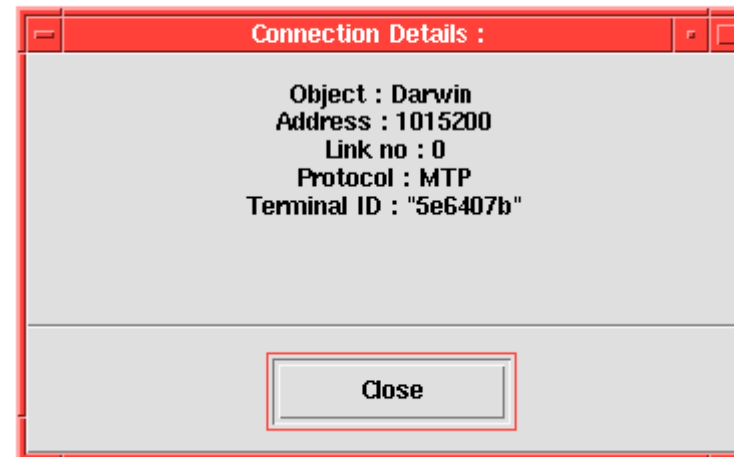
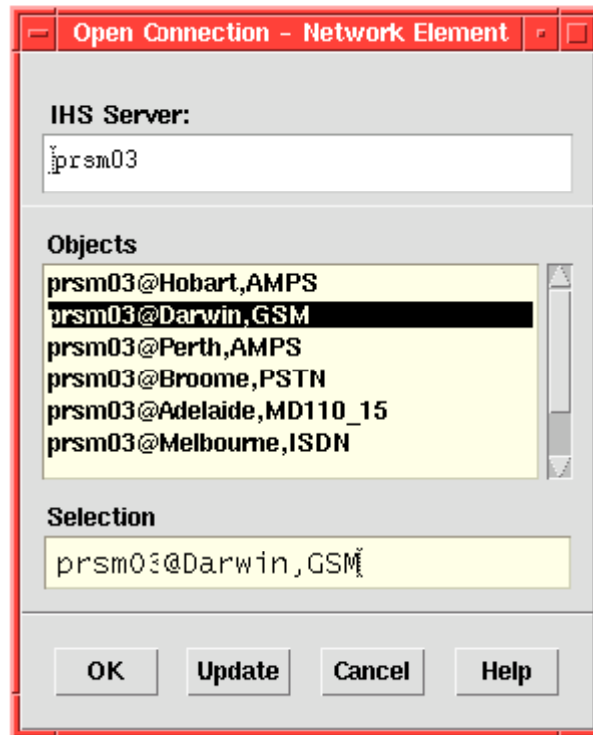
- The system administrator may set up various standard preferences when installing XMATE which you may wish to change to suit yourself.



3.4 Connecting to a network element

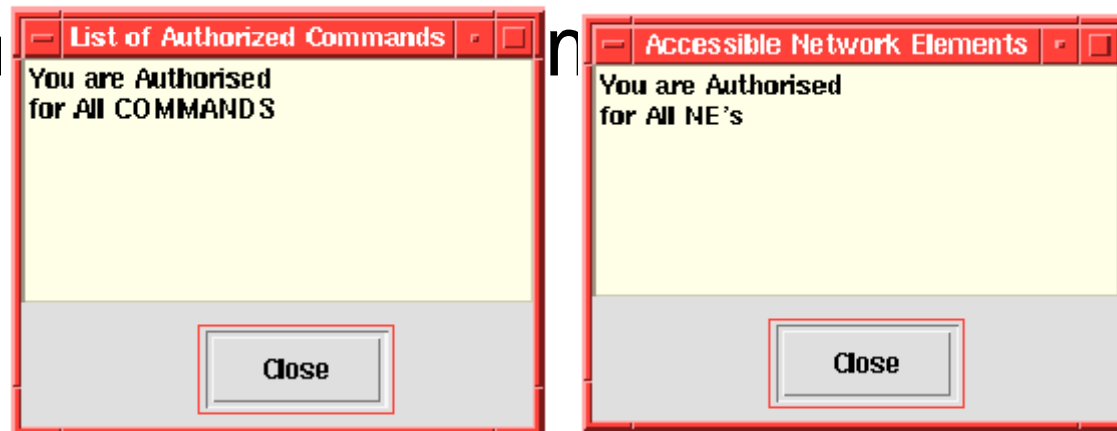
- You can only connect a WiOZ Communication Tool session to a single network element at a time.
- WiOZ Communication Tool session may connect to any network element via a DCS gateway running on any host on your local area network.
- The DCS gateway handles the external connection to remote network elements.
- If you need to connect to several elements, launch additional sessions.

3.5 To open a connection to a network element



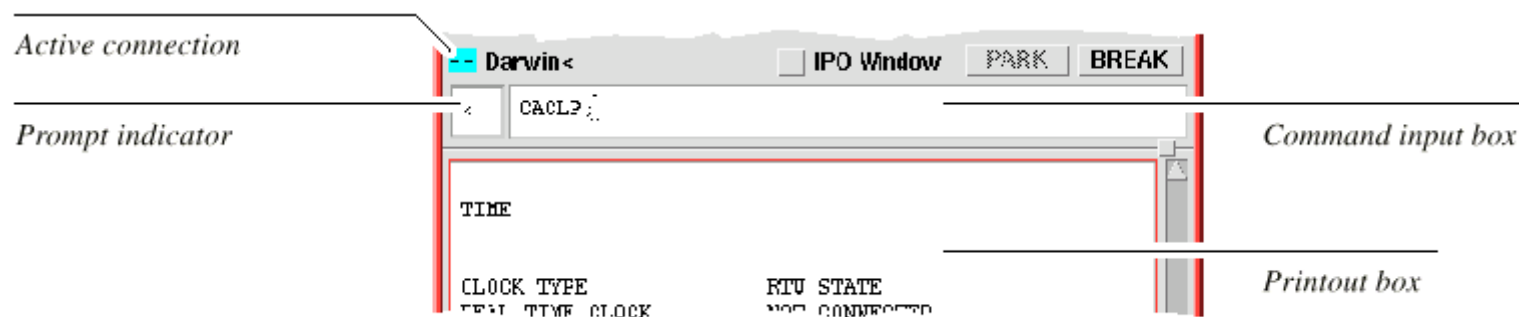
3.6 To view your authorisation settings

- The system administrator sets up your user authorisation file so that you can only connect to particular network elements and send them particular commands. You can view permitted network elements



3.7 Sending commands to network elements

- You send all commands to a network element from the command input box.
- The network element returns all responses – whether immediate printout (IPO) or delayed result printout (RPO) – to the printout box.



3.8 To edit and re-send a command sent previously

- Find the command in the history list and click it only *once*. The command copies to the command input box.
- Edit the command as required and press Return to send it. When the IPO Window button is visible, an immediate response appears in the printout box. The command also appends to the history list regardless if any changes have been made.

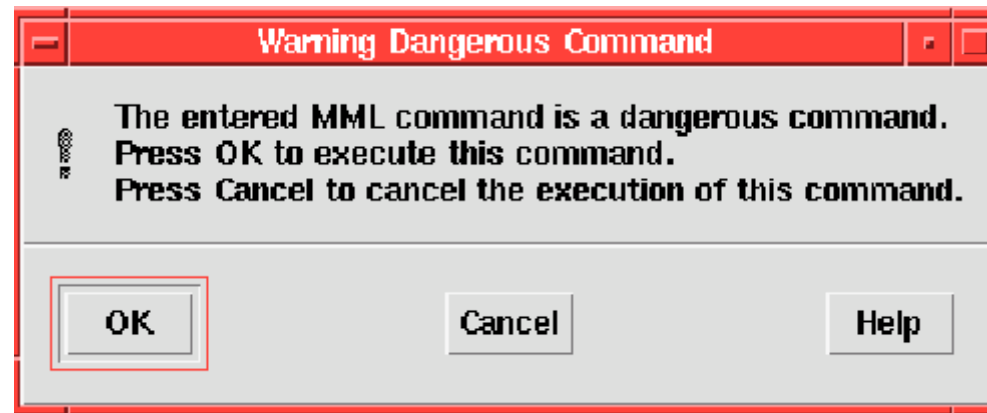
3.9 To immediately re-send a command sent previously

- Find the command in the history list and double-click it.
- WiOZ Communication Tool sends the command immediately without copying it to the command input box. When the IPO Window button is visible, an immediate response appears in the printout box. The command does *not* append to the history list compare with **'To edit and resend a command sent previously'** above.

3.10 Entry Commands and Sub Commands

- Entry command is a command which establishes a session with the specified Support Processor Group (SPG) for various sub-system.
- It enables the operator to subsequently enter sub-commands which are executed in the SPG.

3.11 Dangerous commands



3.10 To step through a command file – *in sequence*

- You must create command files before you can send any to a network element – see.
- This method only lets you send commands in strict sequence from first to last. And you can only see one command at a time.

3.11 To step through a command file – *out of sequence*

- You must create command files before you can send any to a network element.
- This method lets you see all the commands in a command file before you begin sending them.
- You can also send them in any order.

3.12 Handling the output from network elements

- If the IPO window is currently being displayed, the RPO indicator at the top right will illuminate when WiOZ Communication Tool receives a result printout (RPO).
- You can then switch the printout box to view the contents of the RPO.

3.13 To view either immediate or result printouts (IPO or RPO)

- Click the IPO Window button in the WiOZ – Communication Terminal window.
- The button changes to ‘RPO Window’ and the printout box displays the delayed RPO buffer.
- Click the RPO Window button in the WiOZ – Communication Terminal window.
- The button changes to ‘IPO Window’ and the printout box displays the IPO buffer.

3.14 To end a lengthy printout prematurely

- Acknowledgement responses in the immediate printout (IPO) buffer are usually short.
- Result printouts (RPO) can be lengthy and you may wish to cut them short.
- Click the Break button in the WiOZ – Communication Terminal window.
- The response in the printout box ends immediately when viewing either the IPO or
- RPO buffer.

3.15 To save all or part of session printouts to log files

- You may save all or part of the printout box to a log file.
- You can save only the immediate printout (IPO) or only the Result printout (RPO), or you have been switching auto logging on and off, and need to save the entire session.

3.16 To delete the contents of the printout box

- You may want to start with a clean printout box, especially if you wish to save a record of a new session of commands and responses.
- Right-click in the printout box and choose the Clear Window menu option.

3.17 Working with the history list

- When you send a man-machine language (MML) command to a network element, WiOZ Communication Tool appends the command to the history list.
- As you send commands, WiOZ Communication Tool appends them to the top of the history list box, that is, the earliest command is at the bottom and the latest at the top. The line numbers show you the order and help you keep track when resending commands.
- When you save the history list to a command file, the file is ordered as you would expect – earliest commands at the beginning and latest commands at the end.

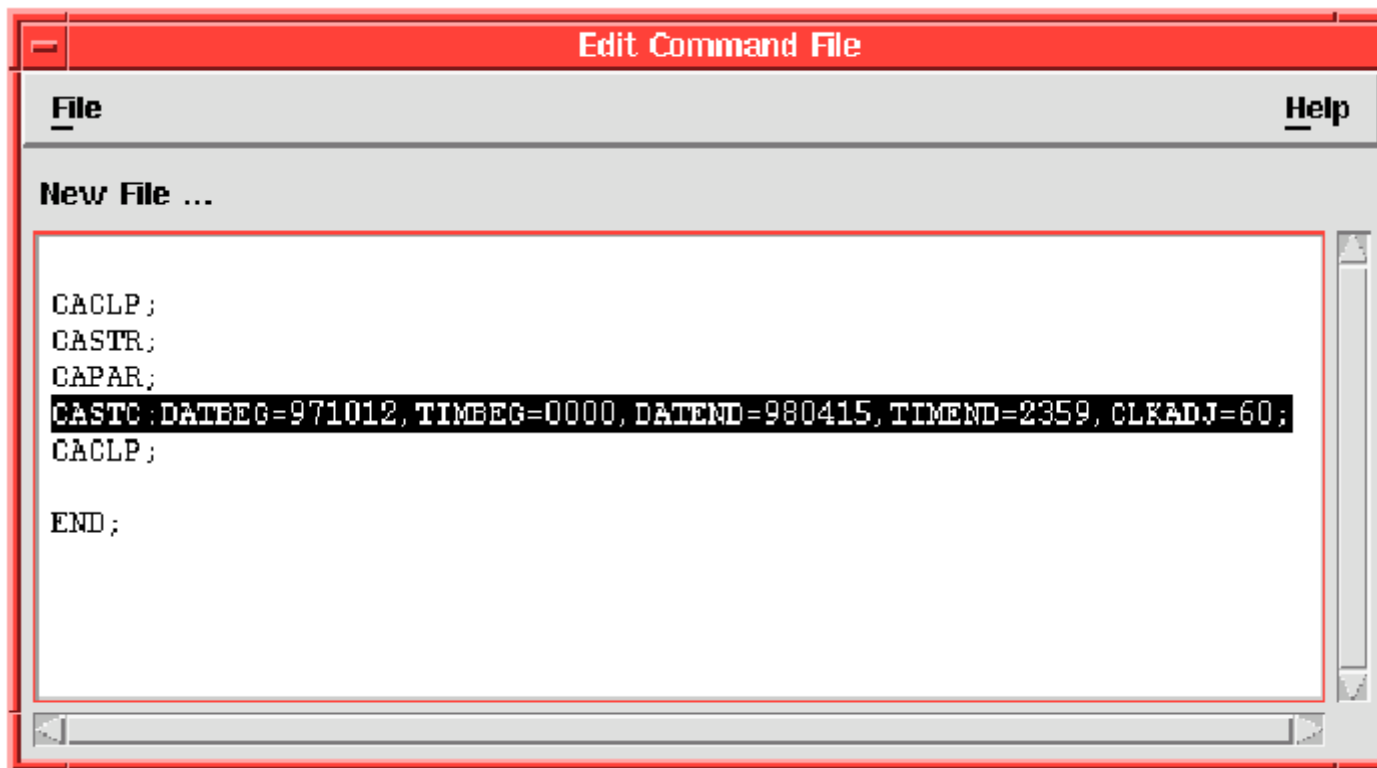
3.18 Working with command files

- Command files consist of a series of man-machine language (MML) statements, one to a line, in the same syntax as you would type them in the command input box.
- In a command file, the first command to execute is at the 'top' or beginning of the file and the last to execute is at the 'bottom' or end.
- When you open a command file in the history list, WiOZ Communication Tool reverses the displayed order.
- The line numbers tell you which are earlier or later. Keep these differences in mind when you are creating and editing command files.

3.19 To save the history list to a command file

- Right-click in the history list and choose the Save To CmdFile menu option. The **File Selection Box** dialogue opens at the default directory for command files. You may navigate to a different directory if you wish.
- Type the name for the new command file and click OK.

3.20 To create new command files



3.21 To edit command files

- A command file is just an ordinary ASCII text file. So you may prefer another editor, such as Text Editor. Or you may use a traditional UNIX editor, such as `vi` or `emacs`.

3.22 To open or import existing command files

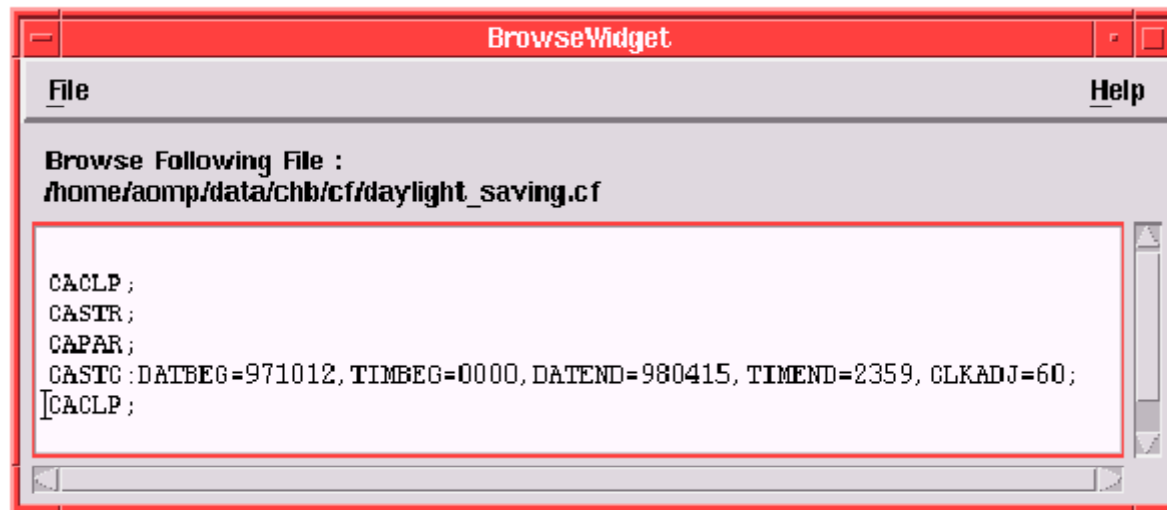
- Consider clearing the current contents of the Edit Command File window.
- A file does not open into a *new* window. Instead, WiOZ Communication Tool inserts the file at the location of the insertion point in the *current* window.
- Choose the File > New menu option to start with an empty window.

3.23 To end an editing session

- **CAUTION No warning of unsaved file**
WiOZ Communication Tool does not warn you if you quit the Edit Command File window while its contents are unsaved.
- Choose the File > Save menu option and save the contents of the Edit Command File window if not already saved.
- Choose the File > Quit menu option.

3.24 Managing command files

- You may use the File Manager of the Common Desktop Environment (CDE) to copy, rename, and move command files. See the Common Desktop Environment.
- **CAUTION Deleted files are gone forever** Once you delete a command file the only way you might be able to recover it is if the system administrator can restore it from

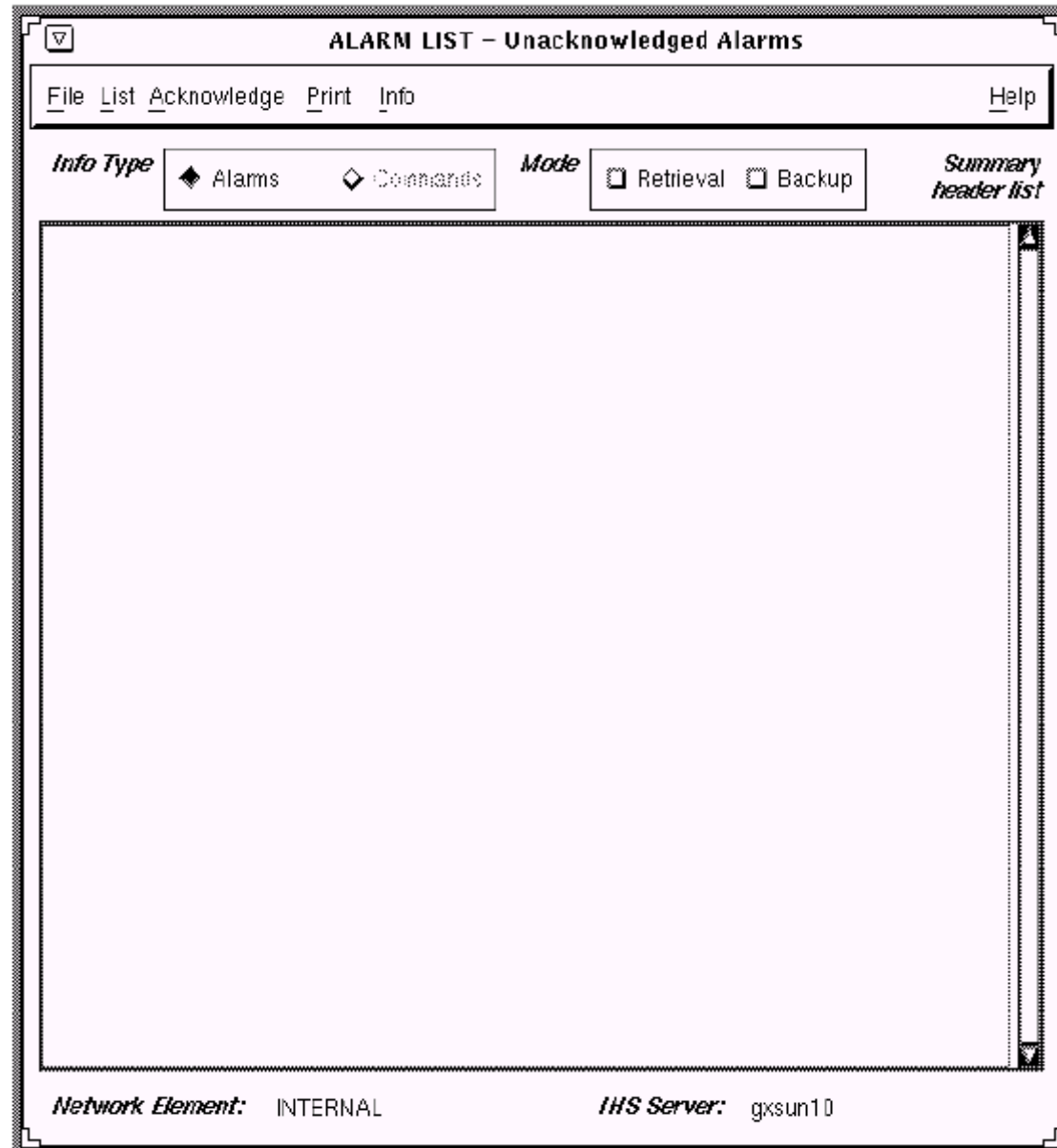


```
File                                     Help  
Browse Following File :  
/home/aomp/data/chb/cf/daylight_saving.cf  
  
CACLP ;  
CASTR ;  
CAPAR ;  
CASTC : DATBEG=971012, TIMBEG=0000, DATEND=980415, TIMEND=2359, CLKADJ=60 ;  
[CACLP ;
```

3.25 Working with session log files

- Log files are a permanent record of the commands sent to a network element and its responses as displayed in the printout box.
- They are useful when you are developing command files and you need a record of the interactions with an network element for debugging.
- Log files can be an audit trail during network operations to record how the behaviour of the network is altered.

3.26 Transaction Log Tool



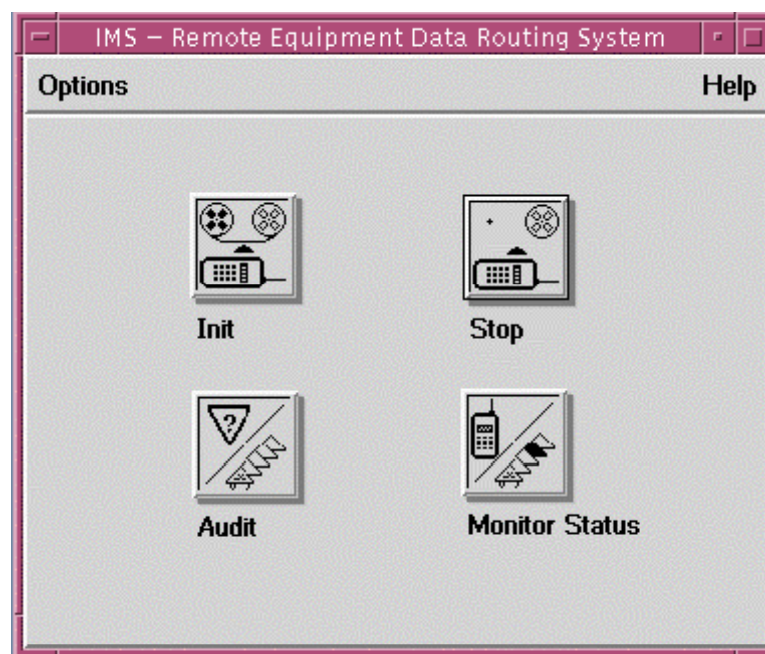
4. IMS Operation

Module Objectives

Be able to:

- Initialise a warrant
- Stop a warrant
- Audit the network
- Monitor network status

4.1 WARRANT MANAGEMENT USER INTERFACE

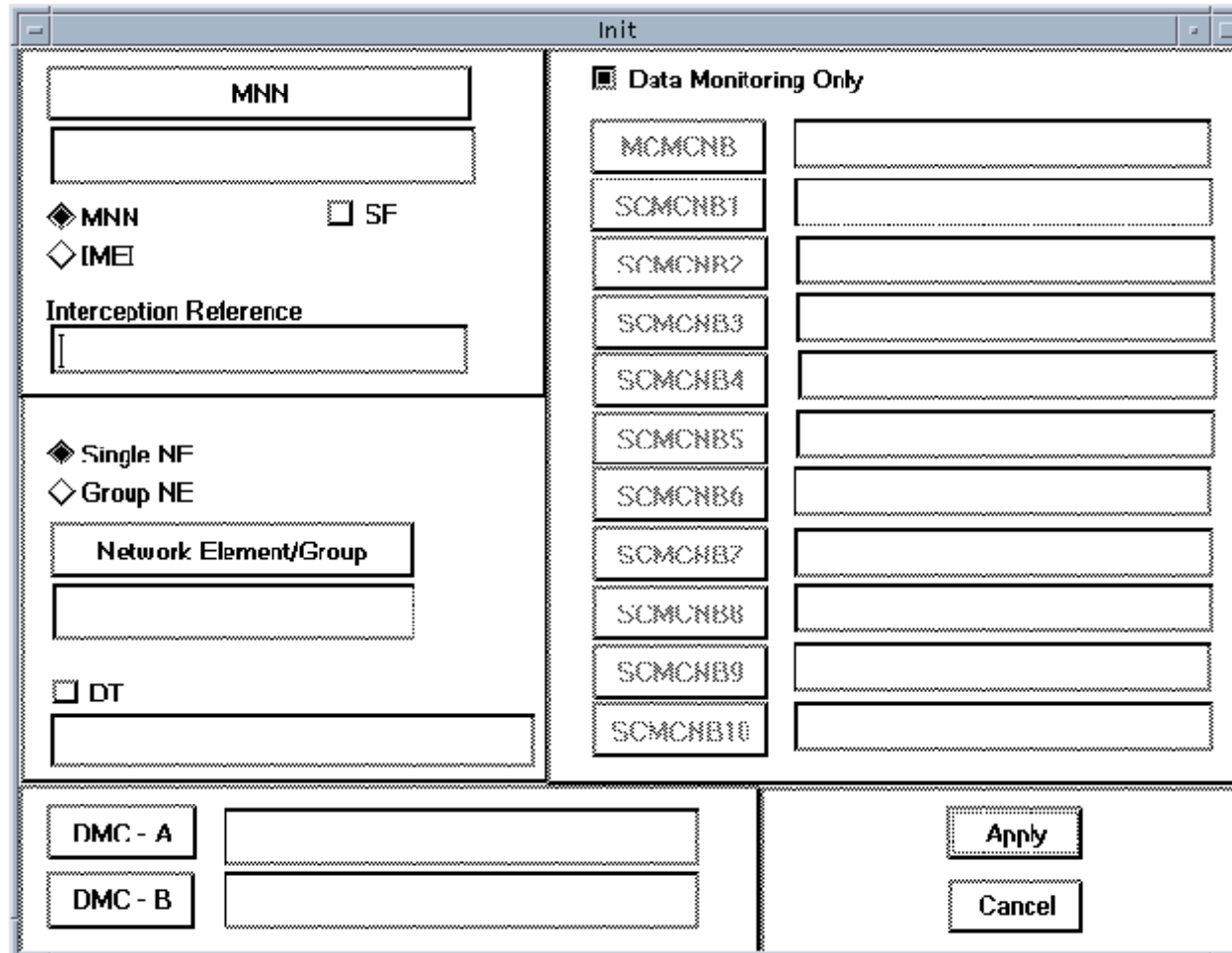


4.2 Warrant Initiation

The screenshot shows a software interface titled "Init" for warrant initiation. It is divided into several sections:

- Left Panel:**
 - A text box labeled "MNN".
 - Below it, a diamond icon followed by "MNN" and a checkbox labeled "SF".
 - A diamond icon followed by "IME".
 - A section titled "Interception Reference" with a text box below it.
 - A section with a diamond icon followed by "Single NF" and a diamond icon followed by "Group NE".
 - A text box labeled "Network Element/Group" with a text box below it.
 - A checkbox labeled "DT" with a text box below it.
- Right Panel:**
 - A checked checkbox labeled "Data Monitoring Only".
 - A vertical list of ten text boxes labeled "MCMCNB", "SCMCNB1", "SCMCNB2", "SCMCNB3", "SCMCNB4", "SCMCNB5", "SCMCNB6", "SCMCNB7", "SCMCNB8", "SCMCNB9", and "SCMCNB10".
- Bottom Panel:**
 - Two text boxes labeled "DMC - A" and "DMC - B".
 - Buttons labeled "Apply" and "Cancel".

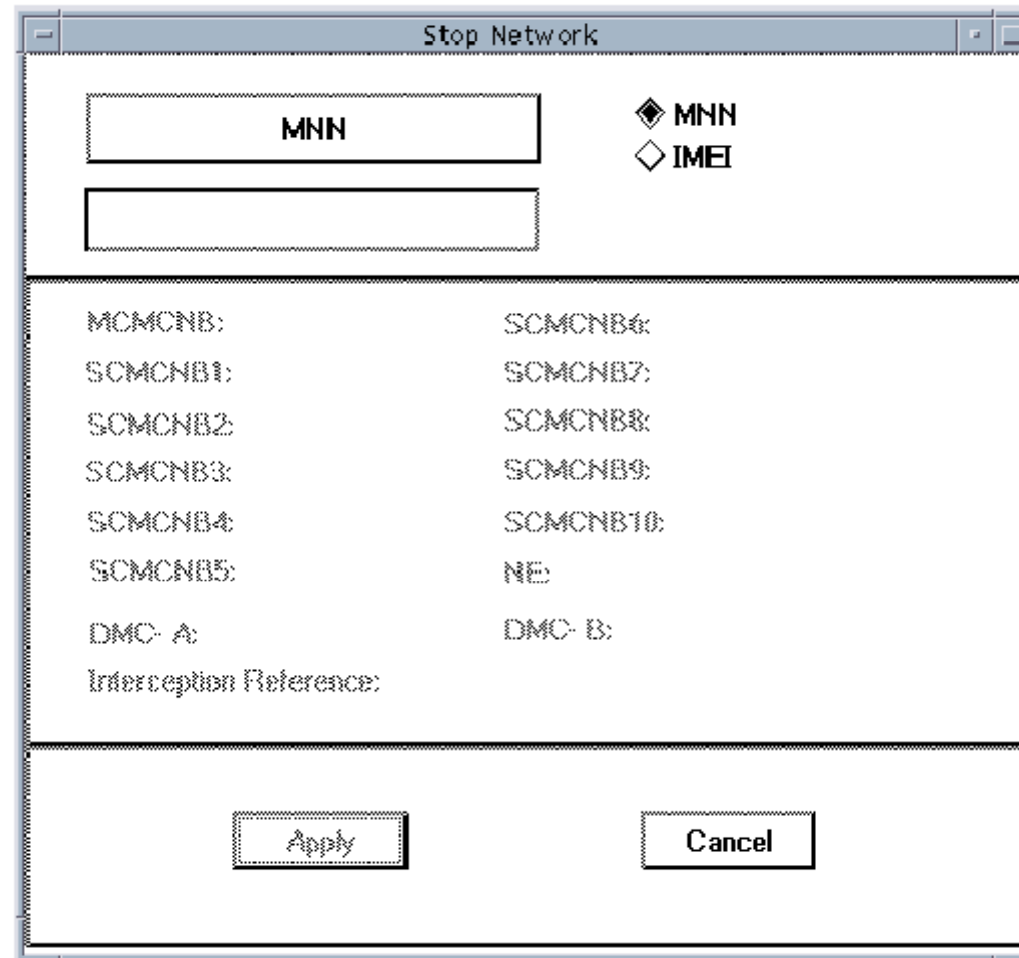
4.3 Warrant Initiation



The screenshot shows a software interface titled "Init" for warrant initiation. The interface is divided into several sections:

- MNN:** A text input field labeled "MNN".
- Options:** Checkboxes for "MNN" (checked), "IMEI", "SF", "Single NF" (checked), "Group NE", and "DT".
- Interception Reference:** A text input field.
- Network Element/Group:** A text input field.
- DMC - A and DMC - B:** Two text input fields.
- Data Monitoring Only:** A section with a checked checkbox and a list of ten SCMCNBs (SCMCNB1 to SCMCNB10), each with an adjacent empty text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

4.4 Warrant Stopping



Stop Network

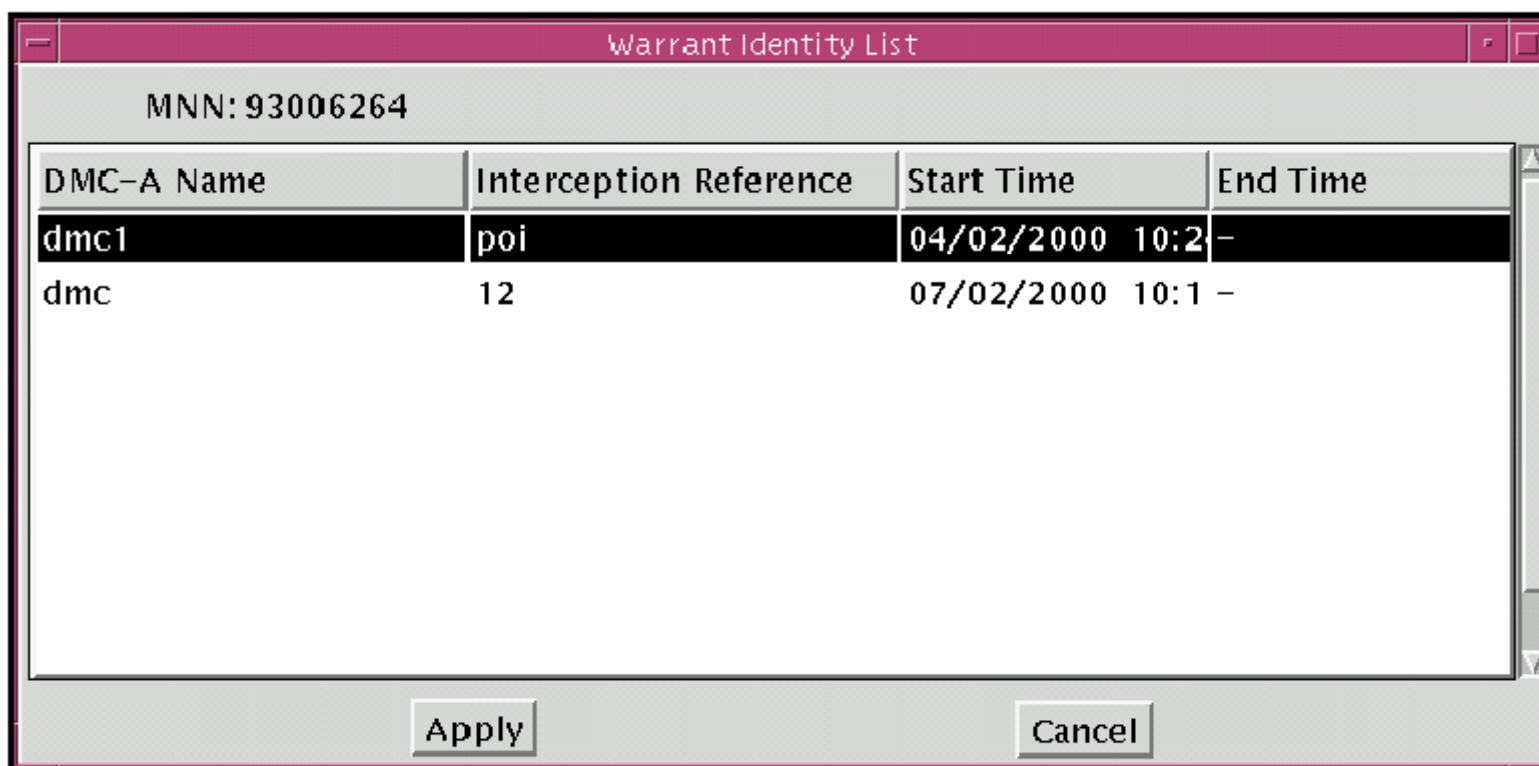
MNN

MNN
 IMEI

MCMCNB: SCMCNB4:
SCMCNB1: SCMCNB7:
SCMCNB2: SCMCNB8:
SCMCNB3: SCMCNB9:
SCMCNB4: SCMCNB10:
SCMCNB5: NE:
DMC- A: DMC- B:
Interception Reference:

Apply Cancel

4.5 Warrant Stopping



MNN: 93006264

DMC-A Name	Interception Reference	Start Time	End Time
dmc1	poi	04/02/2000 10:2	-
dmc	12	07/02/2000 10:1	-

Apply Cancel

4.6 Audit the Network

The audit function can be used to obtain these details:

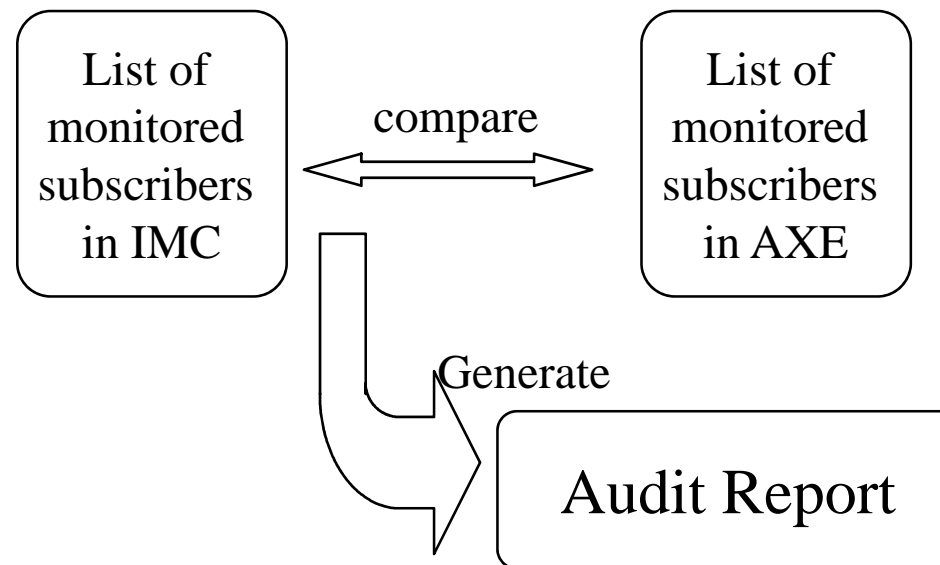
- what interceptions have been initiated for a particular network element or group of network elements.
- which network elements or groups of network elements are actively intercepting calls.
- which subscribers are the targets of interceptions.

4.7 Synchronise the IMS & NE Database

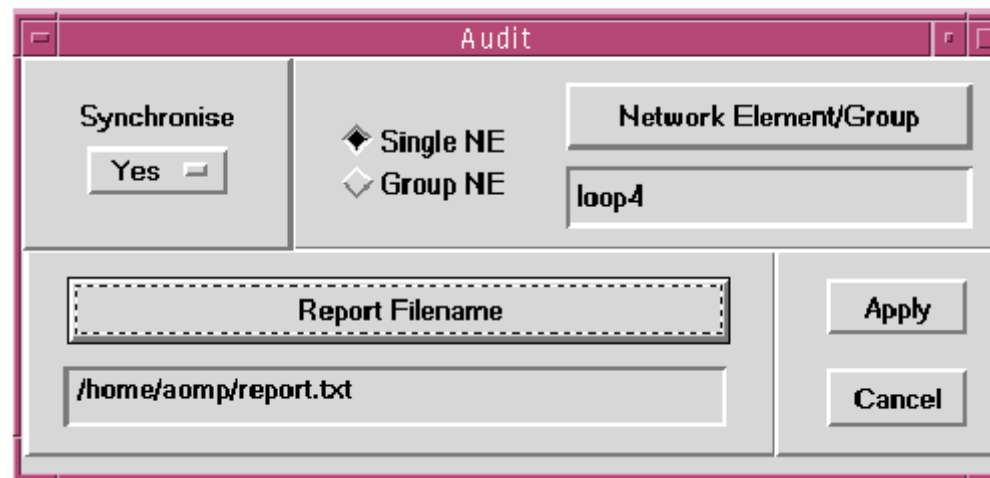
- Synchronising forces the specified network elements to be updated based on the audit report contents.
- The IMS Database is assumed to be correct, hence all activation in the network elements are synchronised to be consistent with the IMS Database.

4.8 Audit Process

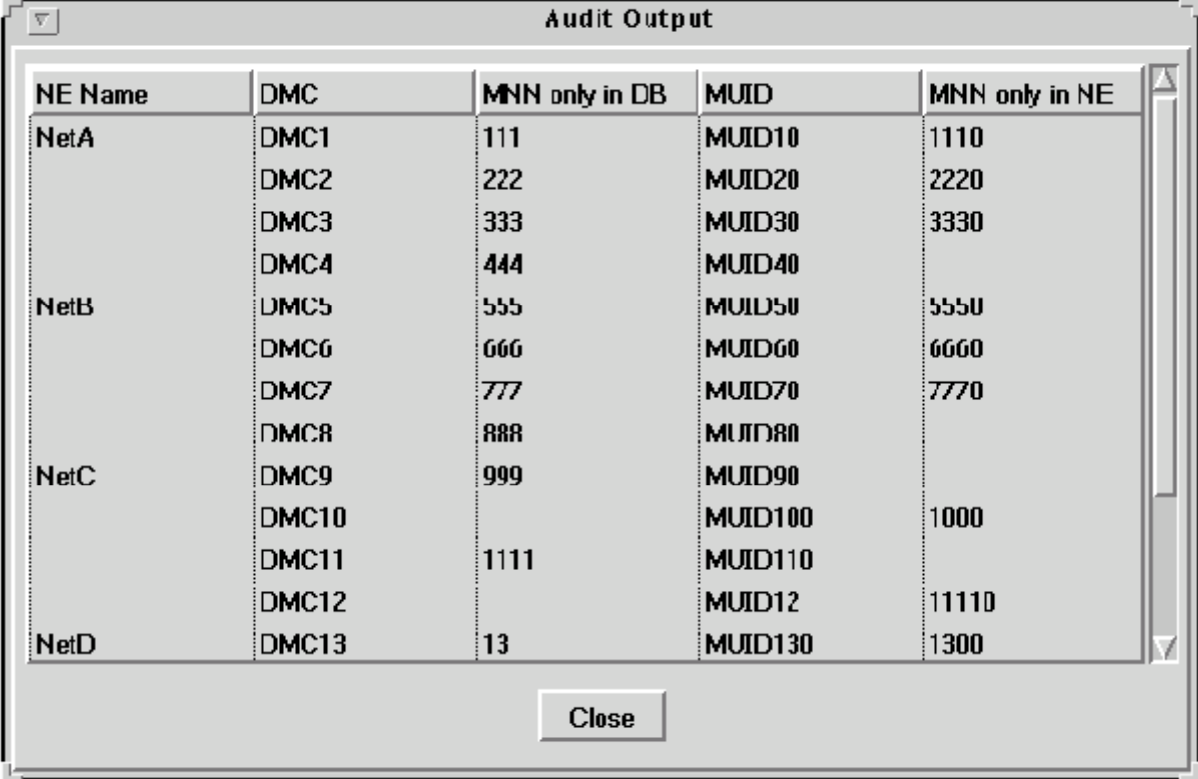
- Provides a comparison between the list of monitored subscribers in an AXE & the IMS.



4.9 Audit User Interface



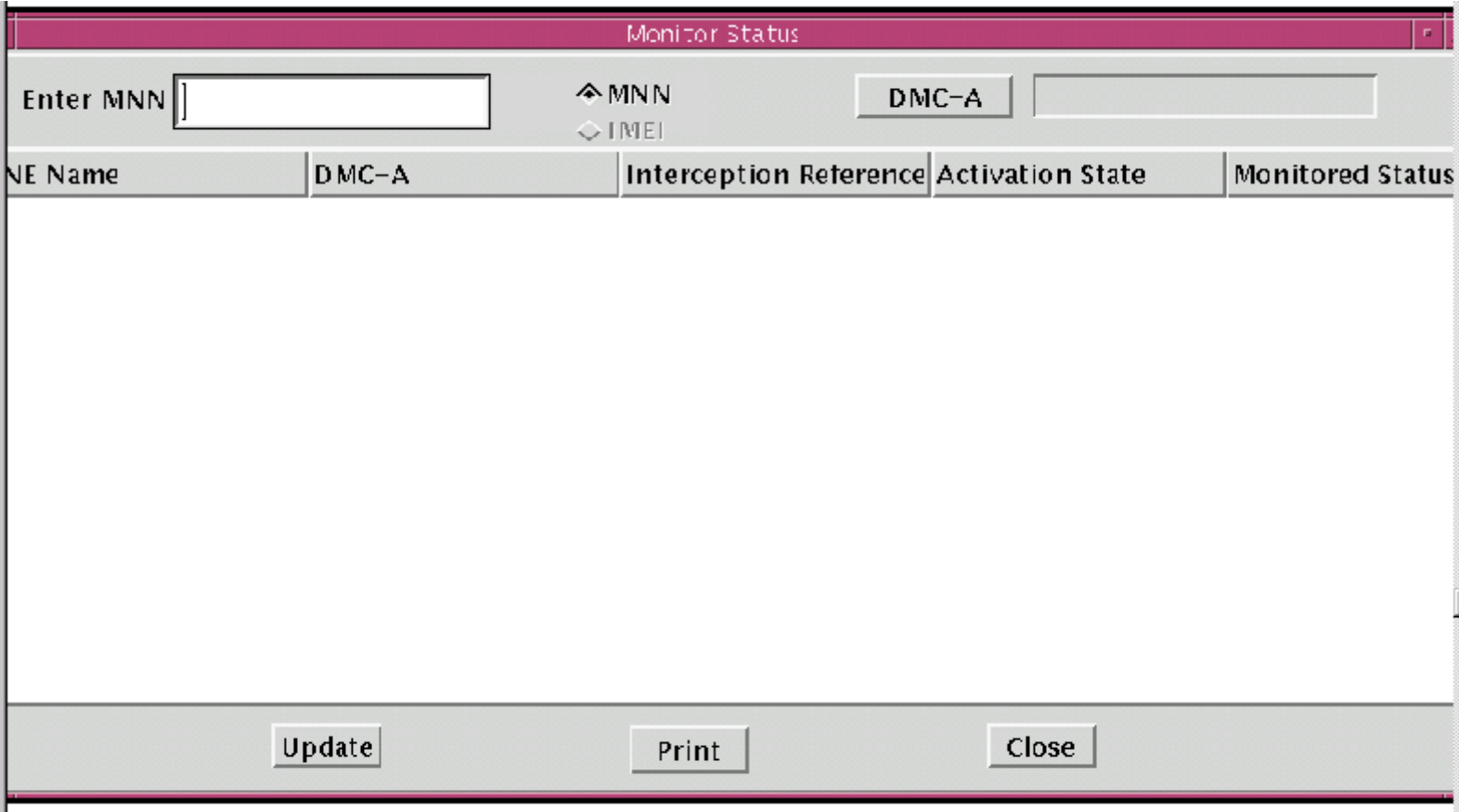
4.10 Audit Output



NE Name	DMC	MNN only in DB	MUID	MNN only in NE
NetA	DMC1	111	MUID10	1110
	DMC2	222	MUID20	2220
	DMC3	333	MUID30	3330
	DMC4	444	MUID40	
NetB	DMC5	555	MUID50	5550
	DMC6	666	MUID60	6660
	DMC7	777	MUID70	7770
	DMC8	888	MUID80	
NetC	DMC9	999	MUID90	
	DMC10		MUID100	1000
	DMC11	1111	MUID110	
NetD	DMC12		MUID12	11110
	DMC13	13	MUID130	1300

Close

4.11 Monitoring Status



Monitor Status

Enter MNN ⬆ MNN DMC-A

⬆ IMEI

NE Name	DMC-A	Interception Reference	Activation State	Monitored Status
---------	-------	------------------------	------------------	------------------