Lucent Technologies
Bell Labs Innovations

AnyMedia® Element Manager - 30 Channel (AEM)

Release 1.7

User Service Manual

363-211-451
Version 1.00
(06.2000)

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Ordering Information

The order number for this document is 363-211-451. For more ordering information, refer to "How to order documents" in the section "About this document".

How to Comment on This Document

A feedback form is located immediately after the legal page of this document. Please send or fax your comments and suggestions to:
Lucent Technologies Network Systems GmbH
Fax no.: +49 911 526-3545

Trademarks

Acrobat Reader is registered trademark of Adobe Systems Incorporated.
AnyMedia is a trademark of Lucent Technologies.
Internet Explorer is a copyright of Microsoft Corporation.
Netscape Navigator is a trademark of Netscape Communications Corporation.
Windows 95 and *Windows 98* are copyrights of Microsoft Corporation.
UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Quality Management System

The Quality Management System (QMS) for Lucent Technologies' Product Realization Center (PRC) Access has been registered to ISO 9001 under the Norwegian Scheme by Det Norske Veritas (DNV) since June 1993. ISO 9001 is an international quality standard recognized by more than 90 countries worldwide. It is a model for quality assurance in design, development, production, installation, and servicing.

Telefax to:
Lucent Technologies Network Systems GmbH
Fax no.: +49 911 526-3545

How Are We Doing?

Lucent Technologies welcomes your feedback on this document. Your comments can be of great value in helping us improve our documentation. Please use a copy of this page for your comments.

1. Please rate the effectiveness of this document in the following areas:

	Excellent	Good	Fair	Poor
Ease of Use				
Clarity				
Completeness				
Accuracy				
Organization Structure				
Appearance				
Examples				
Illustrations				
Overall Satisfaction				

2. Please check the ways you feel we could improve this document:

- ❒ Improve the overview/introduction
- ❒ Improve the tables of contents
- ❒ Improve the organization structure
- ❒ Include more figures
- ❒ Add more examples
- ❒ Add more detail
- ❒ Make it more brief/concise
- ❒ Add more step-by-step procedures/tutorials
- ❒ Add more troubleshooting information
- ❒ Make it less technical
- ❒ Add more/better quick reference aids
- ❒ Improve the index

Please provide details for the suggested improvement:

. . . . . .
. . . . . .
. . . . . .

3. What did you like most about this document?

. . . . . .
. . . . . .
. . . . . .

4. Feel free to write any comments below or on an attached sheet.

. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

If we may contact you concerning your comments, please complete the following:

Name: . . . . . Telephone Number: . . . . . .

Company/Organization: . . . . . Date: . . . . . .

Address: . . . . . .

When you have completed this form, please fax it to the address on top of this page.

Title: *AnyMedia*® Element Manager - 30 Channel (AEM) Release 1.7 User Service Manual

363-211-451 Version 1.00 (06.00)

Contents

About this document XI

1 Overview XI

2 Intended audience XII

3 How to use this document XIII

4 Conventions used XIV

5 General safety information XV

5.1 General notes on safety XV

5.2 General safety requirements XVI

6 Related documentation XVIII

6.1 Print copy (hard copy) XVIII

6.2 CD-ROM XIX

7 How to order this document XIX

8 How to comment on this document XX

1 Functional description 1-1

1.1 About this subject 1-1

1.2 Introduction 1-2

1.2.1 Main functions 1-2

1.2.2 ISO functional areas 1-3

1.2.3 Applications 1-4

1.2.4 System working modes 1-5

1.2.5 Performance, reliability and availability 1-6

1.3 System and software architecture 1-7

1.3.1 Functional groups 1-7

1.3.2 Hardware platform 1-21

1.4 Working with AEM 1-23

1.4.1 Network planning and physical installation 1-24

1.4.2 Configuration management 1-25

1.4.3 Network operation & surveillance 1-26

1.4.4 System security and user groups 1-31

1.5 Network configuration 1-32

Contents

1.5.1 AEM server without clients and external OS (LAN) 1-32
1.5.2 AEM server with clients and without external OS (LAN) 1-33
1.5.3 AEM server without clients and with external OS (WAN) 1-34
1.5.4 AEM server with clients and external OS (WAN) 1-35

2 Software installation and commissioning 2-1
2.1 General 2-1
2.1.1 Introduction 2-2
2.2 Installation procedure 2-7
2.2.1 Full installation 2-7
2.2.2 Installing individual packages 2-75
2.2.3 Cancel installation 2-77
2.2.4 Remove *AnyMedia* package installations 2-77
2.2.5 PC-GUI client installation 2-77

3 System management 3-1
3.1 Overview 3-1
3.2 System access 3-2
3.2.1 Login to operation system 3-2
3.2.2 Logout from operation system 3-3
3.2.3 AEM access bar 3-4
3.2.4 Capacity 3-5
3.3 General information on keyboard and windows 3-5
3.3.1 Keyboard 3-5
3.3.2 Mouse 3-5
3.3.3 Different aspects of the cursor 3-6
3.3.4 Basics on windows 3-6
3.3.5 Window menu 3-9
3.3.6 Menu bar 3-10
3.3.7 Cursor menu 3-10
3.3.8 Workspace manager 3-11
3.3.9 Workspace menu 3-11

Contents

3.3.10 Controls in AEM windows 3-12
3.4 System administration 3-16
3.4.1 General 3-16
3.4.2 Start-up/shutdown of server applications via command line 3-18
3.4.3 System administration window 3-19
3.4.4 View distributed module groups of a package 3-26
3.4.5 Editing distributed module groups 3-27
3.4.6 Editing module groups 3-28
3.4.7 Contents of packages and (distributed) module groups 3-31
3.5 Print out reports 3-34
3.5.1 Page Setup dialog 3-34
3.5.2 Print dialog 3-35
3.5.3 Preview Frame dialog 3-36
3.6 Backup and restore 3-38
3.6.1 Basics on backups and AEM databases 3-38
3.6.2 Commands for backup, archive and restore 3-39
3.6.3 Backup, archive and restore procedures 3-41
3.6.4 Examples for backup schedules 3-43
3.7 Log management 3-46
3.7.1 Different log types 3-46
3.7.2 Configuration of logs 3-46
3.7.3 Log Viewer window 3-47
3.8 Disaster recovery 3-53

4 User management 4-1
4.1 Introduction 4-1
4.2 User 4-3
4.2.1 Create user 4-3
4.2.2 Modify user 4-5
4.2.3 Delete user 4-7
4.3 Domains 4-8
4.3.1 Create domains 4-8
4.3.2 Modify domains 4-10
4.3.3 Delete domains 4-12

Contents

4.4 User groups 4-14
4.4.1 Create user groups 4-14
4.4.2 Modify user groups 4-19
4.4.3 Delete user groups 4-23
4.5 Controlled objects 4-25
4.5.1 Modify controlled objects 4-25

5 NE management/equipment configuration 5-1
5.1 Introduction 5-1
5.2 Overview of the controlled system 5-1
5.2.1 Network element R1.3 5-2
5.2.2 Network element release R1.3.1 5-6
5.2.3 Network element release R1.4 5-6
5.2.4 Broadband applications 5-13
5.2.5 AEM R1.7 new equipment configuration features 5-15
5.3 Initial windows 5-17
5.3.1 Menu bar 5-18
5.3.2 Tool bar 5-19
5.3.3 Background Map 5-20
5.3.4 Status bar 5-21
5.3.5 Cursor menu 5-22
5.4 Groups and NEs Management 5-25
5.4.1 Groups management 5-25
5.4.2 NEs management 5-28
5.4.3 Groups & NEs window 5-29
5.5 Equipment configuration 5-35
5.5.1 Add a network element 5-37
5.5.2 Connection states AEM - telephony agent 5-40
5.5.3 Communication states AEM - data agent 5-44
5.5.4 Shelf View 5-50
5.5.5 Configuration of the packs 5-55
5.5.6 Network element synchronization 5-123
5.5.7 Configuration of timing source (for telephony only) 5-129
5.5.8 Date & Time Telephony window 5-134

Contents

5.5.9	Date & Time Data window	5-136
5.5.10	NE Inventory window	5-138
5.5.11	Network element working mode	5-141
5.5.12	Simplex COMDAC protection scheme	5-141
5.5.13	Equipment protection switching	5-143
5.5.14	Network element software upgrade	5-151
5.5.15	COMDAC program copy	5-159
5.5.16	AFM program copy and validation	5-161
5.5.17	Nonvolatile data storage (NVDS)	5-163
5.5.18	TL1 cut-through (telephony agent)	5-170
5.5.19	Delete network element	5-171

6 Service provisioning 6-1

6.1	Introduction	6-1
6.2	Service provisioning (telephony)	6-1
6.2.1	V5 network interfaces	6-9
6.2.2	Add V5 links to V5 interface	6-20
6.2.3	Physical Feeders List window	6-24
6.2.4	Leased Line Link window	6-26
6.2.5	V5 Link window	6-30
6.2.6	Primary and secondary V5.2 links	6-35
6.2.7	HDSL interface	6-39
6.2.8	User ports	6-48
6.2.9	Move a V5 interface in service	6-132
6.2.10	Move a V5 link in service	6-132
6.2.11	Move a V5 user port in service	6-133
6.2.12	Move a ALL/DLL user port in service	6-133
6.2.13	Move a VLL/GLL user port in service	6-134
6.2.14	Delete a VLL/GLL user port	6-134
6.2.15	Delete an ALL/DLL user port	6-135
6.2.16	Delete a V5 user port	6-135
6.2.17	Delete a V5 link	6-136
6.2.18	Remove a communication channel	6-137
6.2.19	Remove a communication path	6-137

Contents

6.2.20 Remove a primary link 6-138
6.2.21 Remove a secondary link 6-139
6.2.22 Remove a V5 protection group 2 6-139
6.2.23 Delete a V5 interface 6-140
6.3 Service provisioning (data) 6-141
6.3.1 ATM Cross Connections List window 6-141
6.3.2 ATM Cross-Connection window 6-144
6.3.3 Add an ATM cross-connection 6-147
6.3.4 Modify an ATM cross-connection 6-148
6.3.5 Remove an ATM cross-connection 6-148

7 Fault management and maintenance 7-1
7.1 Overview 7-1
7.2 Alarm management 7-1
7.2.1 Overview 7-1
7.2.2 Maintain up-to-date alarm information 7-2
7.2.3 Alarm notification to the user 7-3
7.2.4 Provide access to the current alarm data 7-7
7.2.5 Managing the raising of alarms 7-7
7.2.6 Manage alarm acknowledgment 7-8
7.2.7 Managing the clearing of alarms 7-8
7.2.8 Alarm data synchronization 7-8
7.2.9 AEM alarm log handling 7-9
7.2.10 Periodical deletion of cleared alarms 7-9
7.3 Alarm monitoring 7-10
7.3.1 General 7-10
7.3.2 Starting and terminating the alarm viewer 7-10
7.3.3 Performing Alarm Viewer functions 7-11
7.3.4 System management functions 7-18
7.3.5 Alarm Viewer functions 7-24
7.4 Test management 7-25
7.4.1 Telephony tests 7-26
7.4.2 Data tests 7-43
7.5 Alarms 7-49

Contents

7.5.1 Overview 7-49
7.5.2 Alarm types 7-49
7.5.3 Network element alarms 7-51
7.5.4 General element manager platform alarms 7-51
7.5.5 Element manager alarms concerning network element 7-53
7.5.6 Correlated alarms 7-65

8 Performance monitoring 8-1
8.1 Overview 8-1
8.2 ADSL performance monitoring data 8-1
8.2.1 ADSL Performance Monitoring Data window 8-2
8.2.2 Modify the ADSL performance monitoring 8-5
8.3 AFM feeder performance monitoring 8-6
8.3.1 AFM Performance Monitoring window 8-6
8.3.2 Modify the AFM performance monitoring 8-7
8.4 ATM traffic monitoring 8-9
8.4.1 ATM Traffic Monitoring window 8-9
8.4.2 Modify the ATM traffic monitoring 8-10

A Data communications network (DCN) configuration A-1
A.1 Overview A-1
A.2 DCN introduction A-1
A.3 Terms used in this chapter A-2
A.4 Network element communication capabilities A-3
A.5 AEM communication capabilities A-5
A.6 Recommended DCN configurations A-5
A.6.1 ROC over permanent leased lines DCN A-6
A.6.2 Communication with remote NEs using inband ATM PVC A-10
A.6.3 ROC over semi permanent leased lines (COMDAC R1.4.1 agent) A-14

Contents

B Configuration parameters B-1

B.1 Overview B-1

B.1.1 *AnyMedia* server configuration variables B-1

B.1.2 *AnyMedia* client GUI configuration variables B-7

C Northbound interface C-1

C.1 Overview C-1

C.2 Northbound interface basics C-1

C.2.1 Northbound interface description C-1

C.3 Northbound interface specific TL1 messages C-3

C.3.1 REPT ALM (Report Alarm) C-4

C.3.2 RTRV-ALM (Retrieve-Alarms) C-9

C.3.3 RTRV-ALM-ENV (Retrieve-Alarm-Environment) C-15

AB Abbreviations AB-1

GL Glossary GL-1

IN Index IN-1

About this document

1 Overview

Purpose

This User Service Manual (USM) provides the following information for Lucent Technologies *AnyMedia*® Element Manager - 30 Channel (AEM) Release 1.7:

- a product overview and a functional product description
- system turn-up procedures and system modifications
- user management
- configuration management
- fault management and maintenance
- performance monitoring.

The purpose of the USM is to provide the provisioning personnel with all information necessary to provision an *AnyMedia* Access System via the AEM.

The USM is a network oriented manual and will be shipped to all sites where an AEM is available. It provides the provisioning operator(s) with necessary information to configure or re-configure network elements after local installation.

The philosophy behind the provisioning of network elements within a network is that the network is already installed, configured and service has been provided to the network after first installation and that re-configuration of the NE is necessary. Provisioning takes place from the AEM, located in one or more central offices.

2 Intended audience

The USM is intended for personnel who take care of deploying NEs by carrying out all provisioning activities of the NEs using the AEM.

Tasks to be performed by the Provisioning personnel are:

- collect information of provisioning data (e.g. check shelf layout, units list)
- put ports in-service and out-service
- assign timeslots (cross-connections)
- download and upload the provisioning data to and from the NEs
- testing of assigned ports.
- recognize, interpret, analyze or correct failures, caused by provisioning data that is configured incorrectly.

The personnel should at least have the following education level:

- computer knowledge (e.g. windows applications and/or SUN applications)
- telecommunication network knowledge.

3 How to use this document

The guide is divided into a number of sections (subjects), clearly separated by numbered tabs. The front pages of the guide also describe this division, and list the titles of the subjects together with the corresponding tab numbers. Through this readers can quickly select the subject of their interests and needs.

- **How are we doing**
  A comment form so readers can give feedback to improve the next revision of the document.
- **Table of contents, list of figures, list of tables**
- **Overview**
  Defines the purpose of the document and the intended audience. Also included are topics about the conventions used in the document, related documentation, how to order documents, and how to comment on this document.
- **Chapter 1, Functional description**
  Contains a short overview over the system, its features and capabilities.
- **Chapter 2, Software installation**
  Describes the standard procedure to install the AEM R1.7 server package (server applications) and client package (client applications).
- **Chapter 3, System management**
  Provides the system administrator with all information necessary to administer the AEM so that it can be used as a centralized management system.
- **Chapter 4, User management**
  Describes all actions necessary to create/modify/delete users, user groups and domains and the handling of controlled objects.
- **Chapter 5, NE management/Equipment configuration**
  Describes the database and software management, the default system configuration parameters and the equipment provisioning, the inventory management, clock synchronization management and protection switching.
- **Chapter 6, Service provisioning**
  Describes all actions necessary for provisioning both telephony and data services.
- **Chapter 7, Fault management/maintenance**
  Describes alarms and events, how to use the Alarm Viewer, how to perform tests and trouble clearing procedures.
- **Chapter 8, Performance monitoring**
  Describes the display of performance monitoring data and traffic measurements counts.
- **Appendix A**
  Describes the Data Communications Network (DCN) configurations.
- **Appendix B**
  Provides information about the configuration parameters.

- **Appendix C**
  Describes the TL1 Northbound Interface.
- **Abbreviations and acronyms**
  Lists all abbreviations and acronyms used in this manual.
- **Glossary**
  Defines special terms used in this manual.
- **Index**
  Alphabetical index to quickly search for paragraphs in the manual which provide more information on a certain keyword.

4 Conventions used

The following are terms used in this USM that may have a different meaning than the general or common use of the term.

- In the AEM, the term *access* means that the system provides the primary service interface for the customer to enter the network.
- The term *plug-in* is generally used for circuit pack units (COMDAC, CIU, IO_E1, HDLC and application packs (APs)) which have pre-designated slots with the capability to plug-in the circuit pack.

Numbering

Each fascicle can be identified by its number and contains a chapter which is numbered accordingly (e.g. Chapter 2 is contained in Fascicle 2).

The page, figure and table numbering begins with “1” in every chapter. To be able to identify them easily, these numbers are prefixed with the fascicle number. For example, Figure 2-3 designates the third figure in Fascicle 2.

Cross-references

Cross-reference conventions are identical with those used for numbering, i.e. the first number in cross-references refers to the corresponding fascicle.

Keyword blocks

To facilitate the location of specific text passages, the guide contains so-called keyword blocks. These are placed to the left of the main text and contain either a keyword or a word which indicates the contents of a paragraph or group of paragraphs.

Abbreviations

Each abbreviation used in this guide is listed in Fascicle AB (“Abbreviations”) of the hardcopy version unless it can be assumed that the reader is familiar with this abbreviation.

Commands

Commands and messages are displayed in **`constant-width`** font (e.g., **`sysdef | grep SEMMNU`**).

Trademarks

The trademarks used in this document are identified after the title page. Trademarks of Lucent Technologies and other companies are in italics and the trademarks modify a noun (e.g., the system name contains a trademark, *AnyMedia*™ Access System). A trademark is not treated as an acronym (it is not spelled out or expanded).

Lucent Technologies trademarks

Lucent Technologies trademarks are identified with the registered mark (®) or trademark (™) symbol the first time the trademarks are used in a chapter.

Trademarks of other companies

The trademarks of other companies are identified with a footnote reference the first time the trademarks are used in a chapter.

Typographical conventions

The following table gives examples of the typographical conventions used in this chapter.

Table 1 Typographical conventions

Object	Example	Meaning
Keyboard	**`Return`** or **`A`**	**`Return`** or **`A`** key on the keyboard
	`Shift-Ctrl-B`	**`Shift`**, **`Ctrl`** and **`B`** key pressed simultaneously
	`Esc A B`	**`Esc`**, **`A`** and **`B`** key pressed one after the other
Pushbutton	***Apply***	***Apply*** pushbutton in a window
Menu	***File -> Exit***	Menu option ***Exit*** in ***File*** menu
Objects in windows	**Date**	Designates the object **Date** in a window (e.g. text field, check box, spin box etc.)

5 General safety information

This section lists the safety information needed for the *AnyMedia* Access System for system turn-up after installation has been completed, operating, provisioning and maintaining the system.

5.1 General notes on safety

This system has been developed in line with the present state-of-the-art and fulfils the current national and international safety requirements. It is provided with a high degree of operational safety resulting from many years of development experience and continuous stringent quality checks in our company.

The system is safe in normal operation. There are, however, some potential sources of danger that cannot be completely eliminated. In particular, these arise during the

- opening of housings or equipment covers
- manipulation of any kind within the equipment, even if it has been disconnected from the power supply
- disconnection of optical or electrical connections

through possible contact with

- live parts
- laser light

- hot surfaces
- sharp edges, or
- devices sensitive to electrostatic discharge.

5.2 General safety requirements

In order to keep the technically unavoidable residual risk to a minimum, it is imperative to observe the following rules:

- **Installation, configuration and disassembly must be carried out only by expert personnel and with reference to the respective documentation.**
  Due to the complexity of the unit/system, the personnel requires special training.
- **The unit/system must be operated by expert and authorized users only.**
  The user must operate the unit/system only after having read and understood the chapter on safety and the parts of the documentation relevant to operation. For complex systems, additional training is recommended. Any obligatory training for operating and service personnel must be carried out and documented.
- **Any conversions or changes to the system or parts of the system (including the software) must be carried out by qualified Lucent Technologies personnel or by expert personnel authorized by Lucent Technologies.**
  All changes carried out by other persons lead to a complete exemption from liability.
  No components/spare parts must be used other than those recommended by the manufacturer and those listed in the procurement documents.
- **The unit/system must not be operated unless it is in perfect working order.**
  Any faults and errors that might affect safety must be reported immediately by the user to a person in responsibility.
- **The equipment must be supplied with Safety Extra-Low Voltage (SELV) of -48 V and the positive terminal of this source must be correctly connected to the protective earth.**
  Never connect to –60 V.
- **The unit/system must be operated only with the connections and under the environmental conditions as described in the documentation.**
- **The removal or disabling of safety facilities, the clearing of faults and errors, and the maintenance of the equipment must be carried out by specially qualified personnel *only*.**
  The respective parts of the documentation must be strictly observed.
  The documentation must also be consulted during the selection of measuring and test equipment.

- **Transport, storage and operation of the unit/system must be under the permissible conditions only.**
  See accompanying documentation and information on the unit/system.
- **Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived**.
- **Only use tested and virus-free diskettes.**
- **Do not place the shelves on an unstable cart, stand, or table.**
  The product may fall causing serious damage to the equipment.
- **Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquid of any kind on the product.**

5.2.1 Safety symbols and labels

All safety instructions have a uniform appearance. They include a *signal word* that classifies the danger and a *text block* that contains descriptions of the type and cause of the danger, the consequences of ignoring the safety instruction and the measures that can be taken to minimize the danger. In some safety instructions, a *warning symbol* is placed underneath the signal word.

Classification

There are five classes of safety instructions: “Danger”, “Warning”, “Caution”, “Important” and “Notice”. The classification is shown in the following table.

DANGER	Serious injury is definite or likely.
WARNING	Serious injury is possible.
CAUTION	Minor injury is definite, likely or possible, or material damage to the product or in the product environment is definite or likely.
IMPORTANT	Material damage to the product or in the product environment is possible.
NOTICE	A fault, i.e. considerable impairment to operation, will be caused or may be caused.

6 Related documentation

Document list The following is related documentation for the AEM and for additional components:

Table 2 List of documents

Component	Manual type	Comcode	CIC ordering number [a]
A*nyMedia* Access System	Applications, Planning, and Ordering Guide (APOG) (Issue 3 for R1.3, Issue 4 for R1.3.1, Issue 5 for R1.4)	108 298 670	363-211-110
A*nyMedia* Access System	Command and Message Manual (CMM) (Issue 2 for R1.3, Issue 3 for R1.3.1, Issue 4 for R1.4)	108 298 761	363-211-111
A*nyMedia* Access System	User Service Manual (USM) Vol. 1 (Narrowband Services) (Issue 3 for R1.3, Issue 4 for R1.3.1, Issue 5 for R1.4)	108 298 811	363-211-112
A*nyMedia* Access System	User Service Manual (USM) Vol. 2 (Broadband Services) (Issue 2 for R1.4)	108 543 380	363-211-115
A*nyMedia* Access System	Installation Manual for Indoor Application (ONU-IM1)	108 626 367	363-211-150
A*nyMedia* Access System	Installation Manual (IM) (For Rack Configurations) (Issue 3 for 1.3)	108 298 779	363-211-113
AEM R1.7	Functional Description		363-211-450

a For the ordering address see Chapter 7, How to order this document.

6.1 Print copy (hard copy)

Document packaging and format All listed documents are available in print.

6.2 CD-ROM

The User Service Manual and the Functional Description are available in PDF format on CD-ROM and an Adobe Acrobat Reader [1] is provided to view them.

Table 3 Customer documentation on CD-ROM

Component	CD-ROM	Ordering number
AEM R1.7	Customer Documentation on CD-ROM includes: – User Service Manual (USM) – Functional Description	363-211-452

7 How to order this document

Ordering number The ordering number for the AEM *User Service Manual* is 363-211-451.

Order procedure To order additional hard copies of this document and/or to request placement on the standing order list, send or call in an order as follows:

Mail Order[a]	Telephone order (Monday through Friday)
Lucent Technologies Customer Information Center Attention: Priscilla Stanley, email: pfstanley@lucent.com 2855 N. Franklin Road P.O. Box 19901 USA-Indianapolis, IN 46219	Within USA:1-888-LUCENT8 7:30 a.m. to 6:30 p.m. EST FAX from USA: +1-800-566-9568 FAX Worldwide: +1-317-322-6699

a For ordering, a purchase order number, or charge card number is required with all orders. Make checks payable to Lucent Technologies.

One-time orders One-time orders include the contents for the current document issue in effect at the time of order.

Standing orders You may request an update on the standing order list for all later reissues of any document. The standing order list for each document provides automatic distribution for all reissues of the document.

1 *Acrobat Reader* is a registered trademark of Adobe Systems Incorporated.

8 How to comment on this document

Document comment procedure

The first sheet in this manual (after the title page) is the feedback form *How Are We Doing?*

Please use this form to fax your comments and suggestions concerning the USM, 363-211-451 to:

Lucent Technologies Network Systems GmbH
Fax no.: +49 911 526-3545.

Functional description

1

Contents

1.1 About this subject 1-1

1.2 Introduction 1-2

1.2.1 Main functions 1-2

1.2.2 ISO functional areas 1-3

1.2.2.1 Configuration management 1-3

1.2.2.2 Fault management 1-3

1.2.2.3 Performance management 1-4

1.2.2.4 Security management 1-4

1.2.3 Applications 1-4

1.2.4 System working modes 1-5

1.2.5 Performance, reliability and availability 1-6

1.3 System and software architecture 1-7

1.3.1 Functional groups 1-7

1.3.1.1 Network element management 1-8

1.3.1.2 General components 1-15

1.3.1.3 Software platform 1-18

1.3.1.3.1 Software bus 1-18

1.3.1.3.2 Repository 1-18

1.3.1.4 Graphical user interface (GUI) 1-19

1.3.1.5 Northbound interface 1-20

1.3.1.6 Southbound interface 1-20

1.3.2 Hardware platform 1-21

1.3.2.1 Architecture 1-21

1.3.2.2 Requirements 1-22

1.4 Working with AEM 1-23

Contents

1.4.1 Network planning and physical installation 1-24
1.4.2 Configuration management 1-25
1.4.3 Network operation & surveillance 1-26
1.4.3.1 Fault management 1-26
1.4.3.1.1 Fault identification 1-27
1.4.3.1.2 Fault localisation and diagnosis 1-28
1.4.3.1.3 Fault clearance 1-28
1.4.3.2 Network modification 1-29
1.4.3.2.1 Installation and removal of an NE 1-29
1.4.3.2.2 Modification of NEs 1-30
1.4.3.3 Performance monitoring 1-30
1.4.4 System security and user groups 1-31
1.5 Network configuration 1-32
1.5.1 AEM server without clients and external OS (LAN) 1-32
1.5.2 AEM server with clients and without external OS (LAN) 1-33
1.5.3 AEM server without clients and with external OS (WAN) 1-34
1.5.4 AEM server with clients and external OS (WAN) 1-35

Functional description

1

1.1 About this subject

Scope

This chapter describes the *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7. This release covers the following network element (NE) releases:

- narrowband (NB) releases R1.3, R1.3.1 and R1.4
- broadband (BB) releases R1.1.2 and R1.4.

NOTE:
For the AEM the terms telephony/data are used instead of narrowband/broadband.

Purpose

This chapter provides an overview of the AEM and tries to give an insight into the functioning of the AEM by providing detailed information on the AEM features mentioned.

Contents

The following AEM subjects are described:

- basic functionality
- management features
- system and software architecture
- hardware and software platform
- interfaces
- applications.

1.2 Introduction

General

The AEM is part of a telecommunication management network (TMN). It represents the element management layer and fulfils the tasks of the ISO (*International Organisation for Standardization*) functional areas (see Chapter 1.2.2, page 1-3).

Benefits

This provides some benefits for the operator:

- better control over revenue generating services by local and centralized management
- reduced time and effort for provisioning tasks
- fast and efficient fault detection and isolation
- prevention of unauthorized access by appropriate security mechanisms
- reduction of operator mistakes by easy-to-use graphical user interface (GUI)
- integration with higher management levels for network, service and business purposes.

1.2.1 Main functions

The AEM provides the following main characteristics/functions:

- support of all *AnyMedia* Access Systems features (telephony and data)
- equipment overview
- telephony and data service provisioning
- common alarm handling for all network elements (NEs)
- test management
- data performance monitoring
- report, log, backup and restore functions
- southband interfaces:
  - TL1 NE access via TCP/IP for telephony agents based on data communication network (DCN)
  - SNMP NE access via UDP/IP for data agents based on DCN
- user security handling (user profiles, NE domains)
- online help
- multi user access
- northbound interfaces
  - TL1 pass through interface for telephony alarm collection and COBRA interface
  - CORBA interface (i.e. AEM CORBA IDLs are published so that a network management system can access to them directly or by means of a mediation device).

1.2.2 ISO functional areas

1.2.2.1 Configuration management

The configuration management supports the complete range of graphical functions to provision and maintain the following NE releases: R1.3 NB, R1.3.1 NB R1.4 NB, R1.1.2 BB and R1.4 BB. Network topologies, shelf views and self-explaining menus are navigating the operator to configure the following services:

- telephony
  - POTS
  - ISDN BRA
  - ISDN PRA
  - and leased line services (64 kbps or Nx64 kbps leased lines).
- data
  - ATM virtual paths
  - and ATM virtual channel connections carried over ADSL lines.

The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- inventory management
- equipment provisioning and maintenance (subshelves, packs, ports)
- telephony and data service provisioning
- clock synchronization
- system/equipment/service status
- software download
- NE database backup and restore
- system date/time synchronization.

1.2.2.2 Fault management

The fault management supports the operator in detecting, displaying, localizing and logging any faults occurring in the managed network. The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- handling of alarm severity (critical, major, minor, warning, indeterminate)
- receiving of autonomous alarm messages
- retrieving of alarms per NE, pack, application pack
- retrieving of alarm and event logs from NE
- initialization of tests for fault analysis purposes
- filters to display pre-selected alarm types only.

1.2.2.3 Performance management

The performance management provides facilities for retrieving, storing as logs and printing the logs of the NE performance data to ensure the quality of service.

1.2.2.4 Security management

The security management functions which are based on UNIX®[1] control the access to the AEM and to the managed NEs. The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- AEM user administration
- AEM user security profile
- no additional NE login for current AEM user
- AEM access via login name and password[2]
- inactivity user session time-out[2].

1.2.3 Applications

The AEM provides 6 applications which give access to the management functionality as described in Chapter 1.2.2, page 1-3. The following applications are available:

- System administration
- User administration and profiling
- Log management
- Alarm management
- Groups & NEs management.

Each application is composed by one or more tasks. The default user group assignment to the individual applications/tasks is described in Chapter 1.4.4, page 1-31.

1 UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

2 provided by the SUN Solaris operation system.

1.2.4 System working modes

The AEM can work in the following two modes:

- stand-alone mode
- integrated management mode.

These modes are not mutually exclusive, i.e. the AEM is always able to perform the element management tasks even while it is connected to any higher management system (OS) connected via northbound interface.

Stand-alone mode

In the stand-alone mode the AEM performs the whole management of the NEs on its own. The user is able to perform all management tasks via the GUI.

Figure 1-1 shows the system architecture in the stand-alone mode.

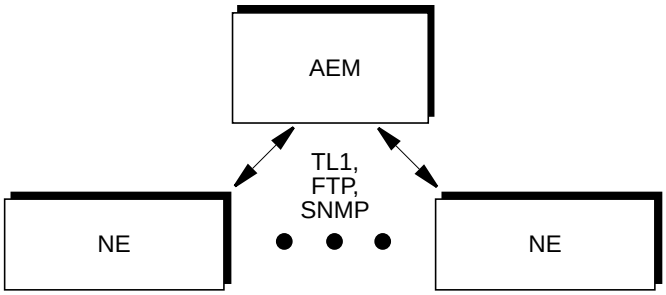


Figure 1-1 Stand-alone mode

Integrated management mode

In the integrated management mode the AEM works as an integral part of the customer's management network, providing higher management systems (OSs) with services to manage NEs in their domains.

The AEM allows other OSs to pass provisioning, testing or fault information to and from the NEs, e.g. a fault management surveillance system can collect fault data using the northbound interface.

Figure 1-2 shows the system architecture of the integrated management mode.

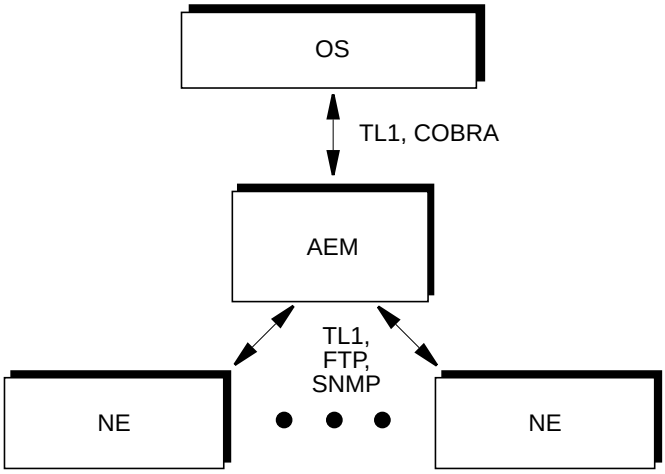


Figure 1-2 Integrated management mode

The complete system and software architecture of the AEM is described in Chapter 1.3, page 1-7.

1.2.5 Performance, reliability and availability

The AEM fulfils the following features:

- 30 simultaneous users
- Support of 600 NEs in the server configuration
- Database re-synchronization

  The AEM can re-synchronize its database with the 600 NE data bases within 24 hours.
- Priority of synchronization

  The AEM provides a mechanism to define the order in which the NEs will be synchronized.
- Maximum software download time

  It is possible to perform software download actions on 80 NEs in 6 hours.
- Scaling

  The AEM provides a scaling capability which defines the most suitable cost effective configuration depending on the number of NEs and number of users to be supported.

1.3 System and software architecture

1.3.1 Functional groups

The AEM software architecture is built with a number of components that can be grouped in the following distinct functional groups:

1. **NE management**
   (equipment management, service management, alarm management, test management, performance management)
2. **General components**
   (Components for operation, administration and maintenance (OAM); common servers)
3. **Software platform**
   (software bus, repository, third party libraries)
4. **Graphical user interface (GUI)**
5. **Northbound interface**
6. **Southbound interface**.

Figure 1-3 shows the six functional groups. The shadowed blocks are part of the AEM.

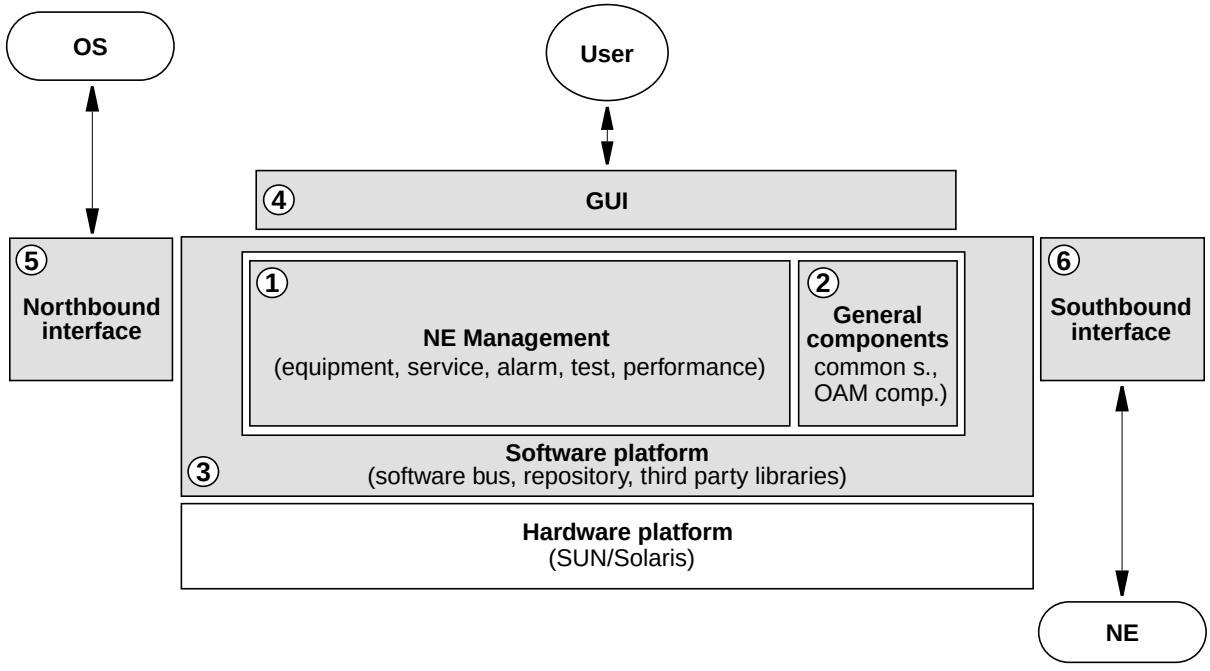


Figure 1-3 AEM functional groups

1.3.1.1 Network element management

The NE management functionality is distributed in 5 areas. These are: Equipment management, Service management, Alarm management, Performance management and Test management.

Equipment management

The equipment management provides the following functionality/features:

- Scrolling list of NEs

  The NEs are displayed in a list covered in a single window called *Network Element Browser*, where the NEs and their components can be handled like files in a file browser.

- NE provisioning

  The operator can create a new NE manageable for the AEM view. The operator must enter the specific configuration data for the new NE such as IP address, NE Name, NE user-id and password.

- Software download to a single NE

  Provides a storage medium for maintaining a copy of the software and a mechanism for downloading that software to an NE (for both data and telephony agents).

- Software download to multiple NEs

  Download of new software to multiple NEs on an individual connection basis.

- NE non-volatile data storage restoration

  Restores NE non-volatile data storage upon user request. Provides a storage medium for maintaining a copy of the NVDS for backup and restore purposes (for both telephony and data agents).

- Maintain a local copy of NE inventory

  The AEM maintains a local copy of specific hardware identifiers and software version identifiers. This local copy accepts automatic inventory notifications. This information can be used for display and report functions in case of loss of communication with the supported NE. The hardware identifiers include all packs.

- Maintain a local copy of NE provisioning configuration data

  The AEM maintains a local copy of all cross-connection and parameter settings for each NE. This information can be used for display and report functions in case of loss of communication with the supported NE.

- Maintain NE software copies

  The system keeps a copy of the versions of the NE software running in the NEs managed by the AEM. Generally, only one version of NE software per NE type is used by all the NEs in a network but the AEM must have the capacity to manage two software versions during the upgrade period.

- AEM database synchronization

  Automatic update of the AEM database records based on NE database changes.

- Internal audits (only applicable to data agents)

  The AEM performs periodic internal audits to ensure the integrity of the configuration data with the NE.

- Protection control

  The management system provides a facility to allow the user to switch operation of one unit in an NE to a standby unit, if that unit exists.

- Telephony equipment protection

  The AEM allows the user to provision the equipment information for the protection scheme. Also the user can force protection switching.

  NB R1.3 and subsequent releases:

  — COMDAC - simplex/duplex

  — IO_HDLC - simplex/duplex.

- NE timing synchronization

  The AEM supports the user to configure the NE synchronization clock sources.

- NE date and time

  The AEM allows the user to set and retrieve the date and time of the NE and allows to automatically configure NEs with AEM date and time.

- Subshelf management for NE R1.4

  Mainshelf and ONU Subshelves can be connected via optical link (155-Mbps). For connecting a ONU Subshelf to an Mainshelf, an Optical Application Pack (OAP) has to be installed in the mainshelf.

  Data transmitted via the network node interfaces (E1s, E3, respectively) are transported within the *AnyMedia* Mainshelf to the OAP. The OAP has access to the telephony and data interfaces of the *AnyMedia* Mainshelf backplane.

  Within the subshelf one ONU Controller Pack (OCP) and up to 8 Application Packs (telephony and/or data packs) can be installed.

- Support of NE standby configuration

  The AEM supports the NE standby configuration via cut-through interface. The standby configuration is used to select the ISDN mode of operation as well as to configure the country code.

- NE disaster recovery from the AEM

  The AEM is able to reconstruct its NE database by polling the NEs for information and from internally maintained backup copies of data.

Data equipment management functions

The data equipment management provides the following functions:

- Configure specific equipment data
  - Circuit pack provisioning/configuration
    - AFM management (e.g. reset, etc.)
    - ADSL pack management (e.g. change of administrative state, reset, etc.)
  - DS3/E3 feeder management
  - ADSL drop configuration
  - Date and time management
  - Timing synchronization provisioning (for this release no timing synchronization is made since local timing is the only mode supported)
  - Enable/Disable traps generation.
- Maintain a local copy of configuration data in the AFM's NVDS
  - Initializing the local copy (i.e. by doing an initial configuration upload)
  - Synchronizing the local copy with the equipment data maintained by the AFM (i.e. by using audits, traps and responses from operations). Note that local copy may not be synchronized because not all the configuration changes provoke traps.
- AFM memory administration

  Management of non-volatile data storage (NVDS) of the AFM. Provides a storage medium for maintaining a copy of the NVDS for backup and restore purposes.
- AFM software management

  Management of non-volatile program storage (NVPS) of the AFM: software download, software validation & activation etc.
- Subshelf management (NE R1.4)
  - Subshelf creation
  - Subshelf configuration and cross-connection
  - Subshelf deletion.
- ADSL profiles management

  The AEM allows to create, delete or change of the performance monitoring and transmission profiles related to ADSL ports.
- Obtain operational state and others status attributes of different entities (i. e. packs, ports, subshelves (NE R1.4) on user demand.

Service management

The service management provides the following functionality/features:

- NE service status

  Provides the aliveness status of the individual NEs providing a customer's service across all NEs under the AEM's control.

- — *V5.1/V5.2 interfaces*
- — *Primary/secondary links*
- — *V5 ISDN BRA user ports*
- — *V5 ISDN PRA user ports*
- — *V5 PSTN user ports*
- — *Analog Leased Line user ports*
- — *Digital Leased Line user ports*
- — *V Leased Line user ports*
- — *G Leased Line user ports*
- — *ISDN signalling configuration*
- — *V5.2 Protection Group 2*
- — *ATM cross-connections.*

- Network interfaces and subscriber service provisioning and activation

  The AEM supports all provisioning functions related to 2-Mbps network interfaces and subscriber services. Provisioning contains the creation, deletion and parameter setting/modification of the different subscriber services. The AEM service activation enables and disables the service.

  2-Mbps network services:

  - — V5.1
  - — V5.2
  - — non-switched services.

  Telephony subscriber services:

  - — analogue telephone (POST) based on V5
  - — ISDN BRA based on V5
  - — ISDN PRA based on V5
  - — analogue leased line
  - — digital leased line
  - — VLL/GLL leased lines.

Data service management functions

The data service management provides the following functions:

- Configuration of ATM layer functions:
  - — shelf virtual path identifier (Shelf VPI)
  - — OAM&P virtual path/virtual channel (i.e. configuration of ATM embedded management channel).
- Management of ATM virtual path services:
  - — creating and deleting virtual path services (i.e. by means of creating and deleting virtual path links and virtual path cross-connections)

  - changing the administrative state of a virtual path cross-connection
  - obtaining the operational state of a virtual path cross-connection.
- Management of ATM virtual channel services:
  - creating and deleting virtual channel services (i.e. by means of creating and deleting virtual channel links and virtual channel cross-connections)
  - changing the administrative state of a virtual channel cross-connection.

Alarm management

The alarm management provides the following functionality/features:

- Integrated display of all the alarms

  The AEM provides a common window (alarm viewer) to show all alarms reported by the managed NEs or generated by the management system itself. The display shows all the information pertaining to the alarm, including alarm type, severity, service affecting indication, date/time of occurrence and clearing.
- Alarm display filters

  It is possible to filter the items shown in the alarm viewer, for instance, to see only the critical alarms.
- Alarm notification to user

  The user is informed by visual alerts when a new alarm has been reported to the AEM.
- Alarm correlation

  Alarms coming from the same NE point through telephony and data agents (i.e the same alarm is reported via both controller cards) are correlated into one single alarm.
- Clearing of alarms

  Alarms in the management system will automatically be cleared when the faults are removed at the source (such as in the NEs or in the platform). Some platform alarms can be cleared by the user. The alarm information will contain the date and time of alarm clearance.
- Acknowledged alarms

  The operator can acknowledge a raised alarm - alarm still active but being investigated.
- Alarm colors

  The management system provides a color scheme based on alarm severities.
- Enable/Disable of autonomous alarms on an NE basis

- Fault localization

  Provides fault localization across all NEs under the AEM control. The COMDAC LEDs show the highest severity alarm for the system. The individual pack unit LEDs show the highest severity alarm for the pack unit. Fault localization is performed at AP level.

- NE alarm log handling

  The AEM is able to retrieve the NE alarm log via the cut-through interface.

- Customized alarm filters and views

  It is possible to filter the alarm records for one or for a list of NEs. The items to be displayed can be sorted in ascending or descending order.

- NE alarm cut-off functionality via GUI

- Alarm audits data application

  The system performs periodic (automatic) and on-demand audits on the NE to ensure integrity of the alarm data.

Performance management

The performance management provides the following functionality/features:

- Handling of performance records

  Records can be displayed, printed and stored in a user-defined file.

- OSs retrieval of data performance data

  The AEM provides a mechanism for other OSs to retrieve data performance data.

- Displaying, printing and storage of the TCA records

- Retrieve performance counter thresholds (only applicable to data agents)

  The user can request the NE to report the assignment of the performance counter thresholds.

- Set/Modify performance counter thresholds (only applicable to data agents)

  The user can set/modify the performance counter thresholds.

- Retrieve the performance data after selecting the record type (15 minutes or 24 hour) - (only applicable to data agents)

- Traffic monitoring (only applicable to data agents)

  The AEM provides the ability to display traffic monitoring data.

Data performance management functions

The data performance management provides the following functions:

- Collect/display ATM layer traffic counters:
  - current 15 minutes and previous 15 minutes.
- Collect/display ADSL port performance counters
  - current 15 minutes, previous 15 minutes, current day and previous day.

- Collect/display E3 feeder performance counters
  - current 15 minutes, previous 15 minutes (up to 96 previous intervals) and total day.
- Management of performance features
  - enabling/disabling generation of feeder PM data
  - clearing of ATM, ADSL and DS3/E3 PM counters.

Test management

The test management provides the following functionality/features:

- Port test

  It is possible to request a test for a particular port on a specific application pack.
- TAP test

  It is possible to check the correct cabling between the communication interface unit and the test application pack.
- Standby card test scheduling (via cut-through)

  It is possible to schedule a test to perform a COMDAC side switch or off-line diagnostic for the standby COMDAC or the protection.
- Built-in self-test

  Each NE performs a built-in self-test of packs periodically.
- Loopback test on the feeder side

  It is possible to set or clear a loopback on particular feeders.
- HDSL loopback test

  A loop closure on a high bit rate digital subscriber line (HDSL) can be requested.
- Support of the ISDN line testing

  Requests a subscriber line testing on a specific list of services (e.g. POTS, ISDN, etc.). The subscriber line tests may consist of the following tests:
  - foreign voltage measurement
  - insulation measurement
  - capacity measurement
  - dial tone
  - short circuit.
- Support of CRC test for ISDN drops
- Support of loopback test on the drop side
- Support of China 112 systems

  Support of testing capabilities for the 112 system as implemented in *AnyMedia* Access System NB R1.4.

Data test management

- The data test management provides the following tests:

- — ADSL port BIST tests
- — ADSL port corrupted CRC tests
- — administration of the set of tests stored in the AFM.

- Support for single pulse feeding test (applicable only for NB R1.3 and subsequent releases).

1.3.1.2 General components

The components of this group do not have or require any knowledge of the NEs the AEM is managing. They provide a platform on which the other AEM components can operate and isolate them from the underlying customer platform.

OAM components

The OAM components provide operation, administration, maintenance and security functionality. This is based on third party-tools (i.e. orbix) and a set of specific applications.

The OAM components provide the following functionality/features:

1. **Operation/administration/maintenance**

- Standard reports

  The system allows the user to generate a set of predefined reports from the information kept by the AEM. The reports cover the following areas:

  - — alarms
  - — equipment configuration
  - — service provisioning
  - — NE inventory
  - — performance.

  The reports are available for displaying, printing and saving in a postscript file.

- Standard reports on multiple NEs

  These reports are applicable to one NE as well as to a list of NEs.

- Backup and restore of system relevant data

  Relevant data includes all information necessary to restore the situation in case of an AEM crash.

- AEM software upgrades

  Provides an established release cycle for AEM software upgrades in a way that minimizes incompatibility with NE software releases, and allows for upgrades to provide for OS compatibility. This upgrade does not affect the services provided by NEs.

- Log administration

  The logs are capable of being printed and visualized. The system limits the size of the system logs. It is possible to make backups of the logs and to remove them from the system. There are logs for:

— Actions

Contains all the information on actions performed by users or the AEM and which imply changes in the AEM configuration, equipment (NE) configuration, service and subscriber configuration, access to the AEM, print reports and backup and restore, i.e. all operations triggered by the user or the AEM and all subsequent actions. The results of operations are also logged in the actions log.

— System Internal Events

Contains all internal events or actions which report unusual changes in the configuration and state of the AEM or indicate errors that occurred in the AEM.

— Autonomous Reports

Contains all information useful for the equipment supplier about alarms (NE and platform), the performance and all TL1 messages sent from all managed NEs and which imply changes in the database.

— Alarms

— Performance Data (feeders)

— Performance Data (ADSL)

— Performance Data (ATM)

- Possibility to sort logs

  It is possible to show items in the logs while visualizing, saving or printing.

- EM time and data source

  The user can set the date & time of the AEM from the platform clock (i.e. operating system), from a network management system or from an external clock source, using NTP.

- SW upgrade

  The AEM provides an easy and transparent mechanism to upgrade the system to AEM R1.7.

- AEM-NE loss of communication

  The AEM periodically polls the NEs (heartbeat) to detect loss of communication and/or NE failures. Loss of communication is reported as an alarm.

2. **Security**

- Possibility of creating/deleting/modifying AEM users

  The AEM uses the security mechanisms provided by the SOLARIS Operating System.

- AEM security privilege levels

  Allows at least three privilege levels within the managed domain. This is mapped to the NE privilege levels accordingly.

  — Administrator: has all the permissions.

  - Maintenance: has configuration and monitoring permissions.
  - Monitoring: has alarm monitoring, testing and performance management permissions.

- NE user security privilege levels

  It is possible to administer the NE users and the privilege levels via the cut-through interface.

- User access is authenticated through user name and password
- Single login to access the domain

  Enables an authorized user to access multiple NEs simultaneously (e.g. multiple windows) using a single login and password.

- Domain partitioning

  Enables the NEs managed by the AEM to be partitioned into separate security domains and permits users access to the domains based on their areas of responsibility and profile.

- User inactivity timer[1]

  The user terminal will be locked with a screen saver once a configurable inactivity timer has expired. To unlock the terminal, the user has to type his/her password. The timer has to be configured by the administrator.

- Second inactivity timer[1]

  Once the terminal is locked, the user will be logged out once a second inactivity timer has expired. The timer has to be configured by the administrator.

- Lock screen[1]

  The user is able to lock the screen whenever he wants. To unlock the terminal the user has to enter his/her password.

- OS/AEM secure access

  The AEM provides security for other OSs/EMs to access the system via northbound interface.

Common servers

Common servers offer general purpose services. A common server

- manages the AEM history and security logs
- logs the history and security data of other processes upon request
- provides log information upon request
- provides a facility to generate and print client reports in the AEM printers
- provides event distribution services based on a supplier/consumer model.

1 provided by the SUN Solaris operation system

1.3.1.3 Software platform

1.3.1.3.1 Software bus

CORBA architecture

The communication between the AEM processes is based on the common object request broker architecture (CORBA) standard. The heart of the CORBA architecture is the object request broker (ORB). The ORB is a software bus to which different applications can connect to offer their services and/or to use other applications' services (from which they are clients).

The ORB provides a transport mechanism that makes connected servers' location, platform and implementation transparent to their clients, making applications easier to distribute and scale.

Protocol

The protocol used by the ORB is the internet inter operability protocol (IIOP).

1.3.1.3.2 Repository

Introduction

The repository contains all the AEM information that must be persistent. It is supported by an object oriented database (ObjectStore) and the underlying operating file system. All components of the system have direct access to the repository to store/retrieve their own data.

Contained information

Information in the repository includes:

- NE inventory
  (for each NE: the hardware identifiers and the software versions)
- equipment and service provisioning data
- history and security logs
- external system communication parameters
- AEM configuration data
- alarms cache.

1.3.1.4 Graphical user interface (GUI)

Introduction

The Java based GUI is responsible for putting up forms, collecting user input (commands and data) and routing it on to the correct component. It also receives data from the relevant process which it uses to update its display. The GUI has direct access to the services provided by the AEM through the ORB.

Functionality, features

The GUI provides the following functionality/features:

- Support TL1 messages

  Supports all TL1 messages for all NE products for dumb terminal access. Allows direct input of TL1 messages. In some markets, direct input of TL1 messages may not be allowed and can be suppressed via the appropriate security permissions.

- Online help

  Provides access to online help which contains at least information on the operation of the AEM, meaning of the buttons, etc.

- Multiple windowing

  Provides multiple windowing for access to multiple NE information on a single screen.

- Multiple user access

  Provides for multiple users access to the AEM at the same time. Multiple users may include multiple OSs or NMSs as well as multiple GUI access.

- Time and date format

  Enables the user to use local/preferred time and date format. For example, the local calendar is supported or optional use of 24 hour clock versus a 12 hour clock.

- User friendly GUIs

  Provides a user-friendly interface and hides the complexities of the information models.

- Manageable objects organized in a hierarchy

  The configuration is implemented within a GUI hierarchy:

  — Network level, containing all groups of NEs

  — NE group level, containing a number of NEs or/and other NE groups

  — NE level, starting with shelf-view.

- Display of NEs in a map

  The NEs can be displayed in a map. The display follows the GUI hierarchy.

- Map handling

  It is possible to use maps for displaying NEs. The AEM provides a default map. Other maps can be loaded in an easy way.

- NE grouping

  Special graphical symbols are used to represent NE groups. It is also possible to expand the NE group level to display the NEs which belong to a specific group as well as to provide access from the NE level to the configuration management application.

- GUI process to be separated

  The graphical interface driver can be placed on a separate platform from the rest of the EMS application.

1.3.1.5 Northbound interface

Tasks

The northbound interface (NBI) performs all the tasks needed to communicate to other OSs. It allows external OSs access to the NEs managed by the AEM directly through TL1 commands via a NBI. This access is controlled by the NBI until the OS is disconnected.

TL1 northbound interface

The TL1 NBI allows an external OS access to the NEs managed by the AEM directly through TL1 commands for provisioning, testing and alarm purposes:

- Support of alarm forwarding.
- Support of 112 system.

COBRA northbound interface

The CORBA NBI allows an external OS access to the NEs managed by the AEM directly using the IDLs that AEM publishes or via a mediation device.

1.3.1.6 Southbound interface

Tasks

The southbound interface performs all the tasks needed to communicate to the NEs managed by the AEM. It provides distributed CORBA access which includes implementation and translation of TL1 commands, response and autonomous messages into equivalent CORBA requests and events.

TL1 southbound adaptors

The TL1 southbound adaptors isolate the main AEM functionality from the specific protocol used by the NEs. They are responsible for translating actions and state changes conveyed through CORBA messages from/into the NE specific message formats.

Functionality, features

The southbound interface provides the following functionality/features:

- Southbound TCP/IP TL1 client application (telephony application)

  Support for the TL1 client application on the southbound TCP/IP interfaces. TL1 is used for most of the OAM&P functions (see Chapter 1.3.1.2, page 1-15).

- Southbound TCP/IP FTP client applications (telephony application)

  Support for the FTP client application on the southbound TCP/IP interfaces. FTP is required for software download and NE data backup/restore.

- Southbound TCP/IP Telnet client applications (cut-through) (telephony application)

  Support for the Telnet application on the southbound TCP/IP interfaces. Telnet is used to provide a direct command line into the NE (i.e. an equivalent ASCII terminal interface).

- Southbound SNMP client applications (data application)

  Support for the SNMP application on the southbound TCP/IP interfaces. SNMP is used for most of the OAM&P functions on data agents.

1.3.2 Hardware platform

1.3.2.1 Architecture

Components

A number of AEM Clients (UNIX workstations) can be added to the AEM Server to support concurrent users or remote access to the server's applications. These clients can be connected through a TCP/IP infrastructure or a local area network (LAN). Examples are shown in Figure 1-9, page 1-32 to Figure 1-12, page 1-35.

Tasks of the components

The tasks of the components are:

- **AEM server:**
  Manages all the AEM applications and provides access to the NEs, the database and the external OS.
- **AEM client**:
  Formats the display of the application screens and manages the users sessions with the application, e.g. database access.

Conceptional representation

Figure 1-4 is a conceptual representation of the various generic components.

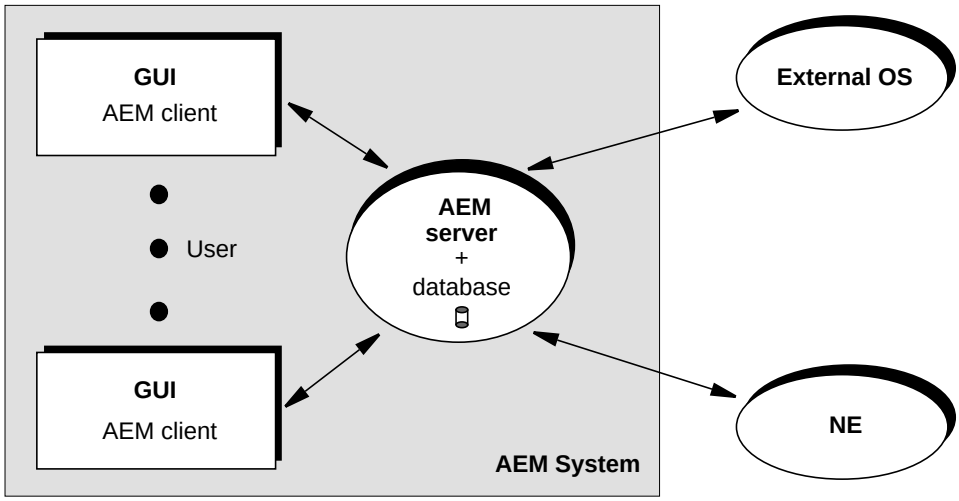


Figure 1-4 Hardware components

Examples of AEMs

Two examples of an AEM system are shown in Figure 1-5.

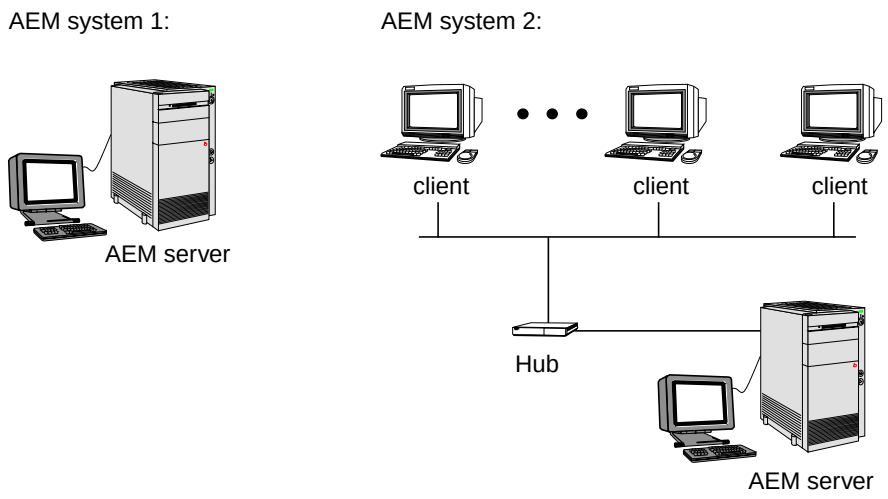


Figure 1-5 Examples of AEMs

1.3.2.2 Requirements

Server/clients

A SUN SOLARIS work station can be used as AEM server as well as AEM client.

Peripherals

The AEM system may use a number of peripherals with the following tasks:

- **CD-ROM:**
  Used for installing the system software.
- **Tape drive or another removable device (optional):**
  Used for backup and restore functions.
- **Printer:**
  Used for obtaining hard copies, e.g. configuration/alarm reports or performance monitoring measurement information.

1.4 Working with AEM

Goal of this chapter

This chapter will outline the management activities and processes in the AEM. The main emphasis is on presenting everyday operation processes. The chapter is structured with respect to the various network life cycle phases (see further below).

User profiles

There are 3 default user profiles: the administrator, maintenance and monitoring profile. The rights belonging to these profiles are described in Chapter 1.4.4, page 1-31.

Life cycle of a network

The individual life cycle of a telecommunication network has the following phases: planning, installation, provisioning, operation and surveillance, modification and finally decommissioning. Modification of a network may take the form of fine adjustment, expansion or restructuring of the network, and addition of new functionality.

Figure 1-6 shows the life cycle of a network.

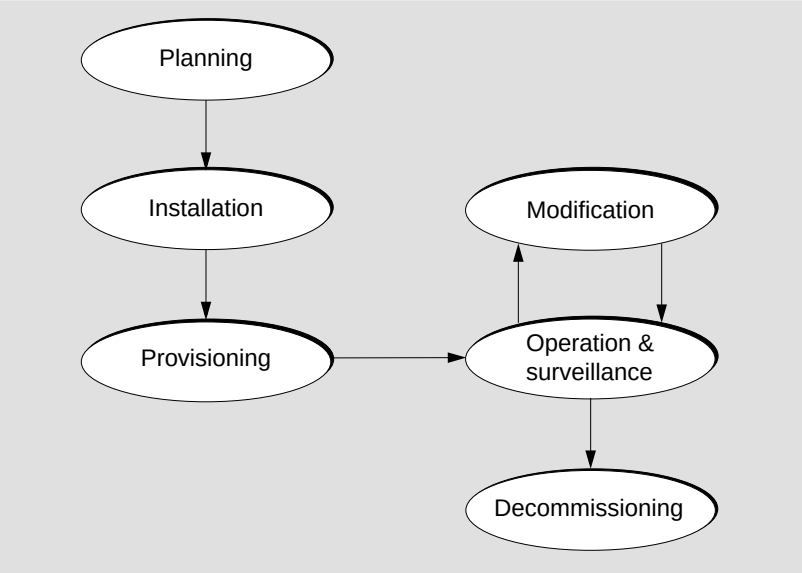


Figure 1-6 Life cycle of a network

Support by AEM

The AEM is mainly used in three life cycle phases: during network provisioning, network modification and network operation & surveillance. The installation phase is supported by the graphical system interface for telephony services (GSI-NB).

1.4.1 Network planning and physical installation

Network planning

In the network planning phase, all specifications and requirements of the future network operation are translated into a concrete network structure. That means, the network planning phase, during which a decision on the network topology, equipment and components is made, has to take place before the operation with the AEM starts.

Physical installation

The installation of the network follows the planning phase. The installation includes the following steps:

- Physical NE installation.
  This includes the installation of racks, packs and cabling of the NEs.
- Creation of a data communication network (DCN) plan

  Communication between the AEM and the NEs is carried out via the DCN. A DCN plan should be drawn up before provisioning the network to ensure that the AEM can reach all NEs and that the administration of the DCN does not lead to an undue increase in performance requirements.
- NE connection to the AEM server
- OS connection to the AEM server (optional)
- Installation of the third-party, application and AEM software on the AEM server.

Network status after physical installation

After completion of these steps, the network operator has at his disposal a network which is connected physically with AEM and which is, in principle, ready for operation.

1.4.2 Configuration management

Introduction

The configuration management in accordance with the specific operating conditions of the network operator is performed by special provisioning actions. It is assumed that the NEs and AEM have already been physically connected.

Provisioning actions

Figure 1-7 provides an overview of the provisioning actions and the text which follows gives a detailed description.

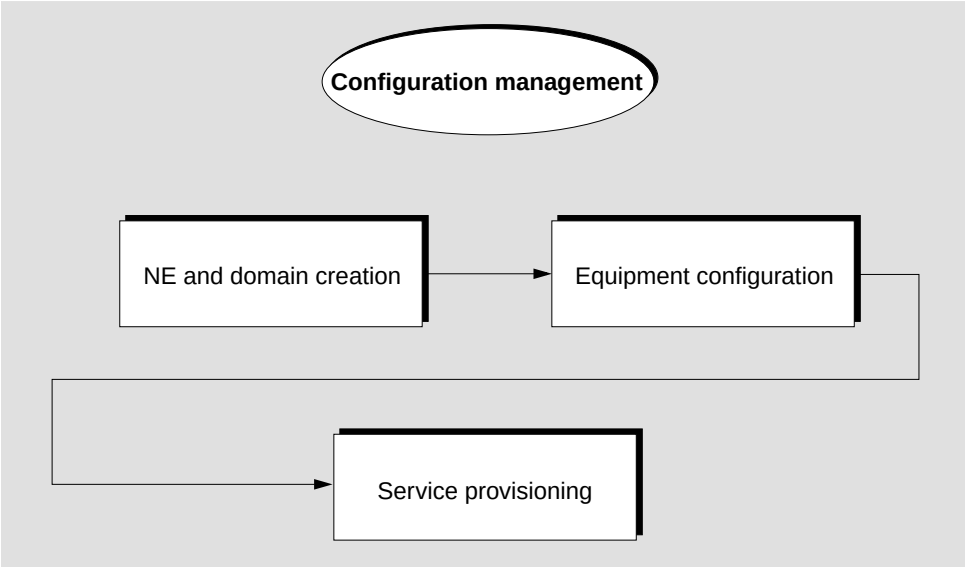


Figure 1-7 Network provisioning

NE and domain creation

Prior to equipment configuration and service provisioning, the NEs must be known in the AEM. To achieve this, the following 4 steps are necessary:

1. creation of domains
2. creation of NEs
3. assignment of NEs to any domain(s)
4. logical connection of NEs.

All steps are described in detail in Chapter 5.

Equipment configuration

NEs can be configured if they are known in the AEM. The following measures should be performed:

- selection of the timing synchronization source
- selection of the COMDAC (simplex/duplex) and IO_HDLC protection scheme
- selection of those slots for which an absence of the pack will be alarmed (only applicable for COMDAC)

- include data equipment configuration (provisioning of card types and ONU Subshelves, ADSL drops configuration)
- provisioning of card types which are inserted in a slot
- configure ISDN in POTS mode via cut-through
- provisioning of the protection switching.

All steps are described in detail in Chapter 5.

Service provisioning

If the NEs are configured and integrated in the network, cross connections can be defined. The following actions are necessary:

- creation of V5 network interfaces
- adding of V5 links to the V5 interfaces
- adding of primary/secondary links
- adding of V5 user ports
- include data service provisioning (configuration of shelf vpi, creation of VP services, creation of VC services).

All steps are described in detail in Chapter 6.

Network status after provisioning

After the provisioning phase the NEs can now be controlled and monitored by the AEM and start operation & surveillance.

1.4.3 Network operation & surveillance

Actions

During network operation & surveillance, the administration, control and supervision of the network mainly include

- Fault management
- Network modification
- Performance monitoring.

Required rights

The administrator rights are sufficient to perform all required operations. The visual check of parameters and displays on the GUI requires monitoring rights only.

1.4.3.1 Fault management

Alarm types

There are two alarm types: alarms generated by the NEs and alarms generated by the AEM itself, e.g. an alarm indicating that log files without archiving is being removed (LOG_DEL_FULL). All alarms are displayed in the alarm viewer. It allows the network operator to detect the alarm and to locate its source.

General fault handling

Figure 1-8 shows the general fault handling. In the following the individual phases are described in more detail.

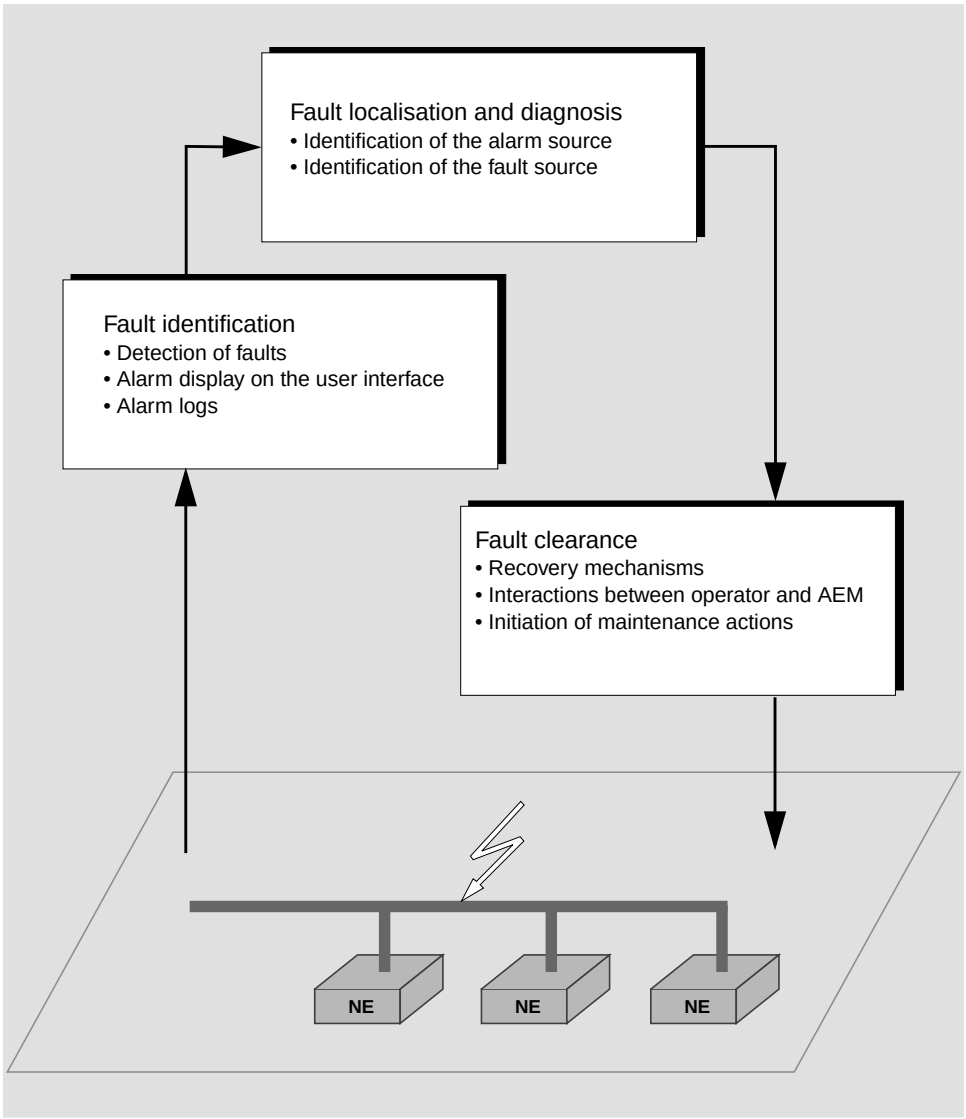


Figure 1-8 General fault handling

1.4.3.1.1 Fault identification

Background

The AEM gathers information about faults occurring in the network and forwards this information to the network operator. This procedure comprises two tasks: on the one hand, the fault must be identified, and on the other hand, the fault information must be processed as alarm notifications to be displayed on the user interface.

Detection of faults

If an NE fault is detected, the NE notifies the AEM. The notification comprises the type of fault and the address of the originating NE. The AEM detects and processes such a notification automatically.

If the circuit of an NE fails that is responsible for the communication with the AEM, the fault is identified differently. No alarm notification will be sent to the AEM. The AEM detects the fault by testing at regular intervals whether the association to the particular NE is dropped. In this case the AEM itself raises an alarm.

Alarm display on the user interface

A complete alarm overview and a detailed alarm description is provided by the alarm viewer. All relevant alarm data (e.g. alarm severity) are shown.

Alarm logs

The AEM keeps alarm logs to store the alarm notifications. Alarm logs are used among other things for long-term observations, e.g. of the fault behaviour in the network. Alarm logs exist for pending alarms, for the alarm history and for clock events in the network.

1.4.3.1.2 Fault localisation and diagnosis

Reaction to fault identification

When a fault has been detected, it is necessary to localise its source and diagnose its cause in order to initiate appropriate repair procedures. To locate the cause of fault, the AEM provides information gathered from alarm notifications and general network data.

Fault source

Each alarm notification contains the name of the network component from which it originates. This network component, however, need not always be the real fault source.

1.4.3.1.3 Fault clearance

Background

The AEM detects faults automatically and clears various software errors by itself (fault recovery). The transmission characteristics of the network will not be impaired by this.

Recovery mechanisms

System recovery protects the AEM and associated users from unnecessary problems and avoids or reduces manual work.

Recovery processes vary depending on the type of failure that occurred, the structures affected, and the type of recovery. If no files are lost or damaged, recovery may amount to no more than restarting an instance. If data has been lost, recovery requires additional steps, such as database restoration using a previous backup.

AEM recovery mechanisms are initiated mainly by the following situations:

- NE software crash
- AEM crash
- Communication between AEM and an NE is interrupted.

In the case of an NE crash, the AEM configures NEs in accordance with the internal state of the AEM database. In the event of an AEM crash or an interruption in communication, the AEM downloads the current NE configuration from the NE to its database.

Interactions between operator and AEM

Faults (software or hardware), the cause of which the AEM cannot eliminate itself by means of a recovery mechanism, must then be handled by the user. The AEM supports this. The AEM first displays the fault on the user interface. The user then initiates appropriate measures to clear the fault and/or to maintain network operation. This includes access to faulty network units and the redirection of the network traffic. The AEM supports both.

Initiation of maintenance actions

Sometimes, additional maintenance actions are necessary to clear a fault. For example, some network disturbances can also originate in hardware faults. Such hardware faults often require the faulty component to be replaced, and this can only be done by maintenance personnel.

NOTE:
More detailed information about maintenance actions is provided in Chapter 7.

Fault clearance

Once the fault has been cleared, the alarm is reset automatically.

1.4.3.2 Network modification

Types of network modification

Usually, network operation & surveillance requires structural modifications in the network. The AEM supports this. There are two types of network modifications:

- installation or removal of NEs
- modification of NEs.

1.4.3.2.1 Installation and removal of an NE

Installation of an NE

For installing a new NE in an existing network the following steps must be carried out:

1. Check whether the new NE can be incorporated in the existing DCN plan drawn up in the network planning phase (if not, the DCN plan must first be revised)
2. creation of the NE
3. assignment of the NE to a domain
4. logical connection of the NE
5. selection of the timing synchronization source
6. selection of the COMDAC protection scheme (simplex/duplex)
7. selection of those slots for which an absence of the pack will be alarmed (COMDAC)
8. provisioning of card types which are inserted in a slot
9. provisioning of subshelves.

All steps are described in detail in Chapter 5.

Removal of an NE

If an NE is no longer managed by the AEM, the administrator deletes it from the AEM database.

NOTE:
When an NE is deleted from the AEM database, it is still fully functional. The TL1 and TCP/IP links between the AEM and the NE will be closed and the management access via the AEM is not possible until the NE is created and connected again.

1.4.3.2.2 Modification of NEs

Adding a pack

NEs can be modified by adding or removing packs. The AEM recognises automatically which pack has been plugged and where. As only default settings are set on the new pack, the system administrator must adapt the configuration.

Removing a pack

When removing a pack, it must be ensured that there are no connections running via this unit. Then the pack may be removed.

1.4.3.3 Performance monitoring

Tasks of performance monitoring

Performance management guarantees that the transmission quality does not fall below a minimum performance threshold.

Another task is the recording of data for analysis at a later date, e.g. storing alarms in logs and print them.

1.4.4 System security and user groups

Protection from unauthorised access

The AEM provides mechanisms which protect the system from unauthorised access. The user groups play a very important role in this context as they define different levels of access rights for the individual users.

User groups

By default there are 3 user groups: the administrator, maintenance and monitoring user group. Further groups can be added.

Access rights

Table 1-1 provides an overview of the access permissions the user groups should have

Table 1-1 Assignment of user groups to applications/tasks

Application	Task	User Group
System Administration	Process Management	Administrator
User Administration and Profiling	Access Policy Management	Administrator
	Domain Management	Administrator
Log Management	Actions	Administrator, Maintenance
	System Internal Events	Administrator, Maintenance
	Autonomous Report	Administrator, Maintenance, Monitoring
Alarm Management	Acknowledge	Administrator, Maintenance
	View[1]	Administrator, Maintenance, Monitoring
	Clear	Administrator, Maintenance
Groups and NEs Management	Equipment and Service Provisioning	Administrator, Maintenance
	View[1]	Administrator, Maintenance, Monitoring
	Test	Administrator, Maintenance, Monitoring
	Cut-through	Administrator
	Groups and NEs Configuration	Administrator, Maintenance
	Performance Management	Administrator, Maintenance, Monitoring

1 If the VIEW task is unassigned but other tasks are still assigned, these tasks are left as assigned to this user group. But the user is not able to perform any kind of operation over these tasks until the VIEW task is assigned again.

1.5 Network configuration

The network configuration depends on the user applications. The most probable configurations are described below and illustrated in Figure 1-9, page 1-32 to Figure 1-12, page 1-35.

NOTE:
If there are various configuration options of the DCN, these are shown in the figures by means of dashed lines. The hubs are optional depending on the number of client platforms and NEs.

1.5.1 AEM server without clients and external OS (LAN)

AEM server connected to the NEs using a local area network (LAN).

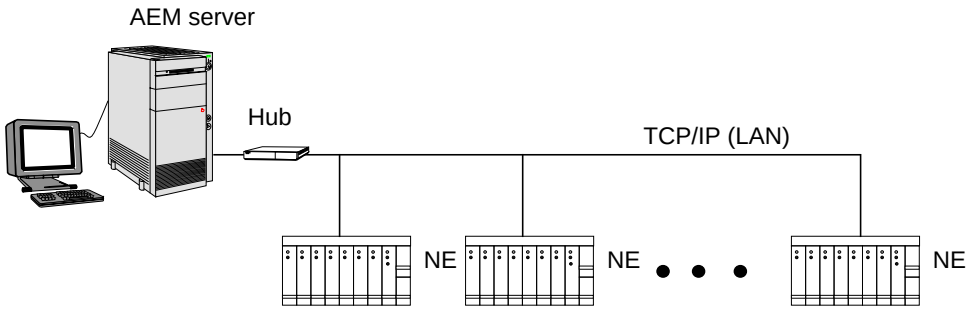


Figure 1-9 AEM server without clients and external OS (LAN)

1.5.2 AEM server with clients and without external OS (LAN)

AEM server and one or more clients connected to the NEs using a LAN.

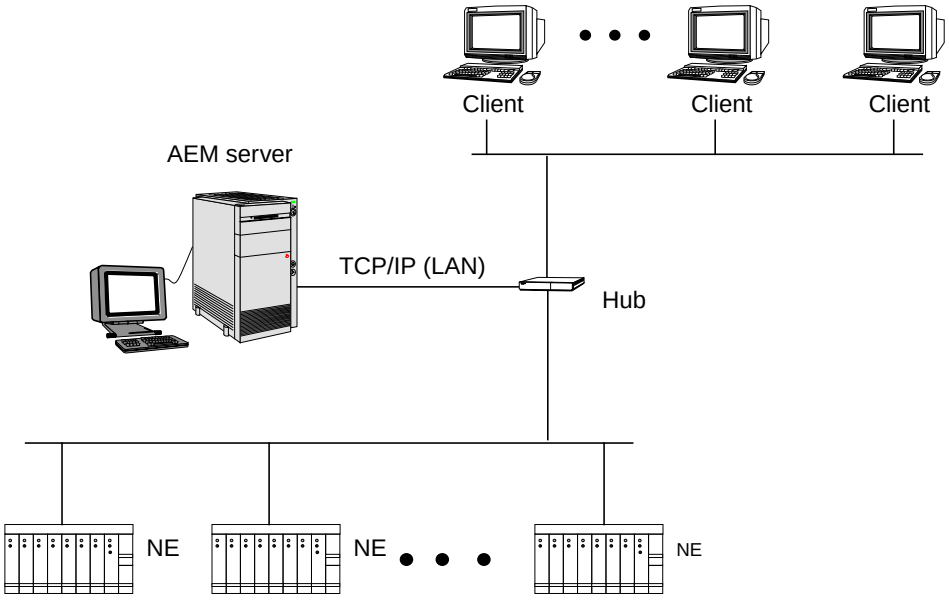


Figure 1-10 AEM server with clients and without external OS (LAN)

1.5.3 AEM server without clients and with external OS (WAN)

AEM server connected to the NEs using a LAN and connected to one or more external OSs using a WAN link.

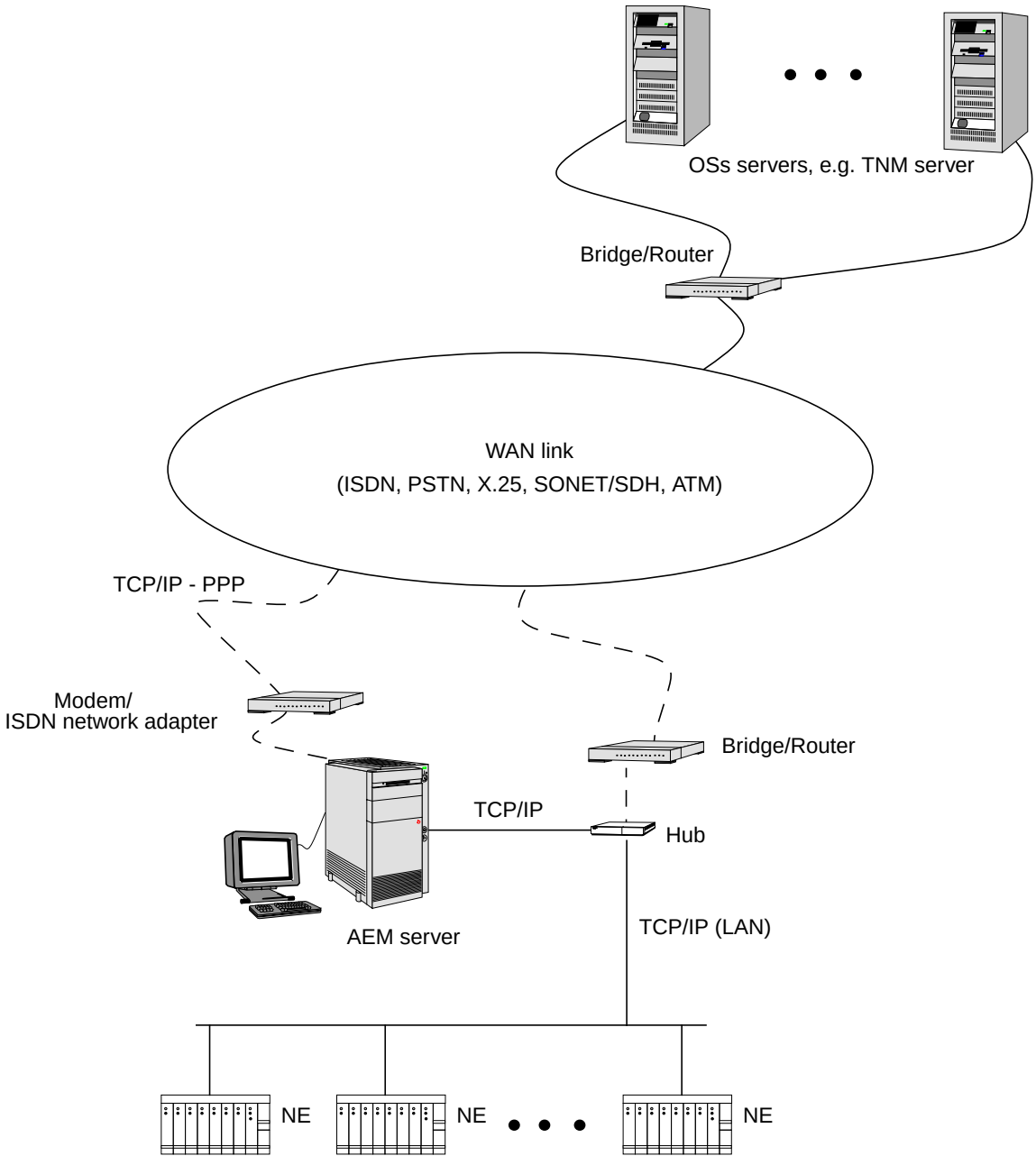


Figure 1-11 AEM server without clients and with external OS (WAN)

1.5.4 AEM server with clients and external OS (WAN)

AEM server and one or more clients connected to the NEs using a WAN link and connected to one ore more external OSs using a LAN connection.

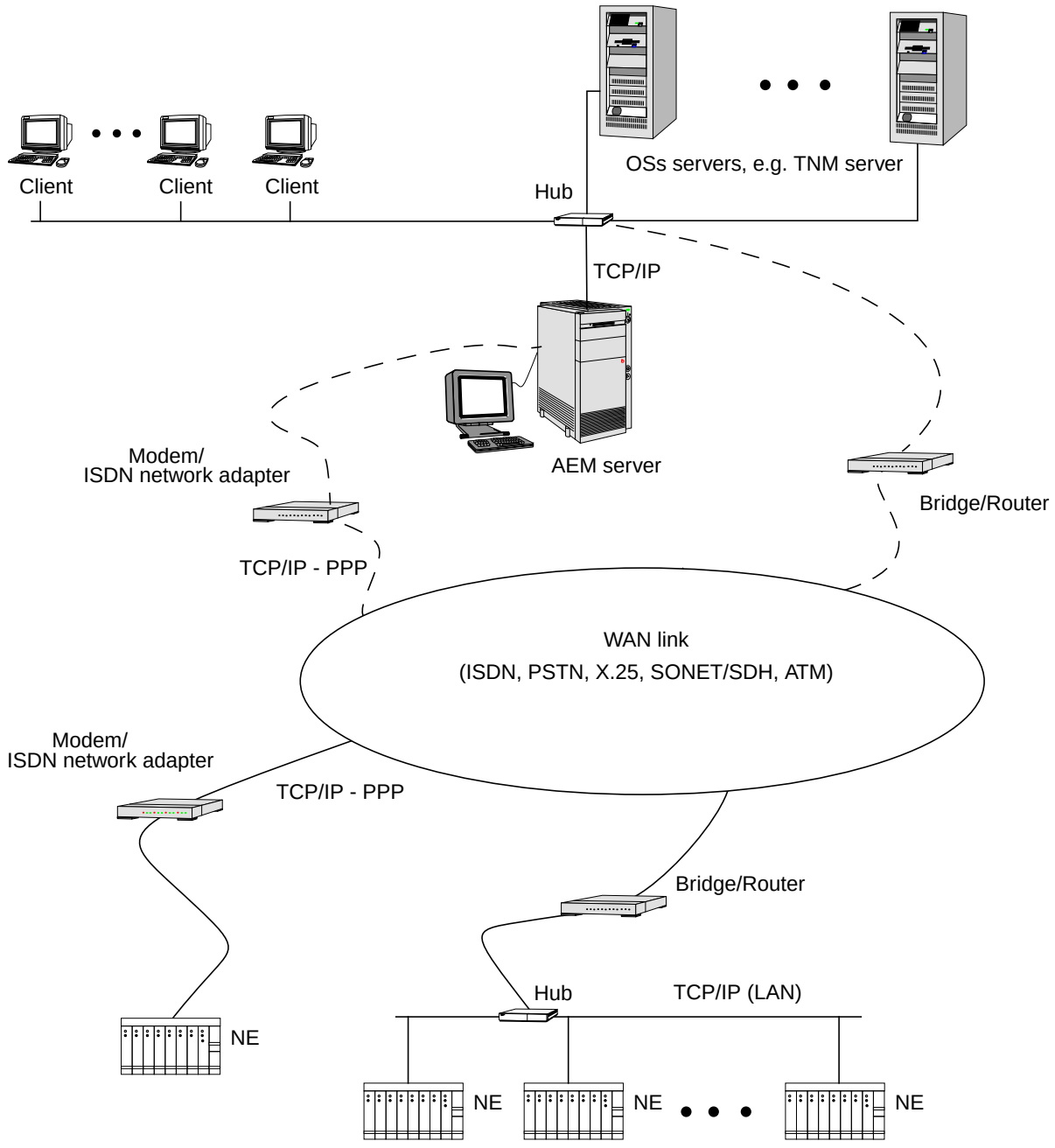


Figure 1-12 AEM server with clients and external OS (WAN)

Software installation and commissioning

2

Contents

2.1 General 2-1

2.1.1 Introduction 2-2

2.2 Installation procedure 2-7

2.2.1 Full installation 2-7

2.2.1.1 Server side installation 2-8

2.2.1.1.1 Installation of the third party software 2-8

2.2.1.1.2 Installation of the common packages 2-20

2.2.1.1.3 Installation of the telephony R1.3 agent (optional) 2-48

2.2.1.1.4 Installation of the telephony R1.4 agent (optional) 2-51

2.2.1.1.5 Installation of the data R1.1.2 agent (optional) 2-55

2.2.1.1.6 Installation of the data R1.4 agent (optional) 2-59

2.2.1.2 Client side installation 2-63

2.2.1.3 Post-install actions 2-75

2.2.1.3.1 AEM server 2-75

2.2.2 Installing individual packages 2-75

2.2.3 Cancel installation 2-77

2.2.4 Remove *AnyMedia* package installations 2-77

2.2.5 PC-GUI client installation 2-77

2.2.5.1 Customizing SystemPreferences.ini 2-79

Contents

Software installation and commissioning

2

2.1 General

The *AnyMedia*® Element Manager- 30 Channel (AEM) R1.7 runs on SUN SPARC Solaris 2 computers running Solaris 2.6 plus the patches recommended by SUN.

In order to successfully install the AEM R1.7 for the SUN Solaris installation the following has to be taken into account:

- **Disk partitioning**:
  HDD partitioning should include, in addition to the standard UNIX entries (e.g. /, /usr, /var, etc.), two entries for the AEM software and the transaction.log (cf. Chapter 2.1.1, page 2-2 for size requirements). Additionally a temporal directory with 2 Gbytes is necessary for uncompressing the installation files.
- **Swap space**:
  In addition to the SUN recommendation, 100MB per platform should be configured for OODBMS requirements.
- **NIS**:
  If more than one AEM platform is to be used, NIS should be configured in the server, so all the AEM clients will share the logins and password which are configured in the server tables. All the users require a NOT null password in order to manage AEM.
- **NFS**:
  Network File Sharing is not required even when using a LAN, but if NIS is used, NFS allows operators to log-in in any client platform having access to their home directories.
- **SUN patches**:
  All the Solaris patches described in the shopping list and included on CD-ROM 1 of 4 under SUN directory must be installed before AEM installation

- **LAN & WAN configuration**:
  E.g. default router to NEs, etc. must be available.

How to install SUN Solaris is described in SUN support/SUN Solaris Installation Guide.

Assumptions

For the following description it is assumed that

- the hardware required to install the AEM R1.7 is prepared
- the AEM R1.7 consists of a number of server and client applications. The software installation may imply the installation of all these applications or only some of them.

JRE

- the AEM R1.7 includes as part of its environment the Java Runtime Environment (JRE) Release 1.1.7. JRE is included here free of charge for the final user.

2.1.1 Introduction

System requirements

This document is intended as a guide for the person(s) who will be responsible for the installation and configuration of the hardware and software required for the AEM R1.7 installation.

The *AnyMedia* distribution can be divided into two parts, server-side installation and client-side installation. Both include specific third-party applications needed to run the *AnyMedia* successfully. The server side application includes obligatory modules and optional ones which will be installed depending upon the customer needs.

Disk space

To store the AEM R1.7 files, your system must have the following amount of free disk space:

- AEM client: 60MB
- AEM server: The space will depend upon the number of NEs managed by the system because of the data size. The recommended size for n NEs is obtained from adding the following (numbers in kbyte):

  software=1000 (aprox.)

  logs=35000 (per NE)

  databases=0.8 + n

  transactions=2*(0.8+0.35*n)+n+25%

  The size calculated is based on maximum configurations and includes the overhead necessary for the temporary data used in operation.

It is recommended to create a separate partition to locate the transaction log file needed by ObjectStore. This partition would be used for this purpose only. It must not be deleted or managed because this file is only created and managed by ObjectStore. Note that without this file ObjectStore is not able to work and also if a new partition or location is chosen, it needs write permissions for the *AnyMedia*

user (login). If you choose a directory under *AnyMedia* location the correct owner and permits will be automatically provided in the installation process of *AnyMedia*.

The following table shows the recommended size of the partitions for a maximum of 10, 40, 100 and NEs:

NEs	/part 1	/part 2
10	475 MB	11 MB
40	500 MB	37 MB
100	530 MB	100 MB
600	700 MB	230 MB

where /part1 contains all the AEM server software and data bases and the /part2 is dedicated to the transaction log.

Distribution media

The AEM R1.7 distribution media is on CD-ROMs which contain all the software plus information and installation scripts.

Figure 2-1, page 2-4 to Figure 2-4, page 2-5 show the full AEMR1.7 distribution tree which consist in directories with the installation/remove scripts plus the installation and licensing documents. Subdirectories named "AnyMediaEMR1.7" contains the software which is divided in several packages.

A package contains a collection of files and directories required for the application and scripts to control how, where and if the package is installed.

These were built using the application packaging tools offered by Solaris (refer to your SUN documentation for more information).

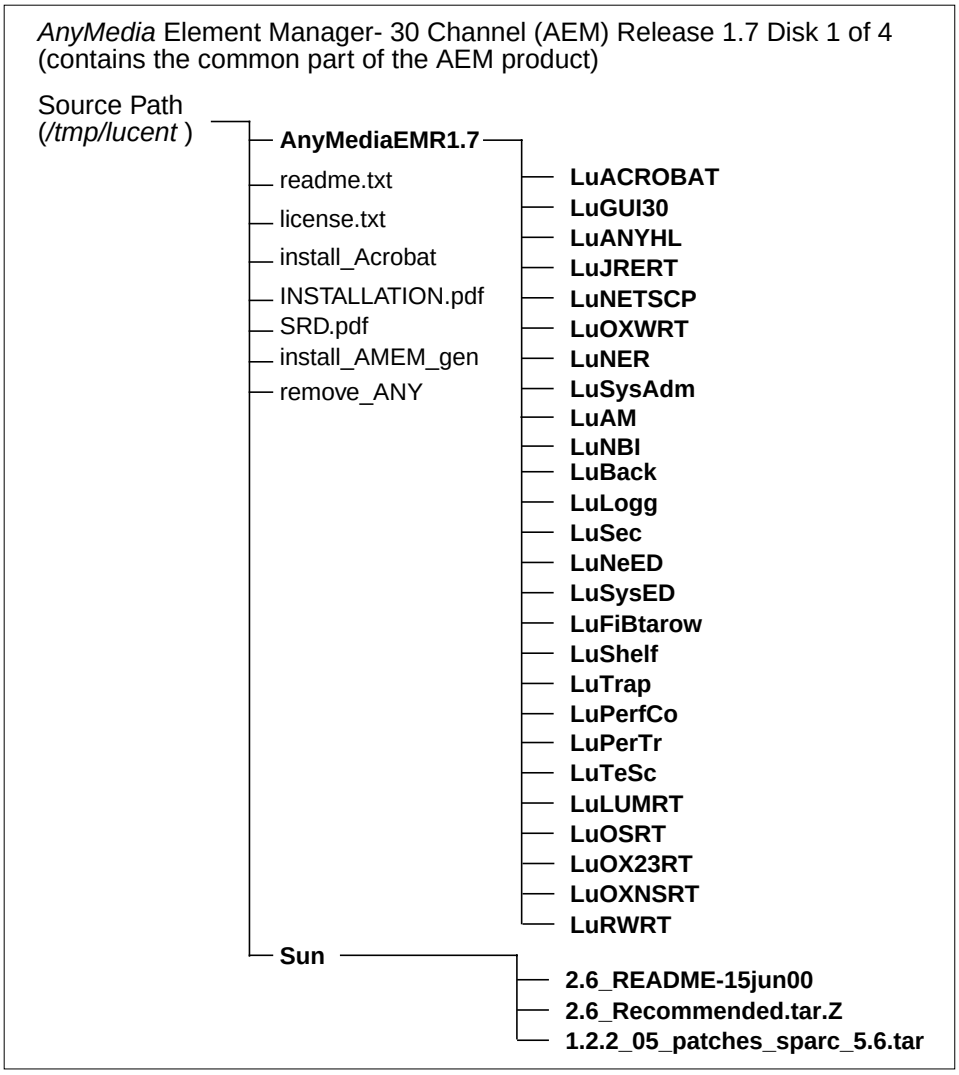


Figure 2-1 AEM R1.7 distribution tree CD-ROM 1

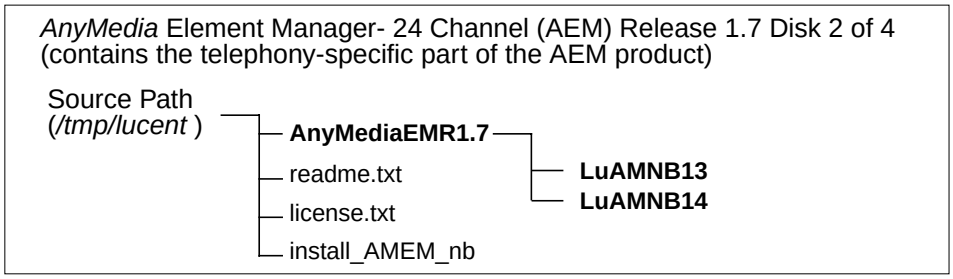


Figure 2-2 AEM R1.7 distribution tree CD-ROM 2

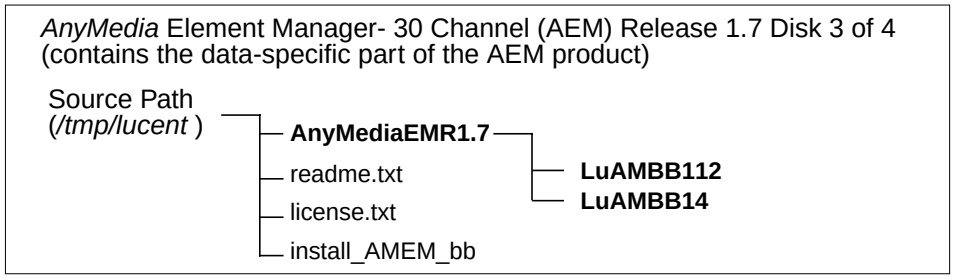


Figure 2-3 AEM R1.7 distribution tree CD-ROM 3

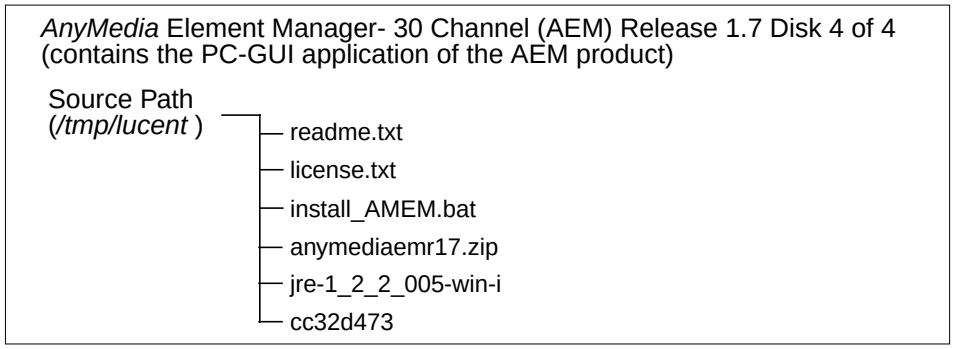


Figure 2-4 AEM R1.7 distribution tree CD-ROM 4

Installation scripts

The install_AMEM_gen, install_AMEM_nb or install_AMEM_bb scripts run in the korn shell <ksh> environment. The install_AMEM.bat (on CD-ROM 4) runs on Microsoft windows NT.

TCP ports

The following TCP ports **must** be available in order to successfully run the AEM R1.7:

- 1570: Orbix daemon uses the TCP port 1570 in order to wait for incoming connections that use the Orbix protocol.
- 1575: Used by Lumos
- 1591 to 1641: As CORBA servers are activated by the Orbix daemon, they are assigned to a port that clients can communicate with.

Time zone

The time zone **must** be the same for the *AnyMedia* client <GUI>, LUMOS, Network Element and OS.

Update process environment

Since the number of AEM R1.7 processes is so high, further process environment customization is needed on the server (related to IPC semaphores).
Carry out the following command to verify the value of the SEMMNU parameter:

```
sysdef | grep SEMMNU
```

The output of this command is like this:

```
30  undo structures in system (SEMMNU)
```

If the number appearing (e.g. 30) is less than 200, edit the */etc/system* file by adding the following line at the end of the file:

```
set semsys:seminfo_semmnu=200
```

Reboot the server workstation.

2.2 Installation procedure

General

The AEM R1.7 distribution includes one installation script per CD-ROM called **`install_AMEM_*`** which shall be used in a full installation of the CD-ROM (it includes all packages stored on the distribution media). Also, the script can be used to install individual packages (it will detect if any package is not installed and ask the user to install it) - cf. Chapter 2.2.2, page 2-75.

This guide shows the flow of the installation - according to the interaction with the administrator - using the installation script provided in the distribution.

Common tasks

Common actions must be make in both cases, as follows:

- You need to be logged on as **`root`**.
- Get ready your distribution medium:

Insert and mount the CDROM

Insert and mount the CD. If the machine is running the vold, it will recognize that the CD is in place and mount it on **`/cdrom/AnyMediaEMR17`** (depending on your system configuration, **`/cdrom/AnyMediaEMR17`** might have to be replaced with a different device name). Depending on the configuration of **`vold`** you may have to append a trailing dot (".") to references to file names on the CD. This is due to **`hsfs`** imposing a suffix on the file names. If the machine is not running the **`vold`**, type:

```
# mount -F hsfs -o ro,notraildot
/dev/dsk/c0t6d0s2/cdrom
```

The device identifier c0t6d0s2 is configuration dependent, and as such will vary from machine to machine.
This will mount the CD on **`/cdrom`** (depending on your system configuration, **`/cdrom`** might have to be replaced with a different mount point. For more information about on how to mount a CD-ROM drive refer to your SUN documentation.

2.2.1 Full installation

This type of installation uses the **`install_AMEM_*`** script in order to install all packages contained in the distribution.

For the following description it is assumed that:

- The hardware and software requirements to install the AEM R1.7 are prepared
- AEM R1.7 software have not been installed previously
- Common actions showed above have been made
- A new user shall be created on the target system, who will be the owner of the AEM R1.7 files. The server workstation shall be a NIS server and the client workstations shall be NIS clients. All the users shall be included in NIS and exported through the network in order to be recognized by the AEM software. For more information about the NIS tools refer to your SUN documentation.

- A NIS group is also necessary. Typically a new group shall be created to include all the AEM users.

Procedure

Complete the following procedure to install the AEM R1.7 application.

NOTE:
Lines with indentation are the system responses. They are included here to guide the installation procedure.

2.2.1.1 Server side installation

The installation of the AnyMedia server side is divided into the following parts:

- Installation of the third party software
- Installation of the common packages
- Installation of the optional packages (currently there are 4 optional packages).

2.2.1.1.1 Installation of the third party software

Complete the following procedure to install the third party software.

Step	Procedure

1. Go to the directory where the installation script is placed on CD-ROM 1 to 4.

2. Type **./install_AMEM_gen** and press **Return**.

```
AnyMedia NB EM R1.7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**

1.- Before attempting to install the applica
tion, please,read the readme.txt file.

2.- AnyMedia EM R1.7 runs on SUN SPARC Solaris 2
computers running Solaris 2.6 plus security and
Y2000 and packs 105490-07, 105568-13,
105210-19, 106040-12, 105633-21,106409-01,
105181-15, 105669-07, 105284-25 patches recom-
mended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
```

```
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it.
It is essential that these ports are not
used by any process on the SAME SUBNET DOMAIN.

4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/usr/bin",
"/usr/sbin" and "/usr/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.

******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation

CopyRight (c) 2000 Lucent Technologies, Inc.

All Rights Reserved.


Please, choose the installation mode

1 ADM  <Administration package installation>

2 GUI <Client package installation>

Enter selection [?,??,q]:
```

NOTE:
Type **?** to get help, type **??** to repeat the prompt and type **q** to exit from the installation.

4. Type **1** and press **Return**

```
                    Packages to install: LuLUMRT, LuRWRT,
                    LuOX23RT, LuOXNSRT, LuOSRT
```

LUMOS build 3.0 installation

```
                    Processing package instance <LuLUMRT> from
                    </home/bldr17/LOAD_36.1.1/build/
                    lucent/AnyMediaEMR1.7>

                    Lumos Runtime for AnyMedia EM R1.7
                    (sparc-solaris) Build 3.0 run-time

                    OK, No previous package LuLUMRT have been found.

                    Here is a list of your partitions and the free
                    space in each of them:

Filesystem          kbytes    used      avail     capacity Mounted on

/dev/dsk/c0t0d0s0   143927    36990     92545     29%      /
/dev/dsk/c0t0d0s4   625262    401569    167420    71%      /usr
/dev/dsk/c0t0d0s3   96455     11161     75649     13%      /var
/dev/dsk/c0t0d0s6   6591133   4250252   2274970   66%      /homelocal
/dev/dsk/c0t0d0s5   240399    8597      207763    4%       /var/cache
swap                1204840   40        1204800   1%       /tmp
masstc1:/export1/bld/2/bldr17 51014048 49174256 1499704 98%  /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048 49174256 1499704 98%  /home/syi_pl

                    Enter install directory [/opt/lucent/LUMOS]
                    [?,q]
```

5. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Checking your DNS domain name...

The DNS domain name found was: es.lucent.com

What is your DNS domain name
[default: es.lucent.com][?,q]
```

6. Type your DNS domain name and press **Return** or press **Return** to accept the default name.

```
Select owner and group for package files.

NBR  USER:GROUP

 1 halt:other

 2 root:other

 3 smtp:root

 4 ver1:staff

Enter selection [?,??,q]:
```

7. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected

Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.

This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuLUMRT> [y,n,?]
```

8. Type **y** and press **Return**.

```
Installing Lumos Runtime for AnyMedia EM R1,7
as <LuLUMRT>

## Installing part 1 of 1.

<files list>

............

[ verifying class <none> ]

## Executing postinstall script.

You have the installation logfile in
/tmp/EM_Install_LuLUMRT.log

Installation of <LuLUMRT> was successful.
```

RogueWave 1.0.7 & 1.1.2 installation

```
Processing package instance <LuRWRT> from
</home/bldr17/LOAD_36.1.1/build/lucent/
AnyMediaEMR1.7>

RogueWave Libraries Runtimes for AnyMedia EM R1.7
(sparc) std0130u thr0130u tls0710u tpr0112u

OK, No previous package LuRWRT have been found.

Filesystem                    kbytes    used      avail    capacity  Mounted on

/dev/dsk/c0t0d0s0             143927    36990     92545    29%       /
/dev/dsk/c0t0d0s4             625262    401569    167420   71%       /usr
/dev/dsk/c0t0d0s3             96455     11256     75554    13%       /var
/dev/dsk/c0t0d0s6             6591133   4294968   2230254  66%       /homelocal
/dev/dsk/c0t0d0s5             240399    8597      207763   4%        /var/cache
swap                          1202064   48        1202016  1%        /tmp
masstc1:/export1/bld/2/bldr17 51014048  49185848  1488120  98%       /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048  49185848  1488120  98%       /home/syi_pl


Enter install directory [/opt/lucent/rw] [?,q]
```

9. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Select owner and group for package files.

NBR  USER:GROUP

  1 halt:other

  2 root:other

  3 smtp:root

  4 ver1:staff

Enter selection [?,??,q]:
```

10. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected

Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.
```

```
This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuRWRT> [y,n,?]
```

11. Type **y** and press **Return**.

```
Installing RogueWave Libraries Runtimes for
AnyMedia EM R1.7 as <LuRWRT>

## Installing part 1 of 1.

<files list>

............

"[ verifying class <none> ]

## Executing postinstall script.

You have the installation logfile in
/tmp/EM_Install_LuRWRT.log

Installation of <LuRWRT> was successful.
```

OrbixMT 2.3c patch 02 installation

```
Processing package instance <LuOX23RT> from
</home/bldr17/LOAD_36.1.1/build/lucent/
AnyMediaEMR1.7>

Orbix 2.3c02 Runtime for AnyMedia NB-EM R1.7
(sparc-solaris) Version 2.3c02MT Run-Time

OK, No previous package LuOX23RT have been found.

Here is a list of your partitions and the free
space in each of them:

Filesystem                    kbytes   used     avail    capacity Mounted on

/dev/dsk/c0t0d0s0             143927   36990    92545    29%      /
/dev/dsk/c0t0d0s4             625262   401569   167420   71%      /usr
/dev/dsk/c0t0d0s3             96455    11285    75525    13%      /var
/dev/dsk/c0t0d0s6             6591133  4313833  2211389  67%      /homelocal
/dev/dsk/c0t0d0s5             240399   8597     207763   4%       /var/cache
swap                          1201856  56       1201800  1%       /tmp
masstc1:/export1/bld/2/bldr17 51014048 49192112 1481856  98%      /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048 49192112 1481856  98%      /home/syi_pl

Where should Orbix be installed?
[/opt/lucent/OrbixMT_2.3c2] [?,q]
```

12. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Checking your DNS domain name...

The DNS domain name found was: es.lucent.com

What is your DNS domain name
[default: es.lucent.com][?,q]
```

13. Type your DNS domain name and press **Return** or press **Return** to accept the default name.

```
Select owner and group for package files.

NBR  USER:GROUP

  1 halt:other

  2 root:other

  3 smtp:root

  4 ver1:staff

Enter selection [?,??,q]:
```

14. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected

Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.

This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuOX23RT> [y,n,?]
```

15. Type **y** and press **Return**

```
Installing Orbix 2.3c02 Runtime for AnyMedia
EM R1,7 as <LuOX23RT>

## Installing part 1 of 1.
```

```
<files list>
.............
[ verifying class <none> ]
<files list>
......
[ verifying class <bin> ]
<files list>
......
[ verifying class <cfg> ]
<files list>
......
[ verifying class <lib> ]
## Executing postinstall script.
You have the installation logfile in
/tmp/EM_Install_LuOX23RT.log
Installation of <LuOX23RT> was successful.
```

OrbixNames 1.1c installation

```
Processing package instance <LuOXNS> from
</home/bldr17/LOAD_36.1.1/build/lucent/
AnyMediaEMR1.7>
OrbixNames 1.1c Runtime for AnyMedia EM R1;7
(sparc-solaris) Version 1.1c Run-Time
OK, No previous package LuOXNSRT have been found.
Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in
/opt/lucent/OrbixMT_2.3c2
Here is a list of your partitions and the free
space in each of them:
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c0t0d0s0	143927	36990	92545	29%	/
/dev/dsk/c0t0d0s4	625262	401569	167420	71%	/usr
/dev/dsk/c0t0d0s3	96455	11326	75484	14%	/var
/dev/dsk/c0t0d0s6	6591133	4355134	2170088	67%	/homelocal
/dev/dsk/c0t0d0s5	240399	8597	207763	4%	/var/cache
swap	1201416	64	1201352	1%	/tmp
masstc1:/export1/bld/2/bldr17	51014048	49193336	1480632	98%	/home/bldr17
masstc1:/export1/bld/2/syi_pl	51014048	49193336	1480632	98%	/home/syi_pl

```
Where should OrbixNames be installed?
[/opt/lucent/OrbixNames1.1c][?,q]
```

16. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Multi-threaded Orbix installation detected, is
this correct? [y] [y,n,?]
```

17. Type **y** and press **Return**.

```
Select owner and group for package files.
NBR  USER:GROUP
  1 halt:other
  2 root:other
  3 smtp:root
  4 ver1:staff
Enter selection [?,??,q]:
```

18. Type **4** and press **Return**.

```
User: <users> and Group: <group>, have been se
lected
Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.
This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.
Do you want to continue with the installation
of <LuOXNS> [y,n,?]
```

19. Type **y** and press **Return**.

```
Installing OrbixNames 1.1c Runtime for AnyMedia
EM R1,7 as <LuOXNSRT>
## Installing part 1 of 1.
[ verifying class <names> ]
```

```
<files list>
.............
[ verifying class <bin> ]
<files list>
.............
[ verifying class <lib> ]
## Executing postinstall script.
-----------------------------------------------
Okay, OrbixNames is now installed.
You have the installation logfile in
/tmp/EM_Install_LuOXNSRT.log
Installation of <LuOXNSRT> was successful.
```

ObjectStore 5.1 installation

```
Processing package instance <LuOSRT> from
</home/bldr17/LOAD_36.1.1/build/lucent/
AnyMediaEMR1.7>
ObjectStore 5.1_SP2 Runtime for AnyMedia EM R1,7
(sparc-solaris) 5.1_SP2 Run-Time
OK, No previous package LuOXNSRT have been found.
Here is a list of your partitions and the free
space in each of them:
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c0t0d0s0	143927	36990	92545	29%	/
/dev/dsk/c0t0d0s4	625262	401569	167420	71%	/usr
/dev/dsk/c0t0d0s3	96455	11359	75451	14%	/var
/dev/dsk/c0t0d0s6	6591133	4383673	2141549	68%	/homelocal
/dev/dsk/c0t0d0s5	240399	8597	207763	4%	/var/cache
swap	1201288	72	1201216	1%	/tmp
masstc1:/export1/bld/2/bldr17	51014048	49193336	1480632	98%	/home/bldr17
masstc1:/export1/bld/2/syi_pl	51014048	49193336	1480632	98%	/home/syi_pl

```
Enter install directory [/opt/lucent/OS51_SP2]
[?,q]
```

20. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Using </> as the package base directory.
## Processing package information.
## Processing system information.
```

```
## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.

The following files are being installed with
setuid and/or setgid permissions: /opt/lucent
/OS51_SP2/ostore/lib/oscminit <setuid root>

Do you want to install these as setuid/setgid
files [y,n,?,q]
```

21. Type **y** and press **Return**.

```
This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuOSRT> [y,n,?]
```

22. Type **y** and press **Return**.

```
Installing ObjectStore 5.0_SP3 Runtime for Any
Media NB-EM R1,7 as <LuOSRT>

## Installing part 1 of 1.

<files list>
.............

[ verifying class <none> ]

## Executing postinstall script.

*****************************************

 * Remember execute "osconfig" to set the
environment *
*****************************************

 You have the installation logfile in
/tmp/EM_Install_LuOSRT.log

Installation of <LuOSRT> was successful.
```

ObjectStore configuration (I)

```
Object Store configuration

The default copy of ObjectStore to configure is
in /opt/lucent/OS51_SP2/ostore.

Is this the copy that you want to configure?
[yes]
```

23. Press **Return**.

```
ObjectStore includes shared libraries. For Ob
jectStore applications and utilities to work,
the dynamic linker must be able to find them.

The recommended arrangement is to have symbolic
links in /usr/lib to the shared libraries.

If you choose not to make these links, then you
will have to instruct all ObjectStore users to
add /opt/lucent/OS51_SP2/ostore/lib to their
LD_LIBRARY_PATH environment variable.

Do you want to create links to ObjectStore li
braries in /usr/lib? [yes]
```

24. Press **Return**.

```
Since you have requested a File-database con
figuration, you must give a pathname for the
transaction log file. Where do you want to put
the transaction log?
```

25. Type **/opt/lucent/transaction.log** and press **Return**.

```
You have configured this machine to run an Ob
jectStore server. The server's transaction log
is in /opt/lucent/transaction.log.

Do you want to proceed? [yes]
```

26. Press **Return**.

```
Writing configuration files and initializing
the server, please wait...

000613 091747 ObjectStore Release 5.1 Service
Pack 2 Database Server

The ObjectStore server is running.

ObjectStore includes a server daemon which must
be running for any application to access an
ObjectStore database.
It is recommended that you auto-start the daemon
via commands in your operating system startup
scripts. If you do not configure automatic
startup, you will have to start the server
daemon by hand, or re-run this utility to
configure auto-start.
```

```
Would you like to configure automatic server
startup and shutdown? [yes]
```

27. Press **Return**.

```
Successfully created /etc/rc2.d/S80ostore4.

Successfully created link from /etc/rc2.d/
K80ostore4 to /etc/rc2.d/S80ostore4.

Note that you must manually remove or edit
existing ObjectStore R3 scripts in /etc/rc2.d in
some situations:

To run only R4 clients or R3 file database
clients, remove all R3 scripts in /etc/rc2.d.

To run all R4 clients and R3 clients, including
R3 rawfs clients, edit existing R3 scripts in
/etc/rc2.d to run only the R3 Directory Manager,
but not the R3 Server.

To run both R3 and R4 clients with separate R3
and R4 Servers, see the documentation on editing
your OS_ROOTDIR/etc/ports file.

This script will now verify the installation:

The ObjectStore Server daemon process is
accessible. Schema databases are accessible.

The cache manager launcher for release 4
(/homelocal/new/OS51_SP2/ostore/lib/oscminit)
has correct modes and ownership.
ObjectStore configuration completed.
```

2.2.1.1.2 Installation of the common packages

Complete the following procedure to install the common packages:

Step	Procedure

1. Go to the directory where the installation script is placed on the CD-ROM number one.

2. Type **./install_AMEM_gen** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**
```

1.- Before attempting to install the application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC Solaris 2 computers running Solaris 2.6 plus security and Y2000 and packs 105490-07, 105568-13, 105210-19, 106040-12, 105633-21, 106409-01, 105181-15, 105669-07, 105284-25 patches recommended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order to succesfully run the AnyMedia EM:
*** 1570: Orbix daemon uses the TCP port 1570 in order to wait for incoming connections that use the Orbix protocol.**
*** 1591 to 1641: As Corba servers are activated by the Orbix daemon, they are assigned a port so that clients can communicate with it. It is essential that these ports are not used by any process on the SAME SUBNET DOMAIN.**

4.- The install_AMEM script runs on K-shell <ksh> environment.

5.- At least the system environment variable PATH MUST include the paths "/sr/bin", "/usr/sbin" and "/uas/ucb" (for instance, "export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any Media Client <GUI>, LUMOS and Network Element. This parameter is needed for installing the Any Media Client.

****

Do you like to continue [y,n,?,q]

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1.7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved.


Please, choose the installation mode
1 ADM  <Administration package installation>
2 GUI <Client package installation>
Enter selection [?,??,q]:
```

4. Type **1** and press **Return**

```
The package <LuLUMRT> is already installed on
the system.
The package <LuRWRT> is already installed on
the system.
The package <LuOX23RT> is already installed on
the system.
The package <LuOXNSRT> is already installed on
the system.
The package <LuOSRT> is already installed on
the system.
##The package/s were already installed in the
System.
```

ObjectStore configuration (II)

```
Object Store configuration
The default copy of ObjectStore to configure is
in /opt/lucent/OS51_SP2/ostore.
Is this the copy that you want to configure?
[yes]
```

5. Press **Return**.

```
ObjectStore includes shared libraries. For Ob
jectStore applications and utilities to work,
the dynamic linker must be able to find them.
The recommended arrangement is to have symbolic
links in /usr/lib to the shared libraries.
```

If you choose not to make these links, then you will have to instruct all ObjectStore users to add /opt/lucent/OS51_SP2/ostore/lib to their LD_LIBRARY_PATH environment variable.

Warning: ObjectStore libraries already exist in /usr/lib.

If you choose not to make links in /usr/lib for the new libraries, ObjectStore users may incorrectly link with old libraries.

Do you want to create links to ObjectStore li braries in /usr/lib? [yes]

6. Press **Return**.

You have configured this machine to run an Ob jectStore server. The server's transaction log is in /opt/lucent/transaction.log.

Do you want to proceed? [yes]

7. Press **Return**.

Writing configuration files and initializing the server, please wait...

000529 170809 ObjectStore Release 5.1 Service Pack 2 Database Server

The ObjectStore server is running.

ObjectStore includes a server daemon which must be running for any application to access an ObjectStore database.
It is recommended that you auto-start the daemon via commands in your operating system startup scripts. If you do not configure automatic startup, you will have to start the server daemon by hand,or re-run this utility to configure auto-start.

What you like to configure automatic server startup and shutdown?[yes]

8. Press **Return**.

Successfully created /etc/rc2.d/S80ostore4.

```
Successfully created link from /etc/rc2.d/
K80ostore4 to /etc/rc2.d/S80ostore4.

Note that you must manually remove or edit
existing ObjectStore R3 scripts in /etc/rc2.d in
some situations:

To run only R4 clients or R3 file database
clients, remove all R3 scripts in /etc/rc2.d.

To run all R4 clients and R3 clients, including
R3 rawfs clients, edit existing R3 scripts in
/etc/rc2.d to run only the R3 Directory Manager,
but not the R3 Server.

To run both R3 and R4 clients with separate R3
and R4 Servers, see the documentation on editing
your OS_ROOTDIR/etc/ports file.

This script will now verify the installation:

The ObjectStore Server daemon process is
accessible.Schema databases are accessible.

The cache manager launcher for release 4
(/opt/lucent/OS51_SP2/ostore/lib/oscminit) has
correct modes and ownership.

ObjectStore configuration completed.


## Packages to install:  LuSysAdm LuAM LuBack
LuFiBrow LuNER LuNBI LuLogg LuPerf LuPerCo
LuNeED LuSec LuShelf LuSysED LuTrap LuPerTr
LuTeSc.
```

System Administration installation

```
Processing package instance <LuSysAdm> from
</home/bldr17/LOAD_36.1.1/build/lucent/
AnyMediaEMR1.7>

AnyMedia Element Manager System Administration
Release 1.7 (Administration)

(sparc) LuSysAdm_36_1.1
**************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**************************************
```

```
OK, No previous package LuSysAdm have been
found.

Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in /opt/lucent/
OrbixMT_2.3c2

Package <LuOXNSRT> OrbixNames Version 1.1c
Run-Time have been found in /opt/lucent/
OrbixNames1.1c

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2

Package <LuLUMRT> Lumos Build 3.0 run-time have
been found in /opt/lucent/LUMOS

Package <LuRWRT> RogueWave Tools and Threads
std0130u thr0130u tls0710u tpr0112u have been
found in /opt/lucent/rw


Where should System Admin be installed?
[/opt/lucent/AnyMediaEM_R1.7] [?,q]
```

9. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
The installation path selected for AnyMedia EM
R1.7 is /opt/lucent/AnyMediaEM_R1.7.

NBR  USER:GROUP

  1 halt:other

  2 root:other

  3 smtp:root

  4 ver1:staff

Enter selection [?,??,q]:
```

10. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected

***Boot processes***


Do you like install the SystemAdmin process on
the system boot [y,n,?,q]
```

11. Type **y** and press **Return**.

```
Clean-up tasks for the AnyMedia-EM system will
be executed every day at 2.00 AM. Do you like
change it [y,n,?,q]
```

12. Type **n** and press **Return**.

```
Using </> as the package base directory.

## Processing package information.

## Processing system information.
16 package pathnames are already properly
installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuSysAdm> [y,n,?]
```

13. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager System
Administration Release 1.7 (Administration) as
<LuSysAdm>

## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.


*** WARNING: The installation process has not
permissions to change the owner and group of the
path containing the Object Store transaction.log
file. If you want that AnyMedia automayicaly
manages this file, the owner and group of its
path (direcory and all sub-directories) must be
changed to ver1 and to staff respectively.
```

```
[ s1224: OrbixNames (Release 1.1) ]
[ s1369: OrbixOTM package (Release 1.0) ]

Checking AnyMedia EM R1.7 naming contexts
Creating data bases
Getting the AnyMedia installation path... OK.
Starting SysAdmDbPopulate process...
Getting SystemAdmin Database path... OK.
Creating SystemAdmin Database... OK

Population successful.
1190 Killed
orbixd daemon pid=1190 have been killed. Was
mine.
1196 Killed
ns daemon pid=1196 have been killed. Was mine.
*****************************************
* Once the installation process if finished *
* Please boot the machine and
* Execute ". AnyMediaEM.sh" to set the
environment *
*****************************************
You have the installation logfile in /opt/
lucent/AnyMediaEM_R1.7/tmp/EM_Install.log

Installation of <LuSysAdm> was successful.'
```

Alarm Management installation

```
Processing package instance <LuAM> from </
homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Alarms Release 1.7
(Administration) (sparc) LuAM_36_1.1


************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
 ************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuAM have been found.
Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuAM> [y,n,?]
```

14. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Alarms
Release 1.7 (Administration) as <LuAM>


## Installing part 1 of 1.
<files list>
.............
[ verifying class <common> ]
```

```
## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2

Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in /opt/lucent/
OrbixMT_2.3c2


Creating data bases

Starting AMDbPopulate process...

Getting the AnyMedia installation path...OK

Getting Alarm data base path... OK

Creating Alarm Data Base...

exit OK

2242 Killed

orbixd daemon pid=2242 have been killed. Was mine.


You have the installation logfile in
/tmp/EM_Install_LuAM.log

Installation of <LuAM> was successful.
```

Backup installation

```
Processing package instance <LuBack> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Backup Release 1.7
(Administration) (sparc) LuBack_36_1.1


*****************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*****************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuBack have been found.
```

```
Do you like install the Backup process as a cron
[y,n,?,q] n
```

15. Type **n** and press **Return**.

```
Do you like install the Archive process as a
cron [y,n,?,q]
```

16. Type **n** and press **Return**.

```
Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.


The following files are already installed on the
system and are being used by another package:

* /opt/lucent/AnyMediaEM_R1.7/Backup <attribute
change only>


* - conflict with a file which does not belong to
any package.


Do you want to install these conflicting files
[y,n,?,q]
```

17. Type **y** and press **Return**.

```
## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuBack> [y,n,?]
```

18. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Backup
Release 1.7 (Administration) as <LuBack>

## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.


You have the installation logfile in
/tmp/EM_Install_LuBack.log

Installation of <LuBack> was successful.
```

File Browser installation

```
Processing package instance <LuFiBrow> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>

AnyMedia Element Manager File Browser Release 1.7
(administration) (sparc) LuFiBrow_36_1.1


*****************************************

 * AnyMedia Element Manager *

 * (c) 1999-Lucent Technologies *

 *****************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuFiBrow have been found.

Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

 1 package pathname is already properly
 installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.
```

```
Installing AnyMedia Element Manager File Browser
Release 1.7 (administration) as <LuFiBrow>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/FileBrowser/bin/
FileBrowser

[ verifying class <common> ]

Installation of <LuFiBrow> was successful.
```

Network Registry installation

```
Processing package instance <LuNER> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Network Register Element Manager
Release 1.7 (Administration)(sparc) LuNER_36_1.1


*****************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*****************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuNER have been found.

Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.
```

```
Do you want to continue with the installation of
<LuNER> [y,n,?]
```

19. Type **y** and press **Return**.

```
Installing AnyMedia Network Register Element
Manager Release 1.7 (Administration) as <LuNER>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2

Oject Store path set to /opt/lucent/OS51_SP2
ostore

Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in /opt/lucent/
OrbixMT_2.3c2


Creating data bases

Starting CreateNER_db process...

Getting the AnyMedia installation path...OK

Getting NER data base path

Creating NER data base...OK

exit OK

2438 Killed

orbixd daemon pid=2438 have been killed. Was mine.


You have the installation logfile in
/tmp/EM_Install_LuNER.log


Installation of <LuNER> was successful.
```

Northbound Interface installation

```
Processing package instance <LuNBI> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia North Bound Element Manager Release 1.7
(Administration) (sparc) LuNBI_36_1.1


*******************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*******************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuNBI have been found.
Using </opt/lucent/AnyMediaEM_R1.7> as th
package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuNBI> [y,n,?]
```

20. Type **y** and press **Return**.

```
Installing AnyMedia North Bound Element Manager
Release 1.7 (Administration) as <LuNBI>


## Installing part 1 of 1.
/opt/lucent/AnyMediaEM_R1.7/NBI/bin/PassThrough
/opt/lucent/AnyMediaEM_R1.7/NBI/bin/
PassThroughConfig
```

```
/opt/lucent/AnyMediaEM_R1.7/NBI/cfg/
NBIDomains.cfg

/opt/lucent/AnyMediaEM_R1.7/NBI/cfg/NBILog.log

[ verifying class <common> ]

## Executing postinstall script.


Installation of <LuNBI> was successful.
```

Log Management installation

```
Processing package instance <LuLogg> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Logging Release 1.7
(Administration)(sparc) LuLogg_36_1.1


**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuLogg have been found.

Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

 1 package pathname is already properly
 installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


Installing AnyMedia Element Manager Logging
Release 1.7 (Administration) as <LuLogg>
```

```
## Installing part 1 of 1.
/opt/lucent/AnyMediaEM_R1.7/Logging/bin/
LogReader
/opt/lucent/AnyMediaEM_R1.7/Logging/bin/
LogWriter
/opt/lucent/AnyMediaEM_R1.7/Logging/cfg/
Logging.cfg
[ verifying class <common> ]


Installation of <LuLogg> was successful.
```

Performance Logging installation

```
Processing package instance <LuPerf> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Performace Release 1.7
(Administration)(sparc) LuPerf_36_1.1


**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
Package <LuLogg> Loggin LuLogg_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuPerf have been found.
Using </> as the package base directory.
## Processing package information.
## Processing system information.
 1 package pathname is already properly
 installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.
```

```
Installing AnyMedia Element Manager Performace
Release 1.7 (Administration) as <LuPerf>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/Logging
Performance/bin/LogWriter <symbolic link>

/opt/lucent/AnyMediaEM_R1.7/
LoggingPerformance/cfg/Logging.cfg

[ verifying class <common> ]


Installation of <LuPerf> was successful.
```

Performance Monitoring installation

```
Processing package instance <LuPerCo> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Performan Monitorin
Release 1.7 (Administration)(sparc)LuPerCo_36_1.1


**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuPerCo have been found.

Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

 1 package pathname is already properly
 installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.
```

```
This package contains scripts which will be
executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation of
<LuPerCo> [y,n,?]
```

21. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Performan
Monitorin Release 1.7 (Administration) as
<LuPerCo>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/PerformanceConfig/
bin/PCDbCreate

/opt/lucent/AnyMediaEM_R1.7/PerformanceConfig
/bin/StatConfig

/opt/lucent/AnyMediaEM_R1.7/PerformanceConfig/
db/PCDSchema.adb

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2

Object Store path set to LuOSRT:ObjectStore:
Release 5.1 Service Pack 3:5.1_SP2
Run-Time:/bin:/lib:osversion:

Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in
/opt/lucent/OrbixMT_2.3c2


Creating data bases

Starting PCDbCreate process...

exit OK

2692 Killed

orbixd daemon pid=2692 have been killed. Was mine.


You have the installation logfile in /tmp/
EM_Install_LuPerCo.log


Installation of <LuPerCo> was successful.
```

NE Event Distributor installation

```
Processing package instance <LuNeED> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Auxiliar Even Dist.
Release 1.7 (administration)(sparc) LuNeED_36_1.1


*********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
 *********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuNeED have been found.
Using </> as the package base directory.
## Processing package information.
## Processing system information.
 1 package pathname is already properly
 installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.


Installing AnyMedia Element Manager Auxiliar Even
Dist. Release 1.7 (administration) as <LuNeED>


## Installing part 1 of 1.
<files list>
.............
[ verifying class <common> ]


Installation of <LuNeED> was successful.


Processing package instance <LuSec> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>
```

Security installation

```
AnyMedia Element Manager Security Release 1.7
(Administration)(sparc) LuSec_36_1.1


**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuSec have been found.

Using </opt/lucent/AnyMediaEM_R1.7> as the
package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuSec> [y,n,?] y
```

22. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Security
Release 1.7 (Administration) as <LuSec>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2
```

```
Oject Store path set to LuOSRT:ObjectStore:
Release 5.1 Service Pack 3:5.1_SP2
Run-Time:/bin:/lib:osversion:

Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in /opt/lucent/
OrbixMT_2.3c2


Creating data bases

OK

Creating Database

2839 Killed

orbixd daemon pid=2839 have been killed. Was mine.


You have the installation logfile in /tmp/
EM_Install_LuSec.log


Installation of <LuSec> was successful.
```

Combined Shelf installation

```
Processing package instance <LuShelf> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Shelf Release 1.7
(Administration)(sparc) LuShelf_36_1.1


*********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuShelf have been found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.
```

```
 1 package pathname is already properly
 installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

Installing AnyMedia Element Manager Shelf
Release 1.7 (Administration) as <LuShelf>

## Installing part 1 of 1.
/opt/lucent/AnyMediaEM_R1.7/CombinedShelf/
bin/NECombined
/opt/lucent/AnyMediaEM_R1.7/CombinedShelf/
cfg/CombinedPacks.cfg
/opt/lucent/AnyMediaEM_R1.7/CombinedShelf/
cfg/CombinedShelves.cfg
[ verifying class <common> ]

Installation of <LuShelf> was successful.
```

General Event Distributor installation

```
Processing package instance <LuSysED> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>

AnyMedia Element Manager System Even Dist.
Release 1.7(administration) (sparc) LuSysED_36_1.1

**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************

Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuSysED have been found.
Using </> as the package base directory.
## Processing package information.
```

```
## Processing system information.
 1 package pathname is already properly
 installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

Installing AnyMedia Element Manager System Even
Dist. Release 1.7 (administration) as <LuSysED>

## Installing part 1 of 1.
<files list>
.............
[ verifying class <common> ]

Installation of <LuSysED> was successful.
```

Trap Dispatcher installation

```
Processing package instance <LuTrap> from
</homelocal/tmp/lucent/AnyMediaEMR1.7/homelo-
cal/tmp/lucent/AnyMediaEMR1.7>

AnyMedia Element Manager Trap Dispacher Release 1.7
(Administration)(sparc) LuTrap_36_1.1

 ******************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
 ******************************************

Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
OK, No previous package LuTrap have been found.
Using </> as the package base directory.
## Processing package information.
## Processing system information.
```

```
 1 package pathname is already properly
 installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


The following files are being installed with
setuid and/or setgid permissions:

/opt/lucent/AnyMediaEM_R1.7/TrapDispatcher/
bin/TrapDispatcher <setuid root>


Do you want to install these as setuid/setgid
files [y,n,?,q]
```

23. Type **y** and press **Return**.

```
This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuTrap> [y,n,?]
```

24. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Trap
Dispacher Release 1.7 (Administration) as <LuTrap>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/TrapDispatcher/
bin/TrapDispatcher

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOXNSRT> OrbixNames Version 1.1c Run-
Time have been found in /opt/lucent/OrbixNames1.1c

Package <LuOX23RT> OrbixMT Version 2.3c02MT Run-
Time have been found in /opt/lucent/OrbixMT_2.3c2

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time have
been found in /opt/lucent/OS51_SP2
```

```
ln: cannot create /usr/lib/libos.so.sun.4.0:
File exists

ln: cannot create /usr/lib/liboscol.so.sun.4.0:
File exists

ln: cannot create /usr/lib/libosqry.so.sun.4.0:
File exists

ln: cannot create /usr/lib/libosthr.so.sun.4.0:
File exists

Package <LuRWRT> RogueWave Tools and Threads
std0130u thr0130u tls0710u tpr0112u have been
found in /opt/lucent/rw


 You have the installation logfile in /tmp
/EM_Install.log_2937


Installation of <LuTrap> was successful.
```

Performance Translator installation

```
Processing package instance <LuPerTr> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Performance Translator
Release 1.7(administration) (sparc) LuPerTr_36_1.1


**********************************************

 * AnyMedia Element Manager *

 * (c) 1999-Lucent Technologies *

**********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuPerTr have been found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.

 1 package pathname is already properly
 installed.

## Verifying disk space requirements.
```

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuPerTr> [y,n,?]
```

25. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Performance
Translator Release 1.7 (administration) as
<LuPerTr>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/
PerformanceTranslator/bin/ReportTranslator

/opt/lucent/AnyMediaEM_R1.7/
PerformanceTranslator/cfg/
PerformanceTranslator.cfg

[ verifying class <common> ]

## Executing postinstall script.


Installation of <LuPerTr> was successful.
```

Test Scheduler installation

```
Processing package instance <LuTeSc> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager TestScheduler
Release 1.7 (administration)(sparc) LuTeSc_36_1.1


**********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
**********************************************
```

```
Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

OK, No previous package LuTeSc have been found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.

 1 package pathname is already properly
 installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


Installing AnyMedia Element Manager TestScheduler
Release 1.7 (administration) as <LuTeSc>


## Installing part 1 of 1.

/opt/lucent/AnyMediaEM_R1.7/TestScheduler/bin/
TestScheduler

/opt/lucent/AnyMediaEM_R1.7/TestScheduler/cfg/
TestScheduler.cfg

[ verifying class <common> ]


Installation of <LuTeSc> was successful.


Installation of AnyMedia EM R1.7 was successful
<ADM side installation>
```

2.2.1.1.3 Installation of the telephony R1.3 agent (optional)

Complete the following procedure to install the telephony R1.3 agent.

Step	Procedure

1. Go to the directory where the installation script is placed (CD-ROM 2 of 4).

2. Type **./install_AMEM_nb** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**

1.- Before attempting to install the
application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC
Solaris 2 computers running Solaris 2.6 plus
security and Y2000 and packs 105490-07,
105568-13, 105210-19, 106040-12, 105633-21,
106409-01, 105181-15, 105669-07, 105284-25
patches recommended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it. It is
essential that these ports are not used by any
process on the SAME SUBNET DOMAIN.

4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/sr/bin",
"/usr/sbin" and "/uas/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.
```

```
******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation

Please, choose one or more Band mode separated
by blank


1  LuAMNB13      <NarrowBand R1.3   installation>

2  LuAMNB14      <NarrowBand R1.4   installation>


Enter selection [?,??,q]:
```

4. Type **1** and press **Return**

```
## Packages to install:  LuAMNB13
```

NE telephony support for R1.3 installation

```
Processing package instance <LuAMNB13> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia NB Element Manager Release 1.7 for NE
release 13 (sparc) LuAMNB13_36.1.1


*******************************************

 * AnyMedia Element Manager *

 * (c) 1999-Lucent Technologies *

*******************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

AnyMedia EM R1.7 path=/opt/lucent/
AnyMediaEM_R1.7

Package <LuAM> Alarms LuAM_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuNBI> NorthBound LuNBI_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7
```

```
Package <LuNER> NER LuNER_36_1.1 have been found
in /opt/lucent/AnyMediaEM_R1.7

Package <LuNeED> NetEvenDist LuNeED_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSec> Security LuSec_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuShelf> ConbinedShelf LuShelf_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSysED> SystemEventDist LuSysED_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuLUMRT> Lumos Build 3.0 run-time have
been found in /opt/lucent/LUMOS

OK, No previous package LuAMNB13 have been
found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

WARNING:

The / filesystem has 185076 free blocks. The
current installation requires 378210 blocks,
which includes a required 150 block buffer for
open deleted files. 193134 more blocks are
needed.

Do you want to continue with the installation of
<LuAMNB13> [y,n,?]
```

5. Type **Y** and press **Return**

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.

Do you want to continue with the installation of
<LuAMNB13> [y,n,?]
```

6. Type **Y** and press **Return**

```
Installing AnyMedia NB Element Manager
Release 1.7 for NE release 13 as <LuAMNB13>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2


Creating data bases

You have the installation logfile in
/tmp/EM_Install_LuAMNB13.log


Installation of <LuAMNB13> was successful.


## The package < LuAMNB13> is not installed in
the system.

## Please try ../install_AMEM again and install
the package < LuAMNB13>.

## to complete the installation.
```

NOTE:
The last message is an error and can be ignored.

2.2.1.1.4 Installation of the telephony R1.4 agent (optional)

Complete the following procedure to install the telephony R1.4 agent.

Step	Procedure
1.	Go to the directory where the installation script is placed (CD-ROM 2 of 4).
2.	Type **./install_AMEM_nb** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**
```

```
1.- Before attempting to install the
application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC
Solaris 2 computers running Solaris 2.6 plus
security and Y2000 and packs 105490-07,
105568-13, 105210-19, 106040-12, 105633-21,
106409-01, 105181-15, 105669-07, 105284-25
patches recommended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it. It is
essential that these ports are not used by any
process on the SAME SUBNET DOMAIN.

4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/sr/bin",
"/usr/sbin" and "/uas/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.

******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation

Please, choose one or more Band mode separated
by blank
```

```
1  LuAMNB13      <NarrowBand R1.3   installation>
2  LuAMNB14      <NarrowBand R1.4   installation>

Enter selection [?,??,q]:
```

4. Type **2** and press **Return**

NE telephony support for R1.4 installation

```
Processing package instance <LuAMNB14> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>

AnyMedia NB Element Manager Release 1.7
(sparc) LuAMNB14_36.1.1

*********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*********************************************

Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
AnyMedia EM R1.7 path=/opt/lucent/AnyMediaEM_R1.7
Package <LuAM> Alarms LuAM_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7
Package <LuNBI> NorthBound LuNBI_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7
Package <LuNER> NER LuNER_36_1.1 have been found
in /opt/lucent/AnyMediaEM_R1.7
Package <LuNeED> NetEvenDist LuNeED_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7
Package <LuSec> Security LuSec_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7
Package <LuShelf> ConbinedShelf LuShelf_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
Package <LuSysED> SystemEventDist LuSysED_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7
Package <LuLUMRT> Lumos Build 3.0 run-time have
been found in /opt/lucent/LUMOS
OK, No previous package LuAMNB14 have been
found.
```

```
Using </> as the package base directory.

## Processing package information.

## Processing system information.

 2 package pathnames are already properly
 installed.

## Verifying disk space requirements.

WARNING:

The / filesystem has 185076 free blocks. The
current installation requires 378866 blocks, which
includes a required 150 block buffer for open
deleted files. 193790 more blocks are needed.


Do you want to continue with the installation of
<LuAMNB14> [y,n,?]
```

5. Type **Y** and press **Return**

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuAMNB14> [y,n,?]
```

6. Type **Y** and press **Return**

```
Installing AnyMedia NB Element Manager Release
1.7 as <LuAMNB14>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
```

```
have been found in /opt/lucent/OS51_SP2


Creating data bases

You have the installation logfile in
/tmp/EM_Install_LuAMNB14.log


Installation of <LuAMNB14> was successful.


## The package < LuAMNB14> is not installed in
the system.

## Please try ../install_AMEM again and install
the package < LuAMNB14>.

## to complete the installation.
```

NOTE:
The last message is an error and can be ignored.

2.2.1.1.5 Installation of the data R1.1.2 agent (optional)

Complete the following procedure to install the data R1.1.2 agent.

Step	Procedure

1. Go to the directory where the installation script is placed (on CD-ROM 3 of 4).

2. Type **./install_AMEM_bb** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**

1.- Before attempting to install the
application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC
Solaris 2 computers running Solaris 2.6 plus
security and Y2000 and packs 105490-07,
105568-13, 105210-19, 106040-12, 105633-21,
106409-01, 105181-15, 105669-07, 105284-25
patches recommended by SUN and 106255-01 patch.
```

```
3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it. It is
essential that these ports are not used by any
process on the SAME SUBNET DOMAIN.

4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/sr/bin",
"/usr/sbin" and "/uas/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.

******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation

Please, choose one or more Band mode separated
by blank


1 LuAMBB112     <BroadBand  R1.1.2 installation>

2 LuAMBB14      <BroadBand  R1.4   installation>


Enter selection [?,??,q]:
```

4. Type **1** and press **Return**

```
## Packages to install:  LuAMBB112
```

NE Data support for R1.1.2 installation

```
Processing package instance <LuAMBB112> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia BB Element Manager Release 1.7 for NE
release 112 (sparc) LuAMBB112_36.1.1


*********************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*********************************************


Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

AnyMedia EM R1.7 path=/opt/lucent/
AnyMediaEM_R1.7

Package <LuAM> Alarms LuAM_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuNER> NER LuNER_36_1.1 have been found
in /opt/lucent/AnyMediaEM_R1.7

Package <LuNeED> NetEvenDist LuNeED_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSec> Security LuSec_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuShelf> ConbinedShelf LuShelf_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSysED> SystemEventDist LuSysED_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuTrap> SystemEventDist LuTrap_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuLUMRT> Lumos Build 3.0 run-time have
been found in /opt/lucent/LUMOS

OK, No previous package LuAMBB112 have been
found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

WARNING:
```

```
The / filesystem has 185076 free blocks. The
current installation requires 203168 blocks, which
includes a required 150 block buffer for open
deleted files. 18092 more blocks are needed.


Do you want to continue with the installation of
<LuAMBB112> [y,n,?]
```

5. Type **Y** and press **Return**

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuAMBB112> [y,n,?]
```

6. Type **Y** and press **Return**

```
Installing AnyMedia BB Element Manager Release
1.7 for NE release 112 as <LuAMBB112>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2

Object Store path set to LuOSRT:ObjectStore:
Release 5.1 Service Pack 3:5.1_SP2
Run-Time:/bin:/lib:osversion:


Creating data bases


You have the installation logfile in
/tmp/EM_Install_LuAMBB112.log
```

```
Installation of <LuAMBB112> was successful.


## The package < LuAMBB112> is not installed in
the system.

## Please try ../install_AMEM again and install
the package < LuAMBB112>.

## to complete the installation.
```

NOTE:
The last message is an error and can be ignored.

2.2.1.1.6 Installation of the data R1.4 agent (optional)

Complete the following procedure to install the data R1.4 agent.

Step	Procedure

1. Go to the directory where the installation script is placed (CD-ROM 3 of 4).

2. Type **./install_AMEM_bb** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**

1.- Before attempting to install the
application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC
Solaris 2 computers running Solaris 2.6 plus
security and Y2000 and packs 105490-07,
105568-13, 105210-19, 106040-12, 105633-21,
106409-01, 105181-15, 105669-07, 105284-25
patches recommended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
```

```
that clients can communicate with it. It is
essential that these ports are not used by any
process on the SAME SUBNET DOMAIN.

4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/sr/bin",
"/usr/sbin" and "/uas/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.

******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation

Please, choose one or more Band mode separated
by blank


1 LuAMBB112     <BroadBand  R1.1.2 installation>

2 LuAMBB14      <BroadBand  R1.4   installation>


Enter selection [?,??,q]:
```

4. Type **2** and press **Return**

```
## Packages to install:  LuAMBB14
```

NE Data support for R1.4 installation

```
Processing package instance <LuAMBB14> from
</homelocal/tmp/lucent/AnyMediaEMR1.7/homelo-
cal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia BB Element Manager Release 1.7 (sparc)
LuAMBB14_36.1.1
```

```
*********************************************
 * AnyMedia Element Manager                  *
 * (c) 1999-Lucent Technologies              *
*********************************************

Package <LuSysAdm> SystemAdmin LuSysAdm_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

AnyMedia EM R1.7 path=/opt/lucent/
AnyMediaEM_R1.7

Package <LuAM> Alarms LuAM_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuNER> NER LuNER_36_1.1 have been found
in /opt/lucent/AnyMediaEM_R1.7

Package <LuNeED> NetEvenDist LuNeED_36_1.1 have
been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSec> Security LuSec_36_1.1 have been
found in /opt/lucent/AnyMediaEM_R1.7

Package <LuShelf> ConbinedShelf LuShelf_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuSysED> SystemEventDist LuSysED_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuTrap> SystemEventDist LuTrap_36_1.1
have been found in /opt/lucent/AnyMediaEM_R1.7

Package <LuLUMRT> Lumos Build 3.0 run-time have
been found in /opt/lucent/LUMOS

OK, No previous package LuAMBB14 have been
found.

Using </> as the package base directory.

## Processing package information.

## Processing system information.

 2 package pathnames are already properly
 installed.

## Verifying disk space requirements.


WARNING:

The / filesystem has 185076 free blocks. The
current installation requires 203474 blocks, which
includes a required 150 block buffer for open
deleted files. 18398 more blocks are needed.
```

```
Do you want to continue with the installation of
<LuAMBB14> [y,n,?] y
```

5. Type **Y** and press **Return**

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuAMBB14> [y,n,?]
```

6. Type **Y** and press **Return**

```
Installing AnyMedia BB Element Manager Release
1.7 as <LuAMBB14>


## Installing part 1 of 1.

<files list>
.............

[ verifying class <common> ]

## Executing postinstall script.

Package <LuOSRT> ObjectStore 5.1_SP2 Run-Time
have been found in /opt/lucent/OS51_SP2


Creating data bases


You have the installation logfile in
/tmp/EM_Install_LuAMBB14.log


Installation of <LuAMBB14> was successful.


## The package < LuAMBB14> is not installed in
the system.
```

```
## Please try ../install_AMEM again and install
the package < LuAMBB14>.

## to complete the installation.
```

NOTE:
The last message is an error and can be ignored.

2.2.1.2 Client side installation

Complete the following procedure to install the *AnyMedia* client side.

Step	Procedure

1. Go to the directory where the installation script is placed (DC-ROM 1 of 4).

2. Type **./install_AMEM_gen** and press **Return**.

```
AnyMedia EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved

**Pre-requisites**

1.- Before attempting to install the
application, please,read the readme.txt file.

2.- AnyMedia EM R1,7 runs on SUN SPARC
Solaris 2 computers running Solaris 2.6 plus
security and Y2000 and packs 105490-07,
105568-13, 105210-19, 106040-12, 105633-21,
106409-01, 105181-15, 105669-07, 105284-25
patches recommended by SUN and 106255-01 patch.

3.- TCP ports:
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it. It is
essential that these ports are not used by any
process on the SAME SUBNET DOMAIN.
```

```
4.- The install_AMEM script runs on K-shell
<ksh> environment.

5.- At least the system environment variable
PATH MUST include the paths "/sr/bin",
"/usr/sbin" and "/uas/ucb" (for instance,
"export PATH=$PATH:/usr/bin/:/usr/sbin:/usr/ucb").

6.- The time zone MUST be the same for the Any
Media Client <GUI>, LUMOS and Network Element.
This parameter is needed for installing the Any
Media Client.

******************

Do you like to continue [y,n,?,q]
```

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

```
AnyMedia NB EM R1,7 installation
CopyRight (c) 2000 Lucent Technologies, Inc.
All Rights Reserved.


Please, choose the installation mode
1 ADM  <Administration package installation>
2 GUI <Client package installation>
Enter selection [?,??,q]:
```

4. Type **2** and press **Return**

Java 1.2.2 -05 runtime installation

```
Packages to be installed: LuJRERT, LuOXWRT,
LuNETSCP, LuGUI30
Processing package instance <LuJRERT> from
</homelocal/tmp/lucent/AnyMediaEMR1.7
JRE 1.2.2-05 for AnyMedia EM R1.7
(sparc-solaris) 1.2.2-05
OK, No previous package LuJRERT have been found.
Applications to install:
1 --> jre version 1.2.2_05
2 --> symantec classes
3 --> report pro classes
```

```
4 --> all
5 --> exit
Selection:
```

5. Type **4** and press **Return**.

```
Here is a list of your partitions and the free
space in each of them:

Filesystem                    kbytes   used     avail    capacity  Mounted on

/dev/dsk/c0t0d0s0             143927   36997    92538    29%       /
/dev/dsk/c0t0d0s4             625262   401583   167406   71%       /usr
/dev/dsk/c0t0d0s3             96455    11928    74882    14%       /var
/dev/dsk/c0t0d0s6             6591133  3366955  3158267  52%       /homelocal
/dev/dsk/c0t0d0s5             240399   8597     207763   4%        /var/cache
swap                          1194560  8600     1185960  1%        /tmp
masstc1:/export1/bld/2/bldr17 51014048 44384096 6289872  88%       /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048 44384096 6289872  88%       /home/syi_pl

Enter install directory [/opt/lucent/
JDK_1.2.2_05][?,q]
```

6. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Select owner and group for package files.
NBR  USER:GROUP
  1 halt:other
  2 root:other
  3 smtp:root
  4 ver1:staff
Enter selection [?,??,q]:
```

7. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected
Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
```

```
## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.

This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package.

Do you want to continue with the installation
of <LuJRERT> [y,n,?]
```

8. Type **y** and press **Return**.

```
Installing JRE 1.2.2-05 for AnyMedia EM R1.7 as
<LuJRERT>

## Installing part 1 of 1.

<files list>

.............

[ verifying class <jre> ]

/opt/lucent/JDK_1.2.2_05/symantec/symbeans.jar

[ verifying class <symantec> ]

## Executing postinstall script.


 You have the installation logfile in
/tmp/EM_Install_LuJRERT.log


Installation of <LuJRERT> was successful.
```

OrbixWeb 3.1 installation

```
Processing package instance <LuOXWRT> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


OrbixWeb 3.1 Runtime for AnyMedia EM R1.7
(sparc-solaris) Version 3.1 Run-Time


Installing Version 3.1 Run-Time.
OK, No previous package LuOXWRT have been found.


Here is a list of your partitions and the free
space in each of them:
```

```
Filesystem                    kbytes    used      avail     capacity  Mounted on

/dev/dsk/c0t0d0s0             143927    36997     92538     29%       /
/dev/dsk/c0t0d0s4             625262    401583    167406    71%       /usr
/dev/dsk/c0t0d0s3             96455     11974     74836     14%       /var
/dev/dsk/c0t0d0s6             6591133   3401428   3123794   53%       /homelocal
/dev/dsk/c0t0d0s5             240399    8597      207763    4%        /var/cache
swap                          1194528   8608      1185920   1%        /tmp
masstc1:/export1/bld/2/bldr17 51014048  44384096  6289872   88%       /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048  44384096  6289872   88%       /home/syi_pl

Enter install directory [/opt/lucent/
OrbixWeb3.1] [?,q]
```

9. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Package <LuJRERT> jre 1.2.2-05 have been found
in /opt/lucent/JDK_1.2.2_05

Checking your DNS domain name...

The DNS domain name found was: es.lucent.com

What is your DNS domain name
[default: es.lucent.com]  [?,q]
```

10. Type your DNS domain name and press **Return** or press **Return** to accept the default name.

```
Enter the NS hostname? [masc216] [?,q]
```

11. Type the AEM server hostname and press **Return** or accept the default hostname by pressing **Return** only.

```
Wait....

Do you agree with NS hostname <masc216>
IP address:<IP address>] [y,n,?,q]:
```

12. Type **y** and press **Return** if the IP adress is correct.

```
Select owner and group for package files.
NBR  USER:GROUP
  1 halt:other
  2 root:other
  3 smtp:root
  4 ver1:staff
Enter selection [?,??,q]:
```

13. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected
Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.
This package contains scripts which will be
executed with super-user permission during the
process of installing this package.
Do you want to continue with the installation
of <LuOXWRT> [y,n,?]
```

14. Type **y** and press **Return**.

```
Installing OrbixWeb 3.1 Runtime for AnyMedia
EM R1.7 as <LuOXWRT>
## Installing part 1 of 1.
<files list>
.............
[ verifying class <none> ]
## Executing postinstall script.
You have the installation logfile in
/tmp/EM_Install_LuOXWRT.log

Installation of <LuOXWRT> was successful.
```

Netscape 4.6 installation

```
Processing package instance <LuNETSCP> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


Netscape Navigator 4.6 (Stand Alone) for
AnyMedia EM R1.7 (sparc-solaris) Version 4.6

OK, No previous package LuNETSCP have been found.


Here is a list of your partitions and the free
space in each of them:

Filesystem                    kbytes   used     avail    capacity Mounted on
/dev/dsk/c0t0d0s0             143927   36997    92538    29%      /
/dev/dsk/c0t0d0s4             625262   401583   167406   71%      /usr
/dev/dsk/c0t0d0s3             96455    12119    74691    14%      /var
/dev/dsk/c0t0d0s6             6591133  3405788  3119434  53%      /homelocal
/dev/dsk/c0t0d0s5             240399   8597     207763   4%       /var/cache
swap                          1194208  8616     1185592  1%       /tmp
masstc1:/export1/bld/2/bldr17 51014048 44384096 6289872  88%      /home/bldr17
masstc1:/export1/bld/2/syi_pl 51014048 44384096 6289872  88%      /home/syi_pl


Enter install directory
[/opt/lucent/Netscape][?,q]
```

15. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Select owner and group for package files.

NBR  USER:GROUP

  1 halt:other

  2 root:other

  3 smtp:root

  4 ver1:staff

Enter selection [?,??,q]:
```

16. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected

Using </> as the package base directory.

## Processing package information.

## Processing system information.
```

```
## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package."

Do you want to continue with the installation
of <LuNETSCP> [y,n,?]"
```

17. Type **y** and press **Return**.

```
Installing Netscape Navigator 4.6 (Stand
Alone) for AnyMedia EM R1.7 as <LuNETSCP>

## Installing part 1 of 1.

<files list>

.............

[ verifying class <none> ]

## Executing postinstall script.


You have the installation logfile in

/tmp/EM_Install_LuNETSCP.log


Installation of <LuNETSCP> was successful.
```

GUI installation

```
Processing package instance <LuGUI30> from
</homelocal/tmp/lucent/AnyMediaEMR1.7>


AnyMedia Element Manager Release 1.7 (Client)
(sparc) LuGUI30_36_1.1


*******************************************
 * AnyMedia Element Manager *
 * (c) 1999-Lucent Technologies *
*******************************************
OK, No previous package LuGUI30 have been found.


Where should AnyMediaEM GUI be installed?
[/opt/lucent/AnyMediaE/opt/lucent/
AnyMediaEM_R1.7/GUI30] [?,q]
```

18. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
Package <LuOXWRT> OrbixWeb Version 3.1 Run-Time
have been found in /opt/lucent/OrbixWeb3.1
Package <LuJRERT> jre 1.2.2-05 have been found
in /opt/lucent/JDK_1.2.2_05
Package <LuNETSCP> Netscape Version 4.6 have
been found in /opt/lucent/Netscape


Select owner and group for package files.
NBR  USER:GROUP
  1 halt:other
  2 root:other
  3 smtp:root
  4 ver1:staff
Enter selection [?,??,q]:
```

19. Type **4** and press **Return**.

```
User: ver1 and Group: staff, have been selected


What is the AnyMediaEM Server Host? [masc216] [?,q]
```

20. Type the host name where the *AnyMedia* AEM servers were installed and press **Return** or press **Return** to select the default name (masc216).

```
Wait....


Login for CutThrough functionallity? [?,q]
```

21. Type a valid login (e.g. ver1) and press **Return**.

```
Password for CutThrough functionallity?  [?,q]
```

22. Type a valid password (e.g. newuser1) and press **Return**.

```
The name of the location where the EM is working
is needed for printing facility.


What is the name of the location?  [?,q]
```

The location name will appear in the document header of the printing facility.

23. Type your AEM location name (e.g. Tres Cantos Lab) and press **Return**.

```
Code for the representation of names of
languages
Refer to ISO 639:1988 (E/F) for more information
1  da     Danish
2  de     German
3  fr     French
4  it     Italian
5  zh     Chinese
6  es     Spanish
7  en     English


Enter selection [?,??,q]: 7
```

24. Type your language code and press **Return**.

```
Code for the representation of names of
countries
```

```
Refer to ISO 3166 for more information
1  DK     DENMARK
2  DE     GERMANY
3  FR     FRANCE
4  IT     ITALY
5  CN     CHINA
6  ES     SPAIN
7  GB     UNITED KINGDOM
8  US     UNITED STATES

Enter selection [?,??,q]: 8
```

25. Type your country code and press **Return**.

```
Code for the representation of names of Time
Zones
1  GMT     (0)    Greenwich Mean Time
2  ECT     (1)    European Central Time
3  EET     (2)    Eastern European Time
4  ART     (2)    (Arabic) Egypt Standard Time
5  EAT     (3)    Eastern African Time
6  MET     (3.5)  Middle East Time
7  NET     (4)    Near East Time
8  PLT     (5)    Pakistan Lahore Time
9  IST     (5.5)  India Standard Time
10  BST     (6)    Bangladesh Standard Time

... 21 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop
display:^D
Enter selection [?,??,q]: 2
```

26. Type the desired time zone and press **Return**.

NOTE:
The time zone **must** be the same for the *AnyMedia* Client (GUI), LUMOS, Network Element and OS.

```
Using </> as the package base directory.

## Processing package information.

## Processing system information.

## Verifying disk space requirements.

## Checking for conflicts with packages already
installed.

## Checking for setuid/setgid programs.


This package contains scripts which will be
executed with super-user permission during the
process of installing this package.


Do you want to continue with the installation of
<LuGUI30> [y,n,?] y
```

27. Type **y** and press **Return**.

```
Installing AnyMedia Element Manager Release 1.7
(Client) as <LuGUI30>

## Installing part 1 of 1.

<files list>

.............

[ verifying class <channels_30> ]

## Executing postinstall script.

**********************************************

* Execute ". AnyMediaEM_GUI.sh" to set the
environment *

 **********************************************

You have the installation logfile in
/tmp/EM_Install_LuGUI30.log


Installation of <LuGUI30> was successful.


Installation of AnyMedia EM R1.7 was successful
<GUI side installation>
```

2.2.1.3 Post-install actions

2.2.1.3.1 AEM server

To be able to start-up the server it is necessary previously to execute the following script:

. <AnyMedia_path>/cfg/AnyMediaEM.sh

This would set all the necessary environment variables. It is recommended to include this line in the user .profile or to create an alias to facilitate the use.

2.2.2 Installing individual packages

The installation script **install_AMEM_*** can be used to install individual packages and will take care of the installation dependencies (that is, if a needed package is not installed previously it will not allow to continue until you install it). If the package is already installed on the target system, the following actions must be done:

- the package must be de-installed previously (refer to “Remove AnyMedia package installations” on page 77 for more information about packages de-installation)
- in order not to affect the rest of the installed packages, the package must be re-installed in the same directory as the previous one.

Installation dependencies are not the same than functional dependencies. In order to the AEM R1.7 to work at least all the obligatory packages should be installed (third parties and common packages for the server and full client installation for the client).

System responses and inputs for this type of installation and for a full installation are similar. Only the following differences could be found:

- When an installation starts, the package checks if a previous installation of the package already exists in the system. If no previous package is found, the following message will appear:

  “OK, No previous package <Package_Name> have been found.”

NOTE:
Refer to “Type 1 and press Return” on page 9 to see this response.

If one of the following messages appears, the installation will stop without changes on the system:

- The following message appears if there is a previous package in the system that was completely installed and has the same version

  “Previous completely installed package <Package_Name> version: <Package_Version> have been found. And it is the same to the new one you want to install:<Package_Version>.”

- The following message appears if there is a previous package in the system that was partially installed and has the same version

  “Previous partially installed package <Package_Name> version: <Package_Version> have been found. And it is the same to the new one you want to install:<Package_Version>. But it is partially installed. Better to use pkgrm <Package_Version>and installed it again.”

- The following message appears if there is a previous package in the system that was (partially or completed) installed and has different version

  “Current administration requires that a unique instance of the <Package_Name> package be cre ated. However, the maximun number of instances of the package which may be supported at one time on the same system has already been met. No changes were made to the system”

After this step, the installation looks for its packages dependencies. If a needed package is found the following message will appear:

“Package <Package_Name> <Application_Name> <Application_Version> have been found in <Application_Path>”

NOTE:
Refer to “Type y and press Return” on page 14 to see this response.

If the package is not found, the installation will prompt about its installation path in order to check this path and the correct application version:

"<Package_Name> needs <Application_Name> <Application_Version> to be installed previ ously. If it isn’t, Answer ’q’ to next question and install the package <Package_Name> otherwise provide the paths required.

What is the base path of <Required_Package_Name> <Package_verision> [?,q]?"

When an input is provided the installation checks the path and the version of the application. If the path is invalid the following message will appear:

“ERROR: Pathname does not exist.”

If the version is invalid one of the following messages could appear:

“Package <Required_Package_Name> have been found but INSTALL_PATH is not defined"

“Package <Required_Package_Name> have been found but with version: <Package_Version> not valid for <Package_Name>"

In both cases, the installation will prompt again for the required package.

- Also, the path where the Orbix.cfg file is located is requested in the OrbixNames, OrbixTalk and *AnyMedia* Servers packages installation, after the request for the installation path of the OrbixMT -the file will be modified by both installations- :

  "Where is Orbix.cfg file located [Orbix_path/cfg] [?, ??, q]?"

- Finally, after the ObjectStore installation the user must execute the **`osconfig server`** command, to configure the ObjectStore daemon.

2.2.3 Cancel installation

There are two ways to cancel the installation, as follows:

- internal cancellation: when the **`install_AMEM_*`** or **`pkgadd`** command detect through information files or installation scripts that something is invalid.
- external cancellation: if the administrator kill the process (kill -9 or Ctrl+C).

In both cases, the `system` informs about if files have been installed on the system. In this case, the administrator must use the **`pkgrm`** command to remove the installation.

2.2.4 Remove *AnyMedia* package installations

In order to remove any *AnyMedia* package installations, the administrator must execute the script **`remove_ANY`**. This script works exactly the same way than the installation one and allows to remove full or partial installations and individual packages also. It will ask confirmation for every package to be removed.

When a package is removed, all files installed by it or created during the *AnyMedia* operation, such as data bases and temporal data files, are erased in the target system.

2.2.5 PC-GUI client installation

This type of installation uses the **`install_AMEM.bat`** script. This script and all necessary files are included on Disk 4 of 4:

- readme.txt
- licence.txt
- install_AMEM.bat
- anymediaemr17.zip
- jre-1_2_2_005-win-i
- cc32d473.

Please read the readme.txt file first and then follow the given instructions.

NOTE:
In order to establish a communication it is necessary that the PC users and the server user are the same (with the same login).

Procedure

PC-GUI R1.7 is distributed on a compressed file named anymediaemr17.zip. This section contains instructions for installing the software once this file is in your system.

1. Change to the appropriate directory on the CD-ROM.

2. Install jre by double click on jre-1_2_2_005-win-i (recommended path for jre is C:\jdk1.2.2) and if netscape 4.7 is not already installed double click on cc32d473

3. Start installation script: double click on install_AMEM.bat

4. Select the extract button and indicate the directory where the system should be installed.

   This instruction generates five directories:

   - *classes*
   - *configuration*
   - *HelpFiles*
   - *Libraries*
   - *icons*.

OrbixWeb properties

Under *configuration* directory OrbixWeb.properties file should be updated with the name of the host, its IP address and the address. With the following format:

OrbixWeb.IT_NS_HOSTNAME=NameOfYourServerMachine
OrbixWeb.IT_NS_IP_ADDR=IP.address.of.your.ServerMachine
*
*
OrbixWeb.IT_LOCAL_HOSTNAME=IP.address.of.this.PC

If name of the PC where installation is taking part is not known by the server then update OrbixWeb.IT_IORS_USE_DNS=false.

AEM.users file

On the AEM.users file include the logging and password of the users that will used the PC client. The AEM.users contains the mappings of logging to host names. Each entry should be kept on an individual line. The name of the user should be placed in the first column followed by the corresponding encrypted password obtained by ypcat command on server side.
The user name and password should end with a colon. For example:

syi_snni:aZv4lkMOlVyD6:

After installation indicate the where PC-GUI had been installed in the file Enviroment_Varialbes.bat in CURRENT_DIR entrance.

If java is installed in different directory that the recommended one indicate the path on the bat file Enviroment_Variables.bat in the variable JDK_PATH.

2.2.5.1 Customizing SystemPreferences.ini

Please modify the SystemPreferences.ini as follows:

- indicate the city or the location where the EM is working in the SITE variable.
- if the cut-through is going to be used please indicated password and logging to connect *Anymedia* in variables PASSTELNET and LOGTELNET.
- indicate the netscape location in the variable HELP_BROWSER and the location of the help on HELP_URL.

The SystemPreferences.ini variables are described in Appendix B.

System management

3

Contents

3.1 Overview 3-1

3.2 System access 3-2

3.2.1 Login to operation system 3-2

3.2.2 Logout from operation system 3-3

3.2.3 AEM access bar 3-4

3.2.4 Capacity 3-5

3.3 General information on keyboard and windows 3-5

3.3.1 Keyboard 3-5

3.3.2 Mouse 3-5

3.3.3 Different aspects of the cursor 3-6

3.3.4 Basics on windows 3-6

3.3.5 Window menu 3-9

3.3.6 Menu bar 3-10

3.3.7 Cursor menu 3-10

3.3.8 Workspace manager 3-11

3.3.9 Workspace menu 3-11

3.3.10 Controls in AEM windows 3-12

3.4 System administration 3-16

3.4.1 General 3-16

3.4.1.1 Introduction and definitions 3-16

3.4.1.2 Start up, shutdown and recovery 3-17

3.4.1.3 Scaling 3-18

3.4.1.4 Load balancing 3-18

3.4.2 Start-up/shutdown of server applications via command line 3-18

3.4.3 System administration window 3-19

3.4.3.1 Menus in the System Administration window 3-19

3.4.3.2 Administration of packages 3-20

Contents

3.4.3.3 Administration of distributed module groups 3-22
3.4.3.4 Administration of module groups 3-24
3.4.4 View distributed module groups of a package 3-26
3.4.5 Editing distributed module groups 3-27
3.4.6 Editing module groups 3-28
3.4.7 Contents of packages and (distributed) module groups 3-31
3.5 Print out reports 3-34
3.5.1 Page Setup dialog 3-34
3.5.2 Print dialog 3-35
3.5.3 Preview Frame dialog 3-36
3.6 Backup and restore 3-38
3.6.1 Basics on backups and AEM databases 3-38
3.6.2 Commands for backup, archive and restore 3-39
3.6.3 Backup, archive and restore procedures 3-41
3.6.3.1 Backup procedure 3-42
3.6.3.2 Archive procedure 3-42
3.6.3.3 Restore procedure 3-42
3.6.3.3.1 General 3-42
3.6.3.3.2 Full restoration procedure 3-42
3.6.3.3.3 Incremental restoration procedure 3-43
3.6.4 Examples for backup schedules 3-43
3.6.4.1 Daily cumulative, weekly cumulative backups 3-43
3.6.4.2 Daily cumulative, weekly incremental backups 3-44
3.6.4.3 Daily incremental, weekly cumulative backups 3-45
3.7 Log management 3-46
3.7.1 Different log types 3-46
3.7.2 Configuration of logs 3-46
3.7.3 Log Viewer window 3-47
3.8 Disaster recovery 3-53

System management

3

3.1 Overview

This chapter provides you with information about:

- accessing the *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7
- general handling of the workspace and AEM windows
- starting up and shutting down applications
- printing out reports from AEM windows
- backup and restore tasks
- basics on log management and how to use the Log Viewer
- disaster recovery.

3.2 System access

To access the *AnyMedia* Element Manager (AEM) application, you need to have an account in the underlying operating system, and this account has to be accepted as a user account of AEM. The user account has to be NIS (Network Information Name Service) based and the NIS can be provided by the *AnyMedia* Server or by another machine. AEM user accounts are managed by the administrator (cf. Chapter 4).

3.2.1 Login to operation system

This chapter describes how to log into the system.

System login

Complete the following procedure to log in:

Step	Procedure
1.	The system asks for your user name. Enter your user name and press **`Return`** or click ***OK***.
2.	The system asks for your password. Enter your password and press **`Return`** or click ***OK***.

Login correct

If the login was correct, the workspace is displayed.

Login incorrect

If the login was incorrect, a warning message appears ("`Login incorrect; please try again`."). Confirm the message by pressing **`Return`** or clicking ***OK*** and repeat the login procedure.

Start AEM

If the AnyMedia EM was not yet started an administrator has to do this (cf. Chapter 3.4.2, page 3-18) before the AEM access bar can be started.

Start AEM access bar

To start the AEM access bar (cf. Figure 3-1, page 3-3) after a correct login, type in a terminal window, which you can open via the workspace manager (cf. Chapter 3.3.8, page 3-11):

```
cd <GUI base path>/GUI/
GUI_Main &
```

A splash screen is displayed and then the AEM access bar is shown.

Figure 3-1 Workspace with AEM access bar

3.2.2 Logout from operation system

This chapter describes how to log out from the system. You can log out manually or be logged out automatically after a certain time of mouse and keyboard inactivity. The automatic logout feature is provided by the operation system.

System logout

Complete the following procedure to log out manually:

Step	Procedure
1.	Close the AEM access bar window.
2.	Click on the **Exit** symbol in the workspace manager or select ***Log out...*** in the workspace menu.
3.	A message box pops up. Press **`Return`** or click ***OK*** to confirm the logout. Press ***Cancel*** not to log out.

After a logout the login screen is displayed again.

NOTE:
During the client installation (cf. 2.2.1.2, page 2-63) a cron process is installed. This cron automatically kills the GUI processes every night due security reason. The execution time of the cron can be changed by the administrator only.

3.2.3 AEM access bar

The AEM access bar allows access to all AEM applications and offers an alarm indication as well as a help feature.

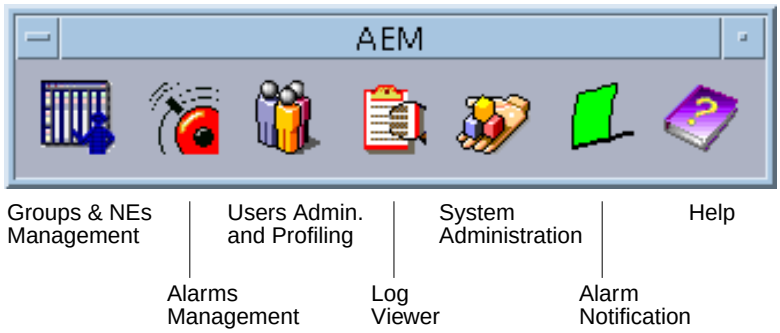


Figure 3-2 AEM access bar

Start access bar

To start the access bar see "Start AEM Access Bar" in Chapter 3.2.1.

Functions

The access bar provides access to the following applications:

- Groups & NEs management (cf. Chapter 5)
- Alarms Management (cf. Chapter 7)
- Users Administration and Profiling (cf. Chapter 4)
- Log Management (cf. Chapter 3.7, page 3-46)
- System Administration (cf. Chapter 3.4, page 3-16)
- Alarm Notification
- Help.

Start applications

To start an application click on the respective icon.

Access control

If an icon of the access bar is grayed, you are not allowed to access this application or the application is not running. Whether access is granted or denied depends on your user group membership. The Help icon is always accessible.

Alarm notification

The Alarm Notification icon displays a flag. If new alarms are received the flag is raised and an audible signal is issued.
The alarm notification can be acknowledged (the flag goes down) by clicking on the icon.

Help icon

The Help icon provides access to the AEM online help. If you click on the Help icon the help index is displayed.

3.2.4 Capacity

For the recommended server and client platforms the AEM allows for a maximum of

- 30 simultaneous users
- 600 NEs to be managed.

3.3 General information on keyboard and windows

3.3.1 Keyboard

The keyboard offers special keys which are pressed individually or in combination with others to perform specific actions.

Special keys

The most important special keys are:

- **`Return`**, to confirm an entry or to start a new line when a text consisting of several lines is entered
- **`Esc`** = "Escape" to initiate an escape sequence, i.e. the keys pressed after pressing Esc are interpreted as an instruction and not as entered text
- **`Ctrl`** = "Control" to initiate a control sequence. **`Ctrl`** is always used in combination with one or several other keys and represents an instruction
- **`Alt`** = "Alternate" is pressed in combination with one or more other keys thereby assigning these keys another meaning
- **`Backspace`** or **`Del`** (= "Delete") to delete all characters to the left of the cursor.

Conventions

The keys on the keyboard are represented in the text in the following way: **`Ctrl`**, **`Backspace`**, **`A`**, **`B`**,...

Two or more of these keys connected by a hyphen ("-") indicate that they must be pressed simultaneously. **`Shift-Ctrl-A`**, for example, means that the "A" key must be typed while holding down **`Shift`** and **`Ctrl`**.

Keys that are separated by blanks only must be pressed one after the other. **`Esc A B`**, for example, means that **`Esc`** must be pressed first followed by **`A`** and then **`B`**.

3.3.2 Mouse

Conventions

When using the mouse, you will frequently find the following terms:

- **Click** or **Select**: Position the cursor on an object and press the left mouse button.
- **Double click**: Click the left mouse button twice in rapid succession.

- **Drag**: Move the mouse keeping the left mouse button pressed.

3.3.3 Different aspects of the cursor

The aspect of the cursor will vary to indicate the actions you may currently undertake using the mouse.

The following symbols show examples for possible cursor aspects:

The arrow up pointing to the left is used to select objects and to press buttons.

The "I" beam is used within a text field to indicate the position where text is to be inserted.

The "clock" cursor indicates that in the window where the cursor is positioned a process requiring a lot of processing time is running and no mouse or keyboard inputs are possible.

3.3.4 Basics on windows

The window which contains the **input focus** evaluates all keyboard and mouse inputs. The window containing the input focus is easy to distinguish from other windows opened on the screen by the different colour of its window frame.

Use the mouse to direct the input focus to a defined window. Click on a position within the window or place the cursor on the window.

The window shown in Figure 3-3, page 3-7 labels the different window controls which allow the user to change the aspect of the window on the screen and the process represented by the window.

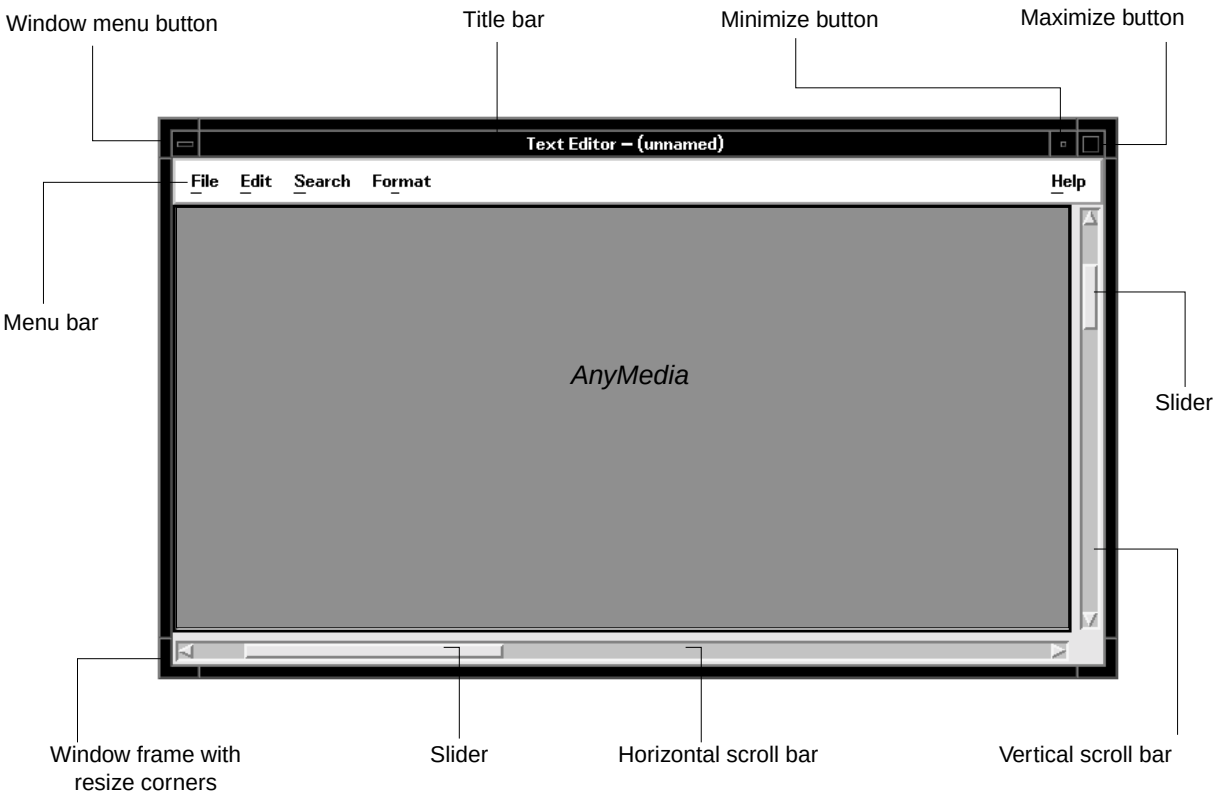


Figure 3-3 Specimen window and window controls

The individual window controls shown in Figure 3-3 are:

Figure 3-4 Controls in a window

Window part	Function
Window frame with resize corners	The frame delimits the window on the screen and its colour indicates whether this window contains the input focus. Drag the frame to shift and resize the window. By dragging the window corners, the window size may be modified to both limiting sides at the same time.
Title bar	The title bar informs you about the function of the window. Drag the title bar to shift the window on the screen.
Minimize button	If you click on the minimize button, the window will be displayed in its minimum size, i.e. it will appear as an icon on the screen, though the process represented by the window will continue running.

Figure 3-4 Controls in a window

Window part	Function
Horizontal scroll bar	Use the horizontal scroll bar and the slider to shift the visible window section to the left or right. ■ Small step to the left or right: Click on the left or right scroll bar arrow. ■ Page left or right: Click on the scroll bar to the left or right of the slider. ■ Shift window section: Use the mouse and drag the slider horizontally until the desired window section becomes visible.
Vertical scroll bar	Use the vertical scroll bar to shift the currently visible window section up or down: ■ Small step up or down: Click on the top or bottom scroll bar arrow. ■ Page up or down: Click on the scroll bar section above or below the slider. ■ Shift window section: Use the mouse and drag the slider up or down until the desired window section becomes visible.
Maximize button	Activate the maximize button by clicking on it to show the window at its maximum size, i.e. the window will occupy the whole screen. If you click again on the maximize button thus activated, the window will be restored to its original size.
Menu bar	The menu bar contains the menu names, each of them containing options related to the topic. These options may be selected to control the process running in this window (cf. Chapter 3.3.6, page 3-10)
Tool bar	The tool bar contains icons that provide quick access to most commonly used actions such as new, open, copy and print (cf. Chapter 5.3.2). Tooltips are also provided for these action icons.
Window menu button	Click this button to open the window menu (cf. Figure 3-5, page 3-9). Double click to exit the application.

3.3.5 Window menu

A window can be provided with a window menu. The window menu allows to alter the appearance of the window or to exit the application represented by the window.

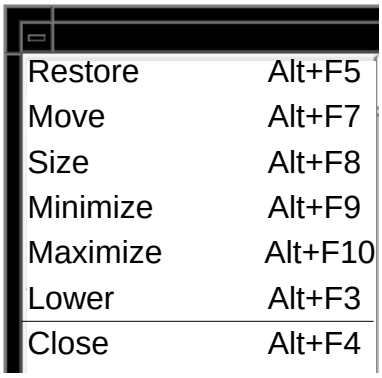


Figure 3-5 Window menu

To open the window menu shown in Figure 3-5, click on the window menu button or click with the right mouse button on the window frame.

The menu options in the window menu are listed in the following table.

Table 3-1 Window menu items and their function

Menu item	Function
Restore	A window currently being represented as an icon or in its maximum size is restored to its original size.
Move	Allows you to move the window interactively on the screen. The window frame will follow the mouse movements until you press the left mouse button.
Size	Allows interactive resizing of the window. Move the cursor appearing in the window to the window edge you wish to move. The edge will follow the mouse movements until you press the left mouse button.
Minimize	The window is shown as an icon.
Maximize	The window is shown in its maximum possible screen size.
Lower	If there are several overlapping windows, the currently active window is shifted to the bottom of the pile.
Close	This function will close the window and remove it from the user interface, exiting the application linked to the window.

3.3.6 Menu bar

Menu options

The menu bar of a window contains the menu names. Once you click on a menu it opens and a series of related menu options will be displayed under the menu name.

Conventions

Each option represents a function, which can be used to control the application running in the window. To call this function, click on the required option. A menu option is referred to in the text as: "***Menu name -> Menu option***" (e.g. in the menu below: ***Network View -> Maps***).

A grayed menu name or option cannot be selected.

Submenu conventions

Submenus are menus opening under a certain menu option and containing a number of related menu options. Some menu options are provided with a small arrow pointing to the right (>). These menu options have a submenu that will open as soon as you click on the menu option. A submenu option is referred to in the text as "***Menu name -> Menu option -> Submenu option***" (e.g. "***Network View -> Submaps -> Open/List...***"). A submenu option again may offer a submenu, then an appropriate number of "**->**" is added.

3.3.7 Cursor menu

Menu at the cursor position

Some objects in windows have a menu associated with them. This menu will pop up at the cursor position when the right mouse button is pressed. The cursor must not, however, be positioned on a menu bar or a window frame. The cursor menu is not available in all windows. The functions which can be executed using this cursor menu depend on the application of the respective window.

Select menu option

Proceed as follows to select a menu option from the cursor menu:

Step	Procedure
1.	Press the right mouse button.
2.	Move the cursor onto the desired menu option.
3.	Click the left or right mouse button to execute the menu option, or if you do not wish to execute a menu option, move the cursor away from the menu and click somewhere outside the menu.

3.3.8 Workspace manager

General

After logging in to the operation system (SUN Solaris), the workspace manager window is situated at the bottom of the screen offering a range of functions and information. A function is initiated by clicking the respective area of the workspace manager. In Figure 3-6 only an example of the workspace manager is given, as the entries are configurable.

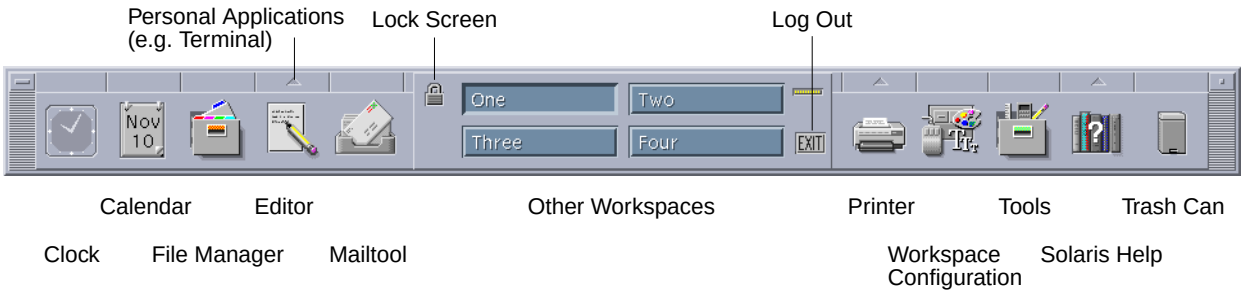


Figure 3-6 Workspace manager

Functions

For a detailed description of the offered functions, please refer to your *Solaris User's Guide* and *Solaris Common Desktop Environment User's Guide*.

3.3.9 Workspace menu

General

The workspace menu opens when you click with the right mouse button on the background of the workspace.

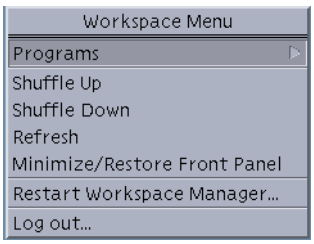


Figure 3-7 Workspace menu

Workspace menu functions

The workspace menu provides the functions listed in the following table:

Table 3-2 Menu items of the workspace menu

Menu item	Function
Programs	A submenu offering several programs.
Shuffle Up	If several windows on the screen are layered on top of one another, "Shuffle Up" brings the window from the very bottom to the top of the pile.
Shuffle Down	If several windows on the screen are layered on top of one another, "Shuffle Down" moves the window from the top of the pile to the very bottom.
Refresh	The contents of the windows on the screen and the screen backdrop are refreshed.
Minimize/Restore Front Panel	The workspace manager window is reduced to an icon or, if already iconized, restored to a window.
Restart Workspace Manager...	The workspace manager is restarted. Some of the changes to the user interface become valid only after the restart of the workspace manager. The restart must be acknowledged in a window.
Log out...	A logout from the system can be initiated.

3.3.10 Controls in AEM windows

Introduction

The windows of the AEM display certain controls (buttons, text fields, etc.). These controls are the same in all AEM windows and explained in this chapter.

Grayed controls

All controls within a window can be activated by clicking on them only if they are not grayed.

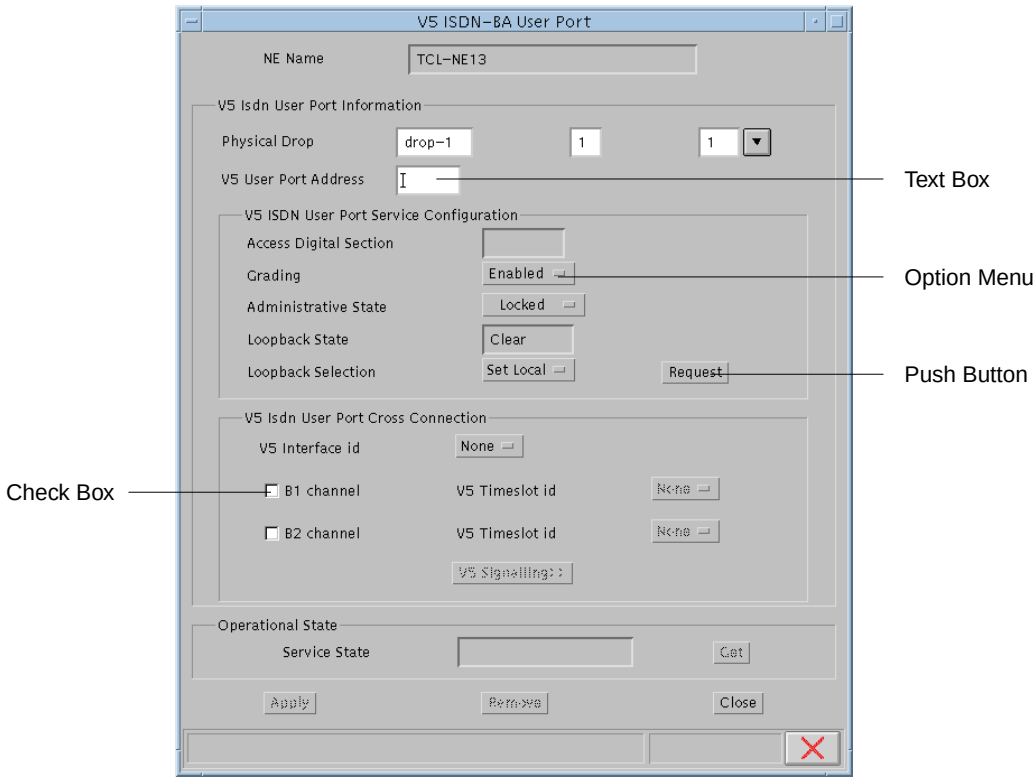


Figure 3-8 Example of an AEM window

Convention

The following font is used when a button is mentioned, e.g. ***Close***.

The following elements are used within windows:

- Push Button

  Each push button is provided with a designation describing its function. If you click on the push button, the function will be executed. If you click on a push button, the designation of which is followed by three dots (e.g.: ***Help...***), a window will open where you may set further parameters. Push buttons which alter their designation depending on context are also called **Label buttons**.

- Check Box

  Check boxes have the same function as an on/off switch. Each time you click on a check box, you will change its toggle status. A (pressed) check box containing a check mark means that the option at this position is selected.

- Radio Button

  Radio buttons have the same function as check boxes, with the difference that of various radio buttons of the same group, only one can be pressed at a time. As with a radio set, a set button will pop out when you press the next one in.

- Text Box

  Text boxes are used to input text via the keyboard.

- List Box

  A list box contains read-only data in list form. To scroll through a list you have to use the scroll bar at the right of the list box. If the list box allows the selection of entries, more than one entry can be selected by clicking on all desired entries once while the **`Ctrl`** key is pressed. If more entries are selected you can deselect a certain one by clicking on it again, while the **`Ctrl`** key is pressed. A range of consecutive entries can be selected simultaneously by clicking on the first entry of the range and then on the last while the **`Shift`** key is pressed.

- Drop-Down List Box

  A drop-down list box allows you to enter data by selecting an entry from a list that drops down after clicking on the triangle on the right of the box.

- Spin Box

  A spin box only allows a limited set of discrete ordered input values. You have to use the up and down arrows to increment or decrement the value.

- Tab

  A window can contain a register of several tabs. Clicking on a tab displays the corresponding contents in the window.

- Option Menu

  The option menu is used to set a certain option. Its designation will indicate the option currently set. Handling of the option menu is the same as for a menu.

Frequently used buttons

The table below provides an overview of buttons which have the same function in every AEM window:

Table 3-3 Function of frequently used buttons

Button	Function
OK	Applies changes; window is closed
Apply	Applies changes; window stays open for further edits
Cancel	Discards changes; running operation is cancelled; window is closed
Close	Discards changes; window is closed

Frequently used menus

The table below provides an overview of menus which have the same function in every AEM window:

Table 3-4 Function of frequently used menus

Menu	Function
File -> Print -> Print Table	Prints the contents of text lists in the window (cf. Chapter 3.5, page 3-34). Opens the Print Dialog window to set parameters for the print out.
File -> Print -> Print Window	Prints a screenshot of the whole window (cf. Chapter 3.5, page 3-34). Opens the Print Dialog window to set parameters for the print out.
File -> Print -> Preview	Shows how it will be printed if the "Print Table" option is used. Opens directly the Print Preview window.
File -> Exit	Closes all windows of this application.
Help -> On Window	Displays online help for this window.
Help -> Index	Displays online help index.

3.4 System administration

3.4.1 General

3.4.1.1 Introduction and definitions

Introduction

The AEM functionality is given by a set of processes of different types whose execution is controlled by the System Administration subsystem. In order to make possible the managing of all the processes running under the AEM, these will be grouped according to functionality, start up and recovery dependencies, into different levels. The lower one is the process level and the upper one is the AEM level. These levels are visible to the AEM administrators, who have managing capacities as start up, or recovery on some of them.

Definitions

The following table gives definitions of terms used in this chapter.

Table 3-5 Definitions

Term	Meaning
Server application	Set of server processes that perform a certain functionality. Server applications provide services for client applications.
Client application	Set of processes that use the services provided by the server applications (e.g. GUI and Northbound users)
Package	Logical parts of the AEM which provide specific functionality and can be started up, used and shutdown independently. There are three packages: ■ Narrowband package, for NB configuration and common functionality (alarms, logging and administration). ■ Broadband package, for BB configuration and common functionality (alarms, logging and administration). ■ Administration package, for common functionality (alarms, logging and administration).
Distributed Module Group (DMG)	Set of module groups of the same type distributed to provide load balancing and protection features.
Module Group (MG)	Set of modules with strong functional dependencies that influence the way they are installed and managed.
Module	Executable that provides a subset of services in the AEM and describes a way to handle its process instances.
Process	Entity of the AEM which has an (physical) operation system process associated.

3.4.1.2 Start up, shutdown and recovery

The AEM administrators can control the start up and shutdown at four levels: AEM level, package level, DMG level (only for optional DMGs) and process level.

AEM startup

The AEM can be started up in two ways:

- At boot time

  Root can configure the system to make the AEM start up at boot time, indicating the packages to be started up: NB, BB, Administration or any combination of them.

- Via command line

  The administrator can start AEM via command line, indicating the packages to be started up: NB, BB, Administration or any combination of them.

Package startup

Once the AEM is up, the administrator can start up from a GUI any non running package. For example, if only Administration package is started up on AEM start up, NB and BB packages can be started up later.

DMG startup

Those DMGs which are not mandatory for the AEM to be up can be as well started up and shutdown by the AEM administrators.

Process startup

The set of processes running under the AEM is also visible to the administrator, and he has the opportunity to start-up new processes up to a maximum number.

Process recovery

An AEM process is able to detect that its associated physical process is not working properly and in that case a recovery is automatically initiated on it. If the recovery fails, the AEM process enters OOS state. The user can request an on-demand recovery on any OOS process.

MG recovery

An MG is able to detect that a module under it is not working properly (its operational state is OOS) and in that case a recovery is automatically initiated on it. If the recovery fails, the MG enters OOS state. The user can request an on-demand recovery on any OOS MG.

AEM recovery

The AEM is able to detect that a package that is ON is not working properly (its operational state is OOS) and in that case a recovery is automatically initiated on it. If the recovery fails, the package remains OOS state. The user can request an on-demand AEM recovery. The AEM recovery command can be manually issued via the System Administration window (***AEM Recovery*** button). The manual AEM recovery request is ignored if none of the packages with administrative state "ON" has the operational state "out of service" (OOS).

Package, DMG and process shutdown

The AEM administrator can shutdown from the GUI packages, optional DMGs and processes.

AEM shutdown

An AEM shutdown terminates all server applications and all graphical user interfaces running at the moment. This command can be issued via the System Administration window (***AEM Shutdown*** button) or the command line (CLEAN).

3.4.1.3 Scaling

Several NEs and users

The number of users the AEM supports and the number of NEs being managed is flexible.

Several processes

The scaling feature is provided by the existence of several DMGs, several module groups in each DMG and several processes per module which allow the load distribution. The concept of several DMGs is used to distribute the set of NEs into different disjoint subsets of NEs. This process is automatically done by the AEM. However, the AEM R1.7 is not yet distributed among several hosts.

3.4.1.4 Load balancing

General

This functionality of the AEM is provided by different types of processes. Depending on the AEM workload, i.e. the activity due to user requests and NE-AEM communication level, less or more processing has to be done by each type of process.

Administrator tasks

In general, the number of manageable users and NEs makes it inefficient to start up a process of each type per user or NE. The load balancing mechanisms allows the AEM to distribute the current load among the running processes. The administrator can start up a reasonable number of processes to assure a certain service level according with the expected workload.

3.4.2 Start-up/shutdown of server applications via command line

The system can be configured at installation time to start-up the server applications automatically on every reboot. An administrator can start-up or shut-down server applications via a command line interface.

Commands for start-up and shut-down

The following table shows which commands have to be entered in a terminal window to start-up or shut-down server applications.

Table 3-6 Commands for start-up and shut-down

If you want to...	type in a terminal window...
start-up all AEM packages	**`SystemAdmin ALL`**
shut-down all AEM packages	**`SystemAdmin CLEAN`**
start-up the Administration AEM package	**`SystemAdmin Administration`**
start-up the NarrowBand AEM package	**`SystemAdmin NarrowBand`**
start-up the BroadBand AEM package	**`SystemAdmin BroadBand`**

SystemAdmin command

Any combination of the parameters **`Administration`**, **`NarrowBand`** and **`BroadBand`** of the **`SystemAdmin`** is possible.

3.4.3 System administration window

Overview

The System Administration window provides functions for AEM recovery and shutdown. Via three tabs (Packages, DMGs and MGs) in this window the packages as well as optional distributed module groups (DMGs) can be started and shutdown. The MGs can be recovered and processed be added to modules or removed from them as well as killed and recovered.

3.4.3.1 Menus in the System Administration window

Menus and functions

The following table provides an overview of the menus of the System Administration window and its functions.

Table 3-7 Menus and functions

Menu Item	Function
File -> Print -> Print Table	Print out all items displayed in the window
File -> Print -> Print Window	Print a screenshot of the whole window.
File -> Exit	Close the System Administration window and exit the application.
View -> Reload	Update the displayed values with the current ones. (The values in the System Administration window are not automatically updated.)
Help -> On Window	Display help for System Administration
Help -> Index	Display help index.

Actions in the System Administration window

The System Administration window displays different information and allows for certain actions depending on the selected tab (Packages, DMGs, MGs). The following table shows actions which do not depend on the selected tab.

Table 3-8 Basic actions in the System Administration window

If you want to...	then...	Result
initiate an AEM Shutdown	press ***AEM Shutdown*** and confirm the shutdown in the warning window which pops up.	The AEM is shut down.
initiate an AEM Recovery	press ***AEM Recovery***	The AEM recovery starts.
close the System Administration windows	select ***File -> Exit*** or press ***Close***.	The System Administration window is closed.

3.4.3.2 Administration of packages

Overview

The Package tab in the System Administration window allows for start up and shutdown of packages. For each displayed package the contained DMGs can be viewed.

Package information

The table in the Package tab displays the following information.

Table 3-9 Package information

Table entry	Meaning
Name	The internally assigned name of the package.
Administrative State	The administrative state of the package. Possible values: **ON**, if the package is up; **OFF** otherwise. The **Administrative State** is changed whenever a startup or shutdown command is issued.
Operational State	The operational state of the package, displayed when the **Administrative State** is **ON** only. Possible values: **IS**, if the package is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise.

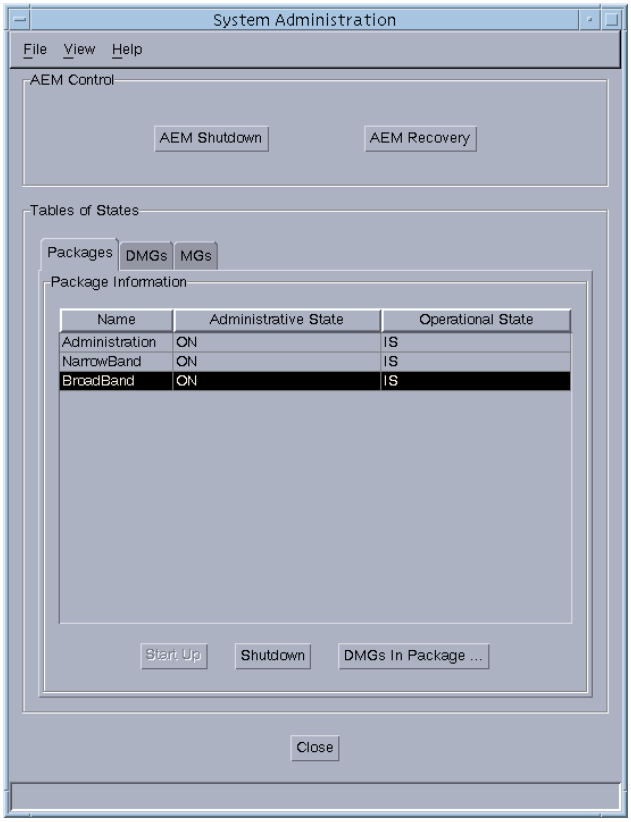


Figure 3-9 System Administration window (Packages)

Actions in Package tab

The following table lists all actions you can perform in the Package tab of the System Administration window.

Table 3-10 Actions for the administration of packages

If you want to...	then...	Result
start up a package	select the package in the table and press ***Start Up***. (The **Administrative State** of the package must be **OFF**.)	The selected package is started up.
shut down a package	select the package in the table, press ***Shutdown*** and confirm the shutdown in the warning window which pops up. (The **Administrative State** of the package must be **ON**.)	The selected package is shut down.
determine which DMGs are in the package	select the package and press ***DMGs in Package...***.	The DMGs in Package window is displayed (cf. Chapter 3.4.4).

3.4.3.3 Administration of distributed module groups

Overview

The distributed module groups (DMGs) tab in the System Administration window allows for start up and shutdown of optional DMGs. For each displayed DMG the contained MGs can be viewed and the DMG can be set up to be launched automatically when its package is started up.

DMGs information

The table in the DMGs tab displays the following information.

Table 3-11 DMGs information

Table entry	Meaning
Name	The internally assigned name of the DMG.
ID	The internally assigned ID of the DMG.
Type	The types of the MGs in this DMG.
Administrative State	The administrative state of the package. Possible values: **ON**, if the package is up; **OFF** otherwise. The **Administrative State** is changed whenever a startup or shutdown command is issued.
Operational State	The operational state of the package, displayed when the **Administrative State** is **ON** only. Possible values: **IS**, if the package is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise.

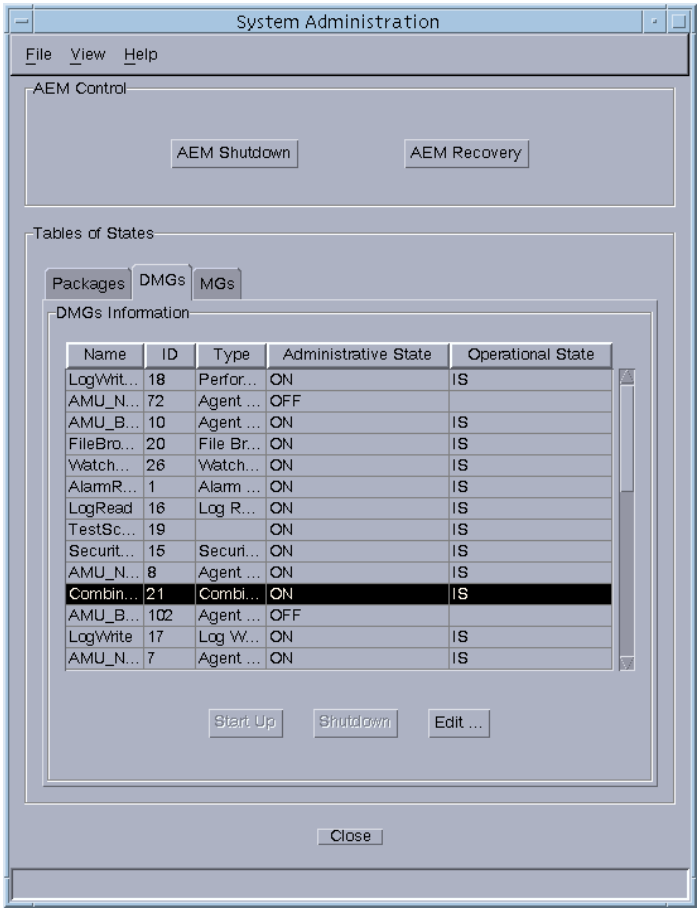


Figure 3-10 System Administration window (DMGs)

Actions in DMGs tab

The following table lists all actions you can perform in the DMGs tab of the System Administration window.

Table 3-12 Actions for the administration of DMGs

If you want to...	then...	Result
start up a DMG	select an optional DMG in the table and press ***Start Up***. (The **Administrative State** of the DMG must be **OFF**.)	The selected DMG is started up.
shut down a DMG	select an optional DMG in the table, press ***Shutdown*** and confirm the shut-down in the warning window which pops up. (The **Administrative State** of the package must be **ON**.)	The selected DMG is shut down.
edit a DMG	select the DMG and press ***Edit...***.	The Edit DMG window is displayed (cf. Chapter 3.4.5).

3.4.3.4 Administration of module groups

Overview The module groups (MGs) tab in the System Administration window allows for recovering an MG. Each displayed MG can be edited.

MG recovery A manual MG recovery should be made for an MG that is in the "out of service" (OOS) state. If a process of the MG is in the state "out of service" (OOS) and its automatic recovery fails the OOS state is propagated to the MG level. The workload of this MG could be distributed among the other MGs which then are overloaded but the OOS state would persist for the failed MG until a new recovery is instigated (manually or automatically).

MGs information The table in the MGs tab displays the following information.

Table 3-13 MGs information

Table entry	Meaning
Name	The internally assigned name of the MG.
ID	The internally assigned ID of the MG.
Type	The type of the MG.
Administrative State	The administrative state of the package. Possible values: **ON**, if the MG is up; **OFF** otherwise. The **Administrative State** is changed whenever a startup or shutdown command is issued.
Operational State	The operational state of the package, displayed when the **Administrative State** is **ON** only. Possible values: **IS**, if the package is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise.

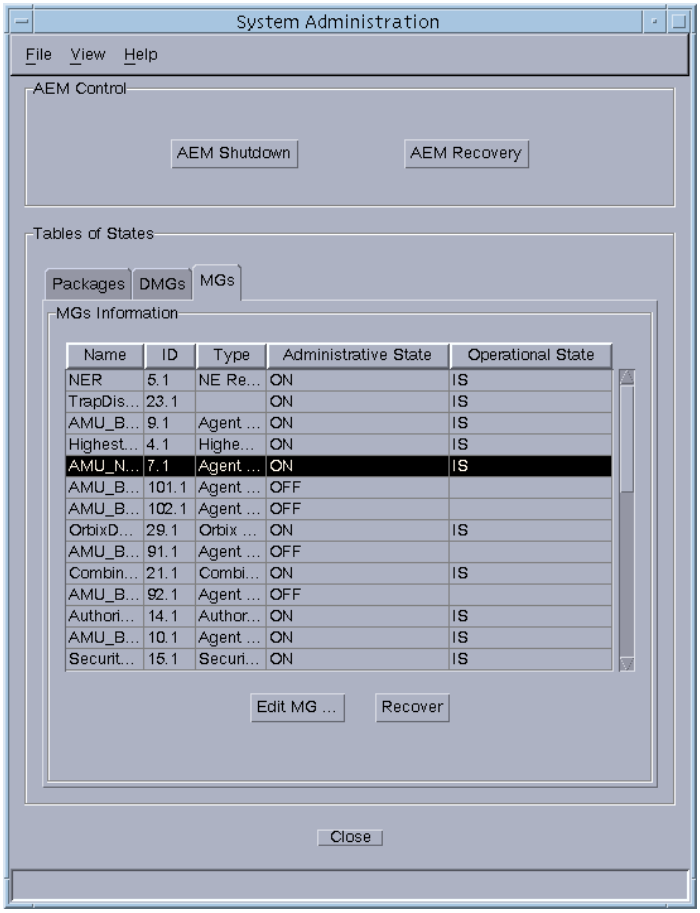


Figure 3-11 System Administration window (MGs)

Actions in MGs tab The following table lists all actions you can perform in the MGs tab of the System Administration window.

Table 3-14 Actions for the administration of MGs

If you want to...	then...	Result
recover an MG	select the MG in the table and press ***Recover***. (The **Administrative State** of the MG must be **ON**.)	The selected MG is recovered.
edit an MG	select the MG and press ***Edit MG...***.	The Edit MGs window is displayed (cf. Chapter 3.4.6).

3.4.4 View distributed module groups of a package

Overview

The DMGs in Package window allows for viewing the DMGs which make up packaged. Additional information for each DMG is displayed.

DMGs information

Next to **Package Name** the name of the selected package is displayed. The table under **DMGs in Package** displays the following information.

Table 3-15 DMGs Information

Table entry	Meaning
Name	The internally assigned name of the DMG.
ID	The internally assigned ID of the DMG.
Type	The types of the MGs in this DMG.
Administrative State	The administrative state of the DMG. Possible values: **ON**, if the DMG is up; **OFF** otherwise. The **Administrative State** is changed whenever a startup or shutdown command is issued.
Operational State	The operational state of the MG, displayed when the **Administrative State** is **ON** only. Possible values: **IS**, if the package is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise.

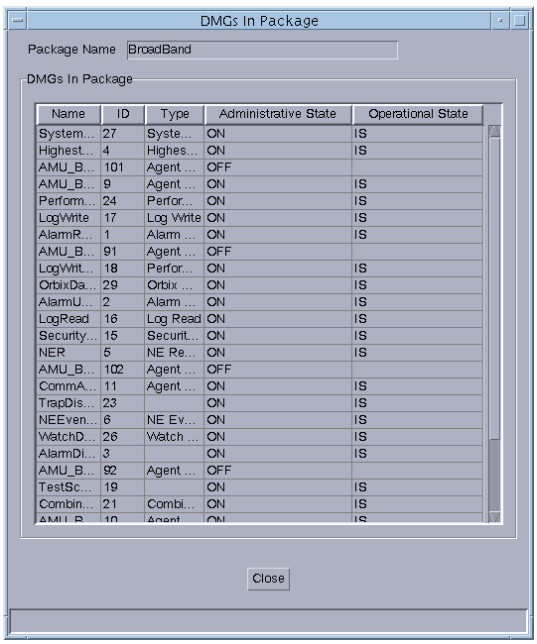


Figure 3-12 DMGs in Package window

3.4.5 Editing distributed module groups

Overview

The Edit DMG window allows for setting up whether a DMG is automatically launched on system start up. It also displays information for each module contained in the DMG.

Launch DMG on package startup

The ***Launch on Package Start Up*** option allows for the configuration of the system to specific needs. If some of the optional DMGs are not needed for a given network configuration they can be set not to be automatically started to save system resources.

DMGs information

Next to **DMG Name** the name of the selected DMG is displayed. The type of the MG is indicated next to **MG Type**. The table under **MGs in DMG** in the Edit DMG window displays the following information.

Table 3-16 DMG information

Table entry	Meaning
Name	The internally assigned name of the MG.
ID	The internally assigned ID of the MG. The ID of an MG contains the ID of the DMG it belongs to.
Administrative State	The administrative state of the MG. Possible values: **ON**, if the MG is up; **OFF** otherwise. The **Administrative State** is changed whenever a startup or shutdown command is issued.
Operational State	The operational state of the MG, displayed when the **Administrative State** is **ON** only. Possible values: **IS**, if the MG is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise.

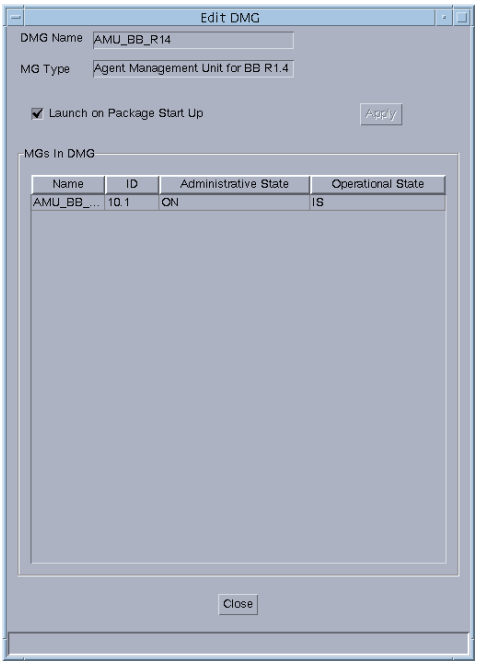


Figure 3-13 Edit DMG window

Actions The following table lists all actions which are possible in the Edit DMG window.

Table 3-17 Actions for editing a DMG

If you want to...	then...	Result
launch the DMG when the package starts up	select the check box ***Launch on Package Start Up*** and press ***Apply***.	Next time when any package containing the DMG is started the DMG is launched.
not launch the DMG when the package starts up	deselect the check box ***Launch on Package Start Up*** and press ***Apply***.	Next time the package is started the DMG is not launched.

3.4.6 Editing module groups

Overview The Edit MG window displays the modules contained in the module group. The processes which make up a module can be added or removed from the module. These processes can also be killed or recovered.

Add a process Each process in the module has a certain load level assigned. The load level is the number of clients that require service from this process. If the load level becomes higher it can be useful to add more processes to the module so that the load can be distributed among the processes.

Recover process

When a process has an operational state of "out of service" (OOS) it can be recovered.

Kill process

It is also possible to kill the physical process. The AEM process is not automatically removed.

Remove process

The AEM process (the object visible in the Edit MG window) can be removed from the module to shutdown the process from the AEM's viewpoint. In this case the physical process is automatically killed.

Module information

Next to **MG Name** the name of the selected MG is displayed. The table under **Modules in MG** displays the following information for all modules in the MG.

Table 3-18 Module information

Table entry	Meaning
ID	The internally assigned ID of the module.
Name	The internally assigned name of the module.
Type	The type of the module.
Operational State	The operational state of the module, displayed when the module is running only. Possible values: **IS**, if the module is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise. (The module is running only if the MG it belongs to has an Administrative State of ON.)

Processes in Module information

Next to **Module Name** the name of the selected module is displayed. How many processes are expected for this module is indicated next to **Expected Number of Processes**. This is the number of processed which are normally needed to manage the expected workload properly. The table under **Processes in Module** displays the following information for the selected module.

Table 3-19 Process information

Table entry	Meaning
ID	The internally assigned ID of the process.
PID	Process ID of this process.
Operational State	The operational state of the process. Possible values: **IS**, if the module is in service; **OOS**, if it is out of service; **TRANSITORY** otherwise. (The process is running only if the module it belongs to is running.)
Load Level	Number of clients which use this process (0 or more). The higher the number the higher the workload for the process.
Service Level	Depending on the service the process provides the value FULL or DEGRADED is displayed.

Table 3-19 Process information

Table entry	Meaning
Reason	Short description why the service is DEGRADED.

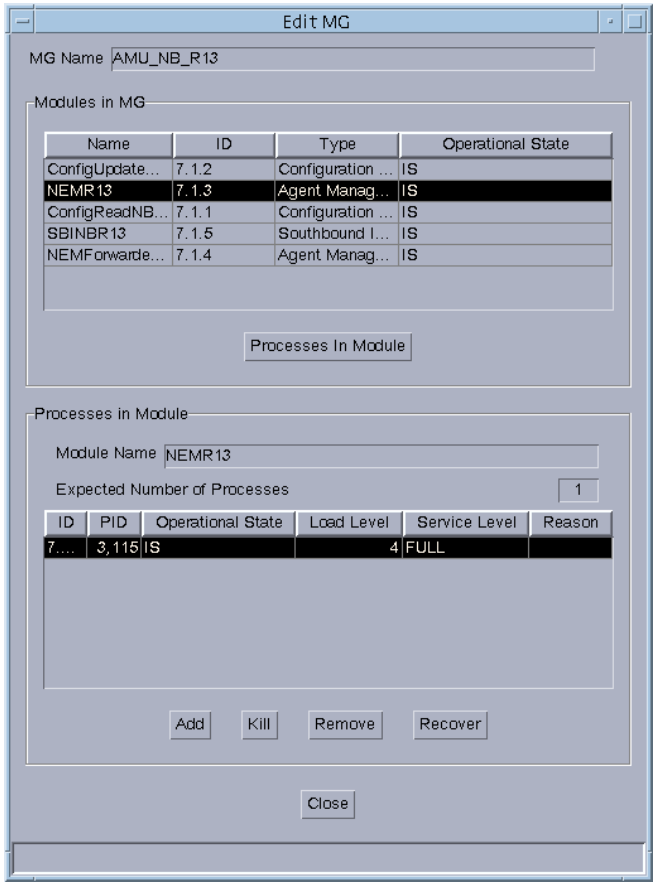


Figure 3-14 Edit MG window

Actions

The following table lists all actions which can be performed in the Edit MG window. Adding, killing, removing and recovering a process from a module is possible only after the "view or change the processes of a module" action was performed.

Table 3-20 Actions for editing an MG

If you want to...	then...	Result
view or change the processes of a module	select the module under **Modules in MG** and press ***Processes in Module***.	The process information for this module is displayed under **Processes in Module**. These processes can now be edited.
add a process to the module	press ***Add***. (The list of processes must not be empty.)	If the maximum number of processes which are allowed to run is reached the status bar displays a message that no more processes can be added otherwise a process is added to the module.
remove a process from the module	select the process which shall be removed and press ***Remove***. Confirm the removal in the warning window which opens.	If the minimum number of processes which have to run is reached the status bar displays a message that no more processes can be removed otherwise the process is removed from the AEM.
kill a process from the module	select the process which shall be killed and press ***Kill***. Confirm the killing in the warning window which opens.	The physical process is killed.
recover a process of the module	select the process which shall be recovered and press ***Recover***.	The process is recovered.

3.4.7 Contents of packages and (distributed) module groups

The following tables show which distributed module groups are contained in a certain package, also which module groups are in a certain distributed module group and finally which modules are contained in a certain module group.

Table 3-21 Module group types in a certain package

Package	Module Group Type
Administration, Narrowband, Broadband	AlarmRead
Administration, Narrowband, Broadband	AlarmUpdate
Administration, Narrowband, Broadband	AlarmDistributor
Administration, Narrowband, Broadband	HighestSeverityAlarmEventDistributor
Narrowband, Broadband	NER
Narrowband, Broadband	NEEventDistributor

Table 3-21 Module group types in a certain package

Package	Module Group Type
Narrowband	AMU_NB_R13
Narrowband	AMU_NB_R14
Broadband	AMU_BB_R112
Broadband	AMU_BB_R14
Narrowband, Broadband	CommAgentEventDistributor
Narrowband, Broadband	ConfigEventDistributor
Administration, Narrowband, Broadband	AccessPolicyManager
Administration, Narrowband, Broadband	AuthorizationService
Administration, Narrowband, Broadband	SecurityEventDistributor
Administration, Narrowband, Broadband	LogRead
Administration, Narrowband, Broadband	LogWrite
Broadband	LogWritePerf
Administration, Narrowband, Broadband	FileBrowser
Narrowband, Broadband	CombinedShelf
Broadband	TrapDispatcher
Broadband	PerformanceConfig
Administration, Narrowband, Broadband	SystemAdmin
Administration, Narrowband, Broadband	WatchDaemon
Administration, Narrowband, Broadband	SystemEventDistributor
Administration, Narrowband, Broadband	NamingService
Administration, Narrowband, Broadband	OrbixDaemon
Narrowband, Broadband	TestScheduler

Table 3-22 Module types in a certain module group type

Module Group Type	ModuleType
AlarmRead	AlarmRead
AlarmUpdate	AlarmUpdate, RemoveAlm
AlarmDistributor	AlarmDistributor, AlarmEventDistributor
HighestSeverityAlarmEventDis-tributor	HighestSeverityAlarmEventDistributor
NER	NER
NEEventDistributor	NEEventDistributor
AMU_NB_R13	ConfigReadNBR13, ConfigUpdateNBR13, NEMR13, NEMForwarderR13, SBINBR13

Table 3-22 Module types in a certain module group type

Module Group Type	ModuleType
AMU_NB_R14	ConfigReadNBR14, ConfigUpdateNBR14, NEMR14, NEMForwarderR14, SBINBR14
AMU_BB_R112	ConfigReadBBR112, ConfigUpdateBBR112, BAMR112, BAMForwarderR112, SBIBBR112, PerformanceCollectBBR112
AMU_BB_R14	ConfigReadBBR14, ConfigUpdateBBR14, BAMR14, BAMForwarderR14, SBIBBR14, PerformanceCollectBBR14
CommAgentEventDistributor	CommAgentEventDistributor
ConfigtEventDistributor	ConfigtEventDistributor
AccessPolicyManager	AccessPolicyManager
AuthorizationService	AuthorizationService
SecurityEventDistributor	SecurityEventDistributor
LogRead	LogRead
LogWrite	LogWrite
LogWritePerf	LogWritePerf
TestScheduler	TestScheduler
FileBrowser	FileBrowser
CombinedShelf	CombinedShelf
TrapDispatcher	TrapDispatcher
PerformanceConfig	PerformanceConfig
SystemAdmin	SystemAdmin
WatchDaemon	WatchDaemon
SystemEventDistributor	SystemEventDistributor
NamingService	NamingService
OrbixDaemon	OrbixDaemon

3.5 Print out reports

General

The Print windows (cf. Figure 3-15, Figure 3-16 and Figure 3-17) are used from any application within AEM to generate an output of data.

System details for printing

If the Unix command "**`lp`**" does not exist or is not configured on your system the AEM software will not be able to print. This is because the print-out is first converted to PostScript format and then piped to the Unix command "**`lp -d printer_name`**" where **`printer_name`** is replaced by the value entered in the **Printer** field of the "Print" dialog.

Print options depend on operation system

The available options in the print dialogue depend on the used operating system and may slightly differ from the descriptions below, e.g. under Solaris it is not possible to change the orientation of the printed page.

3.5.1 Page Setup dialog

Page Setup

The Page Setup dialog pops up after the selection of ***Print Window*** or ***Print Table*** in a window or ***Print*** in the Preview Frame dialog.

Figure 3-16 shows an example of the Page Setup dialog.

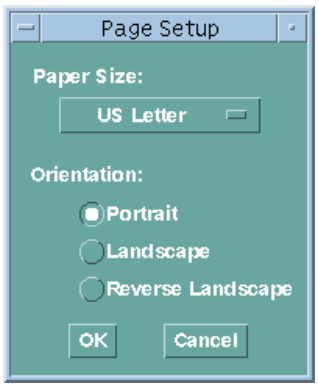


Figure 3-15 Page Setup dialog

Actions in Page Setup dialog

The following table provides an overview of the possible actions in the Page Setup dialog.

Table 3-23 Page Setup dialog actions

If you want to...	then...
select the paper size	use the option menu **Paper Size**.

Table 3-23 Page Setup dialog actions

If you want to...	then...
select the orientation of the print out	click one of the radio buttons below **Orientation**.
start printing and close the window	click on ***OK***. The Print dialog pops up.
close the print window without printing	click on ***Cancel***.

3.5.2 Print dialog

Print dialog

The Print dialog (cf. Figure 3-16) pops up after clicking on ***OK*** in the Page Setup dialog (cf. Figure 3-15, page 3-34).

Figure 3-16 shows an example of the Print dialog.

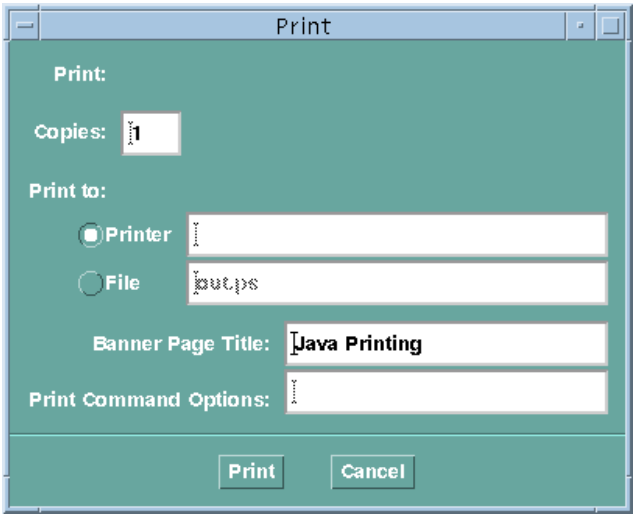


Figure 3-16 Print dialog

Actions in print dialog

The following table provides an overview of the possible actions which can be performed in the Print dialog.

Table 3-24 Print dialog actions

If you want to...	then...
print multiple copies	enter the number of copies in **Copies**.
print to a printer	enter the name of the printer in **Printer**.
print to a file	enter the name of the file in **File**.
have a title over the printed pages	enter the title in **Banner Page Title**.

Table 3-24 Print dialog actions

If you want to...	then...
apply UNIX print options	enter the options in **Print Command Options**.
start printing and close the window	click on ***Print***.
close the print window without printing	click on ***Cancel***.

3.5.3 Preview Frame dialog

Preview Frame

The Preview Frame dialog pops up after the selection of ***Preview*** in a window.

The following figure shows an example of the Preview Frame dialog.

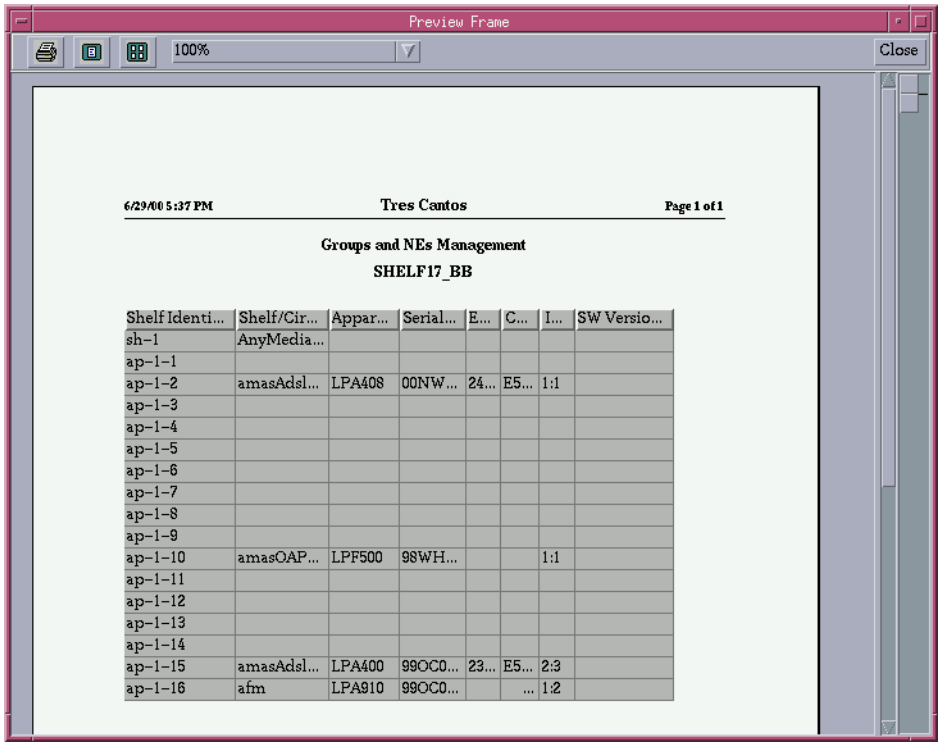


Figure 3-17 Preview Frame dialog

Actions in Preview Frame dialog

The following table provides an overview of the possible actions in the Preview Frame dialog.

Table 3-25 Preview Frame dialog actions

If you want to...	then...
print out	click on the ***printer icon***.
cancel the print out	click on ***Close***.
view a single page preview	click on the ***single page icon***.
view a multi page preview	click on the ***multi page icon***.
change the magnification of the preview	select another magnification with the ***% option menu***.
maximize/restore the preview window	click on the ***monitor icon***.

3.6 Backup and restore

The backup functions of the AEM allow you to copy AEM related file systems to removable media (such as tape) to safeguard against loss, damage, or corruption. The AEM system files and database backup allows to back up and restore system files and databases belonging to the installed applications (e.g. configuration files). Archiving is possible for AEM log files.

The restore functions allow you to restore file systems by copying reasonably current backup files from removable media to a working directory.

3.6.1 Basics on backups and AEM databases

Definitions

The following table gives definitions of terms used in this chapter.

Table 3-26 Definitions

Term	Meaning
Backup	process of copying file systems to removable media (such as tape) to safeguard against loss, damage, or corruption.
Archive	process of copying file systems to removable media (such as tape) and deleting the original files once they have been backed up.
Restore	process of copying backup files from removable media to a working directory, replacing the original files which could have been damaged.
Full Backup	copies a complete file system or directory
Incremental Backup	copies new files and files that have changed since a previous backup. The incremental backups are usually given a dump level which determines which files are backed up. A certain level incremental backup will save all the new or changed files since the last backup with a lower level.
On-line Backup	backups performed on user demand
Off-line Backup	backups performed automatically via any scheduling mechanisms, e.g. cron file

Backup types

There are three different backup types. The following list shows their differences and advantages:

- Full backup

  A full backup copies a complete file system or directory, e.g. all AEM data. This method requires large numbers of backup tapes that take a long time to write and takes also some time to retrieve individual files because the

backup drive has to move sequentially to the point on the tape where the file is located. On the other hand, using full backup makes it easier to retrieve small changes in file systems.

- Incremental backup

  An incremental backup only includes copies of new files and files that have changed since a previous backup. It is available for database files only. Requires less resources, but searching for a certain file on the incremental tapes can take time.

3.6.2 Commands for backup, archive and restore

Default locations of data for backups or archives

If a backup is done, the four AEM databases, the NVDS and the log files are copied to the backup medium. If an archive is made the log files are moved to the backup medium. The files from which a backup or archive is done are shown in the table below. The location of the files is relative to the main installation directory. (For changing default locations refer to Appendix B.)

Table 3-27 Default File Names for Backup and Archive

Database/File	File Name (Directory/File)	Backup Fails if File doesn't exist
Network registry database	NER/db	yes
System Administration database	SystemAdministrator/db	yes
NE management database	NEM/db	yes
Security database	Security/db	yes
Alarm database	AM/db	yes

Manual backup

The non-volatile data storage (NVDS) located at CM/nefiles/NVDS and the configuration files (*.cfg) are not backed-up by the AEM_backup command. A backup of these files can be done manually e. g. with the tar command.

System message

After each backup, archive or restore command a result message is displayed, which indicates whether the operation was successful or not. This message is displayed only if the command was entered on the command line.

Command syntax

In the following description of the commands, square brackets, e.g. **`[-c]`**, indicate optional parameters. The pipe symbol "|" indicates alternative options from which one has to be chosen, e.g. **`INC|FULL`**. All parameters not enclosed in brackets are mandatory. Each command is entered without enclosing parameters in brackets.

Backup files

Use the following command to make a backup of a database or directory. If you enter none of the optional parameters, a backup of all data necessary to restore the AEM will be done:

```
AEM_backup [-c] [-h] [-H] [-p backup_file_path] [-f backup_file_name]
[-t backup_type] [-l dump_level]
```

Parameter description:

-c Aborts a running backup operation.

-h, -H Display command syntax (**-h**) or additional help (**-H**).

-p *backup_file_path* The ***backup_file_path*** is the directory or device to back up. (Default: value of the variable **OAM.backup.backupDirectory**, which is set in the file **AnyMediaEM.cfg**.)

-f *backup_file_name* Location of the backup file. ***backup_file_name*** can be a local file or a locally mounted file (in case a local tape device is used ***backup_file_name*** specifies a "soft label"). (Default file names: EM_SYSBCK_yyyymmdd.fullbck for full backup EM_SYSBCK_yyyymmdd.incbck for incremental backup, with yyyy = year, mm = month, dd = day of the backup.)

-t *backup_type* Type of backup: incremental (**INC**) or full (**FULL**). (Default: FULL). This parameter is ignored if "**-l 0**" is used.

-l *dump_level* Specifies the backup level. Files modified since last backup at a lower level are copied, ***dump_level*** = 0...9. This parameter is ignored if "**-t FULL**" is used.

Restore files

Use the following command to restore a database or directory:

```
AEM_restore [-c] [-h] [-H] [-p backup_file_path]
-f backup_file_name
```

Parameter description:

-c Aborts a running restore operation.

-h, -H Display command syntax (**-h**) or additional help (**-H**).

-p *backup_file_path backup_file_path* is the directory or device to which the restored data should be written. (Default: value of the variable **OAM.backup.backupDirectory**, which is set in the file **AnyMediaEM.cfg**.)

-f *backup_file_name* Location of the backup file. ***backup_file_name*** can be a local file, a locally mounted file or a local tape device.

Archive files

Use the following command to archive log files. This function is primarily intended to archive the AEM log files. If you enter none of the optional parameters, the AEM log files will be archived.

```
AEM_archive [-c] [-h] [-H] [-p backup_file_path]
[-f backup_file_name]
```

Parameter description:

-c Aborts a running archive operation.

-h, -H Display command syntax (**-h**) or additional help (**-H**).

-p *backup_file_path* ***backup_file_path*** is the directory or device to archive. (Default: value of the variable **OAM.backup.archiveDirectory**, which is set in the file **AnyMediaEM.cfg**.)

-f *backup_file_name* Location of the backup file. ***backup_file_name*** can be a local file or a locally mounted file (in case of a local tape device is used ***backup_file_name*** specifies a "soft label"). (Default file name: EM_SYSARCH_yyyymmdd.arc, with yyyy = year, mm = month, dd = day of the archive.)

TAR command

The **`tar`** command is used in backup and restore scripts.

```
tar c|r [v] f tarfile file
tar x|t [v] f tarfile
```

Parameter description:

c Create a tar file. An already existing tar file is overwritten.

r Replace a tar file. An already existing tar file is not overwritten and the new information is appended at its end.

x Extract the data from the tar file.

t Display the table of contents of the tar file.

v The tar command verbosely displays what it does.

f *tarfile* ***tarfile*** is the name of the tar file.

file Name of the file, or a list of files separated by blanks which shall be added to the tar file. (Omitted for extract operations.)

3.6.3 Backup, archive and restore procedures

This section gives an overview of the steps necessary for a backup, archive or restore operation.

Prerequisite for backup, restore and archive

The backup, archive or restore commands require that some path system variables are properly set. This is done by the command **`AnyMediaEM.sh`** during the installation of AEM. If this command was not executed the backup, archive or restore commands will not work.

Different users

When different users perform backup, archive or restore operations the system will display a message asking whether temporary data which remained from the previous user should be deleted. If such a message is displayed you must confirm the deletion of these data.

3.6.3.1 Backup procedure

The backup operation needs no user interaction after the backup command was executed.

3.6.3.2 Archive procedure

The archive operation needs no user interaction after the archive command was executed.

3.6.3.3 Restore procedure

3.6.3.3.1 General

Default locations for restored data

When a backup is restored, all files are restored to their original location. When archives are restored they are copied into the directory **`restored`** (relative to the main installation directory).

Restore one of several backups from tape

When more than one backup is placed on a tape and a particular one shall be restored, the name of this backup must be known and the tape must be positioned at the beginning of this backup. The name can be determined by using the **`tar`** command. For example: **`tar tvf /dev/rmt/0mn`**. The positioning is done as described below.

Position tape

If you know the order of the backups on tape, you can position the tape at the beginning of the desired backup as follows: Rewind the tape (e.g with **`mt -f /dev/rmt/0m rewind`**) and issue a **`tar`** command (see example above) until the backup which comes before the one which shall be restored is displayed. If you do not know the order of the backups on the tape, it can be determined as follows: Rewind the tape and then repeatedly issue a **`tar`** command (see example above) until the backup to be restored is displayed while you note the order of the backups on tape. Then you can position the tape as shown above.

3.6.3.3.2 Full restoration procedure

When the restore command is executed the user must decide which image type should be restored. The restore script displays the following message:

```
Please enter the type of the image to be restored [backup/archive]
```

Type **`backup`** or **`archive`** and press **`Enter`**.

Copy of originals

Copies of the original databases are saved to allow for a cancellation of the operation. If such a copy could not be made the appropriate image can nevertheless be restored, but a warning is issued. For each database for which no copy could be made the following message is displayed:

```
Actual <DATABASE TYPE> is not present or ObjectStore copy operation failed.
The AnyMedia EM system state cannot be recovered if a cancellation is requested.
Do you want to continue? [y/n]
```

Type **`y`** and press **`Enter`** to continue with the restore procedure. If you type **`n`** the restore command stops with an error message, no data are restored and the sys-

tem will not work unless a correct restore is performed. When the original databases are present, the message above is not displayed.

Additional incremental backups

While the different databases are restored certain information is displayed on the screen. Then the restoration tool asks whether additional databases should be restored:

```
Do you wish to restore from any additional incremental backups? (yes/no):
```

Type **no** and press **Enter**.

After that the execution of the restore tool finishes and the restoration is complete.

3.6.3.3.3 Incremental restoration procedure

Before a certain incremental backup can be restored the previous full backups and possibly some previous incremental backups must be restored.

The procedure to restore an incremental backup is the same as the above described procedure for a full backup except for the last ("Additional Incremental Backups") step. In that step the restore tool asks for a confirmation that all needed full backups which are a prerequisite for the incremental backup are present. Answer this question affirmatively. After that the execution of the restore tool finishes and the restoration is complete.

3.6.4 Examples for backup schedules

Introduction

This section gives you some examples for typical backup schedules and explains the backup level.

Backup level

Crucial for the understanding of the backup schedules is understanding the backup level. The backup level is a number which is assigned by you to every backup you make. Each time you make a new backup only those files are put on the back-up media which were altered since the last backup with a lower backup level. A backup level "0" means a full backup.

3.6.4.1 Daily cumulative, weekly cumulative backups

This is the most commonly used backup schedule. It is recommended for most situations.

Schedule characteristics

This schedule has the following characteristics:

- Each weekday backup accumulates all files changed since the end of the previous week (or the initial level 0 backup).
- Each Friday's backup contains all files changed since the first level 0 backup. For the level 9 backups, the previous level 0 or level 5 is the closest backup at a lower level.
- Each Friday's backup contains all files changed during the month to that point.

Example

The following table shows the backup levels for each days backup. Once a month, a backup with backup level 0 must be performed.

Table 3-28 Backup levels of each backup

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		9	9	9	9	5
2nd week		9	9	9	9	5
3rd week		9	9	9	9	5
4th week		9	9	9	9	5

The following table shows how files accumulate in the backup for each weekday.

Table 3-29 Example for files in backup for two weeks

	Mon	Tue	Wed	Thu	Fri
1st week	ab	abc	abcd	abcde	abcdef
2nd week	g	gh	ghi	ghij	abcdefghijk

3.6.4.2 Daily cumulative, weekly incremental backups

Example

The following table shows the backup levels for each days backup. Once a month, a backup with backup level 0 must be performed.

Table 3-30 Backup levels of each backup

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		9	9	9	9	3
2nd week		9	9	9	9	4
3rd week		9	9	9	9	5
4th week		9	9	9	9	6

The following table shows how files accumulate in the backup for each weekday.

Table 3-31 Example for files in backup for two weeks

	Mon	Tue	Wed	Thu	Fri
1st week	ab	abc	abcd	abcde	abcdef
2nd week	g	gh	ghi	ghij	ghijk

3.6.4.3 Daily incremental, weekly cumulative backups

Example

The following table shows the backup levels for each days backup. Once a month a backup with backup level 0 must be done.

Table 3-32 Backup levels of each backup

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		3	4	5	6	2
2nd week		3	4	5	6	2
3rd week		3	4	5	6	2
4th week		3	4	5	6	2

The following table shows how files accumulate in the backup for each weekday.

Table 3-33 Examples for files in backup for two weeks

	Mon	Tue	Wed	Thu	Fri
1st week	ab	cd	ef	h	abcdefghi
2nd week	jk	lmn	o	p	jklmnopqr

3.7 Log management

The log management records information on events in the AEM. The logged events can be viewed with the Log Viewer.

3.7.1 Different log types

There are five log types within the Log Viewer:

- Actions

  It contains all the information on actions performed by users or the AEM and which imply changes in the AEM configuration, equipment (NE) configuration, service and subscriber configuration, access to the AEM, print reports and backup& restore. That means all operations triggered by the user or the AEM and all subsequent actions. Also the results of operations are logged in the actions log.

- System Internal Events

  It contains all internal events or actions which report unusual changes in the configuration and state of the AEM or indicate errors which occurred in the AEM.

- Autonomous Reports

  It contains all TCAs (Threshold Crossing Alert) from NB and BB and all actions performed in the NEs that imply changes in the AEM data base.

- Alarms

  It contains all alarms received from the platform (AEM), telephony agent and data agent.

- ADSL Performance
- ATM Performance
- Feeders Performance.

3.7.2 Configuration of logs

Log size

The following values can be configured (cf. Appendix B) for the log system by the administrator:

- Minimum number of days (incl. current day) in the log (default: 7 days)
- Maximum size of all logged data (default: 5 Mbyte per NE).

The maximum log size is configured per log type, and applies per NE (each NE can have stored logs of a type up to the maximum size configured for that log type).

Log grows too big

The logs are stored as separate files, one file holds one day of one log type. If the size of the logged data has reached the size limit and a new event to be logged

occurs, some of the already logged data has to be deleted. The oldest recorded day of one of the logs holding the largest number of days is always deleted.

Alarms

The log system issues an alarm if

- one of the logs is shortened to a number of days below the minimum number of days. (I.e. also, if a log is shortened that already holds fewer than the minimum number of days.) Alarm name: LOG_DEL_PART.
- the current day log is deleted. Alarm name: LOG_DEL_FULL.

Restore log files

When log files are restored (cf. Chapter 3.6, page 3-38), the log of the current day is not overwritten.

3.7.3 Log Viewer window

The logs can be viewed by means of the Log Viewer application. The logged entries in the Log Viewer cannot be edited.

Start Log Viewer

The Log Viewer is started-up by clicking on the log viewer icon in the access bar. After start-up the default log type is displayed, this value can be configured (default: "Actions").

Access permission

The log types which are visible to you depend on your user group. The following table shows the log types which the different user groups are allowed to see.

Table 3-34 Visibility of a log type for a certain user group

Log type	Visible for user group
Actions	Administrator, Maintenance
System Internal Events	Administrator, Maintenance
Autonomous Reports (this log type includes autonomous reports, alarms and performance of ADSL, ATM and Feeder)	Administrator, Maintenance, Monitoring

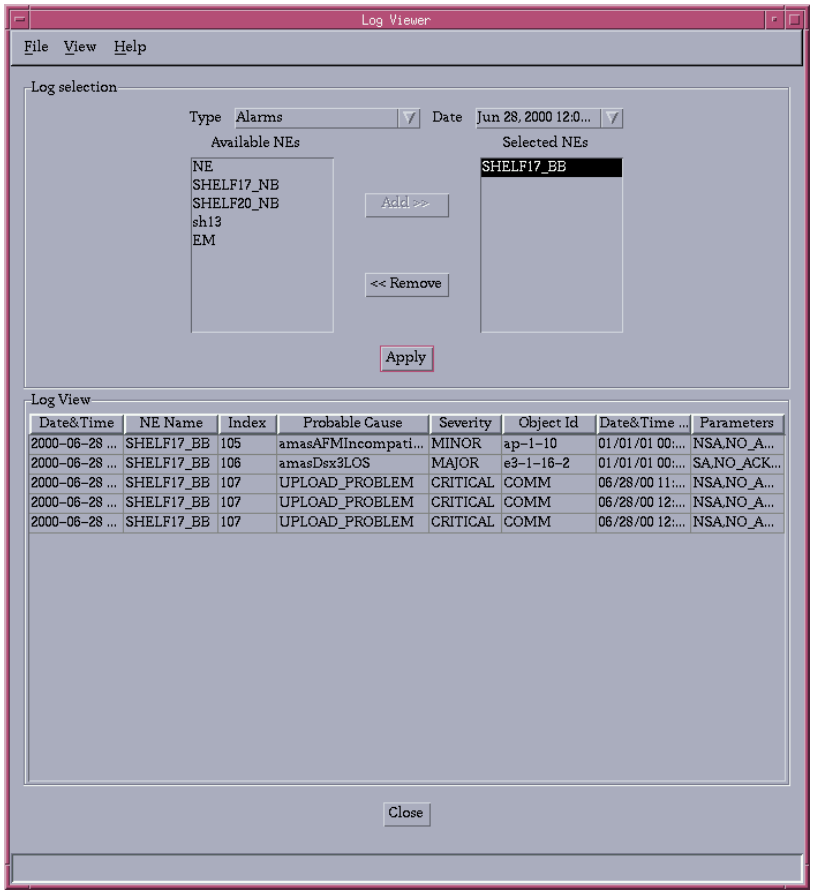


Figure 3-18 Log Viewer

Meaning of columns

The following table explains the meaning of the columns (in alphabetical order) in the Log Viewer table.

Table 3-35 Information displayed in the Log Viewer table

Column	Meaning
Conditions	The condition of a performed action, to indicate whether it is the request or the response. (E.g. START, END_SUCCESS, END_ERROR, CANCEL).
Date&Time	Date and time when the event was registered in the log file. Format: "yyyy-mm-dd hh:mm:ss"
Date&Time Last	Indicates the last severity change.
ES/PSES	Indicates the Errored Second data for a E3 or DS3 feeder (BB).
ES Up, ES Down	Indicates the "Errored Second" data (BB).

Table 3-35 Information displayed in the Log Viewer table

Column	Meaning
Event Type	The event which happened in the AEM.
Feeder Type	Indicates the feeder type (E3 or DS3).
HBER Up, HBER Down	Indicates the "High Bit Error Rate" data (BB).
Index	A sequence number for each different alarm reported to the AEM.
Interval	Interval which is used in the performance data. This value can be 15 minutes or one day (BB).
IP-Address	Indicates the IP-Address of the data agent (BB).
LOF	Indicates the "Loss of Frame" data (BB).
Login	The user name of the user performing an action or "EM"
LOS Up, LOS Down	Indicates the "Loss of Signal" data (BB).
Method	A string explaining the performed action.
NE Name	Indicates in *Autonomous Report*, *Performance Logs* and *Alarms* the NE in which the event has happened. "EM" is displayed if the log messages is related to the AEM.
Object Id	Unique identification of the object for which the log message has been sent.
Parameters	■ For Actions and System Internal Events Shows all parameters involved in the action. ■ For Autonomous Reports Shows all TL1 message parameters in the order they were received (for TL1 messages sent from NE) and the TCAs information from the data agent by SNMP trap. ■ For Alarms Shows the rest of the alarm parameters (except description).
Port Id	Indicates the Port Id where the performance data has been recollected (BB).
Probable Cause	A unique identification string for each alarm type shows the probable cause of the alarm.
RcvCells High, RcvCells Low	Indicates the number of cells received (BB), formatted into two 32 bits integers (high and low part of the counter).

Table 3-35 Information displayed in the Log Viewer table

Column	Meaning
RcvErroredCells High, RcvErroredCells Low	Indicates the number of wrong cells received (BB), formatted into two 32 bits integers (high and low part of the counter).
RFI	Indicates the "Remote Failure Indication" data (BB).
Severity	Severity of an alarm on the object for which the log message has been sent.
Shelf Id	Indicates the Shelf Id where the data agent is placed (BB).
Slot Id	Indicates the Slot Id where the performance data has been recollected (BB).
Time Stamp	Date and Time when a performance data was collected in the NE.
UAS	Indicates the "Unavailable Seconds".

Log types and displayed information

Depending on the chosen log type the table in the Log Viewer displays different information (more or less columns). The following table shows which information is displayed for which log type.

Table 3-36 Log types

Log Type	Contents
Actions	Date&Time, Login, Conditions, Object, Method, Parameters
ADSL Performance	Date&Time, NE Name, IP Address, Shelf Id, Slot Id, Port Id, Time Stamp, Interval, LOF, LOS Up, ES Up, HBER Up, RFI, LOS Down, ES Down, HBER Down, Parameters
Alarms	Date&Time, NE Name, Index, Probable Cause, Severity, Object Id, Date&Time Last, Parameters
ATM Performance	Date&Time, NE Name, IP Address, Time Stamp, RcvCells High, RcvCells Low, RcvErroredCells Up, RcvErroredCells Low, Parameters
Autonomous Reports	Date&Time, NE Name, Parameters
Feeders Performance	Date&Time, NE Name, IP Address, Shelf Id, Port Id, Time Stamp, Interval, Feeder Type, ES/PSES, UAS, Parameters
System Internal Events	Date&Time, Object, Event Type, Parameters

Menus and functions

The following table provides an overview of the menus of the Log Viewer and their functions.

Table 3-37 Menus and functions

Menu Item	Function
File -> New	Start up a new Log Viewer
File -> Print -> Print Table	Print out all logged items displayed in the table of the Log Viewer.
File -> Print -> Print Window	Print a screenshot of the whole window.
File -> Print -> Preview	Shows how it will be printed if the "Print Table" option is used. Opens directly the Print Preview window.
File -> Close	The selected Log Viewer window is closed. Other open Log Viewer windows stay open.
File -> Exit	Close all Log Viewer windows.
View -> Reload Log Data	Update the displayed Log Viewer table with newly logged items.
View -> Reload NE List	Update the NEs Selection list.
Help -> On Window	Display help for Log Viewer
Help -> Index	Display help index.

Actions

The following table lists all actions you can perform in the Log Viewer window.

Table 3-38 Actions in the Log Viewer window

If you want to...	then...	Result
display a certain log type of a specific date and NE	select the desired log type with the pull down control **Log Type,** select the date of interest with the pull down control **Date** and select the NE by using the ***Add >>*** button and press ***Apply***.	The log of the selected type and date of the desired NE is displayed in the Log Viewer table.
view different log types or dates simultaneously	start another Log Viewer with ***File -> New*** and set the desired **Type** or **Date**.	A new Log Viewer window displays the selected log type and date.
print displayed log	select ***File -> Print -> Print Table*** or ***File -> Print -> Print Window***.	The Log Viewer table or a screenshot of the window is printed out.
display updated log	select ***View -> Reload Log Data***	Newly logged entries are displayed.
display updated NEs Selection list	select ***View -> Reload NE List***	The NEs Selection list is updated.

Table 3-38 Actions in the Log Viewer window

If you want to...	then...	Result
sort the log	click on one of the column headers to sort the log according to the column entries alphabetically or by date and time. Click again to reverse the sort order.	The Log Viewer table is displayed sorted alphabetically or by date and time.
close one Log Viewer window	select ***File -> Close*** or press ***Close***	The selected Log Viewer window is closed.
close all Log Viewer windows	select ***File -> Exit***	All Log Viewer windows are closed.

3.8 Disaster recovery

The AEM software has built-in auto recovery features that will allow it to continue working after a problem except in the most critical situations (i.e. corrupted files, hardware failure...). In case of a disaster, the following steps should be performed by the system administrator to repair the AEM and minimize the data loss.

1. Repair/replace any hardware and OS components that may be damaged. Start the system and check that the workstations and network boot properly and the users are able to log into the system.
2. Check if the AEM (including all third-party software) remains installed on the machine. To list all the packages installed type:

   `pkginfo | grep 'application Lu'`
3. Remove all the listed packages using the **pkgrm** command (cf. Chapter 2.2.4, page 2-77).
4. Re-install the AEM software. The procedure is the same as for installing the software for the first time (cf. Chapter 2.2.1, page 2-7).

NOTE:
The packages must be re-installed in the same paths as the original installation, otherwise the data cannot be restored.

5. If any AEM variable was customized, remember to reset it (the installation sets all values to default). Start the AEM server and at least one client. All application windows (Users, Alarms, Configuration) should open but will show only the initial information.
6. Shut down the AEM. Restore the latest backup available (cf. Chapter 3.6, page 3-38). Re-start the AEM server and at least one client. Now the restored data shall be shown and the system will be back at the status prior to the latest backup.

The process between step 2 and step 6 should not take more than 4 hours. If the recovery is not successful call Lucent Technologies Technical Support.

A good backup policy is imperative in order to minimize the data loss (some examples can be found in Chapter 3.6.4, page 3-43).

User management

4

Contents

4.1 Introduction 4-1

4.2 User 4-3

4.2.1 Create user 4-3

4.2.2 Modify user 4-5

4.2.3 Delete user 4-7

4.3 Domains 4-8

4.3.1 Create domains 4-8

4.3.2 Modify domains 4-10

4.3.3 Delete domains 4-12

4.4 User groups 4-14

4.4.1 Create user groups 4-14

4.4.2 Modify user groups 4-19

4.4.3 Delete user groups 4-23

4.5 Controlled objects 4-25

4.5.1 Modify controlled objects 4-25

Contents

User management

4

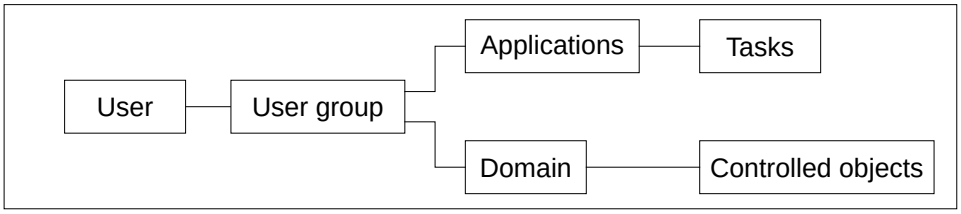
4.1 Introduction

This chapter describes the "User Administration and Profiling" application of the *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7. It allows to

- create/modify/delete users
- assign/unassign users to/from user groups
- create/modify/delete user groups
- assign/unassign user groups access to/from applications, tasks and domains
- create/modify/delete domains
- assign/unassign controlled objects to/from domains.

NOTE:
All actions can only be done by the AEM administrator!

The following figure shows the relation between user, user group, applications and tasks, domains and controlled objects.



The "User Administration and Profiling" application is started via the AEM access bar by clicking on the corresponding icon.

Figure 4-1 Access bar

4.2 User

4.2.1 Create user

Introduction

This chapter describes the process to add a new user to the system. Before adding a new user to the system, please pay attention to the following remarks:

- The AEM administrator must have a system login.
- The user must be created via OS.
- The AEM administrator should know the login ID of the user to be created and the group the user shall belong to.

Procedure

Complete the following procedure to add a new user:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up showing the *Users Table*.

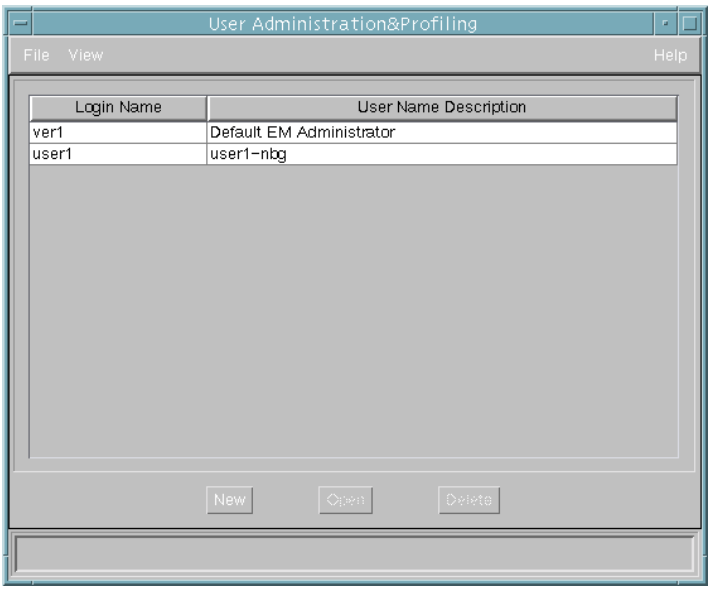


Figure 4-2 User Administration & Profiling window (Users table)

3. Click ***New***. The *User Profile* window pops up.

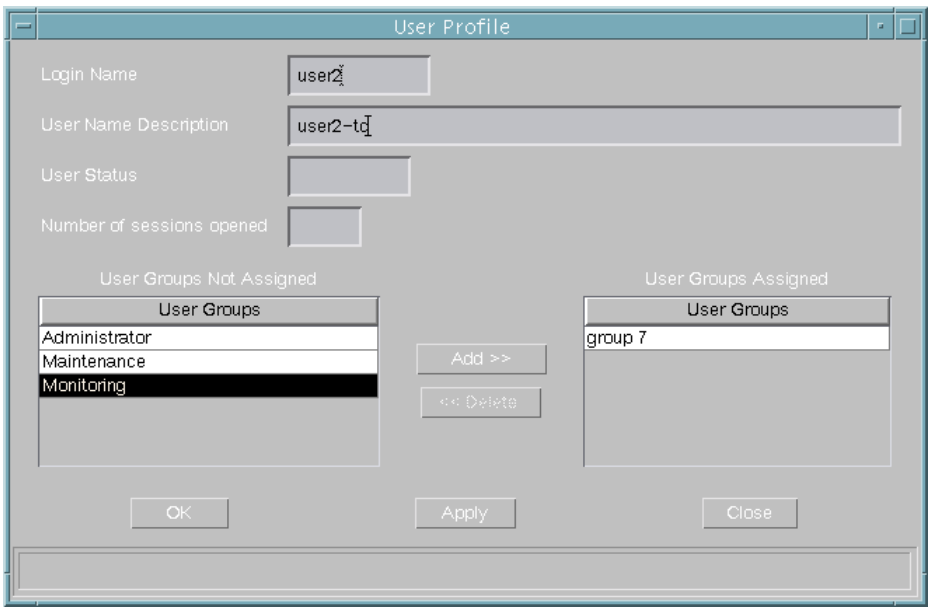


Figure 4-3 User Profile window

4. Enter a new login name in the **Login Name** field (this is mandatory - 3 to 12 characters) and extra information like last name, first name, email, etc. in the **User Name Description** field (this is optional - 0 to 60 characters). Any characters are allowed.

5. Select one or more user groups the user shall belong to in the **User Groups Not Assigned** field and click ***Add>>***.

NOTE:
To create user groups see Chapter 4.4.1, page 4-14.

6. Click ***OK*** or ***Apply*** to save the settings (the system ensures that the new user does not yet exist in the system). After clicking ***OK*** the window will be closed.
   If you want to reject the settings, click ***Close*** before ***OK*** or ***Apply***.

The other fields are described in Chapter 4.2.2, page 4-5.

4.2.2 Modify user

Introduction

This chapter describes the process to modify the information or profile of a user. Before modifying the information or profile of a user, please pay attention to the following remarks:

- To modify the information or profile of a user the AEM administrator must have a NIS based login.
- The AEM administrator is not able to change the system login information of a user, i.e. system login and password.

Procedure

Complete the following procedure to modify the information or profile of a user:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up showing the *Users Table*.

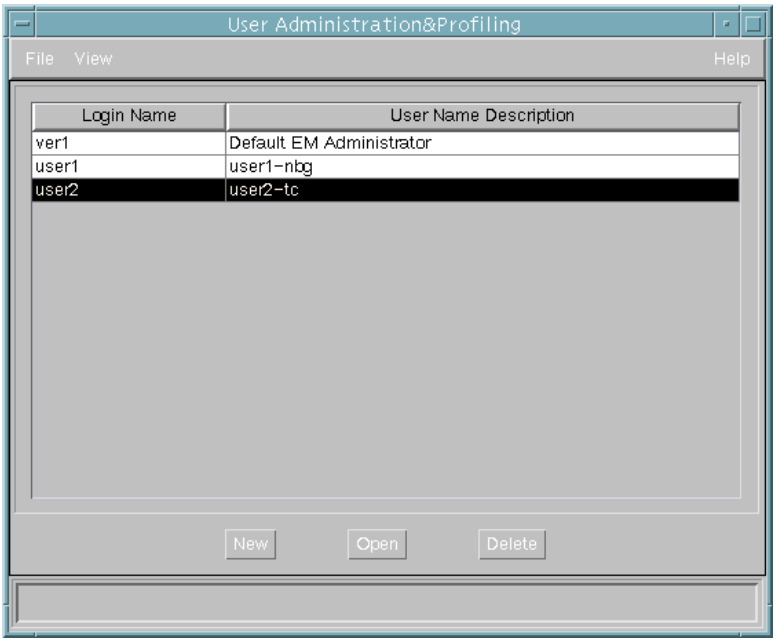


Figure 4-4 User Administration & Profiling window (Users Table)

3. Select one user of the **Login Name** field and click ***Open***.
The *User Profile* window pops up with the current information about the selected user.

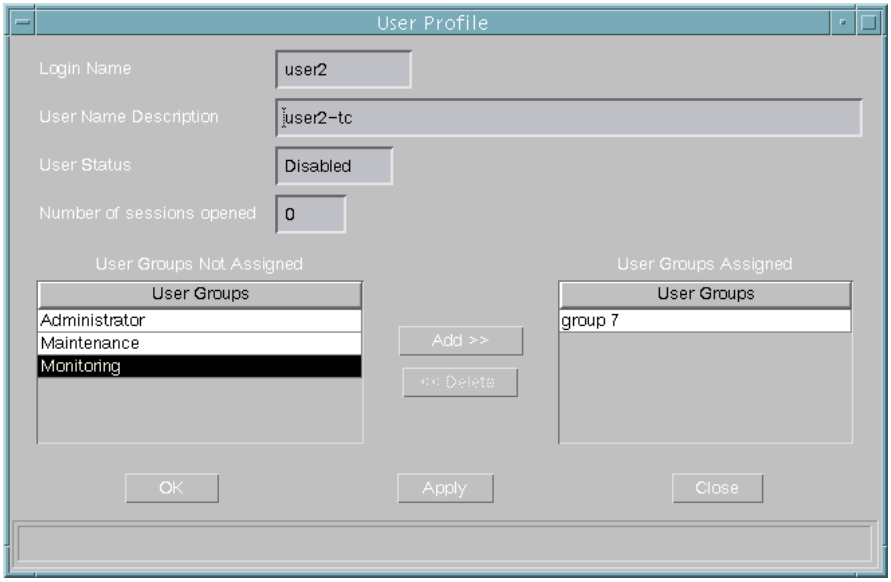


Figure 4-5 User Profile window

Change user name description

To change the user name description like last name, first name, email, etc., enter the new information in the **User Name Description** field (0 to 60 characters). Any characters are allowed.

Adding to user groups

To assign the selected user to further user groups, select one or more user groups in the **User Groups Not Assigned** field and click ***Add>>***.

NOTE:
To create user groups see Chapter 4.4.1, page 4-14.

Removing from user groups

To remove the selected user from user groups, select one or more user groups in the **User Groups Assigned** field and click ***<<Remove***.

Click ***OK*** or ***Apply*** to save the changes. After clicking ***OK*** the window will be closed. If you want to reject the changes, click ***Close*** before ***OK*** or ***Apply***.

Other fields (read-only)

The following fields are read-only fields to display user data:

Login Name:
Displays the label which identifies the user.

User Status:
Displays if the system login associated to this user is created (enabled) or deleted (disabled).

Number of sessions opened:
Displays the number of sessions opened into the AEM by the user.

4.2.3 Delete user

Introduction

This chapter describes the process to remove a user from the AEM. Before removing a user, please pay attention to the following remarks:

- To remove a user from the AEM the administrator must have a system login.
- When a user is deleted, all related information and profiles are removed from the system. This does not include the system login and any other system resources such as home directories or system files which are not managed by the AEM. Furthermore, the user is automatically deleted from the user groups it was included in.
- Before deleting any user assigned to the administrator user group, the AEM checks that this is not the last user assigned to the administrator user group. If this is the last one assigned, the deletion is rejected.

Procedure

Complete the following procedure to remove a user from the AEM:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up showing the *Users Table*.

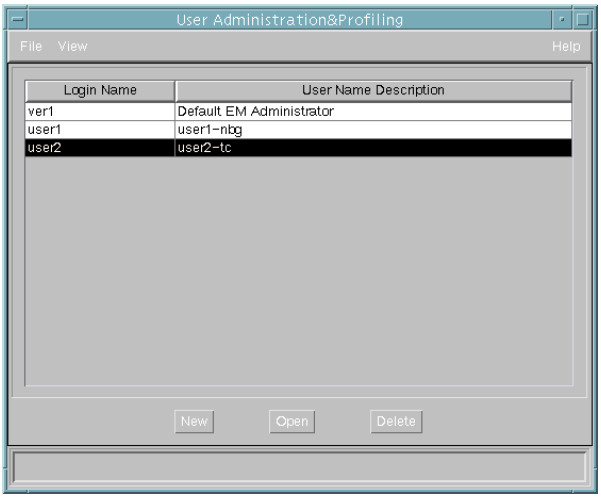


Figure 4-6 User Administration & Profiling window (Users Table)

3.	Select the user which shall be deleted in the **Login Name** field and click ***Delete***.
4.	Confirm your selection. The window will be closed.

4.3 Domains

4.3.1 Create domains

Introduction

This chapter describes the process to create a new domain. Before creating a new domain, please pay attention to the following remarks:

- The AEM administrator must have a system login.
- The controlled objects are defined as sets of managed NEs.
- Only "EM" and "NE" controlled object types are supported.

NOTE:
An "EM" object is generated by default with "Type: EM" and "Value: AnyMedia" which cannot be deleted.

Procedure

Complete the following procedure to create a new domain:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> Domains*** via menu bar. The *Domains Table* appears.

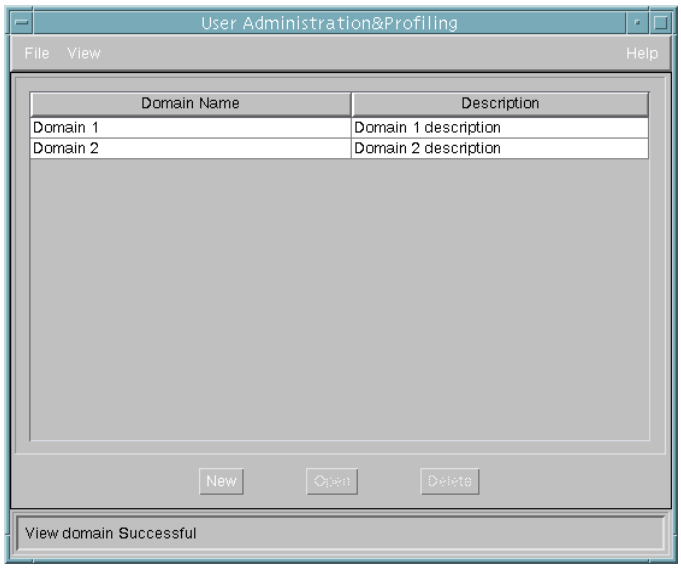


Figure 4-7 User Administration & Profiling window (Domains Table)

4. Click ***New***.
The *Domain Profile* window pops up.

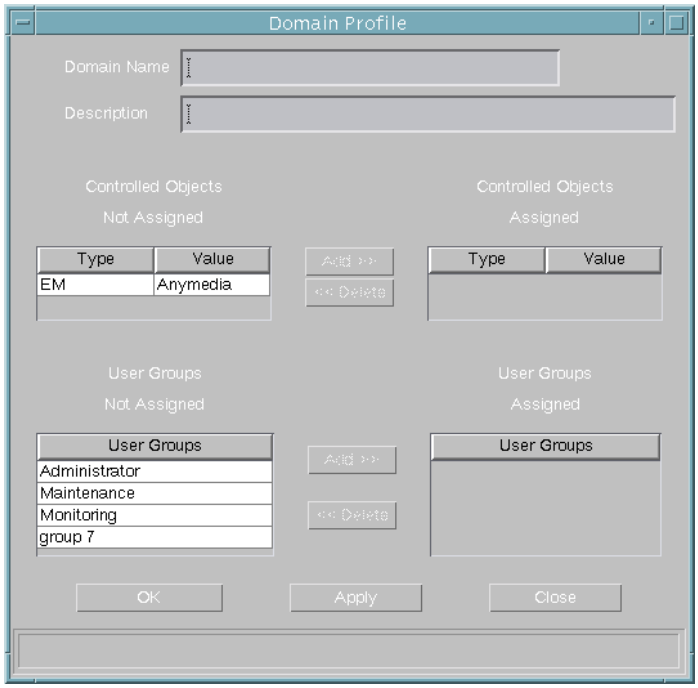


Figure 4-8 Domain Profile window

5. Enter a new domain name in the **Domain Name** field (this is mandatory - 3 to 30 characters) and extra information in the **Description** field (this is optional - 0 to 60 characters). Any characters are allowed.

6. Select one or more controlled objects that shall belong to the new domain in the **Controlled Objects Not Assigned** field and click ***Add>>***.

NOTE:
Each controlled object consists of two fields: *Type* and *Value*.

7. Select one or more user groups that shall have access to the new domain in the **User Groups Not Assigned** field and click ***Add>>***.

NOTE:
To create user groups see Chapter 4.4.1, page 4-14.

8. Click ***OK*** or ***Apply*** to save the settings (the system ensures that the new domain does not yet exist in the system). After clicking ***OK*** the window will be closed. If you want to reject the settings, click ***Close*** before ***OK*** or ***Apply***.

The other fields are described in Chapter 4.3.2, page 4-10.

4.3.2 Modify domains

Introduction

This chapter describes the process to modify the information of a domain, e.g. which devices it includes, etc. Before modifying the information of a domain, the AEM administrator must have a system login.

Procedure

Complete the following procedure to modify the information of a domain:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> Domains*** via menu bar. The *Domains Table* appears.

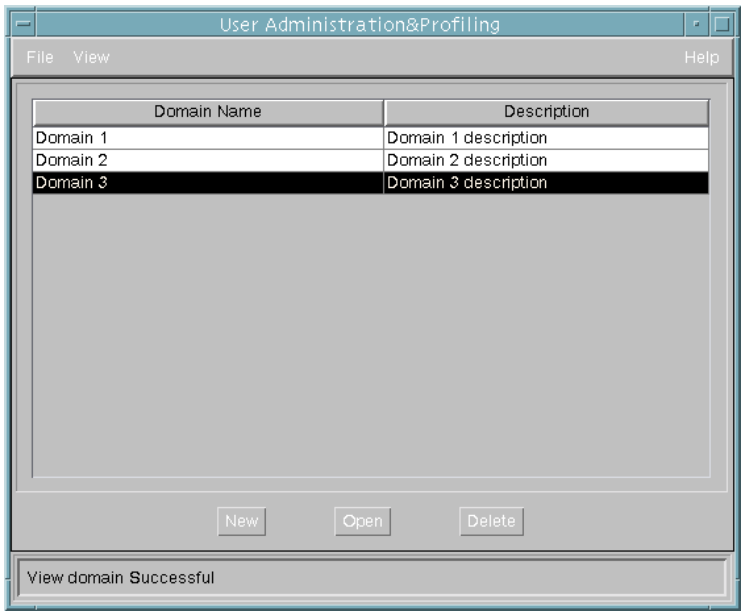


Figure 4-9 User Administration & Profiling window (Domains Table)

4. Select one domain in the **Domain Name** field and click ***Open***.
The *Domain Profile* window pops up with the current information about the selected domain.

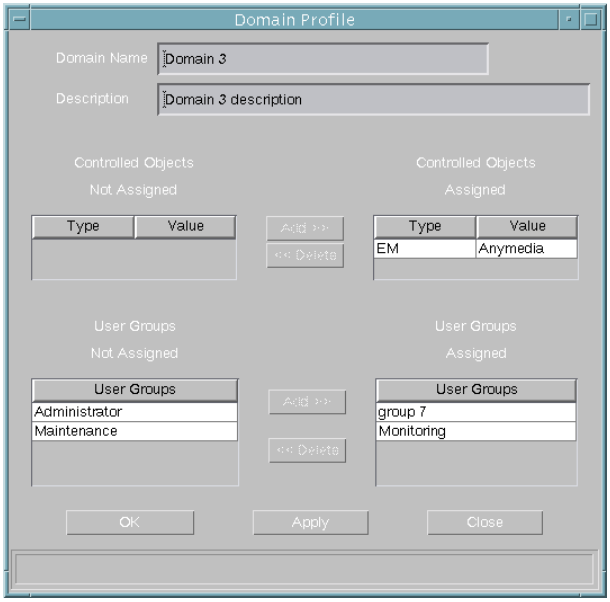


Figure 4-10 Domain Profile window

Change domain name

To change the domain name, enter the new name in the **Domain Name** field (3 to 30 characters). Any characters are allowed.

Change domain description

To change the domain description, enter the new information in the **Description** field (0 to 60 characters). Any characters are allowed.

Adding controlled objects

To assign further controlled objects to the selected domain, select one or more controlled objects in the **Controlled Objects Not Assigned** field and click ***Add>>***.

NOTE:
Each controlled object consists of two fields: *Type* and *Value*.

Removing controlled objects

To remove assigned controlled objects from the selected domain, select one or more controlled objects in the **Controlled Objects Assigned** field and click ***<<Remove***.

NOTE:
Each controlled object consists of two fields: *Type* and *Value*.

Adding user groups

To give further user groups access to the selected domain, select one or more user groups in the **User Groups Not Assigned** field and click ***Add>>***.

NOTE:
To create user groups see Chapter 4.4.1, page 4-14.

Removing user groups

To remove assigned user groups from the selected domain, select one or more user groups in the **User Groups Assigned** field and click ***<<Remove***.

Click ***OK*** or ***Apply*** to save the changes. After clicking ***OK*** the window will be closed.
If you want to reject the changes, click ***Close*** before ***OK*** or ***Apply***.

4.3.3 Delete domains

Introduction

This chapter describes the process to remove a domain from the AEM. Before removing a domain, please pay attention to the following remarks:

- The AEM administrator must have a system login.
- Before deleting a domain, the AEM ensures that there are no controlled objects assigned to this domain. If this is the case, the deletion request will be rejected.
- After a domain deletion, all related information will be removed from the AEM. This does not include the devices (NEs or any other type) which are grouped in that domain or their information. Furthermore, the access permission will be automatically unassigned from the user groups that had access to this domain.

Procedure

Complete the following procedure to remove a domain:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> Domains*** via menu bar The *Domains Table* appears.

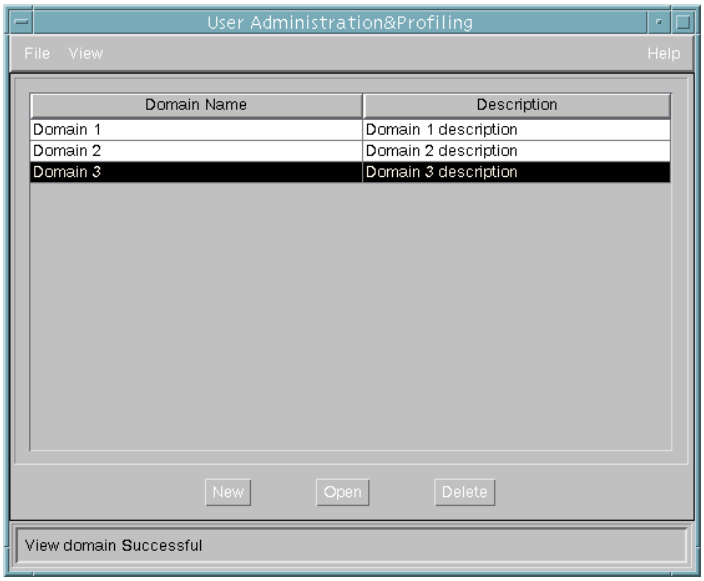


Figure 4-11 User Administration & Profiling window (Domains Table)

4. Select the domain which shall be deleted in the **Domain Name** field and click ***Delete***.

5. Confirm your selection. The window will be closed.

4.4 User groups

4.4.1 Create user groups

Introduction

This chapter describes the process to create a new user group. Before creating a new user group, please pay attention to the following remarks:

- By default the AEM provides three user groups: Administrator, Maintenance and Monitoring.
- The administrator user group has access permissions to all applications and tasks.
- Before a user group can be created, modified or deleted the AEM administrator must have a system login.
- Applications are divided into tasks. A user can be assigned a whole application or only a subset of its tasks.

Procedure

Complete the following procedure to create a new user group:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> User Groups*** via menu bar The *User Groups Table* appears.

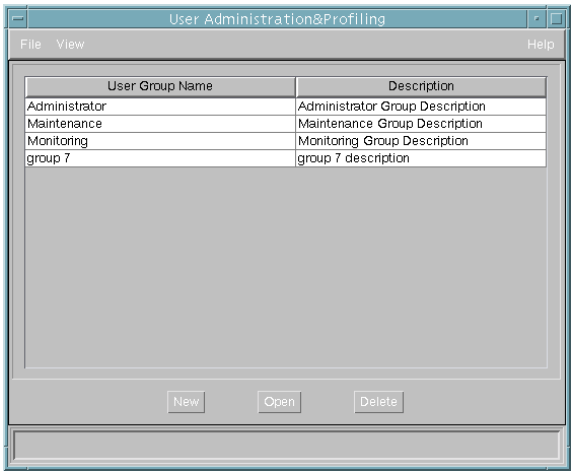


Figure 4-12 User Administration & Profiling window (User Groups Table)

4. Click ***New***. The *User Group Profile* window pops up.

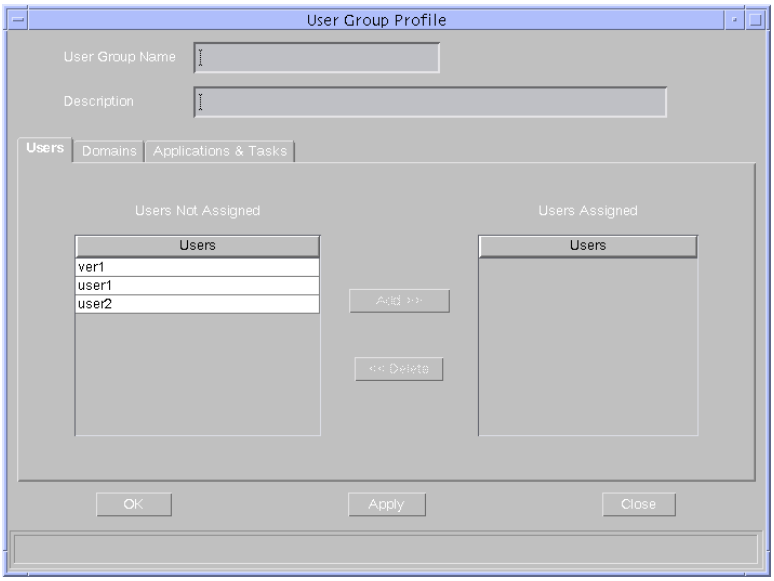


Figure 4-13 User Group Profile window (tab Users)

5. Enter a new user group name in the **User Group Name** field (this is mandatory - 3 to 30 characters) and extra information in the **Description** field (this is optional - 0 to 60 characters). Any characters are allowed.

6. Select one or more users that shall belong to the new user group in the **Users Not Assigned** field and click ***Add>>***.

NOTE:
To create user see Chapter 4.2.1, page 4-3.

7. Change to tab ***Domains***. The window changes its display as shown below.

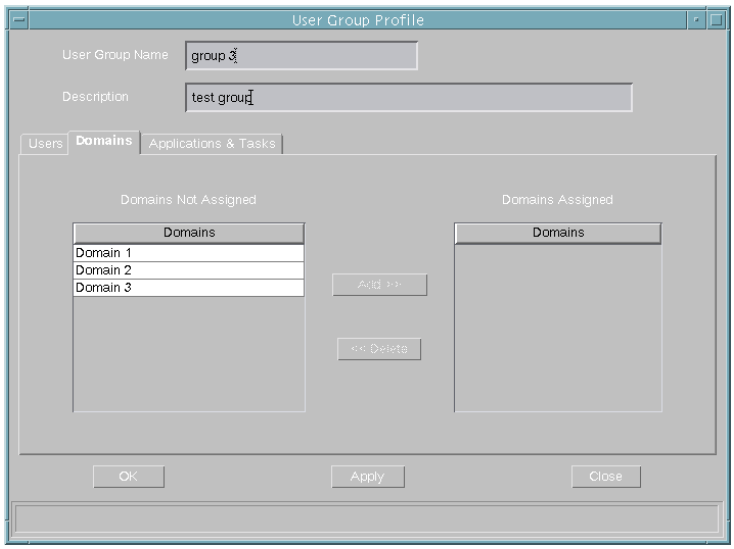


Figure 4-14 User Group Profile window (tab Domains)

8. Select one or more domains the user group shall has access to in the **Domains Not Assigned** field and click ***Add>>***.

NOTE:
If access permission to a domain is granted to a user group, that permission will be automatically granted for each controlled object within that domain.

NOTE:
To create domains see Chapter 4.3.1, page 4-8.

For carrying out the next three steps (10, 11 and 12) please pay attention to Table 4-1. It provides an overview about the access permissions the user groups shall have.

Table 4-1 Assignment of user groups to applications/tasks

Application	Task	User Group
System Administration	Process Management	Administrator
User Administration & Profiling	Access Policy Management	Administrator
	Domain Management	Administrator

Table 4-1 Assignment of user groups to applications/tasks

Application	Task	User Group
Log Viewer	Actions	Administrator, Maintenance
	System Internal Events	Administrator, Maintenance
	Autonomous Report	Administrator, Maintenance, Monitoring
Alarm Viewer	Alarms Acknowledge	Administrator, Maintenance
	Alarms View[a]	Administrator, Maintenance, Monitoring
	Alarms Clear	Administrator, Maintenance
Groups and NEs Management	Equipment and Service Provisioning	Administrator, Maintenance
	Configuration View[a]	Administrator, Maintenance, Monitoring
	Test Management	Administrator, Maintenance, Monitoring
	Cut-through Management	Administrator
	Groups and NEs Configuration	Administrator, Maintenance
	Performance Management	Administrator, Maintenance, Monitoring

a If the VIEW task is unassigned but other tasks are still assigned, these tasks are left as assigned to this user group. But the user is not able to perform any kind of operation over these tasks until the VIEW task is assigned again.

The most of the task names are self-described, but other tasks needs a deeper description:

Access Policy Management provides the functionality to:

- create/modify/delete AEM users
- create/modify/delete AEM user groups
- create/modify/delete AEM domains
- create/modify/delete assignments between AEM users and AEM user groups
- create/modify/delete access assignments between AEM user groups and applications/tasks
- create/modify/delete access assignments between AEM user groups and domains
- modify assignments between domains and controlled objects.

Domain Management provides the functionality to:

- modify assignments between domains and controlled objects.

Autonomous Reports provides the functionality to:

- view logs od log types (autonomous reports, alarm and performance logs).

Groups and NEs Configuration provides the functionality to:

- create/modify/delete NEs
- create modify/delete groups of NEs.

9. Change to tab ***Applications & Tasks***. The window changes its display as shown below.

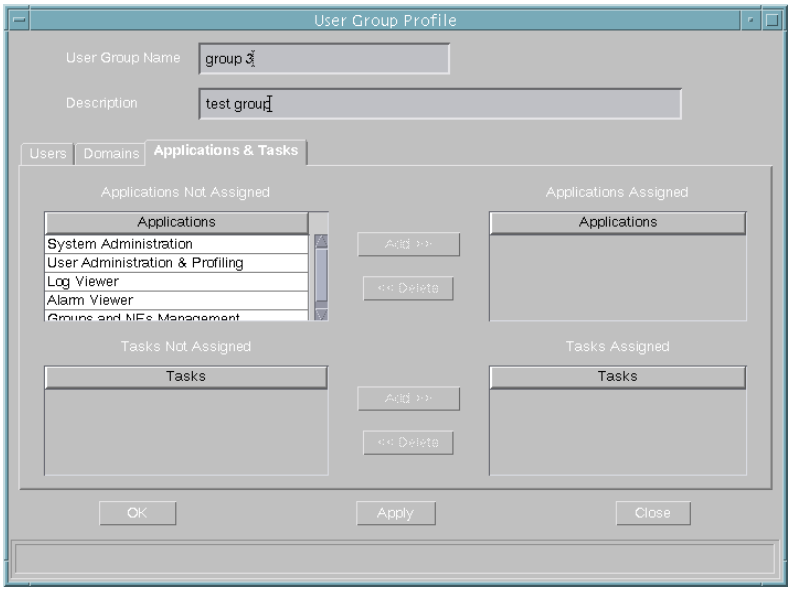


Figure 4-15 User Group Profile window (tab Applications & Tasks)

10. Select one or more applications the user group shall has access to in the **Applications Not Assigned** field and click ***Add>>***.
The corresponding tasks are displayed for selection.

11. Select one or more tasks the user group shall has access to in the **Tasks Not Assigned** field and click ***Add>>***.

12. Click ***OK*** or ***Apply*** to save the settings (the system ensures that the new user does not yet exist in the system). After clicking ***OK*** the window will be closed.
If you want to reject the settings, click ***Close*** before ***OK*** or ***Apply***.

The other fields are described in Chapter 4.4.2, page 4-19.

4.4.2 Modify user groups

Introduction

This chapter describes the process to modify the properties of a user group. Before modifying the properties of a user group, please pay attention to the following remarks:

- The AEM administrator must have a system login.
- The administrator user group has access permissions to all applications and tasks and these access permissions cannot be modified.

Procedure

Complete the following procedure to create a new user group:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> User Groups*** via menu bar The *User Groups Table* appears.

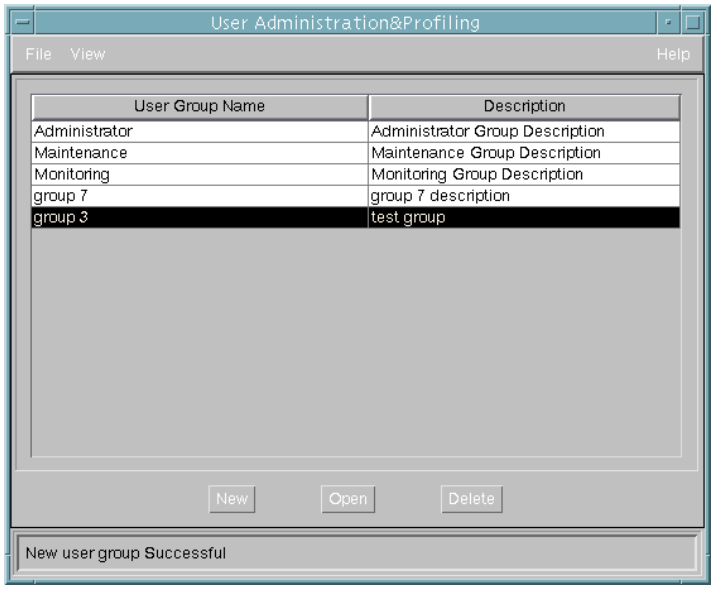


Figure 4-16 User Administration & Profiling window (User Groups Table)

4. Select one user group of the **User Group Name** field and click ***Open***.
The *User Group Profile* window pops up with the current information about the selected user group.

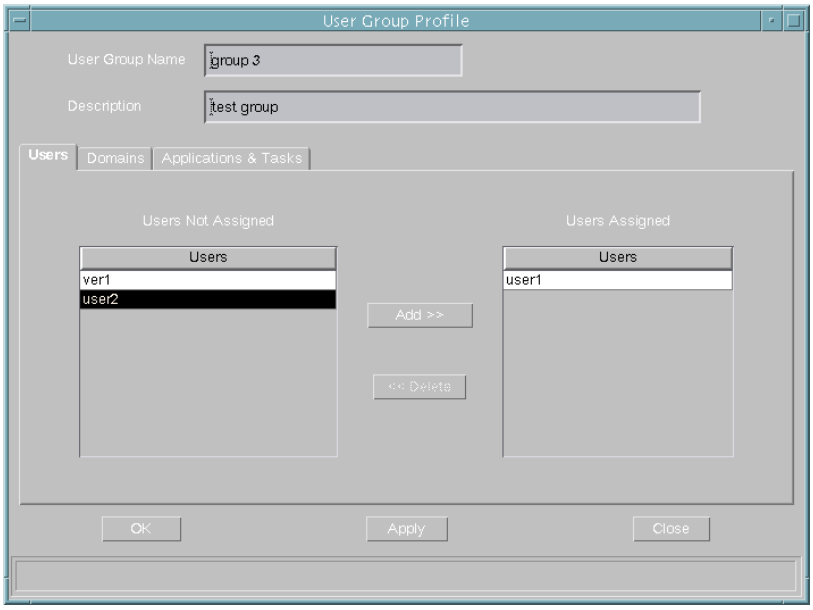


Figure 4-17 User Group Profile window (tab Users)

Change user group name

To change the user group name, enter the new name in the **User Group Name** field (3 to 30 characters). Any characters are allowed.

Change user group description

To change the user group description, enter the new information in the **Description** field (0 to 60 characters). Any characters are allowed.

Adding users

To assign further users to the selected user group select one or more users in the **Users Not Assigned** field and click ***Add>>***.

NOTE:
To a create user see Chapter 4.2.1, page 4-3.

Removing users

To remove assigned users from the selected user group select one or more users in the **Users Assigned** field and click ***<<Remove***.

NOTE:
The last user of user group administrator is protected against deletions.

Adding to domains

To give the selected user group access to further domains, change to tab ***Domains***. The window changes its display as shown below.

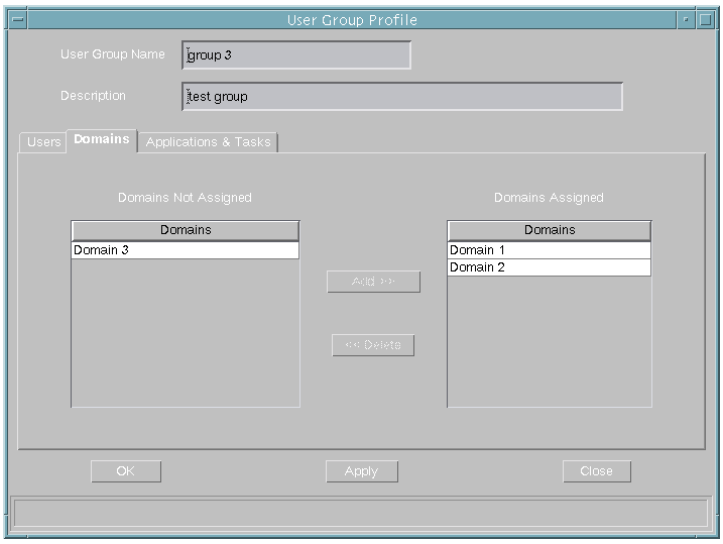


Figure 4-18 User Group Profile window (tab Domains)

Select one or more domains in the **Domains Not Assigned** field and click ***Add>>***.

NOTE:
If access permission to a domain is granted to a user group, that permission will be automatically granted for each controlled object within that domain.

NOTE:
To create domains see Chapter 4.3.1, page 4-8.

Removing from domains

To disable the access to domains select one or more domains in the **Domains Assigned** field and click ***<<Remove***.

NOTE:
The administrator user group has access permissions to all domains and this access permissions cannot be modified.

Adding applications

To give the selected user group access to further applications, change to tab ***Applications & Tasks***. The window changes its display as shown below.

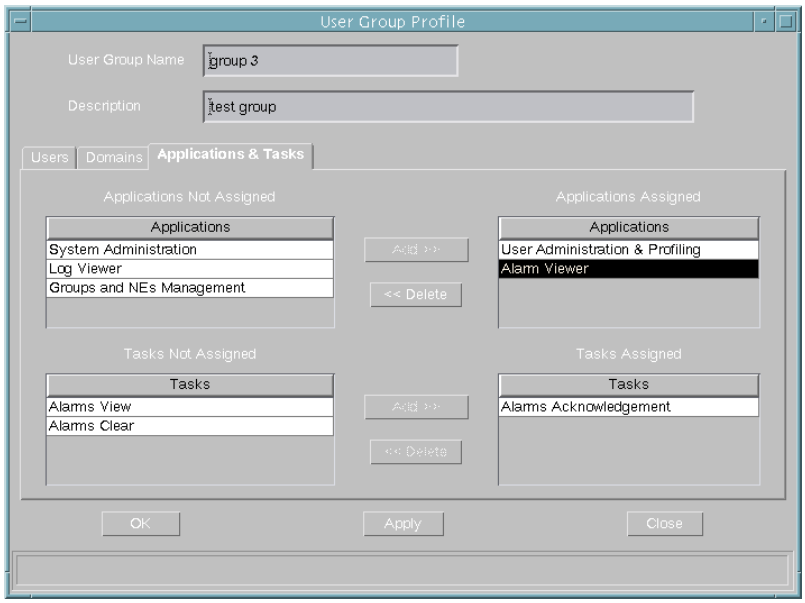


Figure 4-19 User Group Profile window (tab Applications & Tasks)

Select one or more applications in the **Applications Not Assigned** field and click ***Add>>***.

NOTE:
For this action please pay attention to Table 4-1, page 4-16.

Removing applications

To disable the access to applications select one or more applications in the **Applications Assigned** field and click ***<<Remove***. For this action please pay attention to Table 4-1, page 4-16.

NOTE:
The administrator user group has access permissions to all applications and this access permissions cannot be modified.

NOTE:
If the user select an application in the Applications Assigned field, all tasks that are under it will be expanded in the Tasks Assigned and Tasks Not Assigned fields.

Adding tasks

To give the selected user group access to further tasks, select one or more tasks in the **Tasks Not Assigned** field and click ***Add>>***.

NOTE:
For this action please pay attention to Table 4-1, page 4-16.

Removing tasks

To disable the access to one or more tasks, select one or more tasks in the **Tasks Assigned** field and click ***<<Remove***. For this action please pay attention to Table 4-1, page 4-16.

NOTE:
If the task "View" is removed from the Alarm Management or Groups and NEs Management the remaining tasks from the respective application are no more possible (but not removed).

NOTE:
The administrator user group has access permissions to all tasks and this access permissions cannot be modified.

5. Click ***OK*** or ***Apply*** to save the changes. After clicking ***OK*** the window will be closed. If you want to reject the changes, click ***Close*** before ***OK*** or ***Apply***.

4.4.3 Delete user groups

Introduction

This chapter describes the process to remove a user group from the AEM. Before removing a user group, please pay attention to the following remarks:

- The AEM administrator must have a system login.
- The administrator user group is protected against deletions.
- After a user group deletion, all related information is removed from the AEM. This does not include the contained users or their information, but these users will lose the ability to invoke the applications, tasks, devices and maps for which the user group had permission.

Procedure

Complete the following procedure to remove a user group:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> User Groups*** via menu bar. The *User Groups Table* appears.

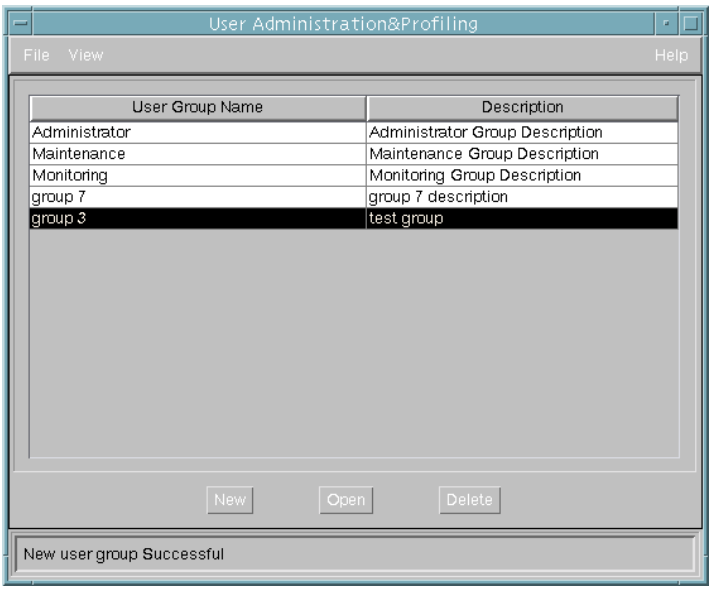


Figure 4-20 User Administration & Profiling window (User Groups Table)

4. Select the user group which shall be deleted in the **User Group Name** field and click ***Delete***.

NOTE:
The administrator user group is protected against deletion.

5. Confirm your selection. The window will be closed.

4.5 Controlled objects

4.5.1 Modify controlled objects

Introduction

This chapter describes the process to modify the information about existing controlled objects. The controlled object creation and deletion are not covered by this document. For NE creation and deletion refer to Chapter 5.5.1 and Chapter 5.5.19.

Before modifying the information about any controlled object the AEM administrator must have a system login.

Procedure

Complete the following procedure to modify the information about existing controlled objects:

Step	Procedure
1.	Login as AEM administrator and start the AEM access bar as described in Chapter 3.2.1. The access bar will be shown.
2.	Select the **User Administration & Profiling** icon. The *User Administration & Profiling* window pops up.
3.	Select ***View -> Controlled Objects*** via menu bar. The *Controlled Objects Table* appears.

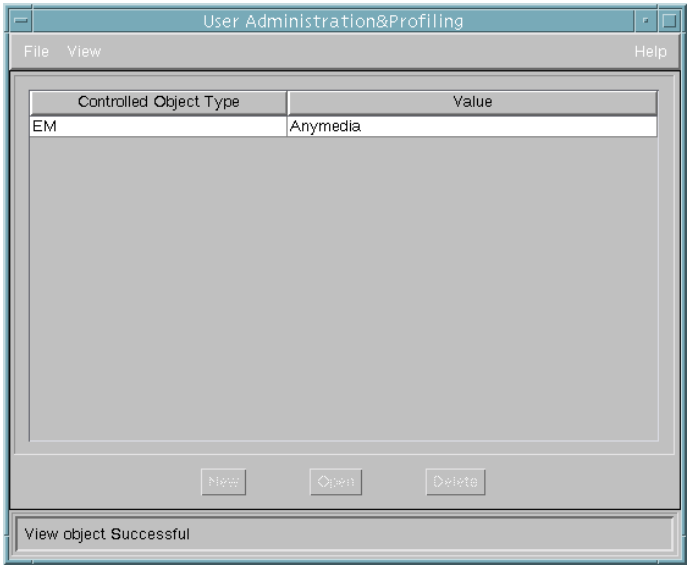


Figure 4-21 User Administration & Profiling window (Controlled Objects Table)

4. Select one controlled object type in the **Controlled Object Type** field and click ***Open***.
The *Controlled Object Profile* window pops up with the current information about the selected controlled object.

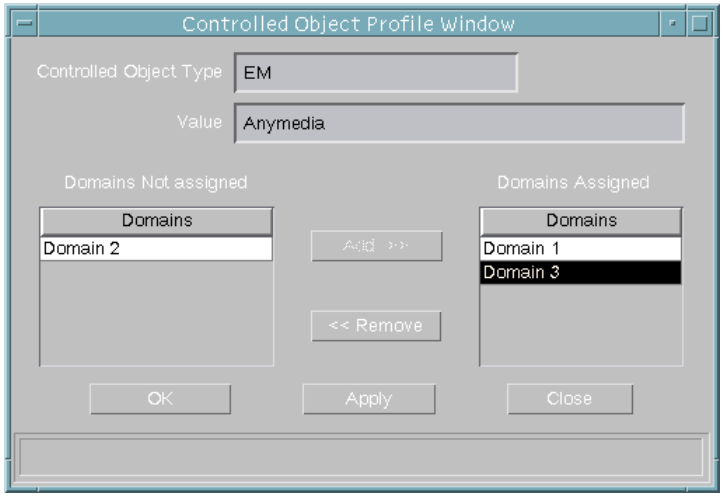


Figure 4-22 Controlled Object Profile window

Adding to domains

To assign the selected controlled object to further domains, select one or more domains in the **Domains Not Assigned** field and click ***Add>>***.

NOTE:
To create domains see Chapter 4.3.1, page 4-8.

Removing from domains

To remove the selected controlled object from domains, select one or more domains in the **Domains Assigned** field and click ***<<Remove***.

NOTE:
The "EM" object generated by default is protected against deletion.

Click ***OK*** or ***Apply*** to save the changes. After clicking ***OK*** the window will be closed. If you want to reject the changes, click ***Close*** before ***OK*** or ***Apply***.

Other fields (read-only)

The following fields are read-only fields to display data of the selected controlled object:

Controlled Object Type:
Displays the controlled object type. Possible values are *EM* and *NE*.

Value:
Displays the characteristics of the selected controlled object. If the controlled object is *EM* it displays "AnyMedia", if it is *NE* it displays the NE Id number.

NE management/equipment configuration

5

Contents

5.1 Introduction 5-1

5.2 Overview of the controlled system 5-1

5.2.1 Network element R1.3 5-2

5.2.1.1 *AnyMedia* Mainshelf configuration example 5-2

5.2.1.2 Synchronization interfaces 5-3

5.2.1.3 OAM&P interfaces 5-4

5.2.1.4 Alarm interfaces 5-4

5.2.1.5 Testing interfaces 5-5

5.2.1.6 Plug & play capabilities 5-5

5.2.1.7 NE equipment configuration-related tasks 5-5

5.2.2 Network element release R1.3.1 5-6

5.2.3 Network element release R1.4 5-6

5.2.3.1 Pack management for HDSL AP 5-7

5.2.3.1.1 ISDN PRA subscriber provisioning 5-7

5.2.3.1.2 N × 64-kbps DLL provisioning 5-8

5.2.3.1.3 HDSL interface loopbacks 5-9

5.2.3.2 NTU inventory data retrieval 5-9

5.2.3.3 Pack management for Optical Application Pack (OAP) 5-10

5.2.3.4 Pack and shelf management for Optical Network Units (ONUs) 5-11

5.2.3.4.1 Optical Network Unit (ONU) configuration 5-12

5.2.4 Broadband applications 5-13

5.2.4.1 Broadband system description 5-13

5.2.4.2 Network E3/DS3 interfaces 5-14

5.2.4.3 E3/DS3 framing and synchronization 5-14

5.2.4.4 Broadband synchronization and timing 5-15

Contents

5.2.5 AEM R1.7 new equipment configuration features 5-15
5.2.5.1 Telephony agent (narrowband) 5-15
5.2.5.2 Data agent (broadband) 5-16
5.2.5.3 Configuration of combined tasks 5-16
5.3 Initial windows 5-17
5.3.1 Menu bar 5-18
5.3.2 Tool bar 5-19
5.3.2.1 Network browser 5-19
5.3.2.2 Network Element Browser 5-20
5.3.3 Background Map 5-20
5.3.4 Status bar 5-21
5.3.5 Cursor menu 5-22
5.3.5.1 Cursor menu entries 5-23
5.3.5.1.1 Network Browser 5-23
5.3.5.1.2 Network Element Browser 5-23
5.4 Groups and NEs Management 5-25
5.4.1 Groups management 5-25
5.4.2 NEs management 5-28
5.4.3 Groups & NEs window 5-29
5.4.3.1 Group window 5-29
5.4.3.2 Create/modify groups 5-31
5.4.3.3 Delete a group 5-31
5.4.3.4 NEs window 5-32
5.4.3.5 Create/modify NEs 5-34
5.4.3.6 Remove an NE 5-34
5.5 Equipment configuration 5-35
5.5.1 Add a network element 5-37
5.5.2 Connection states AEM - telephony agent 5-40
5.5.2.1 Changing connection states 5-41
5.5.2.2 Association maintenance 5-41
5.5.2.3 NE Management window (tab Telephony) 5-42
5.5.2.4 Modify NE Management data (telephony agent) 5-44
5.5.3 Communication states AEM - data agent 5-44
5.5.3.1 Changing connection states 5-45
5.5.3.2 Association maintenance 5-46

Contents

5.5.3.3 NE Management window (tab Data) 5-46
5.5.3.4 Modify NE Management data (data agent) 5-49
5.5.4 Shelf View 5-50
5.5.5 Configuration of the packs 5-55
5.5.5.1 IO_E1 window 5-55
5.5.5.2 Configure an IO_E1 5-57
5.5.5.3 Physical Feeder window 5-59
5.5.5.4 Edit Physical Feeder 5-60
5.5.5.5 View the COMDAC parameters 5-62
5.5.5.6 View the CIU parameters 5-64
5.5.5.7 IO_HDLC window 5-66
5.5.5.8 Configure an IO_HDLC 5-68
5.5.5.9 Subshelves window 5-69
5.5.5.10 Modify subshelves 5-72
5.5.5.11 Common application pack window 5-74
5.5.5.12 Provisioning a slot via common AP 5-76
5.5.5.13 PSTN/ISDN AP window 5-77
5.5.5.14 Modify a PSTN/ISDN AP 5-80
5.5.5.15 TAP AP window 5-82
5.5.5.16 HDSL AP window 5-84
5.5.5.17 Modify an HDSL AP 5-87
5.5.5.18 ONU Application Pack window 5-89
5.5.5.19 Modify an OAP 5-91
5.5.5.20 Read the OCP data 5-92
5.5.5.21 AFM window (data application) 5-94
5.5.5.22 Modify an AFM (data application) 5-97
5.5.5.23 AFM Feeder window (data application) 5-99
5.5.5.24 Modify an AFM feeder (data application) 5-101
5.5.5.25 AFM Feeder PM Threshold window (data application) 5-102
5.5.5.26 Define AFM Feeder PM thresholds (data application) 5-104
5.5.5.27 ADSL Application Pack window (data application) 5-105
5.5.5.28 Modify an ADSL pack (data application) 5-108
5.5.5.29 ADSL Drop window (data application) 5-110
5.5.5.30 Modify an ADSL drop (data application) 5-113
5.5.5.31 Transmission Profile window (data application) 5-115
5.5.5.32 Modify the ADSL transmission profile (data application) 5-119

Contents

5.5.5.33 Threshold Profile window (data application) 5-120
5.5.5.34 Modify the ADSL threshold profile (data application) 5-122
5.5.6 Network element synchronization 5-123
5.5.6.1 Telephony agent 5-123
5.5.6.1.1 Configuration information synchronization 5-123
5.5.6.1.2 Alarm information synchronization 5-123
5.5.6.1.3 Synchronization Telephony window 5-124
5.5.6.1.4 Modify the synchronization telephony parameter 5-125
5.5.6.2 Data agent 5-126
5.5.6.2.1 Configuration information synchronization 5-126
5.5.6.2.2 Alarm information synchronization 5-126
5.5.6.2.3 Synchronization Data window 5-127
5.5.6.2.4 Modify the synchronization data parameter 5-128
5.5.7 Configuration of timing source (for telephony only) 5-129
5.5.7.1 Timing Source Control window 5-130
5.5.7.2 Modify the timing source 5-133
5.5.8 Date & Time Telephony window 5-134
5.5.9 Date & Time Data window 5-136
5.5.10 NE Inventory window 5-138
5.5.10.1 Get the NE inventory data 5-140
5.5.10.2 External Equipment window 5-140
5.5.11 Network element working mode 5-141
5.5.12 Simplex COMDAC protection scheme 5-141
5.5.12.1 COMDAC window 5-142
5.5.12.2 Set the COMDAC protection to simplex 5-143
5.5.13 Equipment protection switching 5-143
5.5.13.1 COMDAC Protection window 5-144
5.5.13.2 Modify the COMDAC protection mode 5-147
5.5.13.3 IO_HDLC Protection window 5-147
5.5.13.4 Modify the IO_HDLC protection mode 5-150
5.5.13.5 Alarm configuration 5-150
5.5.14 Network element software upgrade 5-151
5.5.14.1 Network element software download (telephony agent) 5-151
5.5.14.2 COMDAC Software Download window 5-152
5.5.14.3 Software download to telephony agent 5-153
5.5.14.4 AFM Software Download window 5-156

Contents

5.5.14.5 Software download to data agent 5-157
5.5.15 COMDAC program copy 5-159
5.5.16 AFM program copy and validation 5-161
5.5.17 Nonvolatile data storage (NVDS) 5-163
5.5.17.1 Data backup (telephony agent) 5-164
5.5.17.2 Data backup (data agent) 5-165
5.5.17.3 Data restore (telephony agent) 5-166
5.5.17.4 Data restore (data agent) 5-167
5.5.17.5 File Browser window 5-168
5.5.18 TL1 cut-through (telephony agent) 5-170
5.5.19 Delete network element 5-171

Contents

NE management/equipment configuration

5

5.1 Introduction

This chapter describes the "Groups and NEs Management" application of the *AnyMedia*® Element Manager - 30 Channel (AEM), R1.7. It addresses the following topics:

- Overview of the controlled *AnyMedia* Access System
- Explanation of menu bar, Network Browser and Network Element Browser
- Map handling
- Screen navigation
- NE management
- Equipment configuration.

5.2 Overview of the controlled system

This section provides a short overview of the controlled *AnyMedia* Access System. For more information please refer to the network element documentation for

- Telephony (narrowband) releases R1.3, R1.3.1 and R1.4
- Data (broadband) releases R1.1.2 and R1.4.

AnyMedia Mainshelf configuration

The AEM R1.7 is able to control NEs with the following configuration:

- Telephony-only configuration
- Data-only configuration
- Mixed telephony and data configuration.

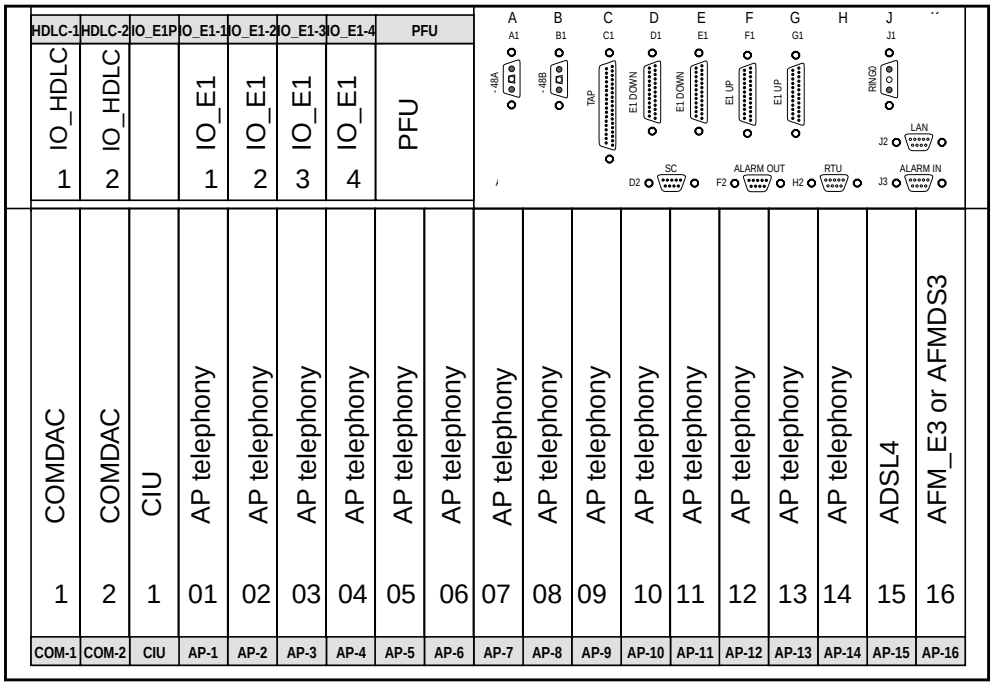
5.2.1 Network element R1.3

The network element architecture of the *AnyMedia* Access System R 1.3 is a single mainshelf with the following components:

- *AnyMedia* Mainshelf
- Power Filter Unit PFU (PFU500)
- Common packs for telephony services:
  - Up to two Common Data and Control COMDAC (COM500)
  - One Communication Interface Unit CIU (DTP500)
  - Up to four E1 Interface Units IO_E1 (FAC500)
  - Up to two High Level Data Link Control packs IO_HDLC (IDC500).
- Up to 16 application packs (APs) for telephony services:
  - POTS AP LPZ100 (32 Z ports)
  - POTS AP LPP100 (24 Z ports)
  - ISDN AP LPU112 (12 U ports).
- Test application pack TAP100
- Packs for data services:
  - ATM Feeder Multiplexer AFM (LPA910 or LPA900)
  - Up to 15 ADSL application packs ADSL4 (LPA400).
- Mainshelf backplane.

5.2.1.1 *AnyMedia* Mainshelf configuration example

Figure 5-1, page 5-3 shows an example of an *AnyMedia* Mainshelf in a mixed configuration for telephony and data services.



- IO_HDLC packs for telephony services
- IO_E1 packs for telephony services
- COMDACs for telephony services
- CIU for telephony services
- AFM pack for data services (AFM_E3 or AFMDS3)
- 15 APs may be mixed telephony APs (POTS/ISDN) and data APs (ADSL4 APs)

Figure 5-1 *AnyMedia* Mainshelf view in mixed configuration

5.2.1.2 Synchronization interfaces

For network synchronization of the telephony part the *AnyMedia* Access System recovers timing from two types of sources:

- From E1 feeders (clock derived from two of 16 E1 feeder signals)
- From an external synchronization equipment delivering a synchronization signal to the station clock interface (SCI) connected at the shelf connection panel (SCP)

Two clocks per IO_E1 pack and the station clock (SC) from the SCI are connected to each COMDAC. Two of these clocks are provisioned as reference clocks.

NOTE:
If both reference clocks fail the system switches to free-running mode.

5.2.1.3 OAM&P interfaces

OAM&P interfaces for telephony services

The *AnyMedia* Access System provides the following maintenance interfaces for operations, administration, maintenance, and provisioning (OAM&P) for telephony services:

- Craft interface terminal (CIT) port
- 10BaseT interface
- Remote operations channel (ROC).

A PC-based graphical system interface, the *AnyMedia* Access System graphical system interface software (GSI) operates over all OAM&P interfaces.

OAM&P interfaces for data services

The *AnyMedia* Access System provides the following OAM&P interfaces for data services:

- 10BaseT interface
- Inband ATM permanent virtual connection (PVC).

Each OAM&P interface supports simple network management protocol (SNMP) and file transfer protocol (FTP) operations.

NOTE:
When multiple shelves are daisy chained, each *AnyMedia* Mainshelf provides these interfaces and must be independently addressed for OAM&P.

NOTE:
It is possible to transport also telephony OAM&P information via the data network. The AFM extracts this information from the ATM PVC and routes it to the 10BaseT port. To transmit the telephony OAM&P information to the COMDAC the 10BaseT ports (AFM and LAN connector in the SCP) have to be connected.

5.2.1.4 Alarm interfaces

The following alarm interfaces exist for the *AnyMedia* Access System:

Local alarm and status indicators

The packs have light emitting diodes (LEDs) on the faceplate to indicate status and alarm conditions. Any alarms indicated by the LEDs are reported also via the OAM&P interfaces.

Office alarm outputs

Three software-controlled relays on the CIU are used as alarm outputs to indicate active alarms. The relays may be connected to audible or visible alarm indication devices. The assignment to the alarm LEDs is provisionable by TL1 commands.

Miscellaneous alarm closure inputs mainshelf

The CIU supports 8 ground closure alarm inputs to indicate environmental fault conditions. Alarms detected at the external alarm inputs are reported also via the OAM&P interfaces. An additional LED *MISC* on the CIU faceplate indicates an active alarm input.

Alarm cut-off function

The alarm cut-off function (ACO) provides the possibility to immediately cut off the audible/visible alarms active on the alarm interface outputs. The ACO function is activated by pressing the ACO button on the CIU faceplate or with a TL1 command.

5.2.1.5 Testing interfaces

Interfaces for manual testing

Interfaces for manual testing

- Faceplate jack *DROP* on the CIU

  This interface is used for metallic test access to the subscriber line and to partly the equipment on the subscriber side.

- Faceplate jack *CHAN/MON* on the CIU

  This interface is used for metallic test access to the port hardware and for listening to an existing call.

Interfaces for integrated testing

Interfaces for integrated testing

- TAP connector on the SCP for metallic test access
- Connector on the faceplate of the TAP100.

Interfaces for external test head testing

Interfaces for external test head testing

- Serial RS-232C RTU port for control access
- TAP connector on the SCP for metallic test access.

The RTU port does not perform a user login and password verification and is therefore limited by the system to the RTU test session commands. On the other management interfaces the RTU test session commands are also available but only with authorization check.

5.2.1.6 Plug & play capabilities

The packs associated with the *AnyMedia* Access System have the capability to self-identify themselves with inventory data. This capability is very useful during the execution of provisioning and maintenance procedures.

For example, upon insertion of the new pack in the *AnyMedia* Mainshelf, the inventory data of the new pack, as well as its serial number, slot and pack entity, are reported to the AEM and/or GSI interface. The removal of any pack unit will be announced also.

5.2.1.7 NE equipment configuration-related tasks

The network element (NE) equipment configuration facilities provided by the AEM cover the operations that control and provision the NE, including the following tasks:

- **Configuration-specific equipment data, which involves:**
  - NE creation and deletion

- Pack management
  - COMDAC management
  - IO_E1 management - physical feeder management
  - IO_HDLC management
  - CIU management
  - AFM management
  - AP management - Z port/U port/ADSL port management
- Protection management
- Slot alarming configuration
- Date & time management
- NE security configuration
- Timing synchronization provisioning.

- **Maintaining a local copy of the NE inventory, which includes:**
  - Initializing the local copy when an NE is add to the AEM.
  - Maintaining the local copy of equipment changes.
  - Synchronizing the local copy with the equipment data maintained by the NE, and reporting differences.
- **Inventory management** - system activity of collecting, updating, and reporting data on *AnyMedia* Access System equipment and system status, including providing users with access to the entire equipment information, whether locally maintained or not.
- **NE memory administration** - this means the management of the nonvolatile data storage (NVDS) of the *AnyMedia* Access System for backup and restore
- **NE software administration** - this involves tasks to manage the nonvolatile program storage (NVPS) of the *AnyMedia* Access System for software download, copying the NVPS between controller packs, etc.

For more information please refer to the network element documentation.

5.2.2 Network element release R1.3.1

The *AnyMedia* Access System R1.3.1 is based on release R1.3 with the addition of a new ISDN AP (LPU430), so its behaviour and management by the AEM is identical to that for R1.3.

5.2.3 Network element release R1.4

The *AnyMedia* Access System R1.4 adds a set of new packs and features which have to be supported by the AEM, that are:

- Up to two Common Data and Control COMDAC (COM501)

- HDSL AP (LPS501) - pack management for High-Data Rate Digital Subscriber Line Application Pack (HDSL AP)
- External equipment inventory retrieval - retrieving of network termination unit (NTU) inventory data
- OAP (LPF500) - pack management for Optical Application Pack (OAP)
- ONU Subshelf with OCP (CPF500) and APs - pack and shelf management for Optical Network Units (ONUs).

5.2.3.1 Pack management for HDSL AP

General

The HDSL AP with the HDSL interfaces supports up to four HDSL ports. The HDSL ports can be used to connect ISDN PRA subscribers as well as n × 64-kbps DLL subscribers via NTU.

The *AnyMedia* Mainshelf R1.4 allows equipage of up to 16 HDSL APs. Consequently the maximum number of HDSL ports supported by the mainshelf is 64.

HDSL subshelf aspects

Up to 8 HDSL APs can also be equipped in the ONU Subshelf. Consequently the maximum number of HDSL ports supported by a mainshelf (up to 8 ONU connections) together with the subshelf for R1.4 is 256.

HDSL interface application modes

The HDSL interface can be operated in different provisionable application modes which impact the supported services:

- Point-to-point mode

  Full bandwidth of 2048-kbps of up to 31 x 64-kbps timeslots for different structured applications. It can support one G.703 service (ISDN PRA or n × 64-kbps) and additionally one n × 64-kbps DLL service according to V.35, V.36, or X.21.

- Single-pair mode, fractional installation

  Half of the 2.048-Mbps payload (n × 64-kbps) can be transported. It can support one G.703 service (ISDN PRA or n × 64-kbps) and additionally one n × 64-kbps DLL service according to V.35, V.36, or X.21.

- Point-to-multipoint mode

  A bandwidth of 30 × 64-kbps timeslots is supported. The 30 timeslots are splitted on two independent HDSL interfaces (2 × 15 × 64-kbps timeslots). Two NTUs located at the same or different subscribers can be connected. Each HDSL interface can support one G.703 service n × 64-kbps and additionally one n × 64-kbps DLL service according to V.35, V.36, or X.21.

5.2.3.1.1 ISDN PRA subscriber provisioning

Provisioning aspects

Prior to provisioning of an ISDN PRA subscriber an HDSL logical interface must be provisioned on top of one or two HDSL ports located on an HDSL AP. The usage of one or two HDSL ports depends on the provisioned HDSL application mode and defines the maximum bearer channel capacity of 15 or 30 bearer channels. HDSL logical interfaces autocreate HDSL logical timeslots which may be used by the services. After that an ISDN PRA subscriber can be provisioned on

top of the HDSL logical interface. The used HDSL logical timeslots are specified in a provisioning command. Note that on top of an HDSL logical interface also other services and a service mix can be provisioned.

Allocated HDSL timeslots

Each provisioned ISDN PRA subscriber allocates HDSL timeslots on an HDSL logical interface. The *AnyMedia* Access System supports retrieval with the physical access identifier as key to show the operator which HDSL timeslots on an HDSL logical interface are already allocated and which ones are not used for any service yet.

Allocated HDSL ports

Each provisioned ISDN PRA subscriber allocates an HDSL port. The *AnyMedia* Access System supports a retrieval with the physical access identifier as key to show the operator which HDSL ports are already allocated and which ones are not used for any service yet.

5.2.3.1.2 N × 64-kbps DLL provisioning

Overview

The *AnyMedia* Access System supports two kinds of n × 64-kbps digital leased line services over HDSL interface:

- VLL

  A digital leased line via a data interface is supported, which can be either V.35, V.36 or X.21

- GLL

  A leased line according to ETS 300 419 is supported via a G.703 interface.

In both cases the interface is provided by means of an NTU which is located on the subscriber side of an HDSL transmission system.

Connection

An n × 64-kbps DLL subscriber has the transmission capability of up to 31 B-channels (31 × 64-kbps) and is connected to the network via a leased line interface with up to 31 64-kbps timeslots. N × 64-kbps DLL subscribers are provided by connecting a number of bearer channels supplied by a VLL or GLL entity with the same number of timeslots of a leased line interface. The association of a VLL or GLL subscriber with a leased line interface is made on the service assignments layer.

Provisioning aspects

Prior to provisioning of an n × 64-kbps DLL subscriber an HDSL logical interface must be provisioned on top of one or two HDSL ports located on an HDSL AP. The usage of one or two HDSL ports depends on the provisioned HDSL application mode and defines the maximum bearer channel capacity of 15 or 31 bearer channels. HDSL logical interfaces autocreate HDSL logical timeslots which may be used by the services. After that an n × 64-kbps DLL subscriber can be provisioned on top of the HDSL logical interface. The used HDSL logical timeslots are specified in a provisioning command. Note that on top of an HDSL logical interface also other services and a service mix can be provisioned.

V5 independency

VLL and GLL are independent of the V5.x interface. They are transported on E1 feeders, which are exclusively used for leased line purposes. A mix of DLL, ALL, VLL and GLL on one E1 feeder is possible.

5.2.3.1.3 HDSL interface loopbacks

Overview

Possible HDSL interface loopbacks are located on the HDSL ports (loopback 1) and on the application interface (loopback 2) of the NTU. The loopbacks are initiated by the operator from the GSI/AEM by a TL1 command with the following parameters:

- loopback location (loopback 1 or loopback 2)
- loopback with or without BER testing.

The HDSL interface loopbacks are reflected in service states of the equipment layer and lines layer model. The relevant service states are IS-TST or OOS-TST.

Application modes for HDSL loopbacks

Depending on the application mode in which the HDSL system is operating, there exists a different set of loopbacks which can be activated from the HDSL AP, that means from the line termination unit (LTU). Following application modes for HDSL loopbacks are possible:

- HDSL loopbacks in point-to-point mode
- HDSL loopbacks in single pair mode
- HDSL loopbacks in point-to-multipoint mode
- HDSL loopbacks including BER test.

5.2.3.2 NTU inventory data retrieval

The HDSL network termination unit (NTU) is not part of the *AnyMedia* Access System.

The NTU is able to provide the following inventory data:

- product name
- HW configuration
- SW version
- serial number
- manufacture date.

This information is stored on the COMDAC. Every time an HDSL interface is newly synchronized, this information is fetched from the NTU.

The information is provided by a TL1 command on the equipment layer to the GSI/AEM.

5.2.3.3 Pack management for Optical Application Pack (OAP)

OAP configuration

The OAP is a two-slot plug-in. It consists of a parent and a child board. The parent board is installed in the even-numbered slots of the mainshelf, the subtending child board in the adjacent left slot. These two boards are connected mechanically to each other. Figure 5-2 shows a possible mainshelf configuration for a mixed telephony/data configuration.

In telephony-only configurations up to eight ONU Subshelves can be connected to one mainshelf. If data services are also provided by the system up to seven ONU Subshelves can be supported because the AFM limits the number of AP slots available for OAP installation.

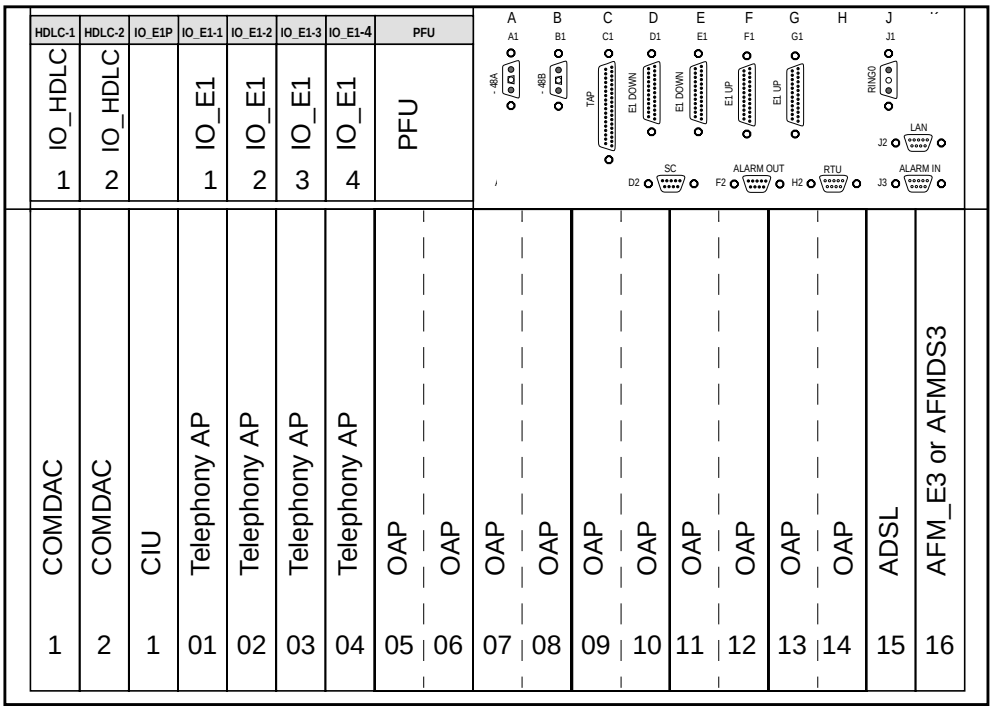


Figure 5-2 Mainshelf view for mixed telephony/data configuration

NOTE:
The OAP requires two slots. The AEM shelf view displays the same faceplate (duplicated) for the two slots where the OAP is inserted (even and odd slots).

OAP software download

The system checks after an OAP recovery whether the OAP is already loaded with the expected software version. If the software version differs the system automatically downloads the correct software to the OAP. For this the OAP software is

stored with the COMDAC software in the COMDAC NVPS area during the initial system turn-up procedure. The OAP software cannot be updated separately from the COMDAC image.

OAP inventory

The OAP inventory data contains the same fields as the existing APs and can be retrieved by the "Retrieve Equipment" TL1 command. The pack type identifies it as a OAP. The inventory data also contains an identification of the loaded and standby software version of the pack.

OAP fault handling

The OAP is also called shared equipment. Shared means that this pack supports telephony as well as data services.

The fault handling of the OAP is done from the COMDAC and the AFM. Both controllers maintain their appropriate domains and do not exchange information about fault conditions or status of the shared pack. To reduce traffic outages as much as possible both domains can be reset independently.

5.2.3.4 Pack and shelf management for Optical Network Units (ONUs)

Overview

Besides mainshelf applications the *AnyMedia* Access System R1.4 supports remote access via the Optical Network Units (ONUs). *AnyMedia* Mainshelf and ONU Subshelf are connected via a single-fiber optical link which provides a transmission rate of 155-Mbps. Figure 5-3 shows the interworking of the *AnyMedia* Mainshelf and the ONU Subshelves.

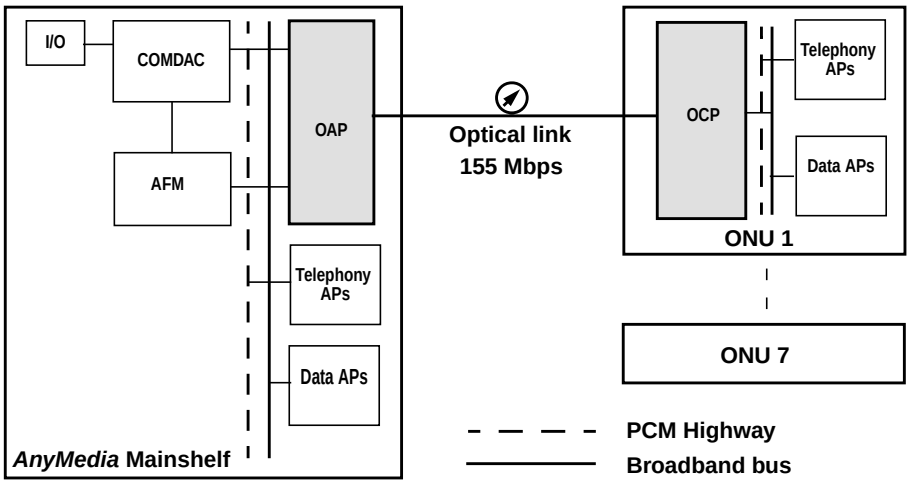


Figure 5-3 Interworking of *AnyMedia* Mainshelf and ONU

For connecting an ONU Subshelf to an *AnyMedia* Mainshelf, an OAP has to be installed in the mainshelf and an OCP in the ONU Subshelf.
Telephony and/or data transmitted via the network node interfaces (E1s, E3, respectively) are transported within the *AnyMedia* Mainshelf to the OAP. The OAP has access to the telephony and data interfaces of the *AnyMedia* Mainshelf backplane.

5.2.3.4.1 Optical Network Unit (ONU) configuration

Within the ONU Subshelf one Optical Controller Pack (OCP) and up to eight APs (telephony and/or data packs) can be installed (cf. Figure 5-4, page 5-12).

The installation of an OCP is required for providing the interface to the *AnyMedia* Mainshelf.

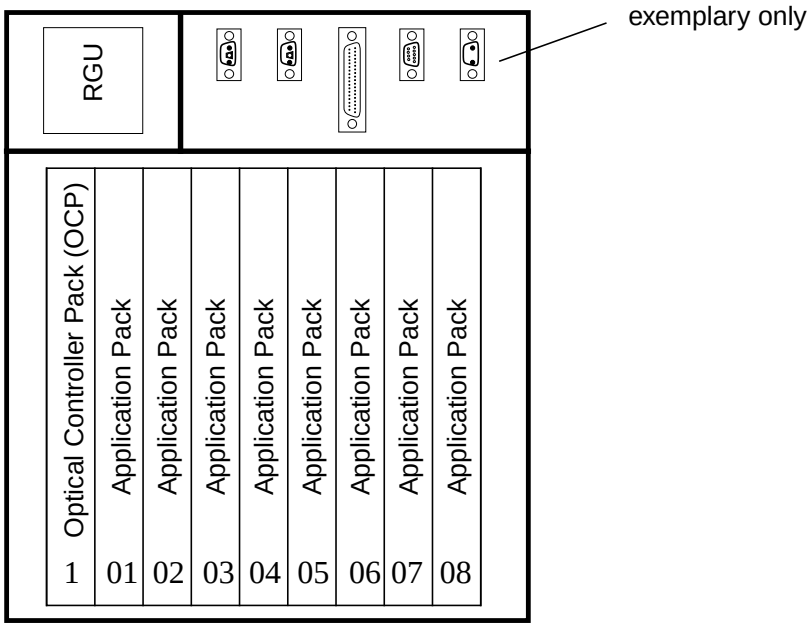


Figure 5-4 ONU Subshelf view

Synchronization interface

The ONU does not require any synchronization interface because the ONU is synchronized by the *AnyMedia* Mainshelf via the optical link.

OCP software download

A software download to the OCP is performed without operator interaction automatically from the *AnyMedia* Mainshelf to the OCP at the detection of a software mismatch. The OCP software is included in the COMDAC software image and downloaded to the ONU Subshelf. The OCP software cannot be updated separately from the COMDAC image.

The *AnyMedia* mainshelf checks during the link turn-up procedure whether the OCP is already loaded with the correct and expected software version. If not, the *AnyMedia* Mainshelf automatically downloads the correct software to the OCP. For this the OCP software is stored with the COMDAC software in the COMDAC NVPS area during the initial *AnyMedia* Mainshelf turn-up procedure.

Shared equipment fault conditions (OAP/OCP)

The shared equipment is divided into two fault units, one for the telephony and one for the data domain. A partly failed shared equipment, with faults related only to one domain, is marked faulty only in this domain whereas in the other domain it is fault free. A detected fault condition at the sanity check, built-in self-test or peri-

odic online check is reported only to the domain the fault condition relates to. The faceplate FAULT LED of the shared equipment indicates in any case a detected fault regardless whether it is a partly fault or a fault which influence both domains.

Examples for shared equipment faults are:

- Pack removal
- Pack not responding to poll
- Power failure
- Hardware errors.

ONU isolation strategy

Raised alarms on ONU subshelf entities are cleared at the loss of the optical link connection if the lost connection disables the COMDAC software to recognize a possible alarm clearance trigger. This includes also alarms of the ONU subshelf environmental alarms inputs.

NOTE:
Power unit failures with total loss of power can not be alarmed to the *AnyMedia* mainshelf as the power unit is not protected in the ONU subshelf configuration.

Inventory for ONU Subshelf entities

If the connection to the ONU Subshelf is lost all subshelf pack inventory data is not retrievable any more and for all equipped packs an "UNPLUG" report is generated.

After recovery of the ONU Subshelf connection the *AnyMedia* Mainshelf performs a new equipage and inventory data retrieval. For all equipped ONU packs (OCP and APs) a new "PLUGIN" report is generated and the inventory data is available again.

5.2.4 Broadband applications

This section contains an overview of the *AnyMedia* Access System data application.

5.2.4.1 Broadband system description

Overview

The *AnyMedia* Access System provides data services to subscribers, using asynchronous transfer mode (ATM) cell transfer and asymmetrical digital subscriber line (ADSL) interface technology.

The *AnyMedia* Mainshelf provides end-to-end ATM cell transfer between customer premise equipment (ADSL modems) and network ATM switches. A mixed telephony/data mainshelf is shown in Figure 5-1, page 5-3. This configuration allows subscriber access to internet service providers (ISP), remote LAN applications or any other related ATM services. ATM connections are established using permanent virtual circuits (PVC).

Full-rate ADSL interface

The full-rate ADSL interface is a twisted 2-wire subscriber interface according to ANSI T1.413 and ITU-T G.992.1. It provides voice and data transmission using

discrete multitone (DTM) technology. The connection can carry ADSL traffic as well as the POTS signal.

ADSL-lite interface The ADSL-lite interface is a twisted 2-wire subscriber interface according to ITU-T G.992.2. It provides voice and data transmission using DTM technology. The connection can carry ADSL traffic as well as the POTS signal.

User interfaces ADSL customer premise equipment is provided by an outside vendor for the *AnyMedia* Access System. The following end-user interfaces are available:

- 10BaseT/Ethernet for LAN interface applications (single or multiple users)
- Universal serial bus 5 (USB)
- PC network interface card (NIC).

The ADSL transmission is based on ANSI T1.413, Issue 2. In later releases, the system supports ADSL transmission based on ADSL-lite.

ATM traffic The AFM pack (AFME3/AFMDS3) interfaces up to 15 ADSL APs which may be installed in the *AnyMedia* mainshelf. ATM traffic multiplexed to and from the ADSL APs are interfaced to the ATM network via an E3/DS3 link. The E3/DS3 link can connect the ATM switch directly to the transmission network.

5.2.4.2 Network E3/DS3 interfaces

E3/DS3 connections The AFM E3/DS3 feeder interface on the AFM has the following connections:

- Two E3/DS3 ports
  - — Port 1 used to interface toward the ATM network
  - — Port 2 used to connect to any other *AnyMedia* Mainshelf that may be daisy-chained.
- Each E3/DS3 has a 34.368-Mbps / 44.736-Mbps transmission rate and carries ATM payload cells
- The network E3/DS3 may terminate directly at an E3/DS3 interface of an ATM network node or may be transported over a synchronous optical network transmission system.
- The network E3/DS3 provides a user network interface (UNI 3.1) cell format toward the network, as defined in the ATM Forum.

5.2.4.3 E3/DS3 framing and synchronization

For E3 framing direct cell mapping is used. For DS3 framing direct cell mapping or PLCP is used. The AFM transmit clock is provisionable to be free running. The status of the E3 (DS3) ports is provided by LEDs on the AFM as well as by the AEM/GSI display.

5.2.4.4 Broadband synchronization and timing

Feeder timing

The timing source used by the AFM is not provisionable. The choices are as follows:

- Loop-timed from the input of E3-1/DS3-1 (default value)
- Free-running.

Loop-timed

When the timing source is set to loop-timed, the AFM recovers timing from the E3/DS3 input that connects toward the ATM network (E3-1/DS3-1). It distributes the recovered timing to the E3-2/DS3-2 (downstream) interface and also to the output of E3-1/DS3-1 (that is, the E3-1 output is loop-timed). The AFM recovers and distributes timing in this fashion regardless where it is in a daisy-chain, or if it is operating alone. Therefore, the AFM recovers timing from E3-1/DS3-1 regardless of whether E3-1/DS3-1 is connected to the ATM transport network or to E3-2/DS3-2 of another AFM.

Free-running

When the timing source is set to free-running, all E3/DS3 timing is derived from an internal crystal oscillator with an accuracy of ±20 parts per million (ppm).

E3-1/DS3-1 failure handling

If the E3-1/DS3-1 signal fails, all E3/DS3 timing is derived from same timing source used when the AFM is provisioned for free-running. When the E3-1/DS3-1 failure clears, the timing source automatically changes back to loop-timed.

When the timing source is set to free-running, all E3/DS3 is derived from the internal oscillator regardless of the health of the E3-1/DS3-1 signal.

ADSL timing

Timing for each ADSL interface is derived from an internal crystal oscillator in the ADSL AP.This timing reference is used regardless of the status of the E3/DS3 signal from the network.

5.2.5 AEM R1.7 new equipment configuration features

5.2.5.1 Telephony agent (narrowband)

The AEM R1.7 manages the following releases of the *AnyMedia* telephony agent of the 30-channel families (international market):

- R1.3, R1.3.1 and R1.4.

The support of all these releases means the following set of new tasks in the equipment configuration area of the AEM:

- New APs: ISDN APs (LPU430), OAPs (LPF500), and HDSL APs LPS501)
- "Stand-by" configuration management (*AnyMedia* R1.3 and all subsequent releases)
- Management of HDSL APs (*AnyMedia* R1.4 only)
- Management of ONU Subshelves (*AnyMedia* R1.4 only)

- External equipment (NTU) inventory retrieval (*AnyMedia* R1.4 only).

5.2.5.2 Data agent (broadband)

Unlike previous releases, the AEM R1.7 integrates the management of the data agent (R1.1.2 and R1.4) in the *AnyMedia* Access System.

The NE equipment configuration facilities provided by the AEM for the data agent include the following tasks:

- **Configuration of specific equipment data**:
  - Circuit pack management
    - AFM management
    - ADSL AP management
  - Physical feeder management
  - ADSL drop management
  - Date & time management
- **Maintaining a local copy of configuration data in the AFM's NVDS**:
  - Synchronizing the local copy with the equipment data maintained by the AFM.
- **Inventory Management** - system activity of collecting, updating and reporting data on equipage and system status, including providing users with access to the entire equipment information, whether locally maintained or not.
- **AFM memory administration** - which means the management of the non-volatile data storage (NVDS) of the *AnyMedia* Access System including AFM for "Backup and Restore".
- **AFM software administration** - which involves tasks to manage the non-volatile program storage (NVPS) of the *AnyMedia* Access System including AFM for software download, software validation and activation, etc.
- **ONU Subshelf management** - for subshelf creation, subshelf edition with cross-connection, and subshelf deletion.
- **Profile management -** for creating, deleting, or applying threshold and transmission profiles. Edit profile variables using a previously defined template.

5.2.5.3 Configuration of combined tasks

The integrated management of both agents, telephony and data, requires not only the equipment configuration features described previously for each agent, but also a unique view of some areas, for example subshelf management, pack provisioning, etc.

5.3 Initial windows

This major application provides the user with the facilities needed to fully configure *AnyMedia* network elements (both equipment and services).

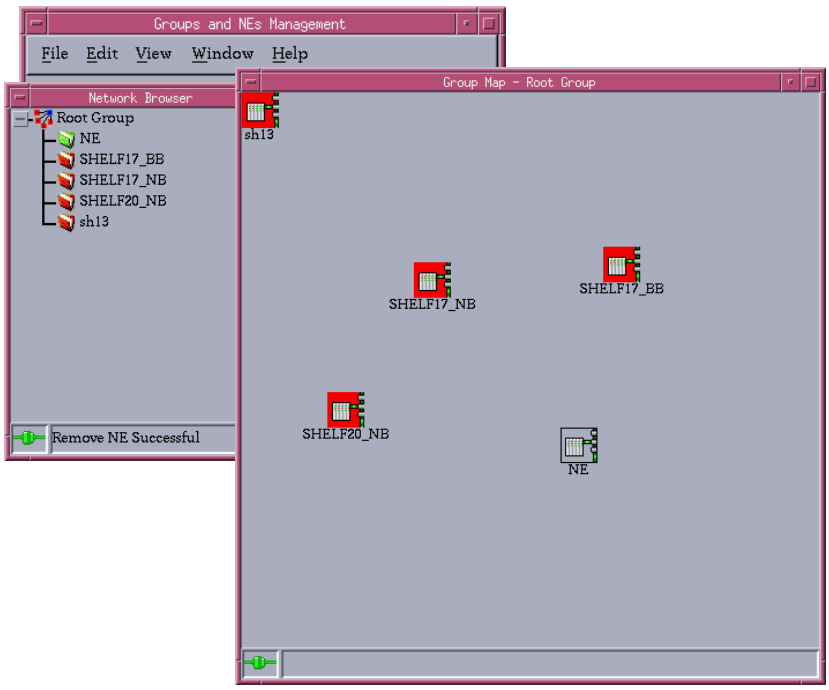


Figure 5-5 Groups and NEs Management window

The initial window consists of three areas:

- At the top, the **menu bar** (cf. Chapter 5.3.1, page 5-18) and the **tool bar** (cf. Chapter 5.3.2, page 5-19).
- On the left-hand side, the **Network Browser** (cf. Chapter 5.3.2.1, page 5-19).
- On the right-hand side, the **Background Map** window shows a background map of a selected NE group (cf. Chapter 5.3.3, page 5-20).

Depending on previous actions the following frames are additionally available:

- On the right-hand side, a common area is used for the display of the information requested through the menu bar, cursor menu or tool bar (if present).
- A **Network Element Browser** (cf. Chapter 5.3.2.2, page 5-20) shows all the components of the NE which has been selected via the **Network Browser**.

- A **status bar** is incorporated at the bottom of screens which execute commands (cf. Chapter 5.3.4, page 5-21).
- The **cursor menu** will pop up at the cursor position when the right mouse button is pressed (cf. Chapter 5.3.5, page 5-22).

5.3.1 Menu bar

The menu bar entries are enabled/disabled depending on the object selected in one of the browser list (NE Browser or Network Browser). The following table describes the menu bar's main entries and subsequent submenus. The right column identifies the item that needs to be selected to have this menu option available.

Menu entries	Available at level
File -> New	Any item in Network Browser (Group or NE)
File -> Remove	Any item in Network Browser (Group or NE)
File -> Print -> Print window	Always
File -> Print -> Print table	Always
File -> Print -> Preview	Always
File -> Exit	Always
Edit -> Cut	Text editing field
Edit -> Copy	Text editing field
Edit -> Paste	Text editing field
Edit -> Clear	Text editing field
View -> Object...	Always
View -> Toolbar	Always
View -> Reload	Always NOTE: This operation is not supported for the Network Browser. The menu appears only when no other Groups & NEs Management window is open.
Window -> Window 1	
Window -> Window 2	
Help -> Contents...	Always (displays the help index for navigation through the EM help information)
Help -> On Window...	Always (case-sensitive online help)

Menu entries	Available at level
Help -> About...	Always

Access keys and shortcuts

The options hidden under the menu name in the menu bar may also be executed via the keyboard. This can be done using various methods.

There are two ways of opening a menu using the keyboard:

- By simultaneously pressing the ***Alt*** key and the underlined character in the menu name (e.g. ***Alt-F*** for ***File***).

  Then select the desired option by typing in the letter underlined in this option. The menu will close and the related function is executed.
  Example: To execute the ***About...*** option under ***Help*** menu (see table above) press ***Alt-H*** followed by ***A***.

- By using short-cuts to cut, to copy or to paste text strings. The short-cuts are the usual ones in the used platform (Solaris or Windows).

5.3.2 Tool bar

The tool bar contains icons that provide quick access to the most commonly used actions: New (create a new object: group, NE, pack), Open (edit an existing object: group, NE, pack), Remove (delete selected object: group, NE), Print, Help, Exit, Reload, Show Parent Group. Tooltips are also provided for these action icons.

5.3.2.1 Network browser

The **Network Browser** displays all groups and NEs created in the AEM in a tree-like structure. The first level in the tree is the root group.

Alarm serverity

The icons change their color to reflect the highest severity alarm (critical, major, minor, indeterminate or warning alarms). The highest severity alarm of a group is the highest severity alarm of all the alarms of its child groups and NEs. The alarm status color is in accordance with the alarm viewer color set (red for critical and major; yellow for minor; white for indeterminate and warning).

Expand display

Any level of the Network Browser (e.g Group_1) can be expanded to its components (e.g. groups and NEs) by clicking on the "+" symbol related to the object to be expanded (only groups can be expanded). Any expanded object can be collapsed by clicking on the "-" symbol related to it. The branch can also be expanded by double-clicking on a group.

NOTE:
The display is not automatically refreshed. The changes are only visible after re-expanding the branch (clicking on the "+" sign).

Move icons It is possible to move an NE or a group from an origin group to a target group by "drag and drop". Once an NE is dropped the mouse pointer converts to a clock until the action has finished. This clock pointer is shown over the browsers and over the background map window (group map).

The old parent group and the new parent group update their group status to the new group status (high severity alarm), this group status depends on the domain to which the operator belongs.

New background group Clicking or double-clicking on a group icon launches a new background map of the selected group.

New Network Element Browser Clicking or double-clicking on an NE icon launches a new Network Element Browser displaying the selected NE.

5.3.2.2 Network Element Browser

The **Network Element Browser** displays all the components of the previously selected NE (through the Network Browser or by double-clicking on NE icons within the background map): shelves and packs.

The Network Element Browser shows the slot_Id if the slot is not equipped. If the slot is equipped, the apparatus code of the inserted pack is shown.

5.3.3 Background Map

In the Group Map a background map of a selected NE group is shown. By double-clicking on a group icon all components of this group will be displayed. The same result can be reached by double-clicking on the group name in the Network Browser.

By clicking on the "Show Parent Group" icon in the tool bar, the background map of the parent group (with all its components) will be displayed.

By double-clicking on an NE icon the Network Element Browser is displayed with the selected NE as root node.

Move icons It is possible to move an icon (group or NE) over the background map by "Drag and Drop" as well as moving icons between Network Browser and the background map.

Once an NE is dropped the mouse pointer converts to a clock until the action has finished. This clock pointer is shown over the browsers and over the background map window (group map).

The old parent group and the new parent group update their group status to the new group status (high severity alarm), this group status depends on the domain to which the operator belongs.

5.3.4 Status bar

Feedback from the NE is displayed on screen, as is progress information related to the commands issued by the AEM. This feedback is provided by the status bar incorporated at the bottom of screens which execute commands.

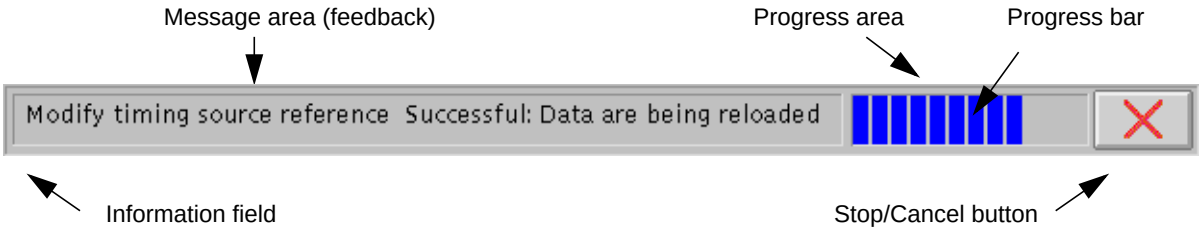
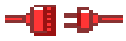


Figure 5-6 Status bar (example)

The status bar is composed of four sub-areas:

- **Information field**: Used to display monitoring information by means of two icons.


Information not updated


Information updated

- **Message area**: Used to display feedback. It indicates what is being done. The last feedback message sent by the NE is displayed until a new command is sent or the window is closed. There is a tooltip available to show the complete message if the message area is smaller than the message.
- **Progress area**: Informs the user there are jobs running.
- **Stop / Cancel button**: For commands: allows cancellation of commands. Note that Cancel does not imply undo.

If the user tries to close the window and the last command executed has not finished yet, they will be informed (*Warning* window) that there are still jobs running:

`You have running jobs. Do you want to continue?`

The user has to decide whether to continue or wait until the job is finished. Note that closing the window does not imply cancelling the action.

Additional messages

The following can be displayed in the message area:

- Feedback (see above)

- Error messages

  Any time a wrong data is entered in the GUI (out-of-range values, inappropriate value types, etc.), an error message indicates the nature of the error. The checking of wrong data is performed when the Apply or Ok button is clicked.

- Failed window opening
  - Failed window refresh.

For windows without status bar the error message will be shown by means of a warning window. This window will be automatically closed after a time (default 10 seconds) which is configurable.

If the error cannot be identified a general error message (recorded in a catalog) will be presented (e.g. "Last Operation or Data request could not execute").

5.3.5 Cursor menu

Menu at the cursor position

Some objects in windows have a menu associated with them. This menu will pop up at the cursor position when the right mouse button is pressed. The cursor must not, however, be positioned on a menu bar or a window frame. The cursor menu is not available in all dialogue boxes. The functions which can be executed using this cursor menu depend on the application of the respective dialogue box.

Select menu option

Proceed as follows to select a menu option from the cursor menu:

Step	Procedure
1.	Press and hold down the right mouse button.
2.	Drag the cursor onto the desired menu option.
3.	Release the right mouse button to execute the menu option, or if you do not wish to execute a menu option, move the cursor away from the menu and release the right mouse button.

5.3.5.1 Cursor menu entries

5.3.5.1.1 Network Browser

Selected icon on Network Browser	Cursor menu entries
Group	***New*** (*Groups & NEs* window) ***Edit*** (*Groups & NEs* window) ***Show Map*** (background map) ***Remove*** (groups) ***Alarm Monitoring*** (group-specific alarms)
NE	***Edit*** (*Groups & NEs* window) ***NE Management*** (*NE Management* window) ***Remove*** (NE) ***Open Network Element Browser*** ***Alarm Monitoring*** (NE-specific alarms) ***Log Viewer***

5.3.5.1.2 Network Element Browser

Selected icon on Browser	Cursor menu entries
NE	***Inventory*** ***Date & Time -> Telephony*** ***Date & Time -> Data*** ***Synchronization -> Telephony*** ***Synchronization -> Data*** ***Timing Source Control*** (only for telephony) ***Create Subshelf -> ONU*** (only NE R1.4) ***Alarms*** ***Logs*** ***List -> V5 Interface*** ***List -> HDSL Interface*** (only NE R1.4) ***List -> Physical Feeder*** ***List -> User Port*** ***List -> ATM Cross-Connections*** (only for data) ***List -> Data Test*** (only for data) ***Backups -> Telephony*** ***Backups -> Data*** ***Restore -> Telephony*** ***Restore -> Data*** ***Software Download -> Telephony*** ***Software Download -> Data***

Selected icon on Browser	Cursor menu entries
NE (continued)	***Program Copy -> Telephony*** ***Program Copy -> Data*** ***Cut-Through -> Telephony*** ***Profiles -> ADSL Transmission*** ***Profiles -> ADSL PM Threshold*** ***Performance -> ATM Traffic*** ***Performance -> Feeder*** ***Performance -> ADSL*** ***AFM Feeder PM Threshold (Data)***
Main Shelf	***View*** ***Protection***
Subshelves	***View*** ***Edit***
AP	***View***

5.4 Groups and NEs Management

This feature is also called map handling and is performed by the following windows:

- Network Browser
- NE Browser
- Group Map.

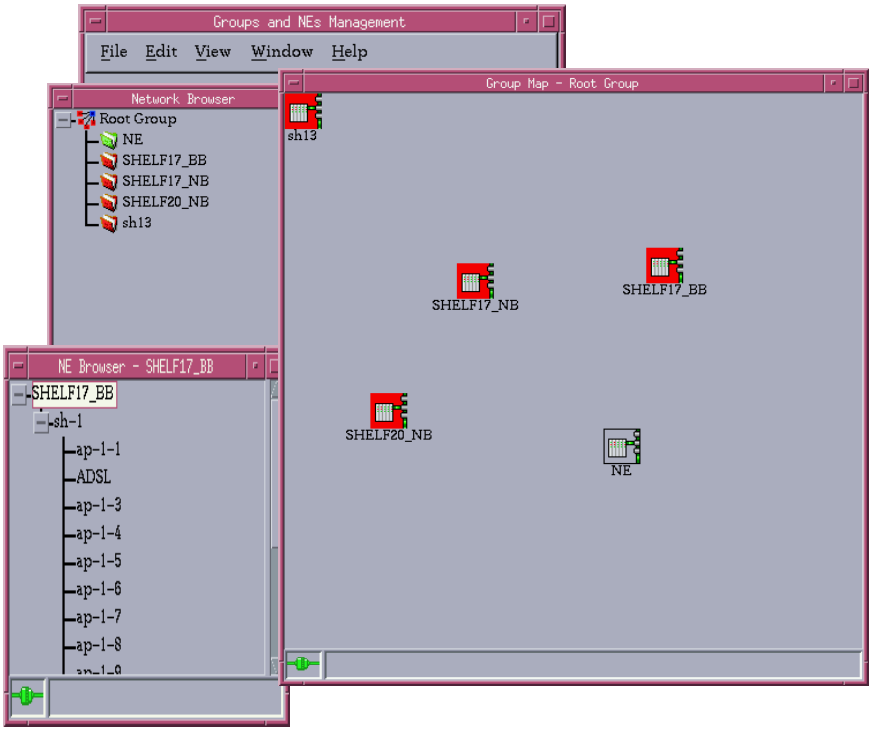


Figure 5-7 Groups and NEs Management windows

5.4.1 Groups management

Overview

Groups management consists of the addition of a new group to the set of groups that can be managed by the AEM as well as the deletion and edition of their attributes. It also involves the movement of a group from an old parent group to a new parent group and the information of the group status parameter.

NE groups

Due to the increase of the number of NEs to be managed by the AEM, they are displayed in a layered way, displaying sets of NEs instead of the whole set of NEs. These groups can contain NEs and/or other groups. Groups and NEs are distributed in a tree hierarchy with the root group as the starting point of the tree.

The root group does not have group icon or group coordinates as it is never shown from an upper layer. Instead, it has a background map to display the icons of the items of the first level.

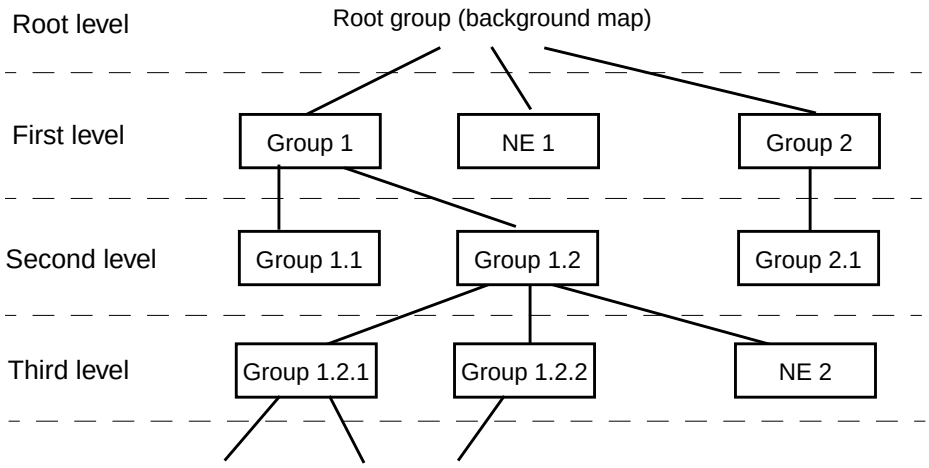


Figure 5-8 Tree hierarchy of groups and NEs

View levels

The root group is a special group that is created at the first start-up and can never be deleted. It is the only item in the root level of Figure 5-8. From this level, only the items of the first level are visible (for example: Group 1, Group 2 and NE1 are directly reachable from the root level).

Allocation to background maps

To facilitate the visualization of the child items of a group, a background map can be allocated to each group to depict the group's child items on it. To implement this, each group must have the following parameters:

- Group name: This identifier must be unique within the group level (groups with the same parent group).
- Group icon: to graphically identify the group when displaying the items of the group's parent group.
- Background map: map on which the group's child items are displayed.
- Group coordinates: to specify the position of the group icon on the background map of the group's parent group.

Allowed names

Two different groups can have the same group name except when their parent groups are the same. It is therefore possible to have two groups named "Group C" with "Group A" and "Group B" as their parent groups respectively (see Figure 5-9, page 5-27).

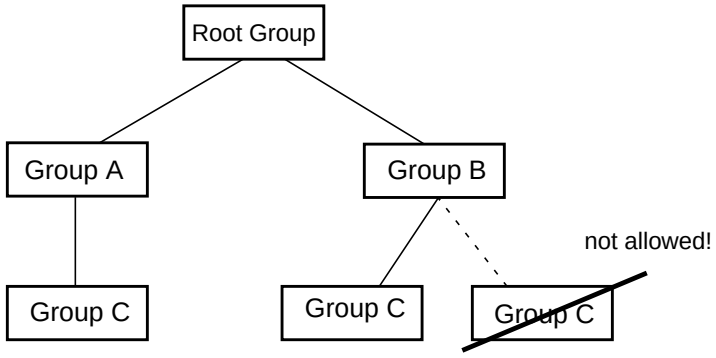


Figure 5-9 Group names allowed

Group identifier

To uniquely identify a group a concatenation of all the group names from the root group to the group being identified is necessary (e.g. the identifier of Group 1.2.1 in Figure 5-8, page 5-26 is: *Root group - Group 1 - Group 1.2 - Group 1.2.1*).

However, when logging data related to a group, that identifier will be truncated due to log requirements. Only the name of the group and the name of the parent group will be logged as the identifier of a group (e.g. the log identifier of Group 1.2.1 in Figure 5-8, page 5-26 is: *Group 1.2 - Group 1.2.1*).

Alarm handling

The only items in the tree hierarchy allowed to report alarms are the NEs. Groups do not generate alarms by themselves, but they show the highest severity of the alarms reported by the contained NEs included in the operator domains. This severity is called the group status.

Example

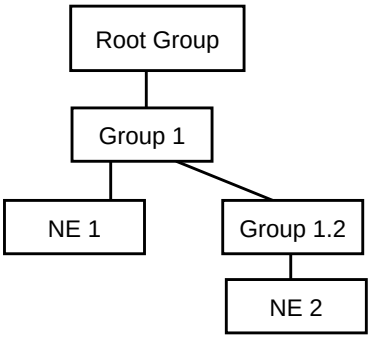


Figure 5-10 Alarm handling (example)

Reported group status

For instance, supposing that NE1 has reported a *critical* alarm and NE 2 has reported a *minor* alarm. Group 1.2 will report a *minor* alarm in its group status because that is the highest severity of the alarms it contains. Nevertheless, group 1 will report a *critical* alarm in its group status because it contains two NEs: NE 2

with *minor* as its highest severity alarm and NE 1 with *critical* as its highest severity alarm. Therefore the root group will report a *critical* alarm.

Each time a new alarm is reported by an NE or an existing alarm changes its state, the following process must be followed:

- Calculate the new group status of the parent group.
- If this group status has changed, calculate the group status of the parent group of the parent group (the grandparent group) and so on.

The process will finish when the group status of a group remains unchanged or the root group is reached.

Moving groups

A group can be moved between parent groups. All the items included in the group are also moved. There are two constraints to this feature:

- The new parent group cannot be a descendant of the group to be moved to avoid inconsistencies.
- The group name of the group being moved is not allowed to exist in the new parent group.

After having moved a group, both old and new parent groups check if their group status have changed. If a group status has changed, the system will rebuild the group status for both parent groups and for the groups above them in the tree hierarchy of groups.

5.4.2 NEs management

Group identifier

NEs management involves the addition of a new NE to the set of NEs that can be managed by the AEM as well as the deletion and edition of their attributes. It also involves the movement of an NE from an old group to a new group.

The user can create NEs within the groups. The NEs are also represented by an icon and coordinates to situate it on the background map of the parent group. Each NE must therefore have the following parameters when being created:

- NE name: This identifier must be unique in the whole tree.
- NE icon: to graphically identify the NE when displaying the items of its parent group.
- Domains
- NE coordinates: to specify the position of the NE icon on the background map of its parent group.

The NE shows the highest severity of all the alarms it reports.

The NEs can be edited, deleted and moved. When an NE is moved from an old parent group to a new parent group, the group status of both parent groups must be updated.

5.4.3 Groups & NEs window

This window is used to create, edit and delete NEs and groups. The window is subdivided into two panes: Groups and NEs.

NOTE:
The windows shown in this chapter are merely meant as an example. The contents (text) within a window, as well as the window itself, may slightly differ from the window as shown on your system.

5.4.3.1 Group window

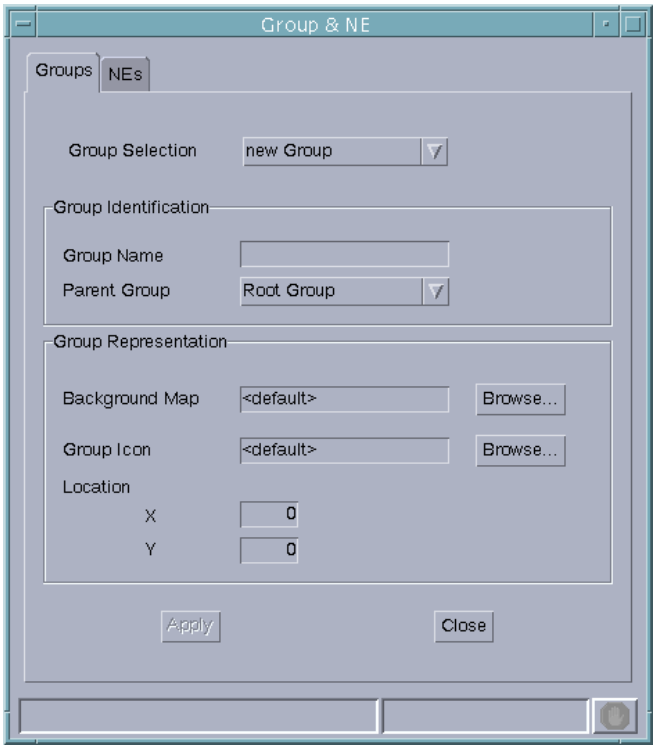


Figure 5-11 Groups & NEs window (tab Groups)

The following table shows the view/edit options of the group parameters:

Parameters/ Buttons	Description
Group Name Selection	This option menu shows all defined group names belonging to the user domain. The first option is NEW. If NEW is selected all parameters within the fields **Group Identification** and **Group Representation** are deleted for a new definition.
Group Identification	**Group Name**: This text field shows the selected group name or is empty if NEW is selected. **Parent Group**: This option menu shows all defined group names of the system. One of them must be selected to enable the creation of a subordinate group.
Group Representation	**Background Map**: This text field is used to enter the path to the map related to the group. ***Browse...***: This button is used to open the *File Browser* window in order to select the background map. **Group Icon**: This text field is used to enter the path to the icon related to the group. ***Browse...***: This button is used to open the *File Browser* window in order to select the icon. **X-Coord**: This text field is used to set the x coordinate to locate the icon on the background map of the parent group. **Y-Coord**: This text field is used to set the y coordinate to locate the icon on the background map of the parent group.
Apply	This button is used to confirm the changes. The button is available only if the **Group Name** is present.

5.4.3.2 Create/modify groups

Procedure Complete the following procedure to create/modify a group:

Step	Procedure
1.	Select the group in the Network Browser or on the background map and ***New*** or ***Edit*** via the cursor menu or select ***File -> New*** or ***View -> Object*** via the menu bar or click on the open icon in the tool bar. The *Groups & NEs* window (tab Groups) pops up (cf. Figure 5-11, page 5-29).

If you want to ...	then ...
edit the parameters of an existing group	use the option menus **Group Name Selection** and **Group Identification** to select the desired group, edit the parameters in the field **Group Representation** and press ***Apply***.
create a new group	use the option menu **Group Name Selection** to select the NEW option, enter an appropriate name in the text field **Group Name**, use the option menu **Parent Group** to select the desired parent group, define the parameters in the field **Group Representation** and press ***Apply***.

2. Click on ***Close*** to exit the window.

5.4.3.3 Delete a group

Procedure Complete the following procedure to create/modify a group:

Step	Procedure
1.	Select the group in the Network Browser or on the background map and click on ***Remove*** in the cursor menu or select ***File -> Remove*** via the menu bar or click on the remove icon in the tool bar. A *Warning* window pops up displaying the following message: **`You are about to delete Group Name. Do you want to continue?`**
2.	Enter ***y*** and press ***Return*** to confirm.

5.4.3.4 NEs window

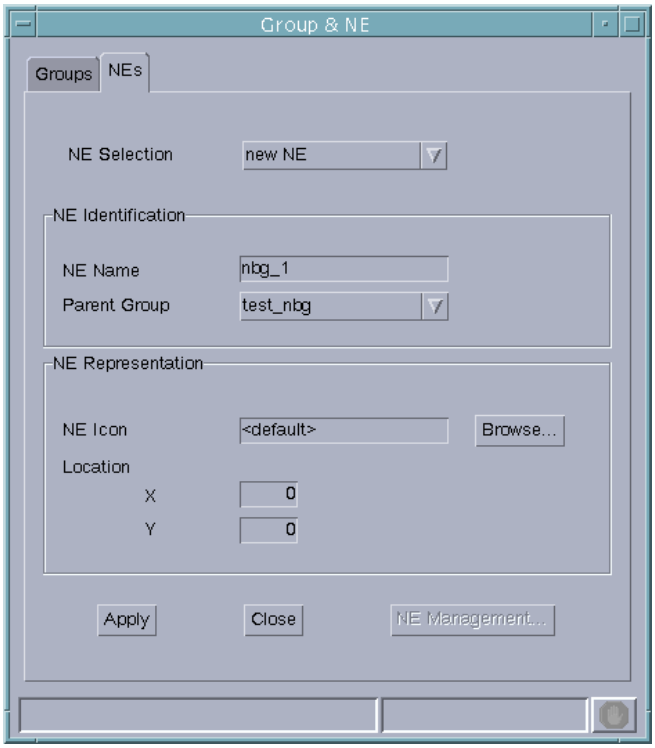


Figure 5-12 Groups & NEs window (Tab NEs)

The following table shows the view/edit options of the NE parameters:

Parameters/ Buttons	Description
NE Selection	This option menu shows all defined NEs belonging to the user domain. The first option is NEW. If NEW is selected all parameters within the fields **NE Identification** and **NE Representation** are deleted for a new definition.
NE Identification	**NE Name**: This text field shows the selected NE name or is empty if NEW is selected. **Parent Group**: This option menu shows all defined group names of the system. One of them must be selected to enable the creation of a subordinate group or NE.

Parameters/ Buttons	Description
NE Representation	**NE Icon**: This text field is used to enter the path to the icon related to the NE. ***Browse...***: This button is used to open the *File Browser* window in order to select the icon. **X-Coord**: This text field is used to set the x coordinate to locate the icon on the background map of the parent group. **Y-Coord**: This text field is used to set the y coordinate to locate the icon on the background map of the parent group.
Command buttons	***Apply***: This button provides access to the *Domain Selection* window (cf. Figure 5-14, page 5-38) to include the NE in one or several domains. The button is available only if the NE name is present. ***NE Management...***: This button provides access to the *NE Management* window (cf. Figure 5-15, page 5-39) to configure the selected NE.

5.4.3.5 Create/modify NEs

Complete the following procedure to create/modify an NE:

Step	Procedure

1. Select the ***NE*** in the Network Browser or on the background map and ***New*** or ***Edit*** via the cursor menu
or select ***File -> New*** or ***View -> Object*** via the menu bar
or click on the Open icon in the tool bar.
The *Groups & NEs* window (tab NEs) pops up (cf. Figure 5-12, page 5-32).

If you want to ...	then ...
edit the parameters of an existing NE	use the option menus **NE Name Selection** and **NE Identification** to select the desired NE, edit the parameters in the field **NE Representation** and press ***Apply***.
create a new NE	use the option menu **NE Selection** to select the NEW option, enter an appropriate name in the text field **NE Name**, use the option menu **Parent Group** to select the desired parent group, define the parameters in the field **NE Representation** and press ***Apply***. The *Domain Selection* window pops up (cf. Figure 5-14, page 5-38).
configure the NE	click on ***NE Management...***. The *NE Management* window pops up (cf. Figure 5-15, page 5-39).

2. Click on ***Close*** to exit the window.

5.4.3.6 Remove an NE

Select the ***NE*** in the Network Browser or on the background map and click on ***Remove*** in the cursor menu
or select ***File -> Remove*** via the menu bar
or click on the remove icon in the tool bar.

5.5 Equipment configuration

Overview

Configuration of specific equipment data is the process of preparing the AEM for control of the *AnyMedia* Access System by configuring and setting the required parameters.

First the AEM must have some knowledge of the equipment. The AEM gets this data during the NE creation process, which is usually followed by pack configuration.
Then, during NE management, some other tasks regarding equipment configuration can be performed by the AEM, e.g. date & time management, timing synchronization management, protection management, etc.
Finally, if the NE is no longer managed by the AEM, it is deleted from the AEM database.

Provisioning model

The *AnyMedia* Access System uses a provisioning model to provide service, which means that the circuit must be prepared to provide service by defining its function and setting of required options. For example, for creation of a service for a subscriber line it is first necessary to provision the corresponding application pack (AP).

AP provisioning set up a desired pack type in a desired slot. To be fully functional an AP must not only be inserted but also provisioned, and the provisioned pack type must fit the actual type of the inserted pack. A pack can be provisioned and configured by the AEM even when the slot is still empty.

The equipment configuration description is divided into three main sections:

- Add a network element (cf. Chapter 5.5.1, page 5-37)
- Edit/view configuration data (cf. Chapter 5.5.5, page 5-55)
- Delete the network (cf. Chapter 5.5.19, page 5-171).

Screen navigation

Figure 5-13, page 5-36 shows an overview of the screen navigation for equipment configuration. In this figure it is assumed that the NE is already connected (cf. Chapter 5.5.1, page 5-37).

Examples

To open the *COMDAC Shelf Protection* window proceed as follows:

- Select ***NE -> Main Shelf -> COMDAC*** via the Network Element Browser and select ***Protection*** via the cursor menu or
- Select ***NE -> Main Shelf -> COMDAC*** via the Network Element Browser, open the *COMDAC* window by means of the menu bar (***View -> Object***) or by means of the tool bar (open icon)
  and click on the ***COMDAC Protection...*** button in the COMDAC window.

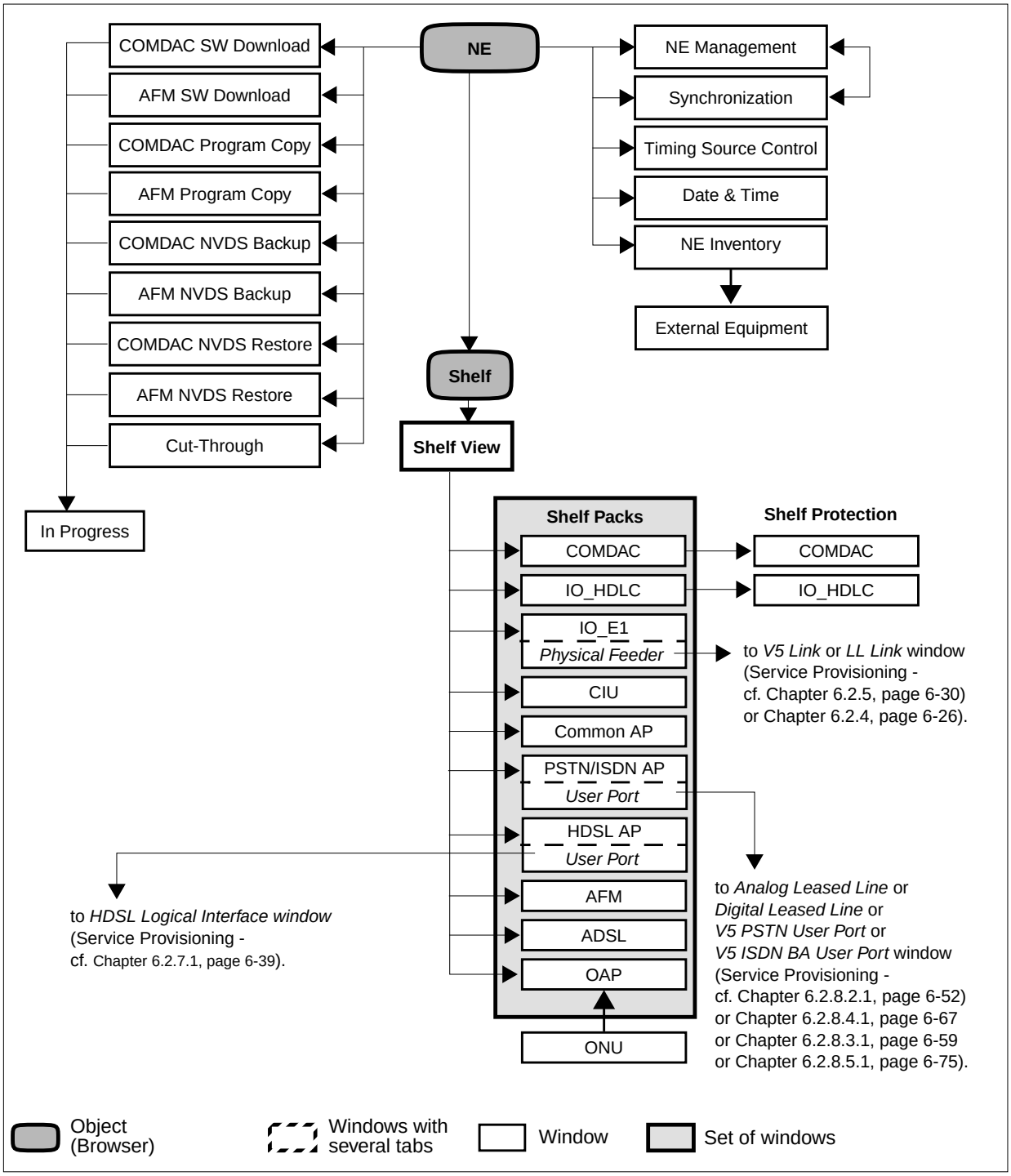


Figure 5-13 Screen navigation for equipment configuration

5.5.1 Add a network element

The following steps are necessary to add an NE:

- Create NE
- Assign domain.

Requirements

To add an NE the following requirements must be fulfilled:

- The PC-based GSI is used to set the NE to a state where NVDS (non-volatile data storage) is populated with the minimum values (i.e. target id, IP address, user id).
- All these parameters are assumed to be known by the user.
- The data communication network (DCN) link with the NEs is available (cf. Appendix A).
- Domains are already created (cf. Chapter 4.3.1, page 4-8).

NOTE:
The windows shown in this chapter are merely meant as an example. The contents (text) within a window, as well as the window itself, may slightly differ from the window shown on your system.

Procedure

Complete the following procedure to add an NE.

Step	Procedure
1.	Select the NE in the Network Browser or on the background map and ***New*** or ***Edit*** via the cursor menu or select ***File -> New*** or ***View -> Object*** via the menu bar or click on the open icon in the tool bar. The *Groups & NEs* window (tab NEs) pops up (cf. Figure 5-12, page 5-32).
2.	Fill in all NE information for a new NE as described in Chapter 5.4.3.5, page 5-34.
3.	Press ***Apply*** to confirm. The *Domain Selection* window pops up.

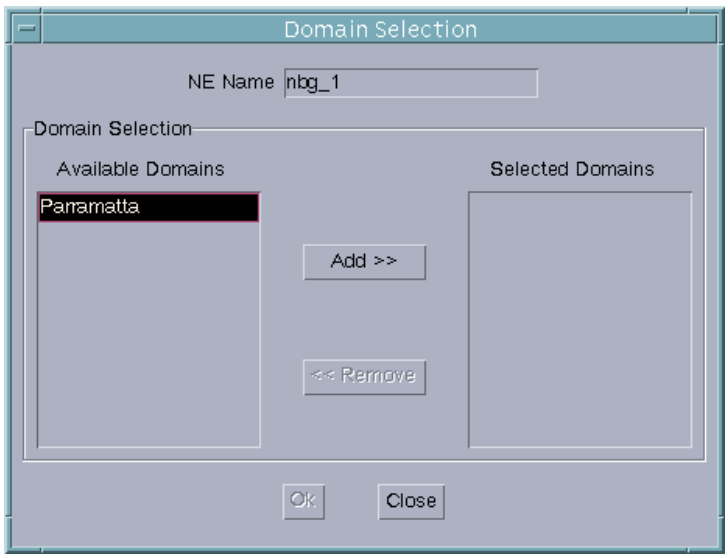


Figure 5-14 Domain Selection window

Assign domain

At creation time, the NE must be included in one or more domains (for domain creation see Chapter 4).

The *Domain Selection* window consists of two lists: **Available Domains** and **Selected Domains**. The window provides the facilities needed to select the domains from which the NE will be accessible.

4. Use the ***Add >>*** button to move the selected domain from the **Available Domains** list to the **Selected Domains** one. Use ***<< Remove*** to remove domains from the **Selected Domains** list.
(The ***Add >>*** button and the ***<< Remove*** button are available only after having selected a domain name from the corresponding list.)

5. Press ***OK*** to confirm. The NE is assigned to the selected domains and the *Domain Selection* window is closed.

NOTE:
If you decide to close this window (via ***Cancel*** or window controls), a *Warning* window pops up informing you of the possible rejection of the NE creation:

```
At least 1 domain must be selected and confirmed.
Otherwise the NE creation operation will be rejected.
Do you want to go back to Domain Selection?
```

If you select ***No***, the creation of the NE is rejected. Otherwise, the *Domain Selection* window is activated. The window remains on the screen until you make a decision.

The ***NE Management...*** button is now enabled.

6. Press the ***NE Management...*** button. The *NE Management* window pops up.

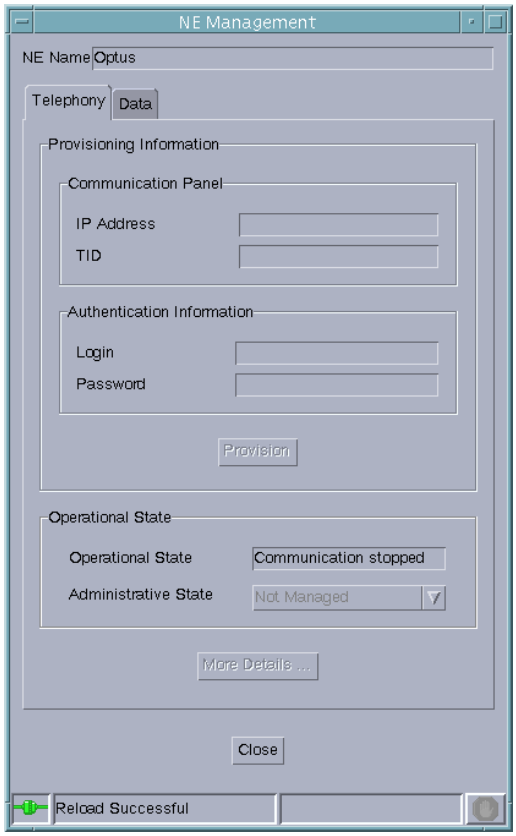


Figure 5-15 NE Management window (tab Telephony)

The following steps describe the procedure for the telephony agent. The procedure for data agents is similar. The corresponding window (*NE Management*, tab Data) is described in Chapter 5.5.3.3, page 5-46.

NE provisioning data

7. Enter the **IP Address** and **TID** (Target ID, the name of the NE to which the connection is addressed) of the new NE in the field **Communications Info**. IP Address format: xxx.xxx.xxx.xxx; where x is a numeric [0, 9]; the TID has a range from 1 to 20 characters.

NOTE:
Once the connection is established, these fields cannot be edited unless the connection is interrupted.

8. Enter the **Login** and **Password** in the **Authentication Information** field.

NOTE:
Once the connection is established, these fields cannot be edited unless the connection is interrupted.

The ***Provision*** button becomes available when the **Communications Info** and/or the **Authentication Information** fields have been changed.

9. Click on the ***Provision*** button.

   Once the NE is provisioned, the **Administrative State** becomes available.

10. Change the **Administrative State** to Managed.

    The AEM starts the connection and synchronization processes with the NB agent. The progress of these processes can be watched in the field **Operational State**.
    Possible values are: Communication Stopped, Communication Stopped (Releasing), Communication Trying, Communication Trying (Problem Detected), Communication Established, Communication Established (Synchronizing).

    When the **Administrative State** has been changed to Managed the ***More Details...*** button becomes available.

11. Click on ***More Details...*** to open the *Synchronization* window (cf. Chapter 5.5.6, page 5-123) in order to view or modify the synchronization data.

Edit and provisioning actions are only possible once the connection is established. Only in this case can the NE be displayed in the browsers and on the background map.

5.5.2 Connection states AEM - telephony agent

There are three AEM - telephony agent connection states:

- **NOT_CONNECTED**

  Initial connection state when there is no connection between AEM and the telephony agent and the AEM is in a "passive" state avoiding any possibility of connection establishment with the telephony agent.

- **TRYING**

  Initial connection state when the TL1 communication session between the AEM and the telephony agent is not available but the AEM is in an "active" state trying to open a connection with the telephony agent.

- **CONNECTED**

  The connection between the AEM and the telephony agent is available and the software version currently stored in the telephony agent is supported by the AEM. When the association process between the AEM and the data agent is completed, the telephony agent state changes to CONNECTED and remains like this until the TL1 communication session is closed on user request or the connection is lost/closed.

5.5.2.1 Changing connection states

The connection state changes can be initiated by the user via the GUI (cf. Chapter 5.5.1, page 5-37, section Add a network element) or they are initiated by the AEM.

Communication The AEM communicates with the telephony agent by using TL1 commands and file transfer protocol (FTP) over TCP/IP.

Not connected The user can initiate the connection establishment process with an telephony agent in connection state NOT_CONNECTED. After initiating this process the connection state changes to TRYING.

Trying When the connection state is TRYING, the AEM tries to establish a connection with the telephony agent. After the successful connection the AEM checks if the AEM supports the software version of the telephony agent. If the software version is supported the connection state becomes CONNECTED, if not it remains TRYING and the AEM continues its attempts to establish a connection. The user can cancel these attempts via the GUI, which will change the connection state to NOT_CONNECTED.

Connected The user can request to close a TL1 communication session with a telephony agent via the GUI. When the communication session is closed by the AEM, the connection state is changed to NOT_CONNECTED. When the connection state is CONNECTED and the connection is lost, the connection state becomes TRYING. If a TL1 communication session loss is detected and the TCP/IP connection is still established, the AEM closes the TCP/IP connection and the connection state also becomes TRYING.

5.5.2.2 Association maintenance

Association An association between the AEM and an telephony agent is established if the TCP/IP connection and the TL1 communication session is open. The connection state changes to CONNECTED.

Agent monitoring The AEM monitors the association state of the telephony agent by periodically sending messages to the telephony agent. If the AEM does not receive a response to a certain number of messages within a certain time, it assumes that the connection to the telephony agent is lost and tries to connect to the telephony agent again.

Default values for monitoring

By default these messages are sent by the AEM every five minutes. The response to a message must be received within four minutes and not more than two responses may be lost, otherwise the connection is closed by the AEM.

These values can be configured by the user via the system variables "NEM.association.heartBeatNumber" and "NEM.association.heartBeatTime" in the file $ANYMEDIAPATH/cfg/AnyMediaEM.cfg.

5.5.2.3 NE Management window (tab Telephony)

This window shows the provisioning information and allows the provisioning and deprovisioning of an NE (telephony agent).

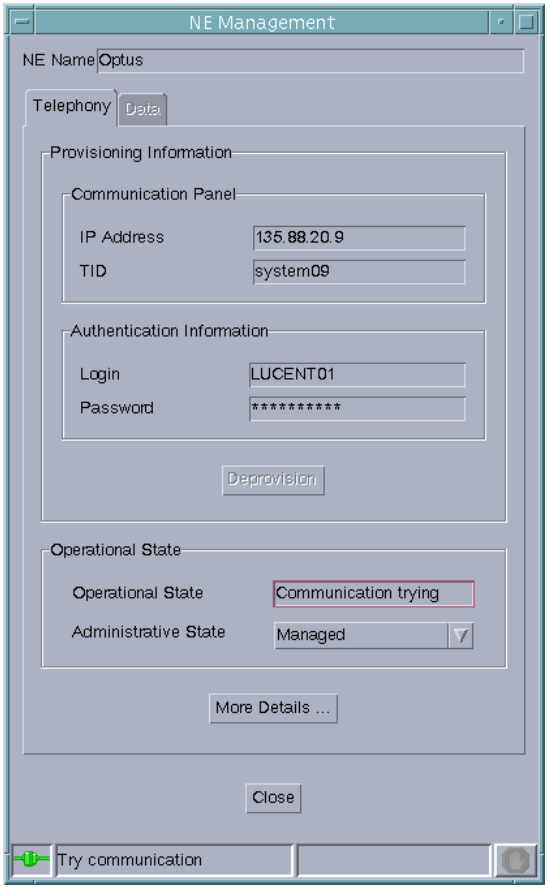


Figure 5-16 NE Management window (tab Telephony)

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Provisioning Information	Once the connection is established, the following fields cannot be edited unless the connection is interrupted (administrative state = Not Managed). **Communications Info**: This field contains the editable text fields **IP Address** and **TID**. This information is mandatory to get a AEM-NE connection. **Authentication Information**: This field contains the text fields **Login** and **Password**. This information is also mandatory to get a AEM-NE connection. The ***Label*** button is used to provision/deprovision the NE. ***Provision***: If the NE is not provisioned or any value has been changed. Provisioning is enabled only if the administrative state is Not Managed (see below). ***Deprovision***: If the NE has been provisioned and no value has been changed.
Operational State	The option menu **Administrative State** shows the possible values: Managed, Not Managed. This option menu is disabled if the telephony agent is not provisioned. The text field **Operational State** shows the current connection state. Possible values: Communication Stopped, Communication Stopped (Releasing), Communication Trying, Communication Trying (Problem Detected), Communication Established, Communication Established (Synchronizing).
More Details...	This button provides access to the *Synchronization Telephony* window (cf. Chapter 5.5.6.1.3, page 5-124). It is available only if the administrative state of the agent is Managed.

5.5.2.4 Modify NE Management data (telephony agent)

Procedure Complete the following procedure to manage an NE (telephony agent).

Step	Procedure

1. Select ***NE*** in the Network Browser or in the background map and ***NE Management*** via the cursor menu. The *NE Management* window pops up.

   This window can also be reached from the *Groups & NEs* window (tab NEs) by clicking on ***NE Management...*** (cf. Chapter 5.4.3, page 5-29).

If you want to ...	then ...
provision the NE	enter or change the values for **IP Address**, **TID**, **Login** or **Password** in the Provisioning Information field and press ***Provision***.
deprovision an provisioned NE	click on ***Deprovision*** in the Provisioning Information field.
change the administrative state	use the corresponding option menu in the Operational State field.
show/edit the synchronization data	click on ***More Details...***.
exit the window	click on ***Close***.

5.5.3 Communication states AEM - data agent

There are three general AEM - data agent communication states:

- **Communication Stopped**

  Initial communication state when there is no communication between AEM and the data agent.

- **Communication Trying**

  The AEM is in an "active" state trying to start the communication with the data agent.

- **Communication Established**

  The AEM and the data agent are able to communicate with each other.

The three described states can be divided in six AEM - data agent communication states as follows:

- **COMM_STOPPED**

  Initial connection state when there is no connection between AEM and the data agent and the AEM is in a "passive" state avoiding any possibility of communication establishment with the data agent.

- **COMM_TRYING**

  The AEM is in an "active" state trying to start a communication with the data agent by sending SNMP PDUs.

- **COMM_TRYING_PROBLEM_DETECTED**

  The AEM has detected a failure in the communication process.

- **COMM_ESTABLISHED**

  The AEM and the data agent are able to communicate with each other. The AEM is able to request data to the data agent and the data agent is able to respond to AEM queries and to send traps to the EM.

- **COMM_ESTABLISHED_SYNCHRONIZING**

  The EM is trying to update its internal information by uploading data from the BB agent.

- **COMM_STOPPED_RELEASING**

  The EM is deleting all the information related to the communication being stopped.

COMM_STOPPED and COMM_STOPPED_RELEASING are sub-states of the general state Communication Stopped.
COMM_TRYING and COMM_TRYING_PROBLEM_DETECTED are sub-states of the general state Communication Trying.
COMM_ESTABLISHED and COMM_ESTABLISHED_SYNCHRONIZING are sub-states of the general state Communication Established.

5.5.3.1 Changing connection states

The connection state changes can be initiated by the user via the GUI or they are initiated by the AEM.

Communication protocol The communication protocol used between the AEM and the data agent is simple network management protocol (SNMP) over user datagram protocol (UDP/IP).

COMM_STOPPED The user can initiate the communication establishment process with a data agent in connection state COMM_STOPPED. After initiating this process the connection state changes to COMM_TRYING.

COMM_TRYING When the communication state goes COMM_TRYING, the AEM tries to establish a connection with the data agent by sending a SNMP PDU. After the successful connection the AEM checks if the AEM supports the software version of the data gent. If the software version is supported the connection state becomes COMM_ESTABLISHED. If the received data from the data agent contains invalid data the state becomes COMM_TRYING_PROBLEM_DETECTED and the whole communication process will be repeated when a timer expires.

COMM_ESTABLISHED

When the communication state is COMM_ESTABLISHED, COMM_ESTABLISHED_SYNCHRONIZING or COMM_TRYING and the user request to finish the communication with the data agent the communication state becomes COMM_STOPPED_RELEASING. The AEM deletes all the data related to the communication and the state is moved to COMM_STOPPED.

When the communication state is COMM_ESTABLISHED or COMM_ESTABLISHED_SYNCHRONIZING and the AEM detects the loss of communication with the data agent the communication state becomes COMM_TRYING. The AEM starts the process to re-establish the communication with the data agent.

The user can request to close a connection with an NE via the GUI. When the communication session is closed by the AEM, the connection state is changed to NOT_CONNECTED. When the connection state is CONNECTED and the connection is lost, the connection state becomes TRYING. If a communication session loss is detected and the connection is still established, the AEM closes the connection and the connection state also becomes TRYING.

5.5.3.2 Association maintenance

Association

An communication between the AEM and an data agent is established if the AEM can send SNMP input commands and can receive SNMP output commands to/from the data agent for management purposes. The connection state is COMM_ESTABLISHED.

Agent monitoring

The AEM monitors the communication state with the data agent by periodically sending messages to the data agent. If the AEM does not receive a response to a certain number of messages within a certain time, it assumes that the connection to the data agent is lost and tries to connect to the data agent again.

Default values for monitoring

By default these messages are sent by the AEM every five minutes. The response to a message must be received within four minutes and not more than two responses may be lost, otherwise the connection is closed by the AEM.

These values can be configured by the user via the system variables "NEM.association.heartBeatNumber" and "NEM.association.heartBeatTime" in the file $ANYMEDIAPATH/cfg/AnyMediaEM.cfg.

5.5.3.3 NE Management window (tab Data)

This window shows the provisioning information and allows the provisioning and deprovisioning of an NE (data agent).

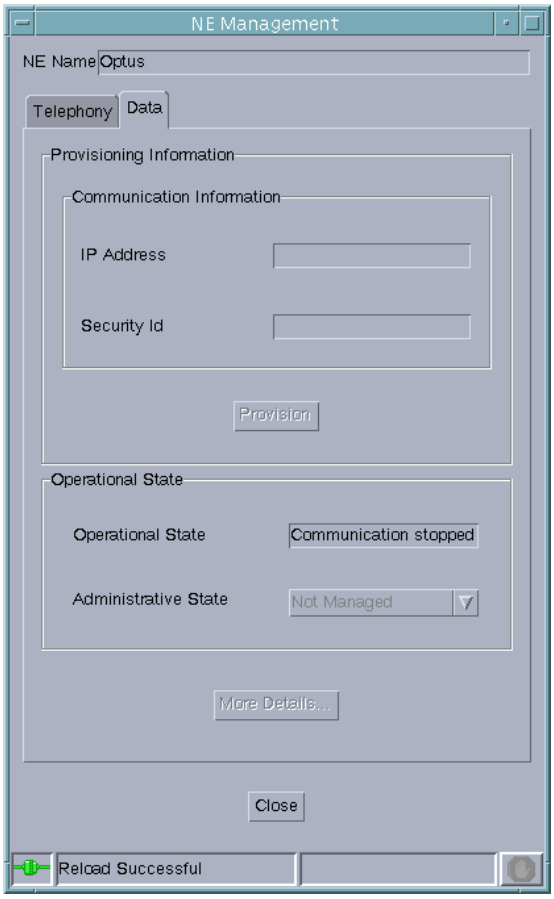


Figure 5-17 NE Management window (tab Data)

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Provisioning Information	Once the connection is established, the following fields cannot be edited unless the connection is interrupted (administrative state = Not Managed). **Communications Info**: This field contains the editable text field **IP Address**. This information is mandatory to get a AEM-NE connection. Format: xxx.xxx.xxx.xxx; where x is a numeric [0, 9]. **Authentication Information**: This field contains the text field **Security Id**. This information is also mandatory to get a AEM-NE connection. The Security Id has a range from 3 to 10 characters. The ***Label*** button is used to provision/deprovision the NE. ***Provision***: If the NE is not provisioned or any value has been changed. Provisioning is enabled only if the administrative state is Not Managed (see below). ***Deprovision***: If the NE has been provisioned and no value has been changed.
Operational State	The option menu **Administrative State** shows the possible values: Managed, Not Managed. The text field **Operational State** shows the current connection state. Possible values: Communication Stopped, Communication Stopped (Releasing), Communication Trying, Communication Trying (Problem Detected), Communication Established, Communication Established (Synchronizing).
More Details...	This button provides access to the *Synchronization Data* window (cf. Chapter 5.5.6.2.3, page 5-127). t is available only if the Administrative State of the agent is Managed.

5.5.3.4 Modify NE Management data (data agent)

Procedure Complete the following procedure to manage an NE (data agent).

Step	Procedure

1. Select ***NE*** in the Network Browser or in the background map and ***NE Management*** via the cursor menu. The *NE Management* window pops up.

   This window can also be reached from the *Groups & NEs* window (tab NEs) by clicking on ***NE Management...*** (cf. Chapter 5.4.3, page 5-29).

If you want to ...	then ...
provision the NE	enter or change the values for **IP Address** or **Security Id** in the Provisioning Information field and press ***Provision***.
deprovision an provisioned NE	click on ***Deprovision*** in the Provisioning Information field.
change the administrative state	use the corresponding option menu in the Operational State field.
show/edit the synchronization data	click on ***More Details...***.
exit the window	click on ***Close***.

5.5.4 Shelf View

The purpose of this window is to provide a simple graphical representation of the NE shelf.

Procedure

Complete the following procedure to display the shelf view:

Step	Procedure
1.	Select ***NE -> Main Shelf*** in the Network Element Browser and ***View*** via the cursor menu or select ***View -> Object*** via the menu bar. The *Shelf View* window pops up.

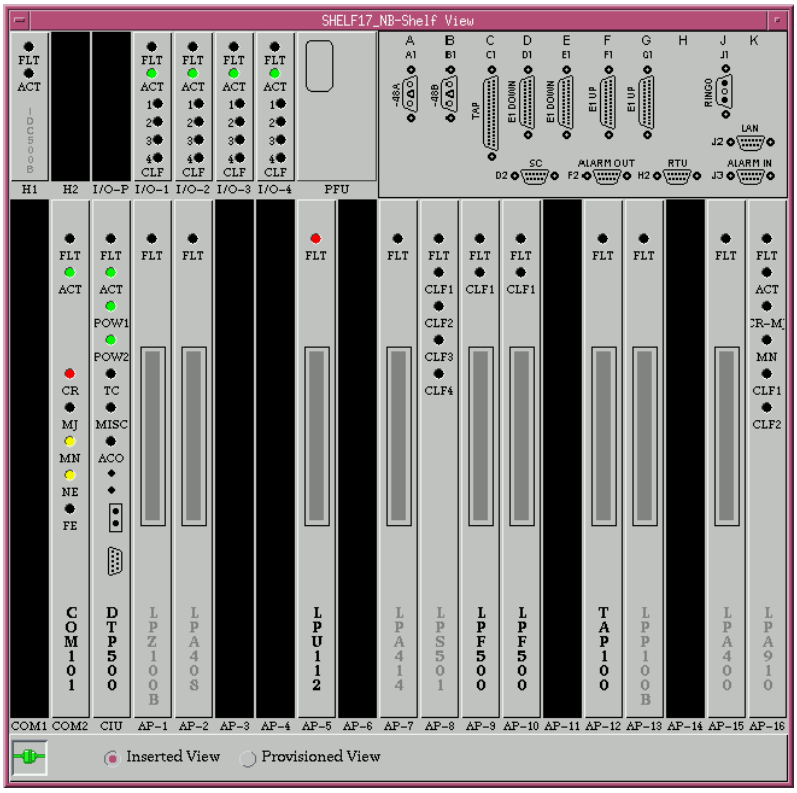
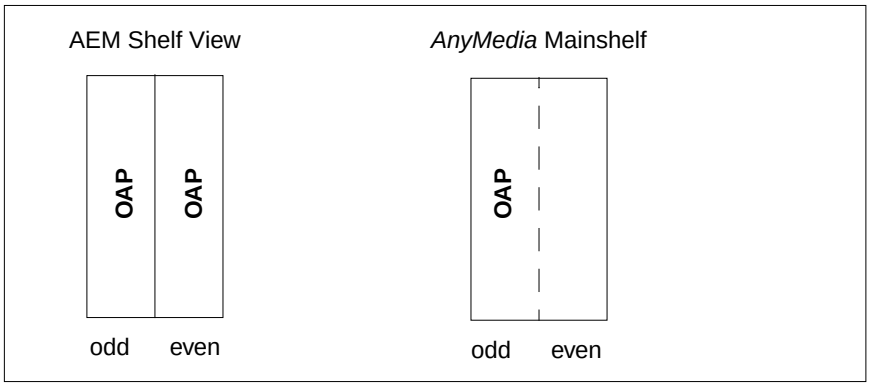


Figure 5-18 Shelf View window

This window provides general inventory information as well as provisioning and alarm information (through the LEDs). Each slot will show either the apparatus code of the inserted card (default view) or the apparatus code provisioned in that slot (provisioned view) or otherwise no apparatus code. If the slot is empty, no card will be shown, otherwise, the slot will display the faceplate of the inserted card with its LEDs (if applicable).

Single clicking on any slot will launch the card-specific window even when the card is not inserted.

NOTE:
For OAPs the shelf view displays the same faceplate (duplicated) for the two slots where the OAP is inserted (even and odd slots).



When the user selects the odd slot the *ONU AP* window pops up (cf. Chapter 5.5.5.18, page 5-89) displaying the even slot number in the Slot Id field. In case of mismatch between the COMDAC view and the AFM view the odd slot number will be displayed.

The following tables shows the related sections where the packs are described:

Card Type	Apparatus Code	Described in ...
COMDAC	COM500 (NE R1.3) COM501 (NE R1.4)	Chapter 5.5.5.5, page 5-62
CIU	DTP500	Chapter 5.5.5.6, page 5-64
IO_HDLC	IDC500	Chapter 5.5.5.8, page 5-68
IO_E1	FAC500	Chapter 5.5.5.2, page 5-57
HDSL	LPS501	Chapter 5.5.5.16, page 5-84
AFME3	LPA910	Chapter 5.5.5.21, page 5-94
OAP	LPF500	Chapter 5.5.5.18, page 5-89
OCP	CPF500	Chapter 5.5.5.20, page 5-92
PSTN/ISDN AP	LPZ100, LPP100, LPU112, LPU430 (NE R1.4)	Chapter 5.5.5.14, page 5-80
ADSL	LPA400B, LPA408	Chapter 5.5.5.27, page 5-105

The *Shelf View* window displays different colors for different types of LEDs. The following table describes the colors that are used for each LED type inside every

card type. The table describes the colors used when the LED is ON or flashing. If the LED is OFF, the color black is used.

Table 5-1 LED meanings

Pack	LED	Color	Meanings
IO_E1	FLT	red	■ Lit during pack failure. ■ Flashes when the pack executes off-line self-test.
	ACT	green	Lit when the pack is service-active.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 4.
COMDAC	FLT	red	■ Lit when a fault is detected on the pack. ■ Flashes during software download and turn-up.
	ACT	green	Indicates that this COMDAC is active.
	CR	red	Lit when the highest severity alarm is critical.
	MJ	red	Lit when the highest severity alarm is major.
	MN	yellow	Lit when the highest severity alarm is minor.
	NE	yellow	Lit when the source of the fault or abnormal condition is near-end.
	FE	yellow	Lit when the source of the fault or abnormal condition is far-end.
CIU	FLT	red	Lit when a fault is detected on the pack.
	ACT	green	Lit when a test is in progress. Pack id in operation.
	POW1	green	Lit when -48V power supply A is in operation.
	POW2	green	Lit when -48V power supply B is in operation.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	ACO	green	Alarm Cut-off reminder

Table 5-1 LED meanings

Pack	LED	Color	Meanings
IO_HDLC	FLT	red	■ Lit when a fault is detected on the pack. ■ Flashes when the pack executes off-line shelf-test.
	ACT	green	Lit when the pack is service-active.
APs	FLT	red	■ Lit when a fault is detected on the AP. ■ Flashes when the AP executes off-line shelf-tests.
HDSL	FLT	red	Lit when a fault is detected on the pack.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 4.
OAP	FLT	red	Lit when a fault is detected on the pack.
	CFL	yellow	Lit when a fault or facility alarm occurs.
OCP	FLT	red	Lit when a fault is detected on the pack.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	CLF	yellow	Lit when a fault or facility alarm occurs.
AFM	FLT	red	Lit when a fault is detected on the pack.
	ACT	green	Indicates that this AFM is active.
	CR-MJ	red	Lit when the highest severity alarm is critical or major.
	MN	yellow	Lit when the highest severity alarm is minor.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.

See Chapter 7.2, page 7-1 for more details about alarm handling.

For cards which need to be provisioned (APs and IO_HDLCs) it is necessary to represent the slot state since the provisioned data may be different to the inserted card. There are two possible views of this window:

- Inserted view (apparatus codes of inserted cards are shown)

- Provisioned view (apparatus code of the provisioned cards is shown).

The user can switch between the two views via two check boxes located below the shelf view of this window.

The following table describes the representation of the different slot states:

Slot state	Description and representation	Inserted view		Provisioned view	
		Pack	Label	Pack	Label
provisioned, inserted and match	The type of the provisioned card is the same as the type of the inserted card.	grey	black	grey	black
provisioned, inserted and mismatch	The type of the provisioned card is different from the type of the inserted card.	grey	dark grey	grey	dark grey
provisioned and not inserted	The operator has provisioned this slot associating it to a type of card but no card is inserted in the slot.	black	-	black	white
not provisioned and inserted	No card type is preprovisioned in the slot but a card is inserted.	grey	dark grey	grey	-
not provisioned and not inserted	No card type is provisioned and no card is inserted in the slot.	black	-	black	-
provisioned, not inserted and agent type mismatch	No card is provisioned, no card is inserted in the slot and there is mismatch between the telephony and the data agent.	black	-	black	grey

NOTE:
"Pack" refers to the slot faceplate, "Label" refers to the apparatus code.

NOTE:
The NE does not send the "match" indication for a provisioned data AP. The shelf view therefore indicates "provisioned, inserted and mismatch" until a re-sync is done.

5.5.5 Configuration of the packs

5.5.5.1 IO_E1 window

The IO_E1 pack provides four physical E1 interfaces to accommodate telephony via standard V5 network interfaces.

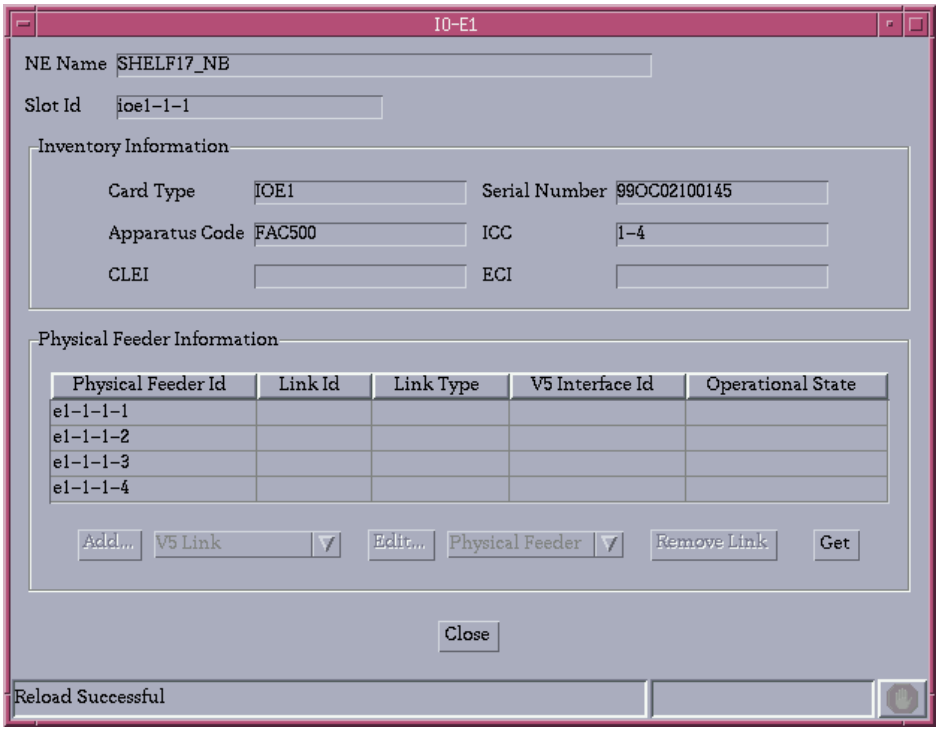


Figure 5-19 IO_E1 window

This window can be displayed even when the pack is not inserted.

The following table shows the view/edit options of the *IO_E1* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	This field displays the slot being used. Possible values: ioe1-{1}-{1,4}.

Parameters/ Buttons	Description
Inventory Information	The following fields are empty if no pack is inserted. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible value: IO_E1. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: FAC500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI** and **ECI**: Not applicable.
Physical Feeder Information	The information in this field is displayed in a table (4 rows, one per E1): ■ **Physical Feeder Id**: Physical address of the E1 feeders. Format: e1-shelf-slot-port. Possible values: e1-1-{1, 4} -{1, 4}. ■ **Link Id**: This id is used to identify the V5 links. V5 link format: {0, 255} Leased line link format: {1, 16}. ■ **Link Type**: Indicates the type of the link: V5 Link, Leased Line Link. ■ **V5 Interface id**: The V5 Interface id is displayed (if present): {0, 16777215} in dec format or {0, FFFFFF} in hex format. ■ **Operational State**: Shows the current operational state of the physical drop by using of the ***Get*** button. The ***Add*** button provides access to the *V5 Link* window or *Leased Line Link* window depending on the selected value in the option menu. The button is available only when a free feeder has been selected. The ***Edit...*** button provides access to the *Physical Feeder* window or *V5 Link* window or *Leased Line Link* window depending on the selected value in the option menu. Which values are enabled in the option menu depends on the selected list entry. The ***Remove Link*** button can be used to remove a link associated to an E1 feeder.

5.5.5.2 Configure an IO_E1

Procedure Complete the following procedure to modify the IO_E1 data:

Step	Procedure

1. Select ***NE -> Main Shelf -> FAC500*** in the Network Element Browser and ***View*** via the cursor menu
or select ***View -> Object*** via the menu bar
or single click on the pack ***IO_E1*** in the *Shelf View* window.
The *IO_E1* window pops up.

If you want to ...	then ...
edit a physical feeder	select the desired row in the **Physical Feeder Information** list, use the option menu near the ***Edit...*** button to select **Physical Feeder** and press ***Edit...*** or double-click on the row. The *Physical Feeder* window pops up (cf. Chapter 5.5.5.3, page 5-59).
edit a leased line link	select a row in which a physical feeder is already associated with a leased line link, use the option menu near the ***Edit...*** button to select **Leased Line Link** and press ***Edit...***. The *Leased Line Link* window pops up (cf. Chapter 6.2.4, page 6-26).
edit a V5 link	select a row in which a physical feeder is already associated with a V5 link, use the option menu near the ***Edit...*** button to select **V5 Link** and press ***Edit...***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30).
add a V5 link	select a row with a free physical feeder, use the option menu near the ***Add*** button to select **V5 Link** and press ***Add***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30).
add a leased line link	select a row with a free physical feeder, use the option menu near the ***Add*** button to select **Leased Line Link** and press ***Add***. The *Leased Line Link* window pops up (cf. Chapter 6.2.4, page 6-26).

If you want to ...	then ...
delete a V5 link	select the appropriate row in the **Physical Feeder Information** list and press ***Remove Link...***. A *Warning* window pops up displaying the following message: **`Removing V5 Link id may be service affecting. Do you want to continue?`** If you decide to continue, the remove operation will be started.

2. Click on ***Close*** to exit the window.

5.5.5.3 Physical Feeder window

This window provides physical information about individual feeders and allows the E1 feeder parameters to be changed.

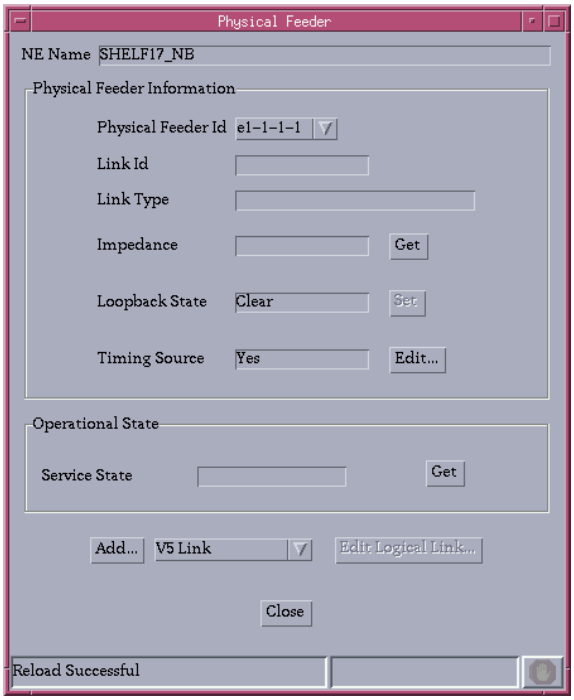


Figure 5-20 Physical Feeder window

The following table shows the view/edit options of the physical feeder parameters:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Feeder Information	**Physical Feeder Id**: This option menu is used to select the specific E1 feeder the user wants to display the information for. The list shows all E1 feeders present in the shelf. Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}. **Link id**: This field is empty when the E1 feeder is not associated to a V5 link or a leased line service. If the E1 feeder is associated to a V5 link the V5 link id is shown in this field. Possible values for V5 link: {0, 255}. Possible values for leased line link: {1, 16}. **Link Type**: This field indicates the type of the link: V5 Link, Leased Line Link or empty.

Parameters/ Buttons	Description
Physical Feeder Information (continued**)**	**Impedance**: Displays the impedance of the E1 feeder termination: 120 Ohm, 75 Ohm. The current value can be retrieved by using the ***Get*** button. **Loopback State**: This field displays the current loopback state (**Clear** or **Set**). This state can be modified via the ***Label*** button on the right-hand side. This button can be used to set or to clear the E1 loopback. Depending on the current state, this button displays the possible operation (***Clear*** if the loopback state is **Set** and ***Set*** if the loopback is **Clear**). NOTE: This button is disabled if the E1 feeder is used as timing source reference (see below). **Timing Source**: Indicates whether the selected E1 is the timing source reference or not. This reference can only be changed via the ***Edit...*** button on the right-hand side (see below). Possible values: Yes, No. ***Edit...***: This button provides access to the *Timing Source Control* window (cf. Chapter 5.2.1.2, page 5-3) to modify the current NE timing source reference.
Operational State	**Operational State**: Shows the current service state of the physical feeder. Possible values: Enabled, Disabled. The ***Get*** button can be used to get the current service state from the NE.
Command buttons	The ***Add*** button provides access to the *V5 Link* window or *Leased Line Link* window depending on the selected value in the option menu. The button is available only when a free feeder has been selected. The ***Edit Logical Link...*** button provides access to the *V5 Link* window or *Leased Line Link* window depending on the selected feeder.

5.5.5.4 Edit Physical Feeder

Complete the following procedure to edit the physical feeder data:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeders List* window pops up (cf. Chapter 6.2.3, page 6-24).

2. Select the desired physical feeder and click on ***Edit Physical Feeder***. The *Physical Feeder* window pops up.

   This window can also be reached from the *IO_E1* window (cf. Chapter 5.5.5.2, page 5-57) by clicking on ***Edit Physical Feeder***.

If you want to ...	**then ...**
modify the current timing source reference	use the option menu **Physical Feeder Id** to select the desired E1 feeder and press ***Edit...***. The *Timing Source Control* window pops up (cf. Chapter 5.5.7, page 5-129).
view the current operational state	use the option menu **Physical Feeder Id** to select the desired E1 feeder and press ***Get*** in the **Operational State** field.
add a V5 link	select a free physical feeder, use the option menu near the ***Add*** button to select **V5 Link** and press ***Add***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30).
add a leased line link	select a free physical feeder, use the option menu near the ***Add*** button to select **Leased Line Link** and press ***Add***. The *Leased Line Link* window pops up (cf. Chapter 6.2.4, page 6-26).
change the loopback state	use the option menu **Physical Feeder Id** to select an appropriate E1 feeder and click the ***Label*** button on the right-hand side of the Loopback field. NOTE: If the loopback state has been changed to "Set" a *Warning* window pops up: **`Setting Loopback for a feeder can be service affecting. Do you want to continue?`** Enter ***Yes*** to confirm (or ***No*** to reject).

3. Click on ***Close*** to exit the window.

5.5.5.5 View the COMDAC parameters

Overview

The COMDAC (Common Data and Control) pack performs the main bandwidth management and control functions for the system.

Procedure

Complete the following procedure to view the COMDAC data:

Step	Procedure
1.	Select ***NE -> Main Shelf -> COM500 (or COM501)*** in the Network Element Browser and ***View*** via the cursor menu or select ***View -> Object*** via the menu bar or single click on the pack ***COMDAC*** in the *Shelf View* window. The *COMDAC* window pops up.

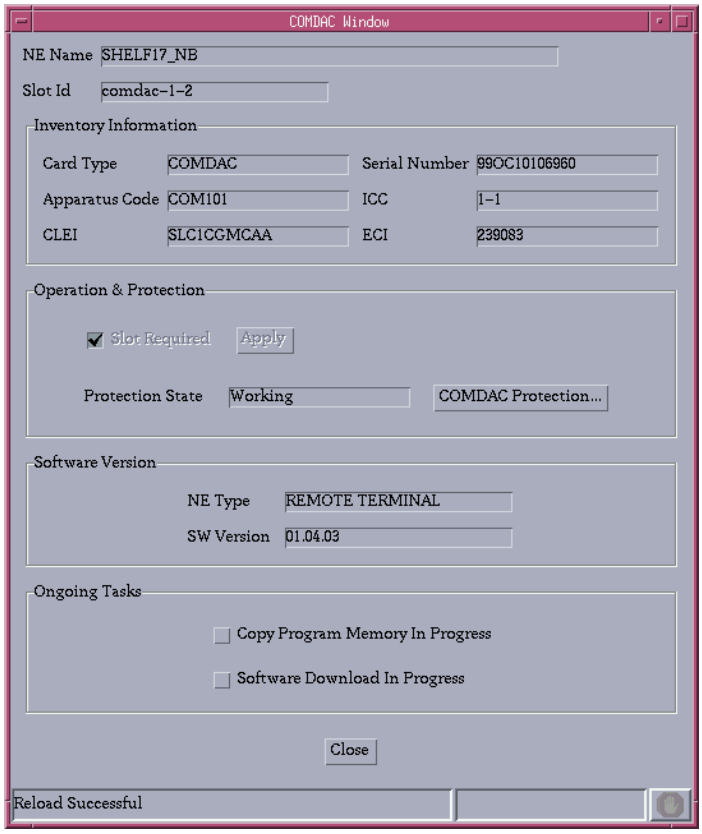


Figure 5-21 COMDAC window

This window contains all the information related to the COMDAC. It can be displayed even when the pack is not inserted.

The following table shows the view/edit options of the *COMDAC* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	Slot number where the COMDAC is plugged in. Slot format: comdac-1-{1,2}
Inventory Information	The read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible value: COMDAC. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: COM500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Operation & Protection	This field is described in Chapter 5.5.12, page 5-141.
Software Version	**NE Type**: Displays whether the NE is a COT or not. Possible values for this release: REMOTE TERMINAL. **SW Version**: Software version that has been obtained from the NE at connection time.
Ongoing Tasks	These check boxes indicate operations in progress which can take a long time and must be known by the operator. They will be refreshed when the window is launched or when refreshing the whole window.

2. Click on ***Close*** to exit the window.

5.5.5.6 View the CIU parameters

The CIU (communication interface unit) pack provides access for circuit and drop testing and craft access functions.

Procedure Complete the following procedure to view the CIU data:

Step	Procedure
1.	Select ***NE -> Main Shelf -> DTP500*** in the Network Element Browser and ***Edit*** via the cursor menu or select ***View -> Object*** via the menu bar or single-click on the pack ***CIU*** in the *Shelf View* window. The *CIU* window pops up:

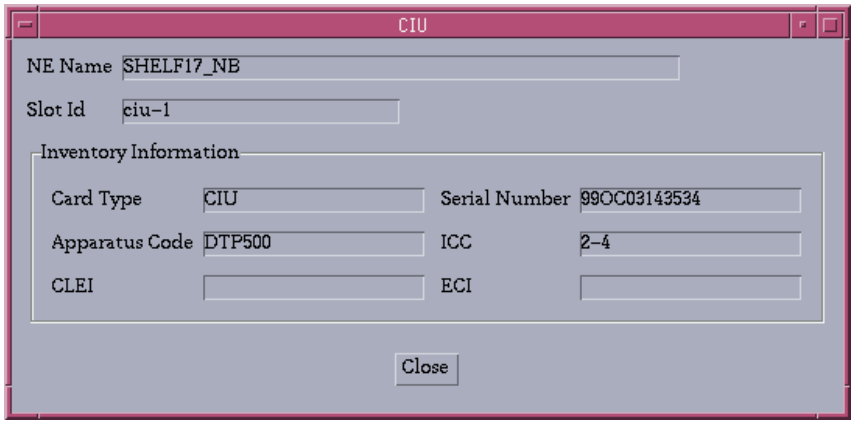


Figure 5-22 CIU window

This window contains all information related to the CIU. It can be displayed even when the pack is not inserted.

The following table shows the view/edit options of the *CIU* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	Slot number where the CIU is plugged in.

Parameters/ Buttons	Description
Inventory Information	The following fields are empty if no pack is inserted. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible value: CIU. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: DTP500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Not applicable. **ECI**: Not applicable.

2. Click on ***Close*** to exit the window.

5.5.5.7 IO_HDLC window

The IO_HDLC (High-Level Data Link Control) pack primarily performs a frame relay function of D-channel messages between the ISDN subscribers connected to an NE and the V5 communication channels.

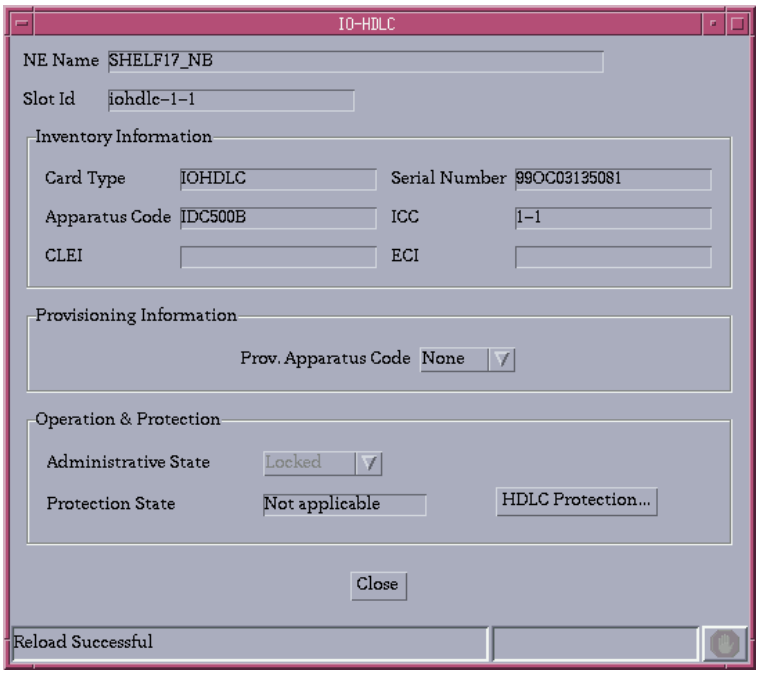


Figure 5-23 IO_HDLC window

This window contains all information related to the IO_HDLC. It includes hardware and software data (inventory) as well as operational and protection state. It can be displayed even when the pack is not inserted.

The following table shows the view/edit options of the *IO_HDLC* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	Slot number where the IO_HDLC is plugged in. Slot format: io-hdlc{1,2}.

Parameters/ Buttons	Description
Inventory Information	The following fields are empty, if no pack is provisioned. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible value: IO_HDLC. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: IDC500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Not applicable. **ECI**: Not applicable.
Provisioning Info	The option menu **Provisioned Apparatus Code** can be used to see and change the slot provisioning information. If nothing is provisioned, this field displays "None". Otherwise it displays the provisioned card type. Possible values: None and IDC500.
Operation & Protection	**Administration State:** This option menu is used to see and select the administrative state of the IO_HDLC. Possible values are: Locked and Unlocked. After creation, the default value is Unlocked. **Protection State** shows whether the selected IO_HDLC is working or not. Possible values: Working, Standby and Not Applicable (protection mode is disabled). The ***HDLC Protection...*** button provides access to the *Shelf Protection* window (tab IO_HDLC) to allow you to modify the protection scheme or to perform protection switching.

5.5.5.8 Configure an IO_HDLC

Procedure Complete the following procedure to view/edit the IO_HDLC data:

Step	Procedure

1. Select ***NE -> Main Shelf -> IDC500*** in the Network Browser and ***View*** via the cursor menu
or select ***View -> Object*** via the menu bar
or single-click on the pack ***IO_HDLC*** in the *Shelf View* window.
The *IO_HDLC* window pops up.

If you want to ...	then ...
change the provisioned card type	use the option menu **Provisioned Apparatus Code**.
modify the protection scheme	press ***HDLC Protection...***. The *Shelf Protection* window pops up (cf. Chapter 5.5.13.3, page 5-147).
change the administrative state	use the option menu **Administration State**. When changing from "Unlocked" to "Locked" a *Warning* window pops up displaying the following message: **`Changing the IO-HDLC administrative state to Locked may be service affecting in mixed (POTS/ISDN) system configurations if no protection switch is possible. Do you want to continue?`** If you decide to continue, the change operation will be started.

2. Click on ***Close*** to exit the window.

5.5.5.9 Subshelves window

This screen is composed of a set of option menus to select the ONU Subshelf to be created or edited and the command buttons to provision / deprovision the subshelf.

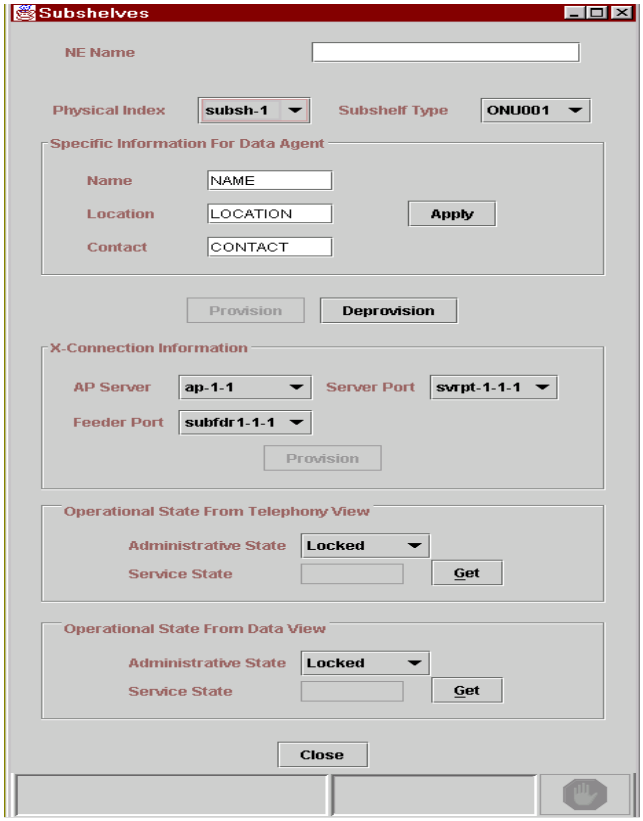


Figure 5-24 Subshelves window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Index	This option menu provides the **Physical Index** or the subshelf identifier. Identifiers which have already been created and provisioned in the NE are shown with a grey background.
Subshelf Type	This option menu shows the possible subshelves that can be created in the NE. NOTE: Only ONU Subshelf is supported.

Parameters/ Buttons	Description
Specific Information For Data Agent	This field is visible only for data agents. **Name**: This text field can be used to enter the name of the contact people who control the subshelf. **Location**: This text field can be used to enter the location where the NE is placed. **Contact**: This text field can be used to enter the contact information of the contact people who control the subshelf. ***Apply***: This button is used to confirm the changes (creating a new subshelf or editing the changes in this field).
Command buttons	The ***Provision*** button is used to provision a new subshelf. This button is enabled only in case of creating a new subshelf. The ***Deprovision*** button is used to deprovision an already provisioned subshelf.
Cross-Connection Information	**AP Server:** This option menu shows all AP servers (slot_Id) that can be cross-connected to the subshelf (if creating) or that are cross-connected to the provisioned subshelf (if editing). The value NONE can be used to delete the cross-connection to the subshelf. **Server Port:** This option menu shows all server ports (drop_id) that can be cross-connected to the selected AP server (if creating) or that are cross-connected to the selected AP server (if editing). **Feeder Port:** This option menu is used to select the feeder port to be used to cross-connect the subshelf. A grey background indicates that the selected server port is already in use. The ***Label*** button is used to confirm the changes (***Provision***: cross-connect the provisioned subshelf or ***Deprovision***: remove the cross-connection to the provisioned subshelf).

Parameters/ Buttons	Description
Operational State from Telephony View	This field is visible only for telephony agents. The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Operational State** shows the state of the telephony agent. Possible values: Enabled, Enabled-NOP, Enabled-MEA, Disabled, Disabled-NAS. The field **Subshelf Identifier** shows the id of the subshelf backplane obtained from the NE by using the ***Get*** button. The ***Get*** button can be used to update the display of the Operational State and the Subshelf Identifier.
Operational State from Data View	This field is visible only for data agents. The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. NOTE: The subshelf can only be put in service (Locked -> Unlocked) if the OAP is already in service (Unlocked). The field **Operational State** shows the state of the ATM feeder obtained (on demand) by the user. Possible values: Normal, Not In Service, Fault Condition, Dormant. The ***Get*** button can be used to update the display of the operational state. Retrieving the operational state is possible only after the subshelf creation if ■ the OAP is provisioned and equipped ■ the administrative state and the operational state of the OAP is "Unlocked" ■ the subshelf is provisioned and equipped ■ the administrative state of the subshelf is "Unlocked" ■ the BB SubShelf Association Mismatch alarm does not exist ■ the COMDAC is equipped.
If there is a mismatch between the COMDAC view and the AFM view an additional field is available. Two radio buttons (**COMDAC View**, **AFM View**) can be used to select the desired view. A text field explains the type of mismatch.	

5.5.5.10 Modify subshelves

Procedure Complete the following procedure to modify a subshelf:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Create Subshelf -> ONU*** via the cursor menu
or select ***NE -> Subshelves*** in the Network Element Browser and ***Edit*** via the cursor menu
or select ***View -> Object*** via the menu bar. The *Subshelf* window pops up

If you want to ...	then ...
create a subshelf	use the option menus **Physical Index** and **Subshelf Type** to select the desired subshelf (for data agent: write the appropriate text strings into the text fields **Name**, **Location**, and **Contact** and confirm with ***Apply***) and finally click on ***Provision*** to provision the selected subshelf.
edit an existing subshelf	use the option menus **Physical Index** and **Subshelf Type** to select the desired subshelf (for data agent: edit the text strings for **Name**, **Location**, and **Contact** and confirm with ***Apply)***.
create a cross-connection to the subshelf	use the option menu **Physical Index** to select the desired subshelf, use the option menus in the field **Cross-Connection Information** to select the corresponding server and ports of the desired cross-connection and click on ***Provision*** in the **Cross-Connection Information** field.
delete a cross-connection to the subshelf	use the option menus **Physical Index** and **Subshelf Type** to select the desired subshelf, use the option menus in the field **Cross-Connection Information** to select the corresponding values for AP Server (NONE), Server Port (NONE) and Feeder Port and click on ***Deprovision*** in the **Cross-Connection Information** field.

If you want to ...	then ...
deprovision a subshelf	use the option menus **Physical Index** and **Subshelf Type** to select the desired subshelf and click on ***Deprovision***.
change the administrative state	use the option menu **Administrative State** NOTE: Changing from "Locked" to "Unlocked" is only possible if the OAP is already "Unlocked". NOTE: When changing from "Unlocked" to "Locked" the following warning message appears: **Changing the administrative state of subshelf may be service affecting. Do you want to continue?**

2. Click on ***Close*** to exit the window.

5.5.5.11 Common application pack window

Background

The *AnyMedia* Access System uses a provisioning model to provide service, i.e. the AP must be preprovisioned by defining its function and setting the required options. For example, a POTS AP has to be preprovisioned first to create a POTS or ALL service for a subscriber. Should the physical inventory change, i.e. if an AP is plugged or removed, any changes in the inventory database will be notified automatically to the *AnyMedia* Access System.

AP provisioning will be performed to establish a desired pack type in a desired slot xx. To be fully functional/operational, an AP must both be inserted and provisioned. In addition, the provisioned AP must match the actual type of the inserted pack. An AP can be provisioned and configured by the AEM even if the slot is still empty.

The following window is used to provision a non-provisioned slot.

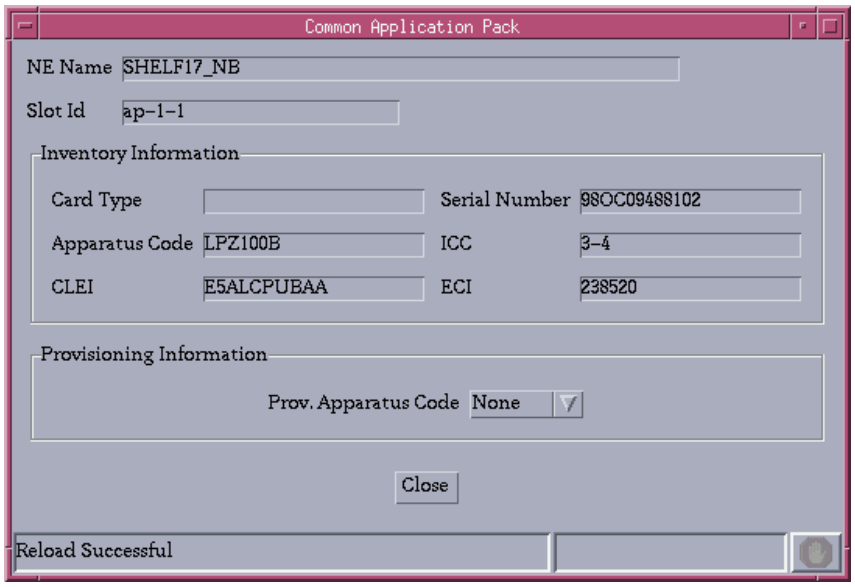


Figure 5-25 Common AP window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE Name of the selected NE (max. 30 characters).
Slot Id	Slot number where the AP is plugged in. Format: ap-1-{1,16} or subap-1-{1, 8}.

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is inserted. Otherwise the read-only text fields provide the following information: **Card Type**: Not applicable. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: LPZ100B, LPP100B, LPU112, TAP100, LPA400, LPA408, LPF500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Info	The option menu **Provisioned Apparatus Code** shows the APs available for the NE release. The default value is NONE, so this window is launched when there is not any provisioned pack in the selected slot. It shows both telephony and data APs. Once the operator has selected the provisioned apparatus code, this window will be replaced by the specific AP window (e.g. *HDSL AP* window). NOTE: The **Provisioned Apparatus Code** may be different from the **Apparatus Code** shown in the Inventory Information field. The **Apparatus Code** is related to a certain card (e.g. LPZ100B) whereas the **Provisioned Apparatus Code** is related to a family of cards (e.g. LPZ100). The OAP apparatus code (LPF500) can be displayed only if an even slot has been selected.

5.5.5.12 Provisioning a slot via common AP

Procedure Complete the following procedure to provision a non-provisioned slot:

Step	Procedure
1.	Select ***NE ->Main Shelf (Subshelves) -> not provisioned AP*** in the Network Element Browser and ***Edit*** via the cursor menu or select ***View -> Object*** via the menu bar or single-click on a non-provisioned AP in the *Shelf View* window. The *Common AP* window pops up.
2.	Use the option menu **Provisioned Apparatus Code** to select the desired AP. The corresponding AP window pops up (PSTN/ISDN - cf. Chapter 5.5.5.13, page 5-77) (HDSL - cf. Chapter 5.5.5.16, page 5-84) (ONU - cf. Chapter 5.5.5.18, page 5-89) (ADSL - cf. Chapter 5.5.5.27, page 5-105).

5.5.5.13 PSTN/ISDN AP window

These APs provide the line-side interface functionality that provides service to end-users.

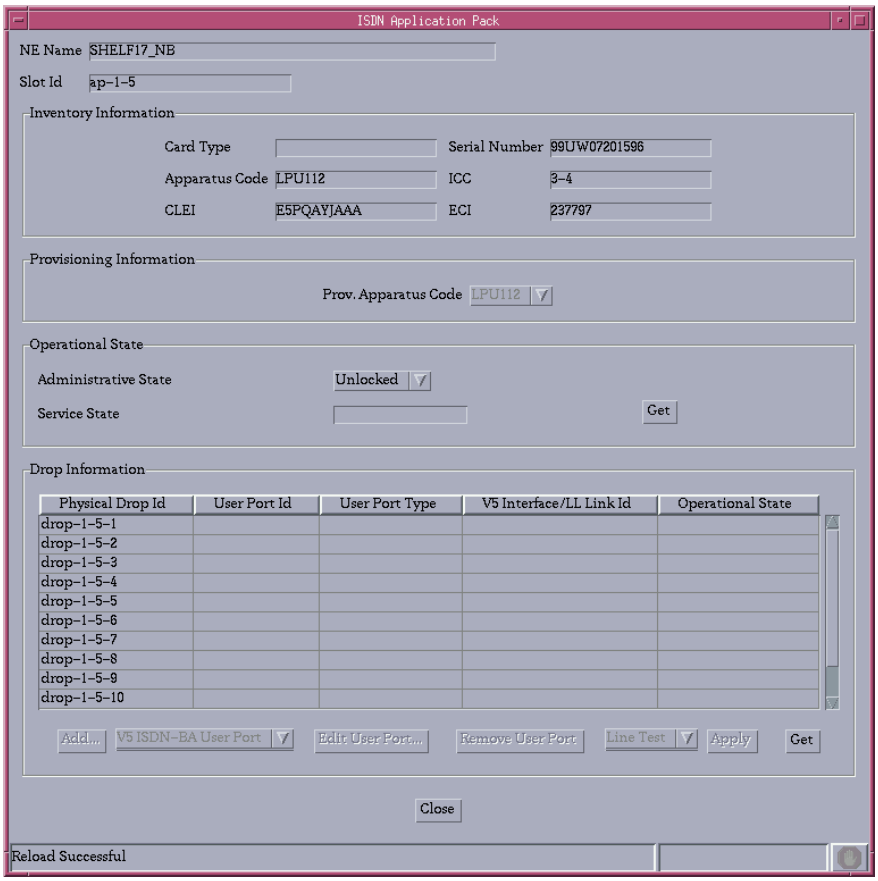


Figure 5-26 ISDN/PSTN AP window

This window contains all information related to the ISDN/PSTN AP. It can be displayed even when the pack is not inserted. The displayed information differs depending on the type of service (PSTN or ISDN).

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE Name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the AP is inserted. Possible values: ap-1-{1, 16} / subap-{1, 8}-{1, 8}

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is provisioned. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: LPZ100B, LPP100B, LPU112, TAP100. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Information	The option menu **Provisioned Apparatus Code** lists the possible apparatus codes or the value **None** (for unprovisioning). This option menu is used to provision an unprovisioned AP (selecting an apparatus code) and vice versa (selecting None). In case of unprovision the *Common AP* window pops up (cf. Chapter 5.5.5.11, page 5-74). This menu is disabled if the pack is provisioned and the administrative state is "Unlocked" because deprovision of an AP in service is not possible.
Operational State	The option menu **Administrative State** (available only for NE R1.4 and above) provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled, Secondary Service State Acronym. The ***Get*** button can be used to retrieve the current Operational State.

Parameters/ Buttons	Description
Drop Information	This field contains a table displaying physical port information. This information is presented in a 4-column table. The table is sorted by **Physical Drop Id**. A scroll bar allows navigation through the table. Rows in the table can be selected to add/edit user port and leased lines, or to remove cross-connections through the use of the ***Add...***, ***Edit User Port...*** or ***Remove User Port...*** buttons (see below). ■ **Physical Drop Id**: Identifies the drop within the AP. The value depends on the inserted card type. ■ **User Port Id**: Indicates the id within the layer 3 (PSTN port) or envelope function address (ISDN BRA port) of the subscriber or the id of a leased line (only available if the user port is cross-connected to a V5 interface or it is a leased line). ■ **User Port Type**: Shows the type of service provided. Possible values: PSTN, ISDN BRA, ALL, DLL. NOTE: PSTN *and* ISDN BRA are not possible in the same application pack. ■ **V5 Interface / LL Link id**: Shows the V5 interface id or the logical link (LL) id. Possible values (V5 interface): {0, 16777215} in dec format or {0, FFFFFF} in hex format. ■ **Operational State**: Shows the current operational state of the physical drop by using of the ***Get*** button. The ***Add*** button is enabled only if a physical port is selected which is not used for any service yet. Depending on the selected entry in the associated option menu it provides access to the *V5 PSTN User Port* window or *V5 ISDN BA User Port* window or *Analog Leased Line* window or *Digital Leased Line* window. The ***Edit User Port...*** button is enabled if a physical port is selected which is already in use. It provides access to the *V5 PSTN User Port* window or *V5 ISDN BA User Port* window or *Analog Leased Line* window or *Digital Leased Line* window, depending on the service being provided by the selected port. The ***Remove User Port*** button removes the cross-connection selected in the list (see above). This option is only available if the port is already cross-connected or is a leased line.

Parameters/ Buttons	Description
Test Management	The ***Apply*** button is used, together with the option menu beside it, to execute one of the following tests: Line test, Port test, CRC test (for ISDN BRA and DLL drops). For more information refer to Chapter 7.4.
If there is a mismatch between the COMDAC view and the AFM view an additional field is available. Two radio buttons (**COMDAC View**, **AFM View**) can be used to select the desired view. A text field explains the type of mismatch.	

5.5.5.14 Modify a PSTN/ISDN AP

Procedure Complete the following procedure to modify a PSTN/ISDN application pack:

Step	Procedure
1.	Select ***NE -> Main Shelf (Subshelf) -> LPZ100 (LPP100, LPU112, TAP100)*** in the Network Element Browser and ***View*** via the cursor menu or select ***View -> Object*** via the menu bar or single-click on ***PSTN/ISDN AP*** in the *Shelf View* (*Subshelf*) window. The *PSTN/ISDN AP* window pops up. This window can also be reached from the *Common AP* window by provisioning a slot not yet provisioned (cf. Chapter 5.5.5.11, page 5-74).
2.	Use the option menus **Slot Id** to select the desired slot.

If you want to ...	then ...
unprovision the AP	use the option menu **Provisioned Apparatus Code** to select **None**.
change the administrative state	use the option menu **Administrative State**. NOTE: When changing from "Unlocked" to "Locked" the following warning message appears: **Changing the administrative state may be service affecting. Do you want to continue?**

If you want to ...	then ...
add a user port	select a physical port which is not used for any service yet, use the option menu near the ***Add*** button, select a corresponding entry and press ***Add***. Depending on the selected entry one of the following windows pops up: *V5 PSTN User Port* (cf. Chapter 6.2.8.3.1, page 6-59) or *V5 ISDN BA User Port* (cf. Chapter 6.2.8.5.1, page 6-75) or *ALL User Port* (cf. Chapter 6.2.8.2.1, page 6-52) or *DLL User Port* (cf. Chapter 6.2.8.4.1, page 6-67).
edit a user port	select an appropriate physical port and press ***Edit User Port...*** or double click on the row entry. Depending on the selected port one of the following windows pops up: *V5 PSTN User Port* (cf. Chapter 6.2.8.3.1, page 6-59) or *V5 ISDN BA User Port* (cf. Chapter 6.2.8.5.1, page 6-75) or *ALL User Port* (cf. Chapter 6.2.8.2.1, page 6-52) or *DLL User Port* (cf. Chapter 6.2.8.4.1, page 6-67).
delete a cross-connection	select an appropriate physical port and press ***Remove User Port...***. A *Warning* window pops up displaying the following message: **`Removing User Port may be service affecting. Do you want to continue?`** If you decide to continue, the remove operation will be started. The information displayed will be updated once the remove operation is finished to show the current list.
exit the window	click on ***Close***.

5.5.5.15 TAP AP window

The TAP AP includes the pack inventory data and enables to start the TAP test.

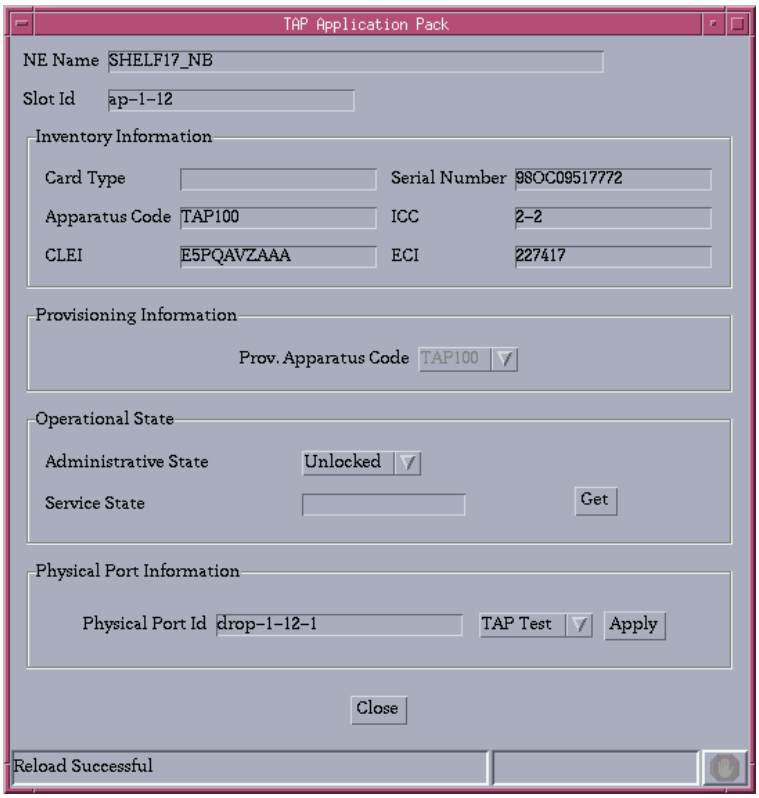


Figure 5-27 TAP AP window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE Name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the AP is inserted.

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is provisioned. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: TAP100. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Info	The option menu **Provisioned Apparatus Code** shows the TAP apparatus codes or the value **None** (for unprovisioning).
Operational State	The option menu **Administrative State** (available only for NE R1.4 and above) provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled, Secondary Service State Acronym. The ***Get*** button can be used to retrieve the current Operational State.
Physical Port Information	**Physical Port Id**: This text field Identifies the drop within the AP. Possible values: drop-1-{1, 16}-1 or subdrop-{1, 8}-{1, 8}-1. The ***Apply*** button is used, together with the option menu beside it, to execute TAP test. For more information refer to Chapter 7.4.

5.5.5.16 HDSL AP window

The HDSL AP supports up to four HDSL links. These links can be used to connect an ISDN PRA subscriber as well as n64DLL subscribers via NTU. The *HDSL AP* window is available only for NE R1.4 and above.

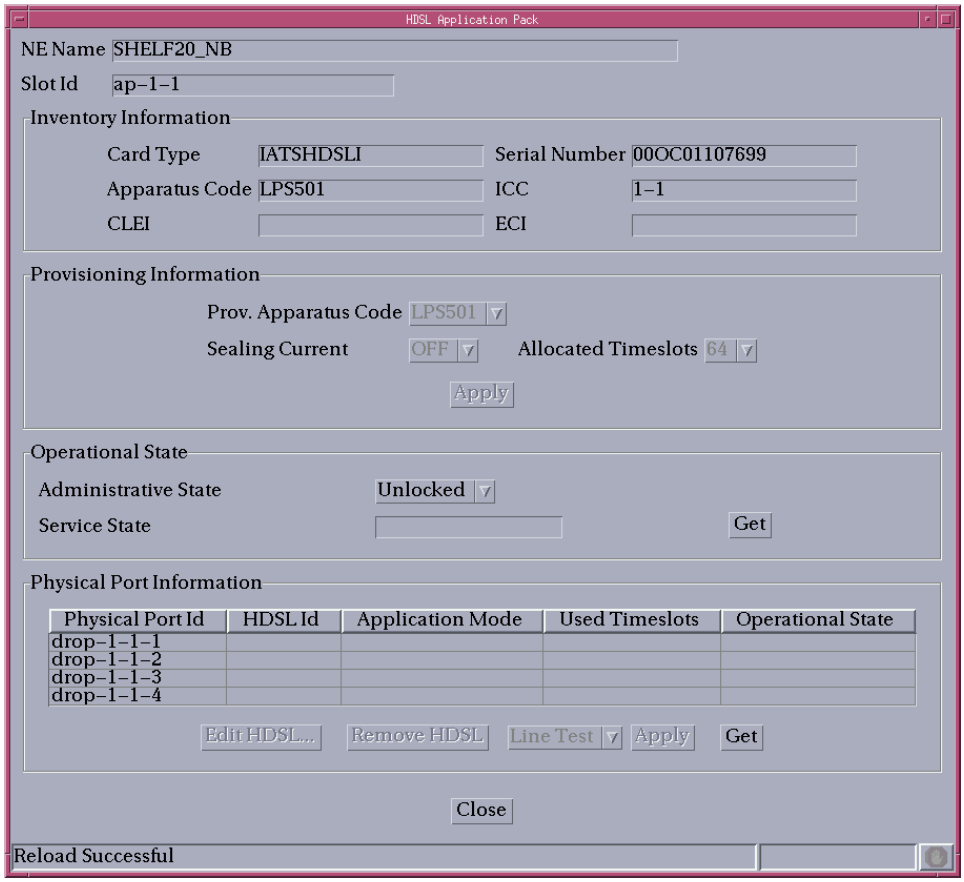


Figure 5-28 HDSL AP window

This window contains all information related to the HDSL AP. It can be displayed even when the pack is not inserted.

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE Name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the AP is inserted.

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is provisioned. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible value: LPS501. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Information	The option menu **Provisioned Apparatus Code** lists the possible apparatus codes or the value **None** (for unprovisioning). The option menu **Sealing Current** is used to define whether a sealing current shall be used on all physical drops of an HDSL or not. The option menu **Allocated Timeslots** is used to specify the available timeslots for service provisioning on the pack. Possible values: 1 to 64, depending on the next consecutive HDSL AP's allocated timeslots. The ***Apply*** button is used to confirm the changes.
Operational State	The option menu **Administrative State** (available only for NE R1.4 and above) provides the possible states that can be used: Locked and Unlocked. The field **Operational State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled, Secondary Service State Acronym. The ***Get*** button can be used to retrieve the current Operational State.

Parameters/ Buttons	Description
Physical Port Information	This pane contains a table displaying physical port information. This information is presented in a 4-column table. The table is sorted by **Physical Port Id**. A scroll bar allows navigation through the table. Rows in the table can be selected to add/edit HDSL interfaces, or to remove cross-connections through the use of the ***Add HDSL..., Edit HDSL...*** or ***Remove HDSL...*** buttons (see below). ■ **Physical Port Id**: Identifies the drop within the AP. Possible values: drop-1-{1, 16}-{1, 4} or subdrop-{1, 8}-{1, 8}-{1, 4}. ■ **HDSL Id**: Indicates the HDSL logical interface id. Possible values: {1, 128}. ■ **Application Mode**: Shows the application mode of this logical interface. Possible values: Single Pair, Point to Point, Point to Multipoint Equal and Point to Multipoint Shift. ■ **Used Timeslots**: Shows the number of timeslots used by this interface. Possible values: {0, 31}. ■ **Operational State**: Shows the current operational state of the physical drop by using of the ***Get*** button. The ***Label*** button provides access to the *HDSL Logical Interface* window. Depending on the selected physical drop id this button is labelled ***Add HDSL...*** or ***Edit HDSL...***. The ***Remove HDSL***button removes the cross-connection selected in the list (see above). This option is only available if the selected drop is already cross-connected. The ***Apply*** button is used, together with the option menu beside it, to execute one of the following tests: Line test, Port test. For more information refer to Chapter 7.4.
If there is a mismatch between the COMDAC view and the AFM view an additional field is available. Two radio buttons (**COMDAC View**, **AFM View**) can be used to select the desired view. A text field explains the type of mismatch.	

5.5.5.17 Modify an HDSL AP

Procedure Complete the following procedure to modify an HDSL application pack:

Step	Procedure

1. Select ***NE -> Main Shelf (Subshelf) -> LPS501*** in the Network Element Browser and ***View*** via the cursor menu
or select ***View -> Object*** via the menu bar
or single-click on ***HDSL AP*** in the *Shelf View* (*Subshelf*) window.
The *HDSL AP* window pops up.

   This window can also be reached from the *Common AP* window by provisioning a slot not yet provisioned (cf. Chapter 5.5.5.11, page 5-74).

2. Use the option menus **Slot Id** to select the desired slot.

If you want to ...	then ...
change the provisioning information parameters	use the corresponding option menus and press ***Apply***.
unprovision the AP	use the option menu **Provisioned Apparatus Code** to select NONE and press ***Apply***. The *Common AP* window pops up (cf. Chapter 5.5.5.11, page 5-74).
change the administrative state	use the option menu **Administrative State**. NOTE: When changing from "Unlocked" to "Locked" the following warning message appears: **Changing the administrative state may be service affecting. Do you want to continue?**
add an HDSL logical interface	select a free physical drop and press ***Add HDSL Logical Interface...*** or double click on the row entry. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).

If you want to ...	then ...
edit an HDSL logical interface	select an appropriate physical drop and press ***Edit HDSL Logical Interface...*** or double click on the row entry. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).
delete a cross-connection	select an appropriate physical drop and press ***Remove HDSL Logical Interface***. A *Warning* window pops up displaying the following message. **`Removing HDSL Logical Interface may be service affecting. Do you want to continue?`** If you decide to continue, the remove operation will be started. The information displayed will be updated once the remove operation is finished to show the current list.
exit the window	click on ***Close***.

5.5.5.18 ONU Application Pack window

This window contains all information related to the ONU server. It is available only for NE R1.4 and above.

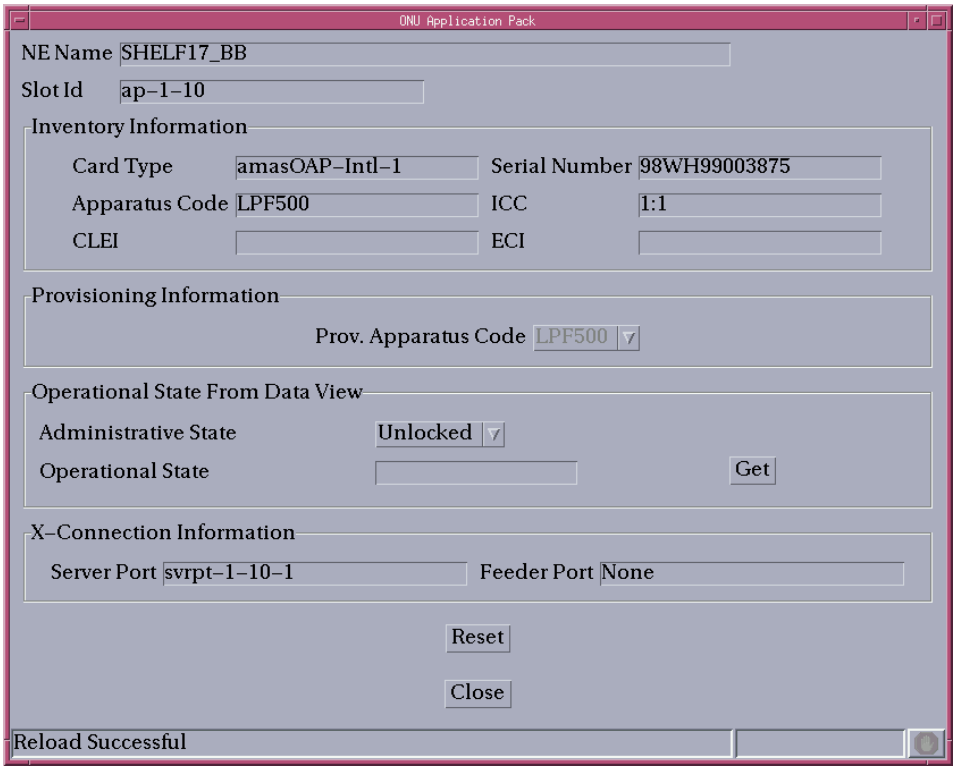


Figure 5-29 ONU Application Pack window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the OAP is inserted.

Parameters/ Buttons	Description
Inventory Information	The read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible values: LPF500. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: LPF500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Information	The option menu **Provisioned Apparatus Code** shows the provisioning info (LPF500) or the value **None** (for unprovisioning).
Operational State from Telephony View (only visible for telephony agents)	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Operational State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled-MON, Disabled-NAC. The ***Get*** button can be used to update the display of the Operational State.
Operational State from Data View (only visible for data agents)	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Operational State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled, Fault condition, Under reboot, Under testing, Under software download, Dormant. The ***Get*** button can be used to update the display of the Operational State.
X-Connection Information	The field **Server Port** identifies the port within the AP. Possible values: svrprt-1-{1, 15}-{1}. The field **Feeder Port** indicates the ONU port which is cross-connected to the server port. Possible values: subfdr-1-{1, 8}-{1}-{1}.
Reset	This button can be used to reset the data part of the pack. This button is available only for data agents.

Parameters/ Buttons	Description
If there is a mismatch between the COMDAC view and the AFM view an additional field is available. Two radio buttons (**COMDAC View**, **AFM View**) can be used to select the desired view. A text field explains the type of mismatch.	

5.5.5.19 Modify an OAP

Procedure Complete the following procedure to modify an OAP:

Step	Procedure
1.	Select ***NE -> Main Shelf -> LPF500*** in the Network Element Browser and ***Edit*** via the cursor menu or single click on ***OAP*** in the *Shelf View* window. The *OAP* window pops up. This window can also be reached from the *Common AP* window by provisioning a slot not yet provisioned (cf. Chapter 5.5.5.11, page 5-74).

If you want to ...	then ...
unprovision the OAP	use the option menu **Provisioned Apparatus Code** to select NONE. The *Common AP* window pops up (cf. Chapter 5.5.5.11, page 5-74).
change the administrative state (for telephony or data)	use the option menu **Administrative State**. NOTE: When changing from "Unlocked" to "Locked" the following warning message appears: **Changing the administrative state may be service affecting. Do you want to continue?**
reset the data part of the pack	click on ***Reset***. The following warning message pops up: **Resetting the ONU Application Pack may affect Data services. Do you want to continue?**

2. Click on ***Close*** to exit the window.

5.5.5.20 Read the OCP data

Procedure Complete the following procedure to read the OCP data:

Step	Procedure
1.	Select ***NE -> Subshelves -> CPF500*** in the Network Element Browser and ***View*** via the cursor menu or single-click on ***OCP*** in the *Subshelf View* window. The *ONU Controller Pack* window pops up.

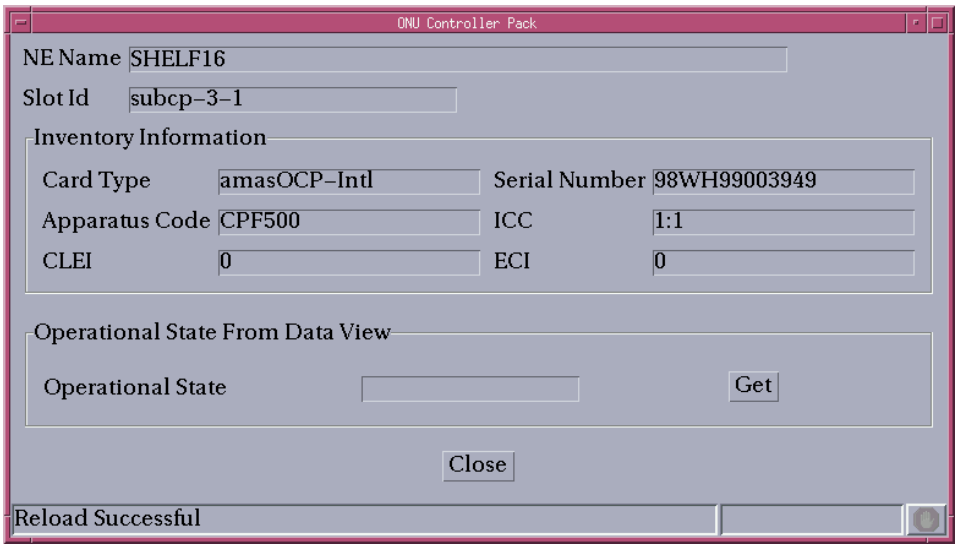


Figure 5-30 ONU Controller Pack window

This window contains all information related to the ONU server. It is available only for NE R1.4 and above.

The following table shows the parameters of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the OCP is inserted. Possible values: subcp-{1, 8}-1.

Parameters/ Buttons	Description
Inventory Information	The read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible values: OCP. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: CPF500. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Operational State from Telephony View (only visible for telephony agents)	The field **Operational State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled-NAC. The ***Get*** button can be used to update the display of the Operational State.
Operational State from Data View (only visible for data agents)	The field **Operational State** shows the state obtained (on demand) by the user. Possible values: Enabled, Disabled, Fault condition, Under reboot, Under testing, Under software download, Dormant. The ***Get*** button can be used to update the display of the Operational State.

2. Click on ***Close*** to exit the window.

5.5.5.21 AFM window (data application)

This screen is used to show/modify the AFM parameters. It can also be used to reset and to edit the feeder ports.

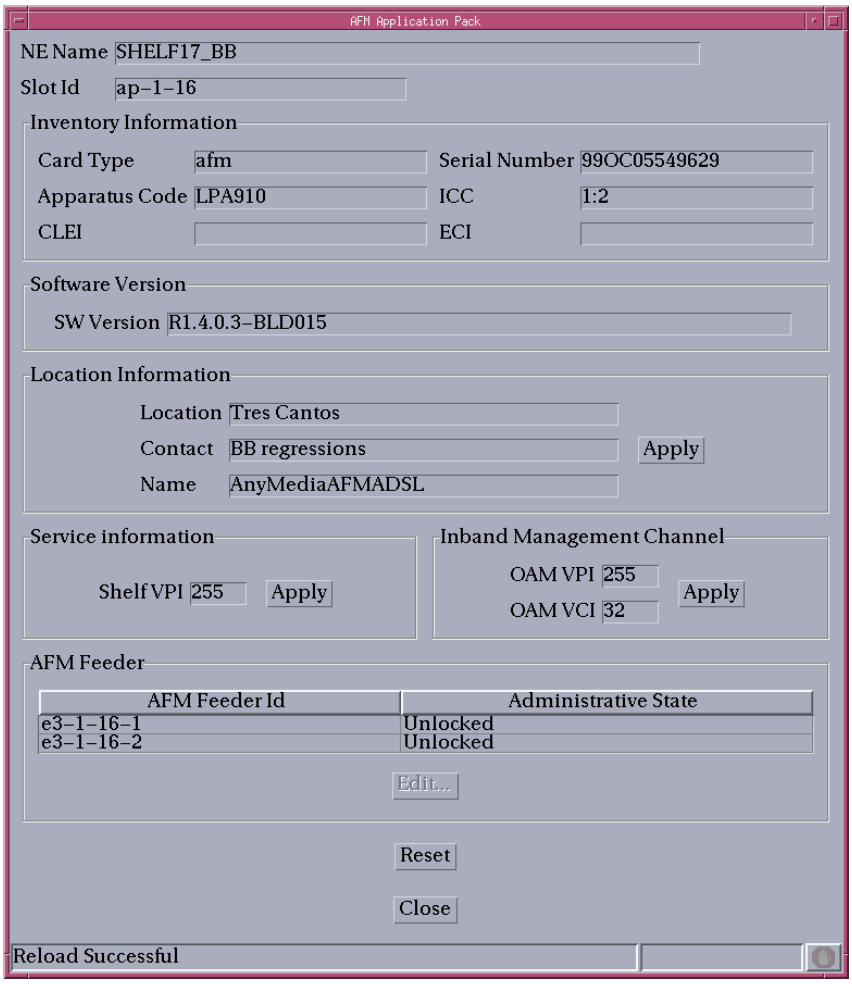


Figure 5-31 AFM window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	This text field shows the slot in which the AFM_E3 is inserted. Possible values: ap-1-{1, 16}. In this release the only possible value is ap-1-16, the AFM_E3 can only be inserted in slot 16.

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is inserted. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible values: AFM_E3 (LPA910). **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: LPA910. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Not applicable. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack.
Software Version	This field shows the software version of the inserted AFM_DS3 pack.
Location Information	NOTE: The following text fields must be filled up. Empty fields are not supported by the AFM. **Location**: This text field is used to define a location name where the NE is placed. **Contact:** This text field is used to enter the name of the people who manage the NE. **Name**: This text field can be used to enter a name for the mainshelf. The ***Apply*** button is used to confirm the changes in the text fields above.
Service Information	**Shelf VPI**: This field is used to show/change the VPI used in all feeder VCIs. Possible values: {1, 255}. The ***Apply*** button is used to confirm the changed Shelf VPI.

Parameters/ Buttons	Description
Inband Management Channel	**OAM VPI**: This field shows the VPI used to communicate with the NE. Possible values: {1, 255}. **OAM VCI:** This field shows the VCI used to communicate with the NE. Possible values: {32, 63}, only 32 if OAM VPI = Shelf VPI. The ***Apply*** button is used to confirm the changes in the text fields above. NOTE: If one of the parameters is changed the communication with the NE could be lost.
AFM Feeder	The information in this field is displayed in a table: ■ **AFM Feeder Id**: Id of the feeder port. ■ **Administrative State**: Administrative state of the feeder port: Locked, Unlocked. The ***Edit*** button provides access to the *AFM Feeder* window. This button is enabled only if a feeder has been selected.
Reset	This button is used to reset the AFM_E3 pack.

5.5.5.22 Modify an AFM (data application)

Procedure Complete the following procedure to modify an AFM_D3 pack:

Step	Procedure

1. Select ***NE -> Main Shelf (Subshelf) -> LPA910*** in the Network Element Browser and ***Edit*** via the cursor menu
or select ***View -> Object*** via the menu bar
or single-click on ***AFM _E3*** in the *Shelf View* (*Subshelf*) window.
The *AFM* window pops up.

If you want to ...	then ...
edit the location information	edit the parameters in the field **Location Information** and press ***Apply***.
edit the service information	enter a new value for **Shelf VPI** and press ***Apply***. The following warning message pops up: **`Changing the Shelf VPI may be service affecting and it will take a time. Do you want to continue?`**
edit the inband management channel NOTE: If one of the parameters is changed the communication with the NE could be lost.	enter new values for **OAM VPI** and **OAM VCI** and press ***Apply***. The following warning message pops up: **`Changing the OAM VPI/VCI may be service affecting. It will take a time and it can make that communication with NE is not recovered if OAM PVC is used for management communications. Do you want to continue?`** NOTE: If the same value has been entered for OAM VPI as for Shelf VPI, the only possible value for OAM VCI is 32!
edit an AFM feeder	select the desired feeder and press ***Edit*** or double click on the row entry. The *AFM Feeder* window pops up (cf. Chapter 5.5.5.23, page 5-99).

If you want to ...	then ...
reset the AFM_E3 pack	click on ***Reset***. The following warning message pops up: **Resetting the AFM may be service affecting and will take a time. Do you want to continue?**

2. Click on ***Close*** to exit the window.

5.5.5.23 AFM Feeder window (data application)

This screen is used to configure the AFM feeder parameters. It can be reached from the *AFM* window (cf. Chapter 5.5.5.21, page 5-94).

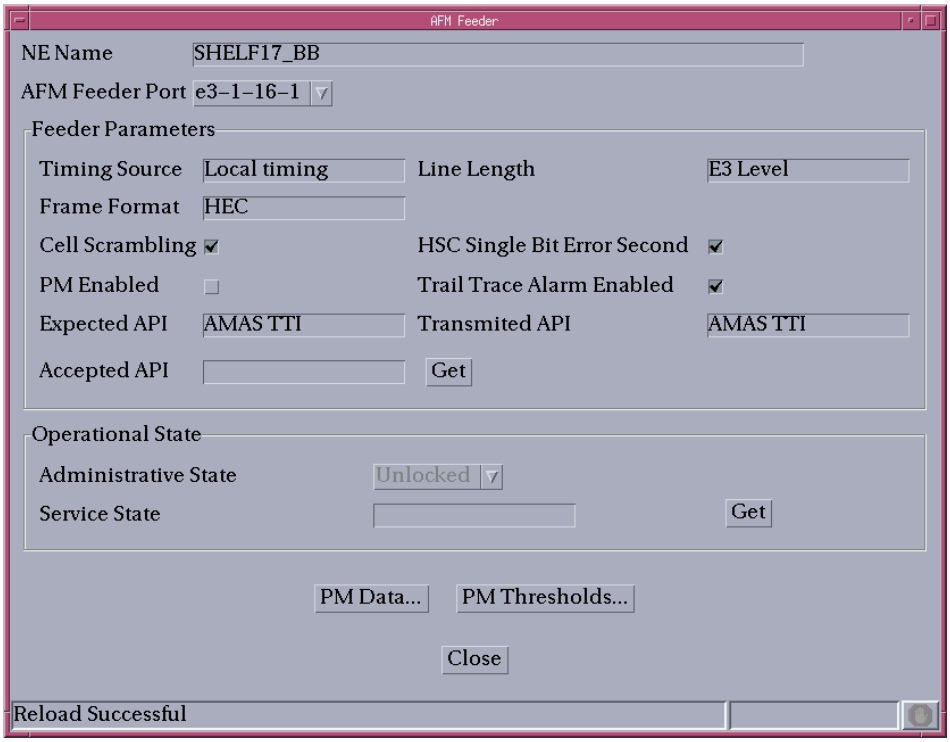


Figure 5-32 AFM Feeder window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
AFM Feeder Port	This option menu displays the available feeder ports which can be selected.

Parameters/ Buttons	Description
Feeder Parameters	**Timing source:** This text field shows the used timing source: Free Running or Looped Timed. **Line Length**: This option menu can be used to select the desired line length. Possible value: E3 Level (0 ... 450 feet). **Frame Format:** This option menu is used to select the two frame format: HEC. **Cell Scrambling:** This check box can be used to enable/disable the scrambling of cells. **HSC Single Bit Error Second:** This check box can be used to discard all cells with uncorrected header errors. Possible values: Enabled, Disabled. **PM Enable:** This check box can be used to enable/disable the creation of performance monitoring data. **Trail Trace Alarm Enable**: This check box can be used to enable/disable the trail trace alarm. **Expected API**: only for E3. **Transmitted API**: only for E3. **Accepted API**: only for E3. Possible values: Enabled, Disabled. The ***Get*** button can be used to update the display of the **Accepted API**.
Operational State	The option menu **Administrative State**provides the possible states that can be used: Locked and Unlocked. NOTE: The communication with daisy-chained NEs can be lost when changing from "Unlocked" to "Locked". The field **Service State** shows the state of the AFM feeder obtained (on demand) by the user. Possible values: Enabled, Disabled, Testing, Unknown, Dormant. The ***Get*** button can be used to update the display of the Operational State.
PM Data	This button provides access to the *AFM Feeder PM Data* window.
PM Thresholds	This button provides access to the *AFM Feeder PM Threshold* window.

5.5.5.24 Modify an AFM feeder (data application)

This window is reached from the *AFM* window (cf. Chapter 5.5.5.21, page 5-94) by pressing the ***Edit*** button.

Procedure Complete the following procedure to modify an AFM feeder:

Step	Procedure

1. Use the option menu **Feeder Port** to select the desired port:

If you want to ...	then ...
change the feeder parameters	use the option menus and check boxes to change the corresponding parameters.
get the performance monitoring data	click on ***PM Data***. The *AFM Performance Monitoring* window pops up (cf. Chapter 8.3).
modify the performance monitoring thresholds	click on ***PM Thresholds***. The *AFM Feeder PM Threshold* window pops up (cf. Chapter 5.5.5.25, page 5-102).
change the administrative state NOTE: The communication with daisy-chained NEs can be lost when changing from "Unlocked" to "Locked".	use the option menu **Administrative State of Second Feeder**. NOTE: When changing from "Unlocked" to "Locked" the following warning messages appears: **Changing the administrative state of second AFM feeder may be service affecting if there are daisy-chained AFMs. Do you want to continue?**

2. Click on ***Close*** to exit the window.

5.5.5.25 AFM Feeder PM Threshold window (data application)

This screen is used to configure the feeder PM threshold parameters. It can be reached from the *AFM Feeder* window (cf. Chapter 5.5.5.23, page 5-99).

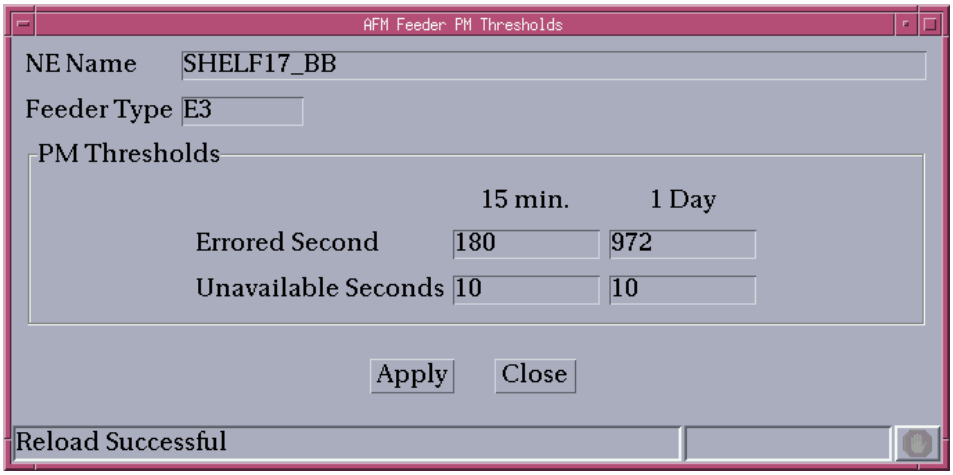


Figure 5-33 AFM Feeder PM Thresholds window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Feeder Type	This field displays the feeder type: E3.

Parameters/ Buttons	Description
PM Thresholds	The following parameters are applicable to all feeders. **Errored Second (ES)**: These text fields show the ES thresholds for 15-minute/1-day periods. The following is counted for the upstream direction: ■ crc-i or crc-f anomalies ■ los or sef defects. The following is counted for the downstream direction: ■ febe-i or febe-f anomalies ■ felos or rdi defects. The maximum value for 15 minutes is 900, the maximum value for 1 day is 86 400. **Unavailable Second (UAS):** These text fields show the UAS thresholds for 15-minute/1-day periods. The UASs are calculated by counting the number of seconds that the interface is unavailable. The maximum value for 15 minutes is 900, the maximum value for 1 day is 86 400.
Apply	This button is used to confirm the changes.

5.5.5.26 Define AFM Feeder PM thresholds (data application)

Procedure Complete the following procedure to define the feeder PM thresholds:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***AFM Feeder PM Threshold*** via the cursor menu. The *AFM Feeder PM Thresholds* window pops up. This window can also be reached from the *AFM Feeder* window (cf. Chapter 5.5.5.23, page 5-99) by pressing the ***PM Thresholds*** button.
2.	Use the corresponding text fields to define the desired thresholds and press ***Apply***.
3.	Click on ***Close*** to exit the window.

5.5.5.27 ADSL Application Pack window (data application)

This window includes inventory data, operation and protection information as well as general drop information.

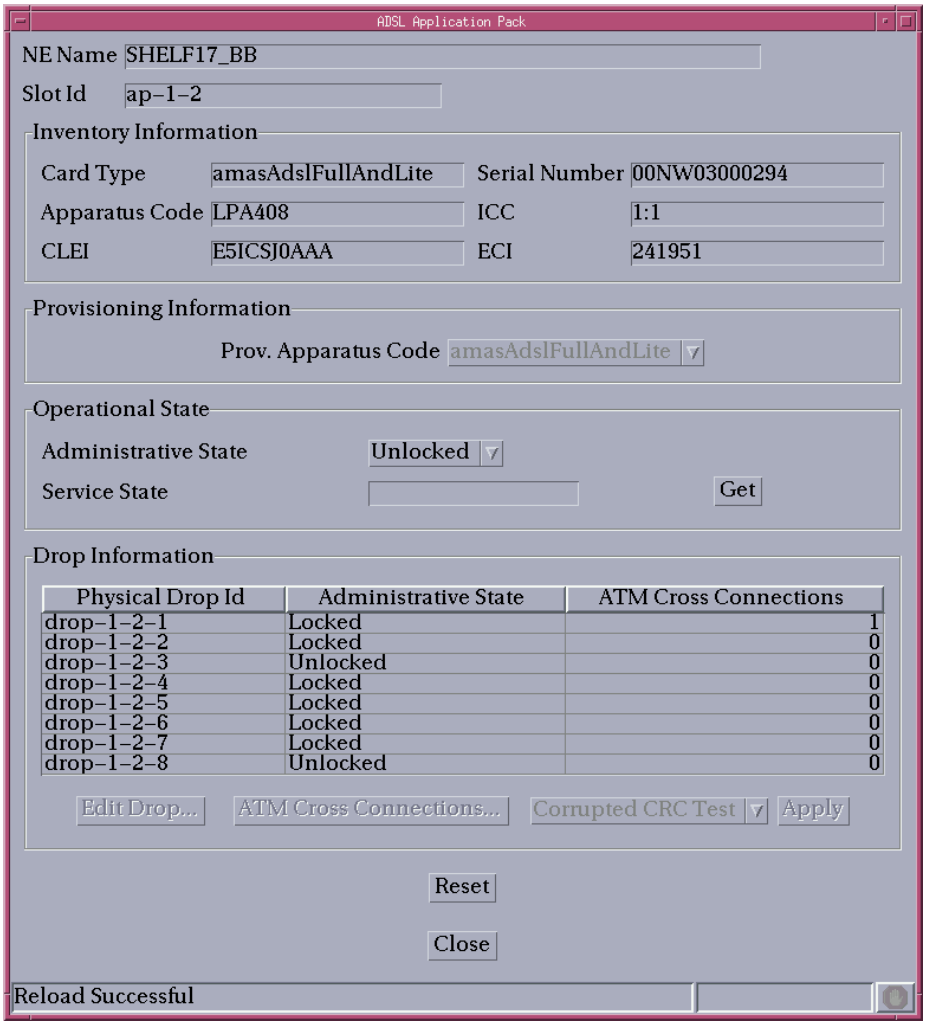


Figure 5-34 ADSL Application Pack window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Slot Id	This field displays the slot id. Possible values: ap-1-{1, 16} or subap-{1, 8}-{1, 8}.

Parameters/ Buttons	Description
Inventory Information	The following fields will be empty if no pack is inserted. Otherwise the read-only text fields provide the following information: **Card Type**: 11-character mnemonic used to identify the general type of function provided. Possible values: ADSL. **Serial Number**: 12-character alphanumeric code that includes the date and place of manufacture. **Apparatus Code**: Specifies the function of the pack. Possible values: LPA400, LPA400B, LPA408. **ICC (InterChangeability Code)**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the series number. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes.
Provisioning Information	The option menu **Provisioned Apparatus Code** shows ADSL (for a provisioned slot) and the value **None** (for a non-provisioned slot). This option menu is available only if the administrative state is Locked. NOTE: The **Provisioned Pack Type** may be different from the **Apparatus Code** shown in the Inventory Information field. The **Apparatus Code** is related to a certain card (LPA400B) whereas the **Provisioned Pack Type** is related to a family of cards (ADSL).
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the state of the AFM feeder obtained (on demand) by the user. Possible values: Enabled, Disabled, Fault Condition (NE R1.4), Under Reboot, Under testing, Under SW Download (NE R1.4), Dormant (NE R1.4). The ***Get*** button can be used to update the display of the Operational State.

Parameters/ Buttons	Description
Drop Information	A table shows the ADSL drops and the created cross-connections. The table is sorted by ADSL drops. ■ **Physical Drop Id**: Identifies the ADSL drop within the AP. ■ **Administrative Status**: Shows the current state: Locked, Unlocked. ■ **ATM Cross-Connections**: Indicates the number of created cross-connections. The ***Edit Drop...*** button provides access to the *ADSL Drop* window. It is enabled if a drop is selected in the table above. The ***ATM Cross-Connections...*** button provides access to the *ATM Cross-Connectio*n window. It is enabled if a drop is selected in the table above. The ***Apply*** button can be used to start the Port BIST Test or the Corrupted CRC Test. The desired test is selected by means of the option menu. For more information refer to Chapter 7.4.
Reset	This button can be used to reset the pack.
If there is a mismatch between the COMDAC view and the AFM view an additional field is available. Two radio buttons (**COMDAC View**, **AFM View**) can be used to select the desired view. A text field explains the type of mismatch.	

5.5.5.28 Modify an ADSL pack (data application)

Procedure Complete the following procedure to modify an ADSL pack:

Step	Procedure

1. Select ***NE -> Main Shelf (Subshelf) -> ADS*** in the Network Element Browser and ***Edit*** via the cursor menu
or select ***View -> Object*** via the menu bar
or single-click on ***ADSL*** in the *Shelf View* (*Subshelf*) window.
The *ADSL AP* window pops up.

If you want to ...	then ...
unprovision the AP	use the option menu **Provisioned Apparatus Code** to select NONE. The *Common AP* window pops up (cf. Chapter 5.5.5.11, page 5-74).
change the administrative state	use the option menu **Administrative State**. NOTE: When changing from "Unlocked" to "Locked" the following warning messages appears: **Changing the administrative state of the ADSL pack may be service affecting. Do you want to continue?**
edit an ADSL drop	select the desired ADSL drop in the **ADSL Drop Information** table and click on ***Edit Drop*** or double click on the row entry. The *ADSL Drop* window pops up (cf. Chapter 5.5.5.29, page 5-110).
edit/create an ATM cross-connection	select an ADSL drop with an assigned cross-connection in the **ADSL Drop Information** and click on ***ATM Cross-Connections***. The *ATM Cross-Connection* window pops up (cf. Chapter 6.3.2, page 6-144).

If you want to ...	then ...
start the BIST test	use the option menu near the ***Apply*** button to select **BIST Test** and press ***Apply***. See also Chapter 7.4.2.3.
start the corrupted CRC test	use the option menu near the ***Apply*** button to select **Corrupted CRC Test** and press ***Apply***. See also Chapter 7.4.2.2.
reset the pack	Click on ***Reset***. The following warning message pops up: **Resetting the ADSL Pack may be service affecting. Do you want to continue?**

2. Click on ***Close*** to exit the window.

5.5.5.29 ADSL Drop window (data application)

This screen is used to configure the ADSL drops. It can also be used to remove the related cross-connections.

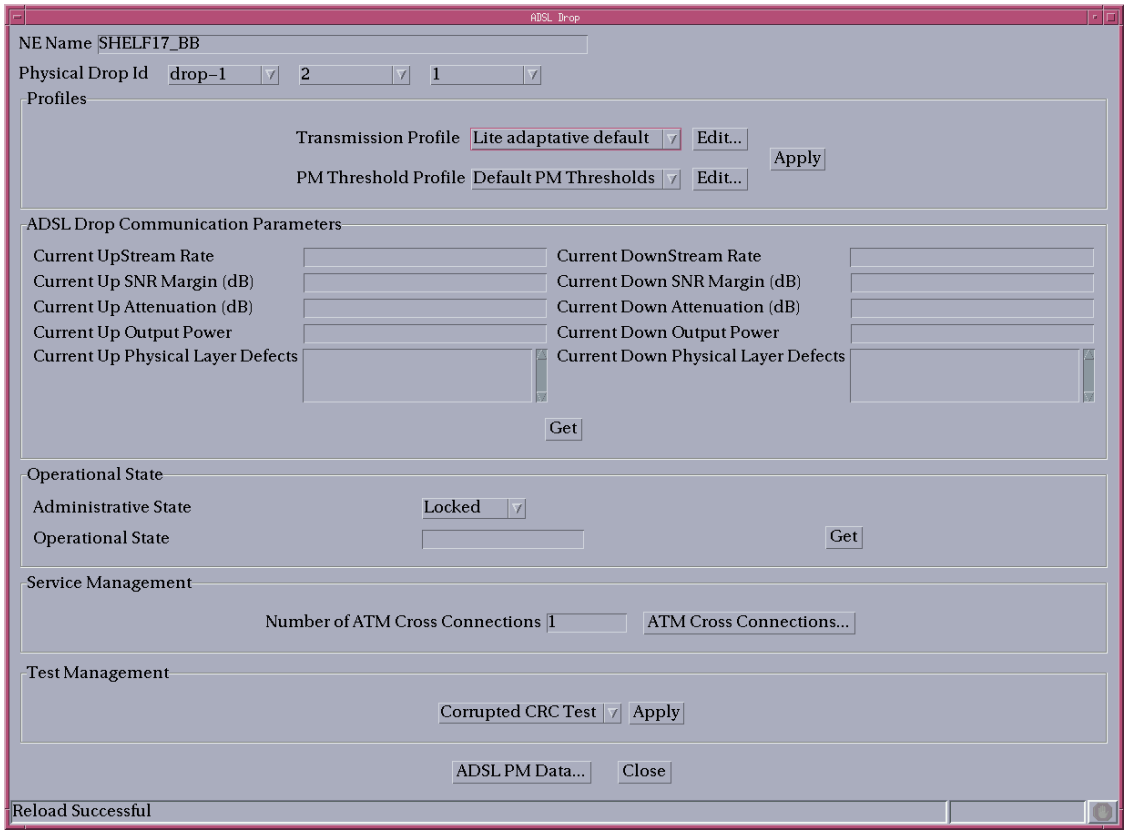


Figure 5-35 ADSL Drop window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Physical Drop Id	These fields display the ADSL drop id by means of three option menus: ■ The first one contains the drop shelf. Format: drop-1 or subdrop-{1, 8}. None is also allowed. ■ The second one contains the slot number inside the NE, but only for slots in which an ADSL pack is provisioned. Format: {1, 16} for main shelf or {1, 8} for subshelf None is also allowed. ■ The third one contains the drop number inside the slot indicated on the previous list {1, x}. Format: drop-shelf-slot-port. Possible values: drop-1-{1, 16}-{1, x} or subdrop-{1, 8}-{1, 8}-{1, x}. None is also allowed. (depending on the ADSL type x can be 4 or 8).
Profiles	**Transmission Profile**: This option menu lists all available transmission profiles. Selection of a profile is possible only if the administrative state is "Locked". The following profiles are available by default: ■ 1-lite_flexible_default ■ 2-full_flexible_default ■ 3-lite_explicit_default ■ 4-full_explicit_default. ***Edit***: This button provides access to the *ADSL Transmission Profile* window (cf. Chapter 5.5.5.31, page 5-115). **PM Threshold Profile:** This option menu lists all available PM profiles. Selection of a profile is possible only if the administrative state is "Locked". The following profiles are available by default: ■ 1-disable_all_Thresholds ■ 2-default_PM_Thresholds. ***Edit***: This button provides access to the *ADSL Threshold Profile* window (cf. Chapter 5.5.5.33, page 5-120). The ***Apply*** button is used to confirm the changes of the selected profiles. It is only enabled if any of the profiles have been modified. NOTE: If the physical drop is in service this operation is not allowed.

Parameters/ Buttons	Description
ADSL Drop Communication Parameters	This field shows the values of the following ADSL drop parameters: **Current Upstream Rate**, **Current Downstream Rate**, **Current Up SNR Margin (dB)**, **Current Down SNR Margin (dB)**, **Current Up Attenuation (dB)**, **Current Down Attenuation (dB)**, **Current Up Physical Layer Defects**, **Current Down Physical Layer Defects**, **Current Up Output Power**, **Current Down Output Power**. The ***Get*** button can be used to retrieve the current values from the NE.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Operational State** shows the state of the ADSL drop obtained (on demand) by the user. Possible values: Enabled, Disabled, Testing, Unknown, Dormant (NE R1.4). The ***Get*** button can be used to update the display of the Operational State.
Service Management	**Number of ATM Cross-Connections**: This field indicates the number of ATM cross-connections related to the ADSL port. The ***ATM Cross-Connections*** button provides access to the *ATM Cross-Connection* window.
Test Management	The ***Apply*** button can be used to start the Port BIST Test or the Corrupted CRC Test. The desired test is selected by means of the option menu. For more information refer to Chapter 7.4.
ADSL PM Data...	This button provides access to the *ADSL Performance Monitoring Data* window.

5.5.5.30 Modify an ADSL drop (data application)

This window is reached from the *ADSL AP* window (cf. Chapter 5.5.5.27, page 5-105) by pressing the ***Edit Drop*** button in the **ADSL Drop Information** field.

Procedure

Complete the following procedure to modify an ADSL drop:

Step	Procedure

1. Use the option menus **Physical Drop Id** to select the desired ADSL drop.

If you want to ...	then ...
edit a transmission profile	use the option menu **Transmission Profile** to select the desired profile and press ***Edit***. The *ADSL Transmission Profile* window pops up (cf. Chapter 5.5.5.31, page 5-115). Back in the *ADSL Drop* window, after modifying the profile, press ***Apply*** to confirm the changes.
edit a threshold profile	use the option menu **PM Profile** to select the desired profile and press ***Edit***. The *ADSL Threshold Profile* window pops up (cf. Chapter 5.5.5.33, page 5-120). Back in the *ADSL Drop* window, after modifying the profile, press ***Apply*** to confirm the changed profile.
change the administrative state	use the option menu **Administrative State**. NOTE: When changing from "Unlocked" to "Locked" the following warning message appears: **Changing the administrative state of the ADSL drop may be service affecting. Do you want to continue?**
add/edit/remove cross-connections	click on ***ATM Cross-Connections***. The *ATM Cross-Connection* window pops up (cf. Chapter 6.3.2, page 6-144).

If you want to ...	then ...
start the BIST test	use the option menu near the ***Apply*** button to select **BIST Test** and press ***Apply***. See also Chapter 7.4.2.3.
start the corrupted CRC test	use the option menu near the ***Apply*** button to select **Corrupted CRC Test** and press ***Apply***. See also Chapter 7.4.2.2.
edit the ADSL PM data	click on ***ADSL PM Data***. The *ADSL Performance Monitoring Data* window pops up (cf. Chapter 8.2.1).

2. Click on ***Close*** to exit the window.

5.5.5.31 Transmission Profile window (data application)

This window is used to create/modify/remove ADSL transmission profiles.

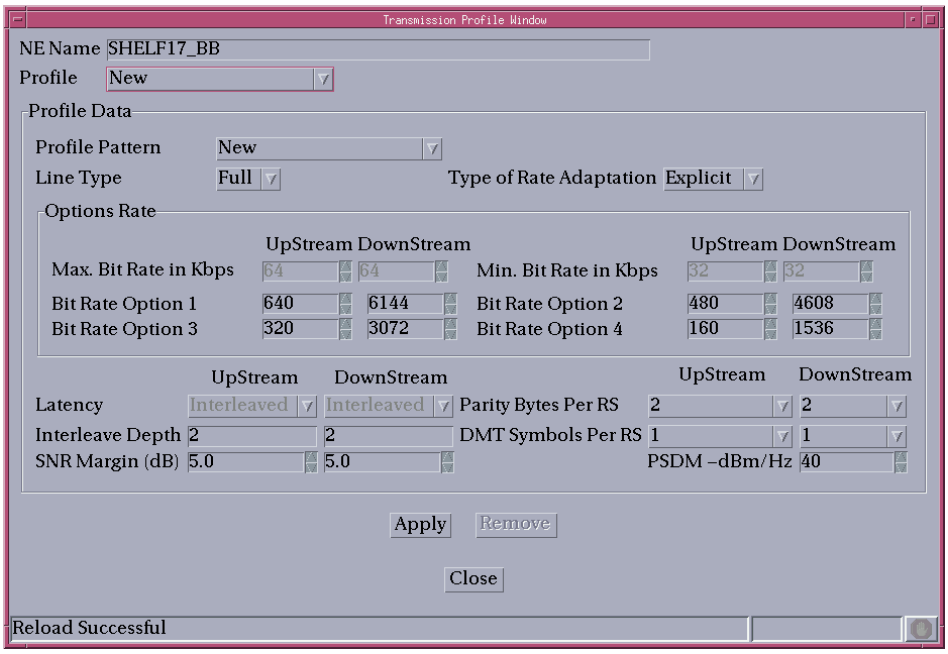


Figure 5-36 Transmission Profile window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Profile	This option menu contains the available profiles (for editing) and NEW (for creating a new profile). Format: txp-{1, 128}. NOTE: The first four default profiles (txp-1 to txp-4) can neither be edited nor removed. 1-lite_flexible_default 2-full_flexible_default 3-lite_explicit_default 4-full_explicit_default.

Parameters/ Buttons	Description
Profile Data	**Profile Pattern**: This option menu is used to get an example for a new profile. It is enabled only if NEW is selected in the option menu above. Otherwise the name of the selected profile is displayed. **Line Type**: This option menu shows the possible sub-types for a new profile: Full, Lite. **Type of Rate Adaption**: This option menu is used to select one of the following values: Explicit (default), Flexible.
Profile Data Options Rate	The parameters in this field are enabled or disabled depending on the selected value in the **Type of Rate Adaption** field. The following two parameters are enabled only if the **Type of Rate Adaption** is Flexible. **Max. Bit Rate in kbps**: Two spin buttons (upstream and downstream) can be used to define the values for the maximum bit rate. Possible values: upstream: 32 ... 1440 (steps of 32), downstream: 32 ... 13120 (steps of 32). **Min. Bit Rate in kbps**: Two spin buttons (upstream and downstream) can be used to define the values for the minimum bit rate. Possible values: upstream: 32 ... 1440 (steps of 32), downstream: 32 ... 13120 (steps of 32).

Parameters/ Buttons	Description
Profile Data Options Rate (continued)	The following four parameters are enabled only if the **Type of Rate** is explicit. **Bit Rate (kbps) Option 1**: Two spin buttons (upstream and downstream) can be used to define the values for the option 1 bit rate. Possible values (ADSL): upstream: 32 ... 1440 (default = 640) downstream: 32 ... 13120 (default = 6144). **Bit Rate (kbps) Option 2**: Two spin buttons (upstream and downstream) can be used to define the values for the option 2 bit rate. Possible values (ADSL): upstream: 32 ... 1440 (default = 480) downstream: 32 ... 13120 (default = 4608). **Bit Rate (kbps) Option 3**: Two spin buttons (upstream and downstream) can be used to define the values for option 3 bit rate. Possible values (ADSL): upstream: 32 ... 1440 (default = 320) downstream: 32 ... 13120 (default = 3072). **Bit Rate (kbps) Option 4**: Two spin buttons (upstream and downstream) can be used to define the values for option 4 bit rate. Possible values (ADSL): upstream: 32 ... 1440 (default = 160) downstream: 32 ... 13120 (default = 1536).

Parameters/ Buttons	Description
Profile Data	**Latency**: Two option menus (upstream and downstream) shows the value: Interleaved. **Interleave Depth**: These two text fields (upstream and downstream) are enabled only if the value for **Latency** is Interleaved. Possible values: {0, 255} (default in both directions = 2). **Parity Bytes per RS**: These two option menus (upstream and downstream) allow the following values to be selected: 0, 2, 4, 6, 8, 10, 12, 14, 16 (default in both directions = 2). These option menus are enabled only if the **Type of Rate Adaption** is Explicit. **DMT Symbols per RS**: These two option menus (upstream and downstream) are enabled only if the **Type of Rate Adaption** is Explicit. Possible values: 1, 2, 4, 8, 16 (default in both directions =1). **SNR Margin (dB)**: These two option menus (upstream and downstream) allow the following values to be selected: 0 ... 31 (default in both directions = 5). **PSDM dBm/Hz**: This option menu is used to set the line power. Possible values: 60 ... 40 (default = 40).
Remove	This button can be used to remove any profile except one of the first four default profiles.
Apply	This button is used to confirm the changes. The window remains open for further use.

5.5.5.32 Modify the ADSL transmission profile (data application)

Procedure Complete the following procedure to create/modify/remove a transmission profile:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Profiles -> ADSL Transmission*** via the cursor menu. The *ADSL Transmission Profile* window pops up.

   This window can also be reached from the *ADSL Drop* window (cf. Chapter 5.5.5.29, page 5-110) by pressing the ***Edit*** button for transmission profile.

If you want to ...	then ...
modify a transmission profile (not possible for the four default profiles)	use the option menu **Profile** to select the desired profile, edit the parameters in the fields **Profile Data** and **Profile Data Option Rate** and click on ***Apply*** to confirm.
create a new transmission profile	use the option menu **Profile** to select NEW, use the option menu **Profile Pattern** to select an available profile as an example, define the parameters in the fields **Profile Data** and **Profile Data Option Rate** and click on ***Apply*** to confirm.
remove a transmission profile (not possible for the four default profiles)	use the option menu **Profile** to select the desired profile and press ***Remove***. NOTE: The first four default profiles can not be removed. In case one of these profiles has been selected the ***Remove*** button is disabled.

2. Click on ***Close*** to exit the window.

5.5.5.33 Threshold Profile window (data application)

This window is used to create/modify/remove threshold profiles.

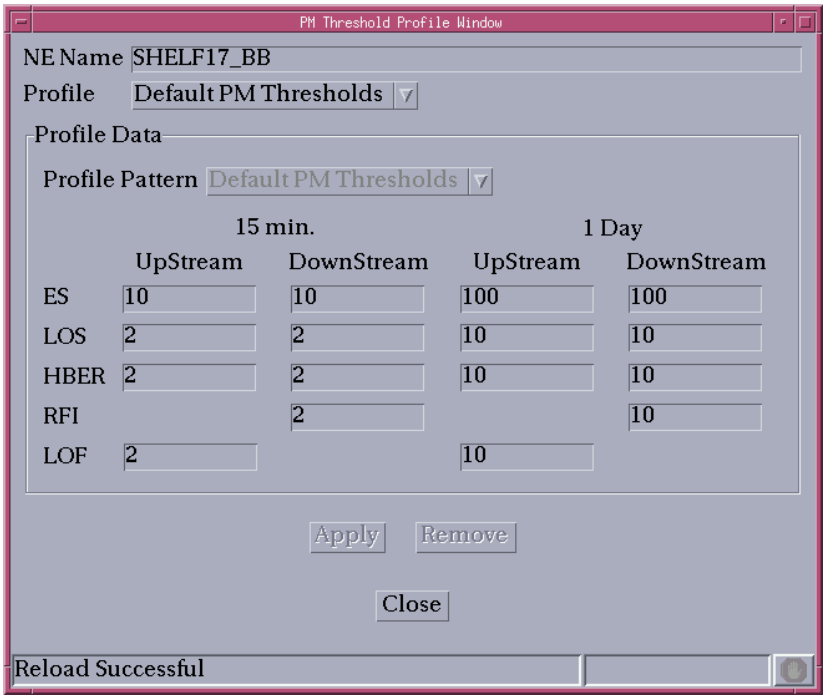


Figure 5-37 Threshold Profile window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Profile	This option menu contains the available profiles (for editing) and NEW (for creating a new profile). Format: pmtp-{1, 128}. NOTE: The first two default profiles (pmtm-1 and pmtm-2) can neither be edited nor removed. 1-disable_all_Thresholds 2-default_PM_Thresholds.

Parameters/ Buttons	Description
Profile Data	**Profile Pattern**: This option menu is used to select a profile to get an example for a new profile. It is enabled only if NEW is selected in the option menu above. Otherwise the name of the selected profile is displayed. **ES**: Four text fields show the values for two different time periods (15 min, one day) for the two directions (upstream and downstream). Possible values: 1 ... 900 for 15 min, 1 ... 86400 for one day. **LOS (Loss of Signal)**: Four text fields show the values for two different time periods (15 min, one day) for the two directions (upstream and downstream). Possible values: 1 ... 90 for 15 min, 1 ... 8640 for one day. **HBER (High Bit Error Rate)**: Four text fields show the values for two different time periods (15 min, one day) for the two directions (upstream and downstream). Possible values: 1 ... 90 for 15 min, 1 ... 8640 for one day. **RFI (Remote Failure Indication)**: Two text fields show the values for two different time periods (15 min, one day) for the downstream direction. Possible values: 1 ... 90 for 15 min, 1 ... 8640 for one day. **LOF (Loss of Frame)**: Two text fields show the values for two different time periods (15 min, one day) for the upstream direction. Possible values: 1 ... 90 for 15 min, 1 ... 8640 for one day.
Remove	This button can be used to remove any profile except one of the first two default profiles.
Apply	This button is used to confirm the changes. The window remains open for further use. NOTE: All profiles are applied on a port.

5.5.5.34 Modify the ADSL threshold profile (data application)

Procedure

Complete the following procedure to create/modify/remove an ADSL threshold profile:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Profiles -> ADSL Thresholds*** via the cursor menu. The *ADSL Threshold Profile* window pops up (cf. Chapter 5.5.5.33, page 5-120).

   This window can also be reached from the *ADSL Drop* window (cf. Chapter 5.5.5.29, page 5-110) by pressing the ***Edit*** button for the threshold profile.

If you want to ...	then ...
modify a threshold profile (not possible for the two default profiles)	use the option menu **Profile** to select the desired profile, edit the parameters in the field **Profile Data** and click on ***Apply*** to confirm.
create a new threshold profile	use the option menu **Profile** to select NEW, use the option menu **Profile Pattern** to select an available profile as an example, define the parameters in the fields **Profile Data** and click on ***Apply*** to confirm.
remove a threshold profile (not possible for the two default profiles)	use the option menu **Profile** to select the desired profile and press ***Remove***. NOTE: The first two default profiles can not be removed. In case one of these profiles has been selected the ***Remove*** button is disabled.

2. Click on ***Close*** to exit the window.

5.5.6 Network element synchronization

5.5.6.1 Telephony agent

5.5.6.1.1 Configuration information synchronization

Overview

The possibility exists for the AEM database to become inconsistent with the information stored locally in the telephony agent (non-volatile data storage (NVDS)). A database re-synchronization capability provides a mechanism for the AEM database to be made consistent (synchronized) with the locally stored NE information.

Two NE configuration data synchronization states can be identified:

- **SYNC**: The AEM database is consistent with the locally stored telephony agent information and all the autonomous messages concerning configuration changes are enabled (database changes, LED status reports, switch reports and some events of type protection switches, lockout and loopback).
- **ASYNC**: The AEM database and the telephony agent configuration data are out of synchronization and/or configuration reports are inhibited and/or the AEM configuration message buffer is overflowing.

For more information refer to the NE documentation for the NE releases.

5.5.6.1.2 Alarm information synchronization

Overview

In general alarms can be considered independently of each other (any alarm report can be processed by the AEM independent of other alarm reports). The AEM distinguishes two possible states for alarm handling: alarms from telephony agent are enabled or they are inhibited.

Two telephony agent alarm processing states can be considered:

- **PROC**: The AEM alarm database is consistent with the current telephony agent alarms. If NE alarm and/or environment alarm reports are inhibited, the AEM database is only a snapshot of telephony agent alarm information at a certain moment in time.
- **BLOCK**: The AEM alarm database and the current telephony agent alarms are out of synchronization due to alarm buffer overflow. The AEM alarm database is only a snapshot of telephony agent alarm information at a certain moment in time.

For more information refer to the NE documentation for the NE releases.

5.5.6.1.3 Synchronization Telephony window

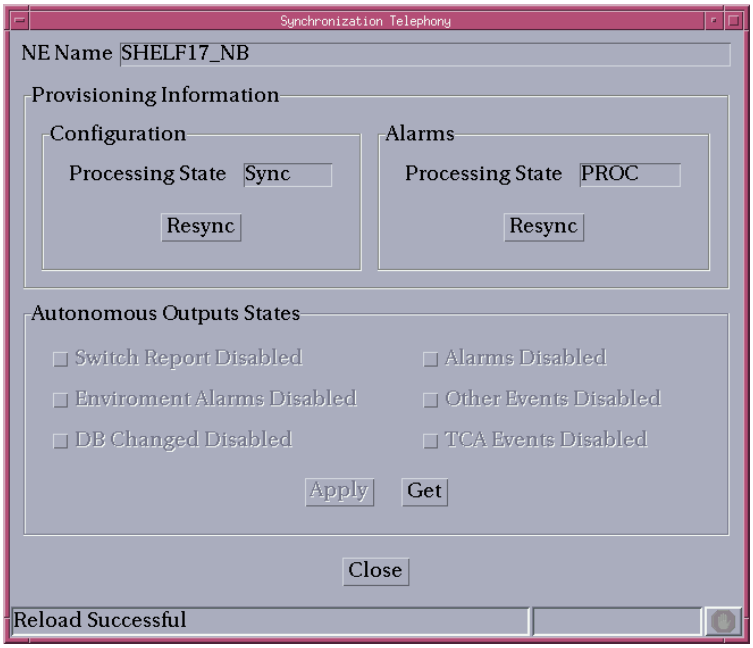


Figure 5-38 Synchronization Telephony window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Configuration	The **Processing State** represents the synchronization state between the AEM and NE. This information is automatically updated. Possible values: SYNC and ASYNC. The ***Label*** button (Resync or Sync) is used to change the synchronization state.
Alarms	The **Processing State** represents the alarm processing state between the AEM and NE. This information is automatically updated. Possible values: PROC and BLOCK. The ***Resync*** button is used to re-synchronize the alarm processing state.

Parameters/ Buttons	Description
Autonomous Output States	Check boxes show the state of the autonomous outputs (check box is marked: disabled; check box is not marked: enabled): TCA Events Disabled, Switch Reports Disabled, DB Changes Disabled, Other Events Disabled, Alarms Disabled, Environmental Alarms Disabled. This information is obtained from the NE by means of the ***Get*** button. After pressing this button the states can be changed by clicking in the boxes.
Apply	This button confirms the changes of the autonomous output states. The button is enabled only after the ***Get*** button has been pressed for the first time.
Get	This button is used to get the current values of the autonomous output states from the NE.

5.5.6.1.4 Modify the synchronization telephony parameter

Procedure

Complete the following procedure to modify the synchronization telephony parameter:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Synchronization -> Telephony*** via the cursor menu.
   The *Synchronization Telephony* window pops up.

   This window can also be reached from the *NE Management* window (tab Telephony - cf. Chapter 5.5.2.3, page 5-42) by pressing the ***More Details...*** button.

If you want to ...	then ...
change the processing state	use the ***Label*** button in the field **Configuration**.
re-synchronize the alarm processing state	use the ***Resync*** button in the field **Alarms**.
change the states of the autonomous outputs	click on ***Get*** in the field **Autonomous Output States,** use the check boxes to define the states and press ***Apply***.
exit the window	Click on ***Close***.

5.5.6.2 Data agent

5.5.6.2.1 Configuration information synchronization

General

The data agent is able to inform the AEM of its internal configuration changes. The data agent sends traps to the AEM to inform it about these changes. Currently the data agent only generates traps when specific changes occur. Besides that, the traps are not responded to by the AEM, so the data agent does not know if the AEM has received the trap or not. As a result the AEM does not show an updated view of the data agent. To solve this problem the AEM periodically polls the data agent in order to retrieve the internal information the data agent stores in its NVDS. This process is launched in a scheduled way as well as on user demand.

Autonomous reports

Each time a configuration synchronization process is done, the AEM retrieves all the configuration information from the data agent and then updates the AEM database to reflect the current state of the configuration information in the data agent. During the process the data agent state will be moved from COMM_ESTABLISHED to COMM_ESTABLISHED_SYNCHRONIZING.

Two NE configuration data synchronization states can be identified:

- **PROCESSING**: The AEM is processing all the traps concerning configuration changes and is updating the AEM database in accordance with the traps.
- **NOT_PROCESSING**: The AEM is discarding the configuration traps coming from the data agent. In this case it is possible that the AEM database and the data agent configuration data are out of synchronization.

5.5.6.2.2 Alarm information synchronization

Overview

The data agent informs the AEM of changes in alarms the data agent has generated by using alarm traps. Alarms can be considered independent of one of another (any alarm trap can be processed by the AEM independent of other alarm traps).

The data agent can not assure that the AEM has received each of the alarm traps because the AEM does not confirm receipt of the traps. The AEM periodically polls the data agent in order to retrieve all the alarms reported by the data agent and to update the AEM database to reflect the current state of the alarms in the data agent. This process is called an alarm synchronization process. This process is launched in a scheduled way as well as on user demand. During the process the data agent state changes from COMM_ESTABLISHED to COMM_ESTABLISHED_SYNCHRONIZING.

Two data agent alarm processing states can be considered:

- **PROCESSING**: The AEM is processing all the alarm traps coming from the data agent and is updating the AEM database in accordance with the traps. The AEM alarm database is consistent with the current data agent alarms, although it is possible that a trap could have been lost.

- **NOT_PROCESSING**: The AEM is discarding the alarm traps coming from the data agent. The AEM alarm database is only a snapshot of data agent alarm information at a certain moment in time. The alarms shown in the AEM do not match the current alarms of the data agent.

5.5.6.2.3 Synchronization Data window

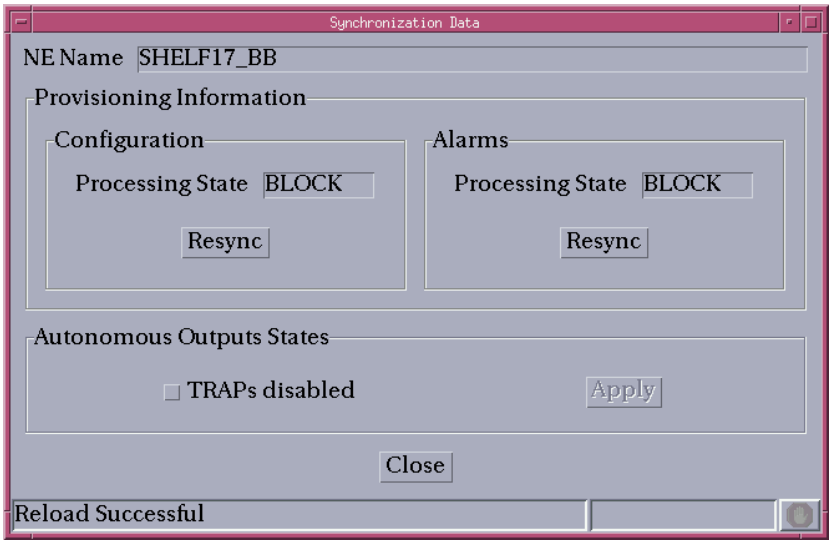


Figure 5-39 Synchronization Data window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Configuration	The **Processing State** represents the synchronization state between the AEM and NE. This information is automatically updated. Possible values: PROC and BLOCK. The ***Resync*** button is used to re-synchronize the data from the NE to the AEM database for configuration data.
Alarms	The **Processing State** represents the alarm processing state between the AEM and NE. This information is automatically updated. Possible values: PROC and BLOCK. The ***Resync*** button is used to re-synchronize the data from the NE to the AEM database for alarms.

Parameters/ Buttons	Description
Autonomous Output States	The check box **Traps Disabled** shows the state of this autonomous output (check box is marked: disabled; check box is not marked: enabled).
Apply	This button confirms the changes of the autonomous output state.

5.5.6.2.4 Modify the synchronization data parameter

Procedure

Complete the following procedure to modify the synchronization data parameter:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Synchronization -> Data*** via the cursor menu.
   The *Synchronization Data* window pops up.

   This window can also be reached from the *NE Management* window (tab Data - cf. Chapter 5.5.2.3, page 5-42) by pressing the ***More Details...*** button.

If you want to ...	then ...
re-synchronize the AEM database for configuration data	use the ***Resync*** button in the field **Configuration**.
re-synchronize the AEM database for alarms	use the ***Resync*** button in the field **Alarms**.
change the state of the autonomous output	use the check box **Traps Disabled** to define the state and press ***Apply***.
exit the window	Click on ***Close***.

5.5.7 Configuration of timing source (for telephony only)

Overview

The *AnyMedia* Access System supports two timing modes[1]: free running and loop timed.

- **Free running mode:** For free-running operation, the NE derives timing from an internal crystal oscillator (XO) with an accuracy not worse than ±32 parts-per-million (ppm) over full power supply, temperature, and lifetime. The free-running mode is intended only for turn-up and failure conditions.
- **Loop timed mode**: In this mode the NE recovers the clock from one of the up to 16 feeder E1 interfaces or from a Station Clock Interface (SCI).

Timing Inputs

The two timing inputs are identified as **Primary** (reference source) and **Secondary** (protection source). The first E1 feeder of the first IO_E1 pack is the default primary input, and the first feeder of the second IO_E1 pack is the default secondary input. The network provider can tailor the set of valid timing inputs and their priorities via provisioning. The primary and secondary reference signals can be selected from any physical feeder inputs on any two IO_E1 packs, or from two feeder inputs on the same pack. The NE can continue to derive timing from the reference inputs if one or both of the physical inputs is (are) switched to the protection IO_E1 pack.

For more information refer to the NE documentation.

Upon initialization, the NE selects the primary input as the active reference, and the secondary input as its alternate source. If the primary reference fails, the NE hardware switches to the alternate source, providing synchronization reference source protection is available (cf. Chapter 5.5.13, page 5-143).

1 The *AnyMedia* Access System hardware also supports external timing via a composite office clock; however, this mode is not supported in the release software.

5.5.7.1 Timing Source Control window

This window provides the operator with the facilities needed to configure the NE timing source for telephony service.

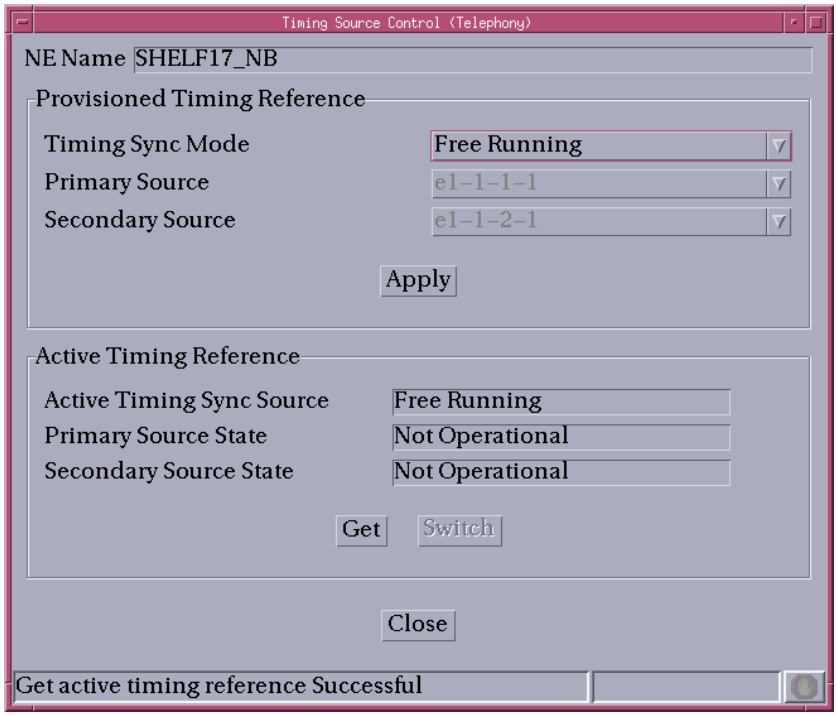


Figure 5-40 Timing Source Control window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Provisioned Timing Reference	**Timing Sync Mode:** This option menu displays the current timing synchronization mode. Possible values: Free Running, Loop Timed. Only in case of Loop Timed are the next two fields (**Primary Source** and **Secondary Source**) available. **Primary Source:** If **Timing Sync Mode** is Loop Timed, the primary source (working) and (optionally) the secondary source (standby) can be selected. Possible values: e1-1-{1, 4}-{1, 4} or station clock. Once the source(s) of synchronization has (have) been selected, click on the ***Apply*** button. **Secondary Source:** If **Timing Sync Mode** is **Loop Timed** and **Primary Source** has been selected, the secondary source can be selected as a protection timing synchronization source if the primary source fails. Possible values: e1-1-{1, 4}-{1, 4} or station clock. Once the protection source of synchronization has been selected, click on the ***Apply*** button. NOTE: The secondary source must be different from the primary source. Otherwise there is no protection available. The ***Apply*** button is available only if: ■ **Timing Sync Mode** has been changed. ■ **Synchronization Mode** is **Loop Timed** and at least one source has been modified. NOTE: During the apply operation, the ***Get*** and ***Switch*** buttons (see below) are disabled. The whole subpane will be updated as a result of the operation.

Parameters/ Buttons	Description
Active Timing Reference	If the ***Get*** button has not been pressed the following fields are empty. **Active Timing Sync Source**: Shows the active timing sync source of the NE. Possible values: Free Running, Loop Timed / PRI, Loop Timed / SEC. **Primary Source State**: Shows the primary source operational state. Possible values: Operational, Not Operational, Empty field (no value received). **Secondary Source State**: Shows the secondary source operational state. Possible values: Operational, Not Operational, Empty field (no value received). The ***Get*** button can be used to retrieve the **Active Timing Synchronization Source** and the operational state of primary and secondary sources (if applicable) from the NE. NOTE: During the get operation, the ***Apply*** and ***Switch*** buttons are disabled. The provisioned timing reference subpane will also be updated as a result of this operation. The ***Switch*** button can be used to switch between the working and standby sources of synchronization. In other words, the standby source becomes the working source and the working source becomes the standby source. This button is disabled if the **Active Timing Sync Source** is **Free Running** or the **Active Timing Sync Source** field is empty because the ***Get*** button has not been pressed yet or the operational state of the secondary source is **Not Operational**. NOTE: During the switch operation, the ***Apply*** and ***Get*** buttons are disabled. All fields will be updated as a result of this operation.

5.5.7.2 Modify the timing source

Procedure

Complete the following procedure to configure the timing source control parameter for telephony service:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Timing Source Control*** via the cursor menu.
   The *Timing Source Control* window pops up.

If you want to ...	then ...
change the provisioned timing synchronization mode	use the corresponding option menu in the **Provisioning Timing Reference** field and press ***Apply***.
change the provisioned primary source	use the corresponding option menu in the **Provisioning Timing Reference** field and press ***Apply***.
change the provisioned secondary source	use the corresponding option menu in the **Provisioning Timing Reference** field and press ***Apply***.
get the active timing synchronization source and the source states	press the ***Get*** button in the **Active Timing Reference** field.
switch between the working and standby sources of synchronization	press the ***Get*** button in the **Active Timing Reference** field to get the active values and click on ***Switch***.
exit the window	click on ***Close***.

5.5.8 Date & Time Telephony window

This window can be used to set the date and time of the telephony agent of the managed NE. Also it is possible to retrieve the date and time of any NE.

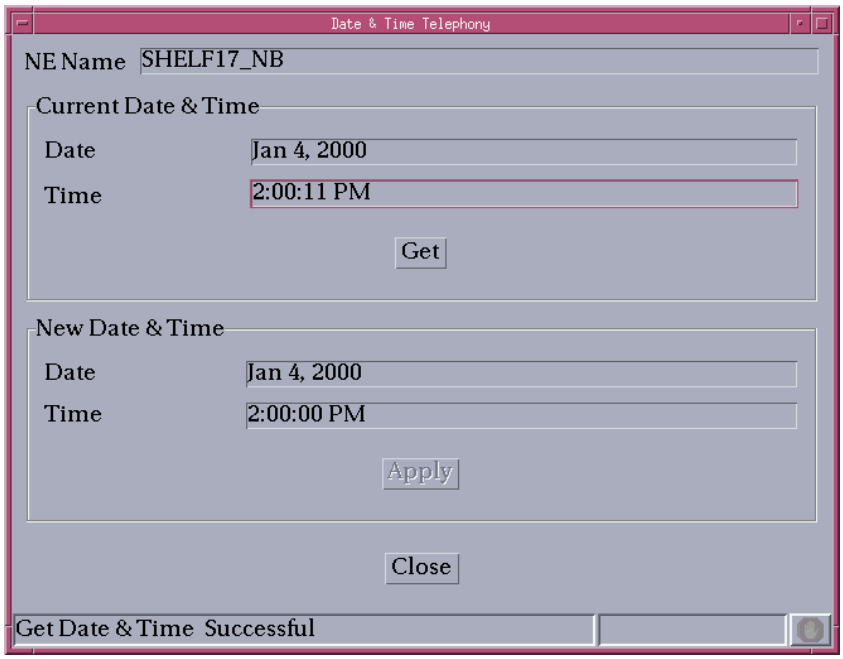


Figure 5-41 Date & Time Telephony window

The following values are possible:

- 12.00 AM to 11.59 PM for time
- Jan. 1, 1980 to Dec. 12, 2036.

The format follows the locale and platform conventions (e.g. for Spain the date format is day/month/year).

Procedure

Complete the following procedure to retrieve/set the date and time of the telephony agent of an NE.

Step	Procedure

1. Select the ***NE*** in the Network Element Browser and ***Date & Time -> Telephony*** via the cursor menu.
The *Date & Time Telephony* window pops up.

If you want to ...	then ...
to retrieve the current date and time data	Click on ***Get*** in the **Current Date & Time** field. The corresponding data will be shown.
to set the date and time data	use the text fields in the **New Date & Time** field to enter the corresponding values and press ***Apply***.
exit the window	click on ***Close***.

5.5.9 Date & Time Data window

This window can be used to set the date and time of the data agent of the managed NE. Also it is possible to retrieve the date and time of any NE.

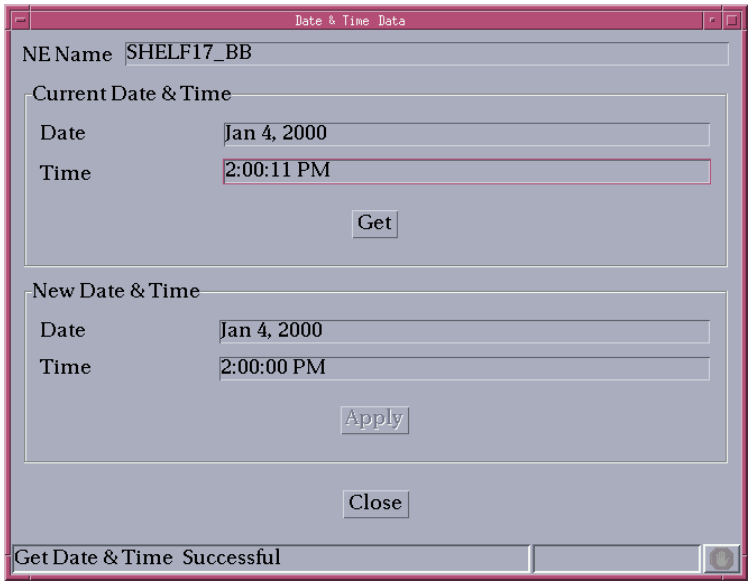


Figure 5-42 Date & Time Data window

The following values are possible:

- 12.00 AM to 11.59 PM for time
- Jan. 1, 1980 to Dec. 12, 2036.

The format follows the locale and platform conventions (e.g. for Spain the date format is day/month/year).

Procedure

Complete the following procedure to retrieve/set the date and time of the telephony agent of an NE.

Step	Procedure

1. Select the ***NE*** in the Network Element Browser and ***Date & Time -> Data*** via the cursor menu.
   The *Date & Time Data* window pops up.

If you want to ...	then ...
to retrieve the current date and time data	Click on ***Get*** in the **Current Date & Time** field. The corresponding data will be shown.
to set the date and time data	use the text fields in the **New Date & Time** field to enter the corresponding values and press ***Apply***.
exit the window	click on ***Close***.

5.5.10 NE Inventory window

This window provides inventory and summary information for both telephony and data services. Two non-editable tables display NE inventory information. The first table contains per slot data, while the second one provides summarized information per card type.

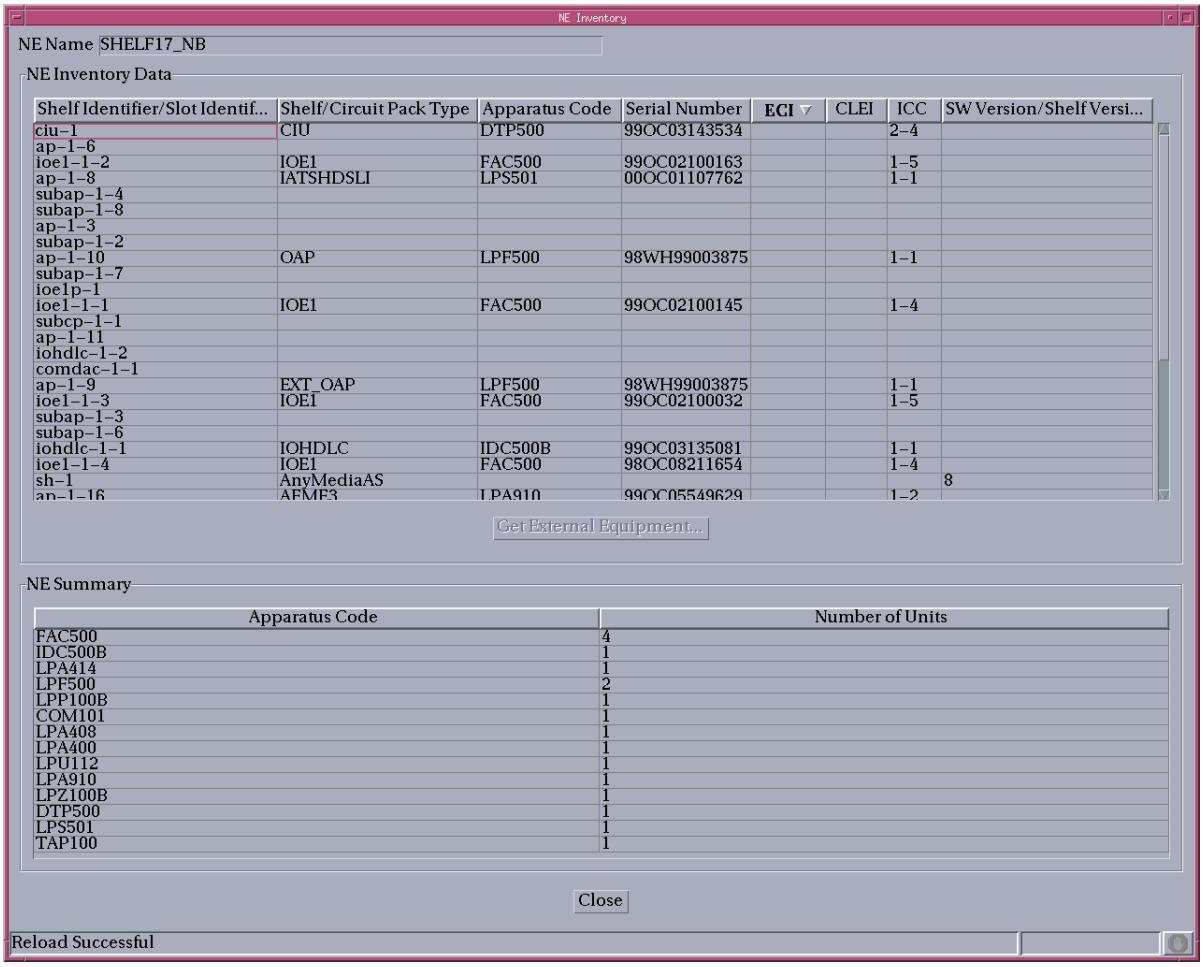


Figure 5-43 NE Inventory window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
NE Inventory data	**Shelf Number/Slot Number**: Numeric field that identifies the position of each pack. **Shelf Type/Circuit Pack Type**: Mnemonic that identifies the shelf type and the pack type. Possible shelf types: AnyMediaAS, Intl_ONU. Possible pack types: COMDAC, CIU, IO_E1, IO_HDLC, PROG2W, COIN, ZEUS, ISDN12_U, TAP, AFME3, ADSL4. **Apparatus Code**: Identifies the specific function provided by the pack. Possible values: COM500, COM501 (R1.4), DTP500, FAC500, IDC500, LPZ100B, LPP100B, LPZ120 (not available in R1.1), LPU112 (not available in R1.1), TAP100, LPA910, LPA400, LPA408, LPA900. **Serial Number**: A 12-character alphanumeric code that identifies each pack. It includes the date and place of manufacture. **ECI**: Code that corresponds to the bar-coded label on the faceplate of the pack. There is a one-to-one correspondence between CLEI and ECI codes. **CLEI**: Code assigned by Bellcore that provides information about the functionality of the pack. **ICC**: Indicates the interchangeability among packs to specify forward/backward compatibility. Format of the ICC is **m:n** where **m** is the issue number and **n** the Series Number. **SW Version/Shelf Version**: The software version is only applicable for COMDACs and AFMs. For these packs it is obtained from the NE at connection time. Internally, the AEM verifies whether the mentioned SW Version is manageable by the system. The shelf version applies to shelves and subshelves. ***Get External Equipment...***: This button provides access to the *External Equipment* window to display external equipment information of the whole NE. The button is enabled only for HDSL packs.
NE Summary	**Apparatus Code**: Displays a mnemonic that identifies the apparatus code type. Possible values: COM500, DTP500, FAC500, IDC500, LPZ100B, LPP100B, LPZ120 (not available in R1.1), LPU112 (not available in R1.1), LPU 430 (not available in R1.3), TAP100, LPA910, LPA400, LPA408, LPA900. **Number of Units**: Displays two numbers: the number of packs and the number of unplugged units.

5.5.10.1 Get the NE inventory data

Procedure Complete the following procedure to display the NE inventory data.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Inventory*** via the cursor menu. The *NE Inventory* window pops up (cf. Chapter 5.5.10, page 5-138).
2.	Clicking on one of the column headers sorts the inventory data according to the column entries. Clicking again reverses the sort order.

If you want to ...	then ...
display the external equipment information of the whole NE	click on ***Get External Equipment...***. The *External Equipment* window pops up (see the following chapter).
display the external equipment information of a specific HDSL pack	select the desired pack and click on ***Get External Equipment...***. The *External Equipment* window pops up (see the following chapter).
exit the window	click on ***Close***.

5.5.10.2 External Equipment window

This window displays the external equipment information (Equipment ID, Description) of an NE, subshelf, etc. It can be reached only from the *NE Inventory* window (see above). External equipment is possible only if an HDSL pack is available.

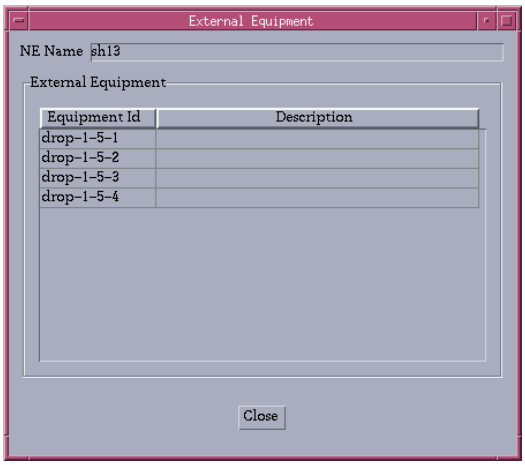


Figure 5-44 External Equipment window

5.5.11 Network element working mode

Selection of the working mode via GUI is not yet implemented. It is only possible via Cut-Through interface (cf. Chapter 5.5.18, page 5-170) using TL1 commands (Set-CFG-ISDN, SW-CFG).

The system supports an active system configuration which is currently used and a standby system configuration which is set with the command "Set-CFG-ISDN". Possible values for the configurations are: POTS or POTS/ISDN Mixed.

The standby system configuration is activated with the switch configuration command "SW-CFG".

5.5.12 Simplex COMDAC protection scheme

Overview

The NE automatically sets the COMDAC protection mode (or duplex mode) when both COMDACs are plugged in. Then the alarming state of both COMDACs slots is set to **Required** and the AEM is not able to change it until one of the COMDACs is removed. When a COMDAC is removed, the AEM is then able to set that slot to **Not-Required**, so the COMDAC protection mode is disabled (simplex).

5.5.12.1 COMDAC window

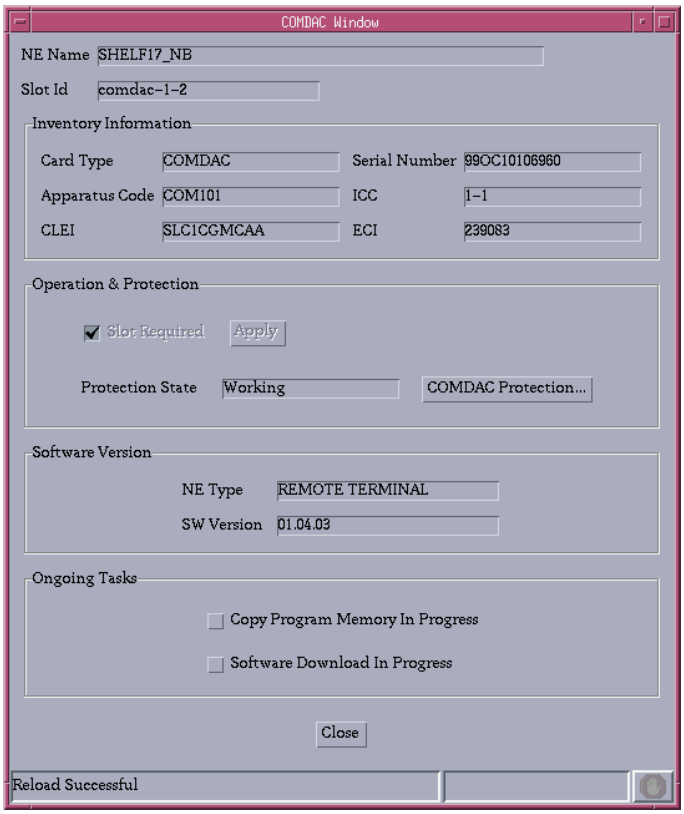


Figure 5-45 COMDAC window

This window includes hardware and software data (inventory) as well as the operational and protection state. The **Inventory Information** field contains read-only fields (cf. Chapter 5.5.5.5, page 5-62).

For configuring the protection scheme the field **Operation & Protection** is used.

Parameters/ Buttons	Description
Slot Required	This check box displays the required state of the shelf slot. This state can be changed by the user (from REQUIRED to NOT REQUIRED or vice versa) as long as the pack is **not** inserted. However, it is **not** possible to set both COMDACs to **not** required. The ***Apply*** button is available if a change in the **Slot Required** check box has been made.
Protection State	This non-editable field shows whether the selected COMDAC is working or not. Possible states are: Working (providing service) or Standby (not in service) or Not Equipped (slot is un- equipped).
COMDAC Protection...	This button provides access to the *Shelf Protection* window (COMDAC tab) to allow modification of the current protection scheme or for performing protection switching (cf. Chapter 5.5.13.1, page 5-144).

5.5.12.2 Set the COMDAC protection to simplex

Procedure

Complete the following procedure to set the COMDAC protection to simplex:

Step	Procedure
1.	Select ***NE -> Main Shelf -> COM500*** in the Network Element Browser and ***View*** via the cursor menu or select ***View -> Object*** via the menu bar or single click on the pack ***COMDAC*** in the *Shelf View* window. The *COMDAC* window pops up:
2.	Deselect the check box **Slot Required**.
3.	Click on ***Apply*** to confirm (the window remains on screen for further use).
4.	Click on ***COMDAC Protection...*** to open the *Shelf Protection* window (COMDAC tab) (cf. Chapter 5.5.13.1, page 5-144) or click on ***Close*** to exit the window.

5.5.13 Equipment protection switching

General

Equipment protection switching provides an automatic recovery mechanism in the *AnyMedia* Access System when a fault is detected. NE entities that are involved in carrying service to a large number of end users are generally required to be protected with a redundant unit. However, the NE provides customer options to have

none or some entities protected with redundant units. These entities can be either 1:1 or 1:N protected. For 1:1 protected entities, one of them serves as the active or primary unit and the other serves as a "protection" or standby unit. For 1:N protected entities, one entity serves as the "protection" or standby unit for all N active units. If an active unit fails, the failure is detected and service is automatically “protection switched” to the protection unit. The protection switching can also be requested on demand.

Revertive/non-revertive

Equipment protection switching can be revertive or non-revertive. Revertive protection switching implies that the active and standby units will return to their original configuration once the failure causing the protection switch has been repaired. Non-revertive switching does not return the entities to their original configuration. With non-revertive switching, the repaired unit becomes the new standby unit.

The *AnyMedia* Access System R1.7 supports the following protection features:

- COMDAC pack - 1:1 protection; non-revertive switch (cf. following section).
- IO_HDLC packs - 1:1 protection; non-revertive switch - (cf. Chapter 5.5.13.3, page 5-147).
- Synchronization reference source - 1:1 protection; non-revertive switch (cf. Chapter 5.5.7, page 5-129).

Definitions

The different kinds of switching (COMDACs and IO_HDLC circuit packs) are defined as follows:

- **Side switching:** refers to the operation of deactivating the active core entity and activating the standby core entity.
- **Manual (normal) switch:** refers to an AEM-initiated switch command that instructs the NE to perform a switch only if the protection unit is in service and there are no known faults.
- **Forced switch:** refers to an AEM-initiated switch command that instructs the NE to perform a switch no matter what the conditions of the protection unit.
- **Inhibit switch:** refers to an AEM-initiated switch command that instructs the NE to inhibit a side switch no matter what the conditions of the active unit.

5.5.13.1 COMDAC Protection window

Overview

The COMDAC is the core pack of the *AnyMedia* Access System. The NE supports both duplex and simplex operations, i.e., the COMDAC can be protected or unprotected. In duplex operation, the COMDAC will run in an active and standby mode.

The NE automatically sets the COMDAC protection mode when both COMDACs are plugged in. Then the alarming state of both COMDACs slots is set to **Required** and the AEM is not able to change it until one of the COMDACs is removed. When a COMDAC is removed, the AEM is then able to set that slot to **Not-Required**, so the COMDAC protection mode is disabled (simplex).

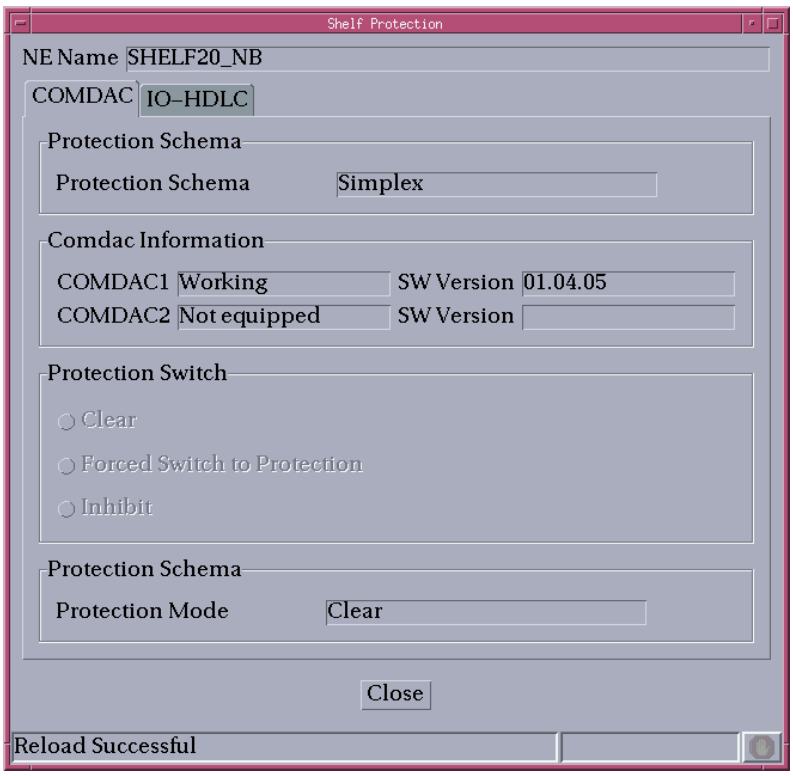


Figure 5-46 Shelf Protection window (tab COMDAC)

This window provides COMDAC protection information. It also provides the mechanisms needed to perform changes in the protection scheme as well as protection switches.

The following table shows the view/edit options of the *Shelf Protection* window (tab COMDAC):

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Protection Schema	Represents the protection scheme used in the NE. If only one COMDAC is present in the shelf, the protection scheme is **Simplex**. If both COMDACs are present, **Duplex** is the value shown. Only in this case (Duplex configuration) is the **Protection Switch** field available (see below).

Parameters/ Buttons	Description
COMDAC Information	**COMDAC 1 (2):** This non-editable fields display the current COMDAC working state. The following values are possible: Working, Standby and Not Equipped (if there is no COMDAC inserted in the corresponding slot). **SW Version:** Shows the SW Version for the respective COMDAC.
Protection Switch	Radio buttons allow protection switching to be specified. Only the working COMDAC is inhibited. With the **Forced Switch to Protection** request the working COMDAC becomes standby and vice versa. All radio buttons are disabled if the current protection scheme is **Simplex**. The NE rejects a switch request if the **Protection Mode** is **Inhibit**. Therefore before you can switch from **Forced Switch to Protection** to **Inhibit** or vice versa you have to **Clear** the current protection. The ***Apply*** button is used confirm the changes within this field.
Protection Mode	This field displays the current protection mode which will be updated as a result of a protection switch. Possible values: Clear, Inhibit.

5.5.13.2 Modify the COMDAC protection mode

Procedure Complete the following procedure to modify the protection mode for the COMDAC.

Step	Procedure

1. Select ***NE -> Main Shelf*** in the Network Element Browser and ***Protection*** via the cursor menu
   The *Shelf Protection* window pops up (tab COMDAC).

   This window can also be reached from the *COMDAC* window (cf. Chapter 5.5.5.5, page 5-62) via ***COMDAC Protection...***.

2. Use the radio buttons in the field **Protection Switch** to switch the protection: **Clear** or **Forced Switch to Protection** or **Inhibit.**

3. Press ***Apply*** to confirm. A *Warning* window pops up:

   `Protection switching may be service affecting.`
   `Do you want to continue?`

   If you decide to continue, the switch operation will be started. The information displayed will be updated once the switch is finished to show the current state.

The following events set off error messages:

- The NE detects an error in the switch request (i.e. the request cannot be executed due to another activity in the AEM).
- The NE rejects a switch request because the **Protection Mode** is **Inhibit**.
- The NE cannot execute the request as the NE software installation is in progress.

4. Click on tab HDLC to change the window (see next section) or click on ***Close*** to exit the window.

5.5.13.3 IO_HDLC Protection window

Overview For the IO_HDLC pack 1:1 protection applies where one IO_HDLC pack serves as the active or primary and the other serves as a "protection" or standby unit. If an active unit fails, the failure is detected and service is automatically "protection switched" to the protection unit. The protection switching can also be requested on demand. IO_HDLC protection switching is only possible in R1.7.

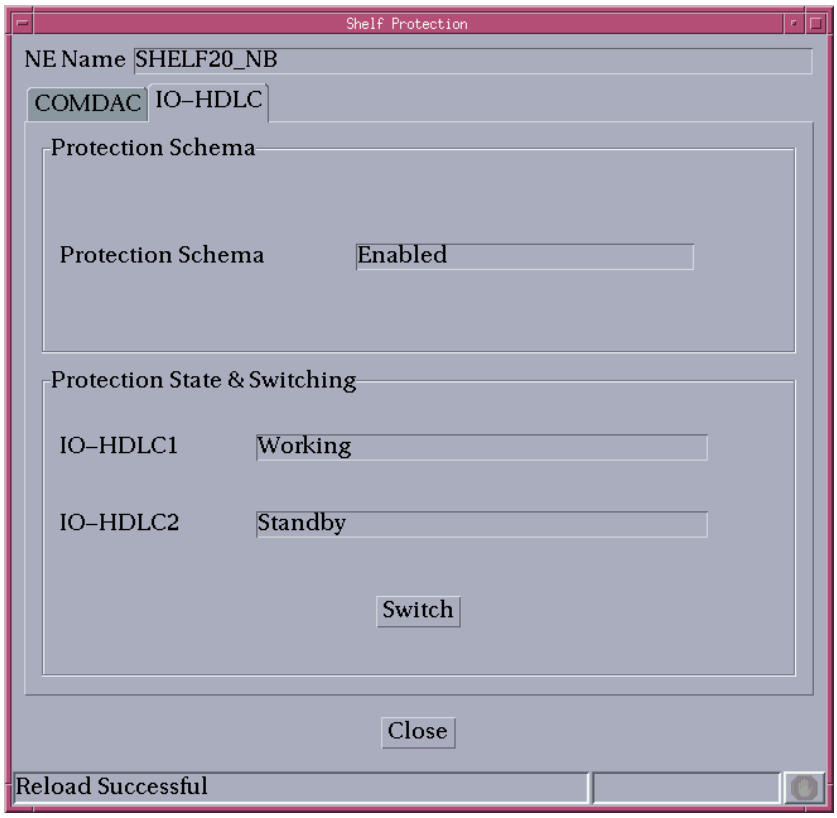


Figure 5-47 Shelf Protection window (tab IO_HDLC)

This window provides IO_HDLC protection information. It also provides the mechanisms needed to perform changes in the protection scheme as well as protection switches.

The following table shows the view/edit options of the *Shelf Protection* window (tab IO_HDLC):

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Protection Schema	This field shows the protection scheme for IO-HDLCs used in the NE. Possible values: Enabled (if switching between IO_HDLCs is enabled) Disabled / Not Equipped, Disabled / Not in service (i.e. the card is not pre-provisioned or its administrative state is "Locked"), Disabled / POTS-only mode.

Parameters/ Buttons	Description
Protection State & Switching	**IO-HDLC 1 (2):** This non-editable fields display the current IO-HDLC working state. Possible values: Working, Standby and Not applicable (if there is either no IO_HDLC inserted in the corresponding slot, no IO_HDLC provisioned for this slot or the NE is operating in POTS-only mode, or a combination of the previous conditions). The ***Switch*** button is enabled if the protection scheme is enabled. In that case, pressing the button causes the working/standby states to be switched in the NE.

5.5.13.4 Modify the IO_HDLC protection mode

Procedure Complete the following procedure to modify the protection switching for IO_HDLC.

Step	Procedure

1. Select ***NE -> Main Shelf*** in the Network Element Browser and ***Protection*** via the cursor menu.
   The *Shelf Protection* window pops up.

2. Click on tab ***IO_HDLC***.

   This window can also be reached from the *IO_HDLC* window (cf. Chapter 5.5.5.7, page 5-66) via ***HDLC Protection...***.

3. Press ***Switch*** to switch the protection state. The *Warning* window pops up:

   `Protection switching may be service affecting. Do you want to continue?`

   If you decide to continue, the switch operation will be started. The information displayed will be updated once the switch is finished to show the current state.

The following events set off error messages:

- The NE detects an error in the switch request (i.e. the request cannot be executed due to another activity in the AEM).
- The NE cannot execute the request as the NE software installation is in progress.
- The forced switch is denied as the protecting slot is locked out.
- The manual switch is denied either because there is a higher protection switch active (Inhibit, Forced) or because an automatic switch is already protecting that protected slot.

4. Click on ***Close*** to exit the window.

5.5.13.5 Alarm configuration

Configuration of the alarm severities is only possible via the cut-through interface (cf. Chapter 5.5.18, page 5-170). The corresponding TL1 commands are available on-line using the GSI help on *AnyMedia* Access System.

5.5.14 Network element software upgrade

This function is subdivided into two parts: NE software download (for telephony and data agents) and program copy (only for telephony agent - COMDAC).

5.5.14.1 Network element software download (telephony agent)

Overview

There are two software versions, the one in the active COMDAC and the new one to be downloaded (must be placed in $ANYMEDIA/CM/nefiles/NVPS). It is assumed that the user has a copy of the software currently running in the active COMDAC.

The software download procedure is as follows:

- start download
- load software into the standby COMDAC.

Assumptions

For the following description it is assumed that the NE is already connected and the NE hardware platform is prepared to receive and work with the new program version.

5.5.14.2 COMDAC Software Download window

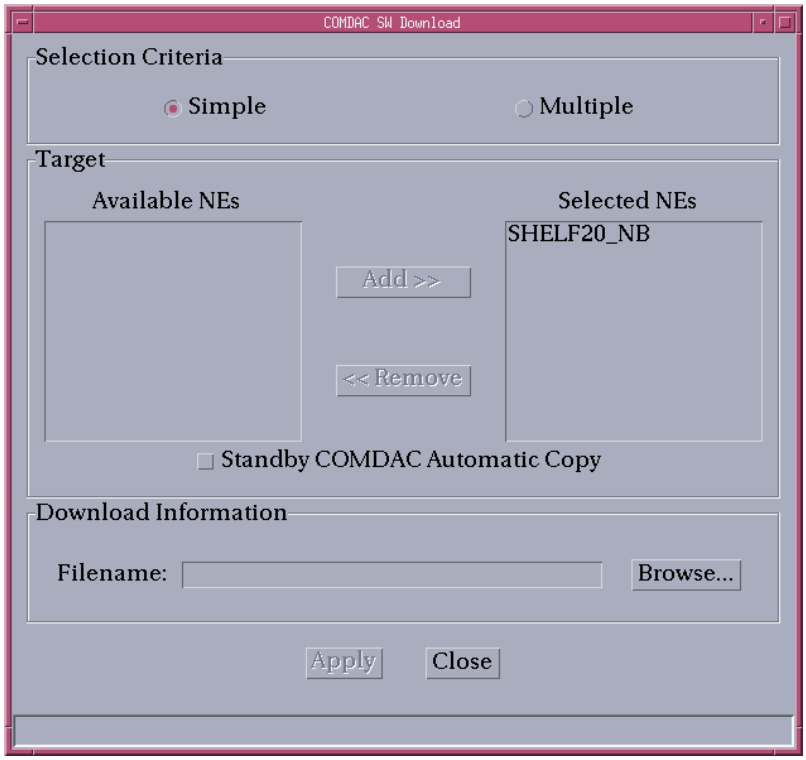


Figure 5-48 COMDAC Software Download window

This window provides the functionality needed to download files to an NE or to a set of NEs with telephony agent. The following table shows the parameters of this window:

Parameters/ Buttons	Description
Selection Criteria	Two radio buttons are used to define the target of the download file. **Single**: The target is the pre-selected NE, only its name is in the **Selected NEs** list (see below). The **Add** and **Remove** buttons are disabled. **Multiple**: The **Available NEs** list shows all existing NEs. By means of the ***Add*** button the NEs can be moved to the S**elected NEs** list.

Parameters/ Buttons	Description
Target	The **Available NEs** list shows all existing NEs (with telephony agents) sorted alphabetically. The **Selected NEs** list shows all NEs to which the download is being done. The ***Add >>*** button can be used to move the selected NE from the **Available NEs** list to the **Selected NEs** list. The ***<< Remove*** button can be used to remove domains from the **Selected NEs** list. (The ***Add >>*** button and the ***<< Remove*** button are available only after having selected an NE from the corresponding list.) The check box **Standby Comdac Automatic Copy** can be used to initiate the automatic copying of the software from the working COMDAC to the standby COMDAC after the software download is completed successfully.
Download Information	**Filename:** This text field shows the name of the file which will be downloaded. The ***Browse...*** button opens the *File Browser* window where the file can be selected.
Apply	This button is used to start the software download.

5.5.14.3 Software download to telephony agent

Procedure Complete the following procedure to start the software download:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Software Download -> Telephony*** via the cursor menu. The *COMDAC Software Download* window pops up.
2.	Use the radio buttons in the field **Selection Criteria** to define single or multiple download. For single download proceed with step 4, for multiple download proceed with step 3.
3.	Use the ***Add >>*** button in the field **Target** to move the desired NEs to the **Available NEs** list.
4.	Set the check box **Standby Comdac Automatic Copy** if you want to copy automatically the software from the working COMDAC to the standby COMDAC after the software download is completed successfully (the copy can also be done later by means of the *COMDAC Program Copy* window - cf. Chapter 5.5.15, page 5-159).

5. Click on the ***Browse...*** button in the **Download Information** field to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select the file (example of the file structure: NE Files/NVPS/COMDAC R1...) that should be downloaded.

6. Click on ***OK*** to confirm. The chosen file name appears in the field **Filename** in the *COMDAC Software Download* window

7. Click on ***Apply*** to initiate the download process. A *Warning* window pops up (the *Software Download* window remains on the screen after the download is finished):

   SW Download is service affecting and the command can not be cancelled while its execution. Continue anyway?

   If you decide to continue the AEM starts the download procedure. The *COMDAC SW Download In Progress* window pops up:

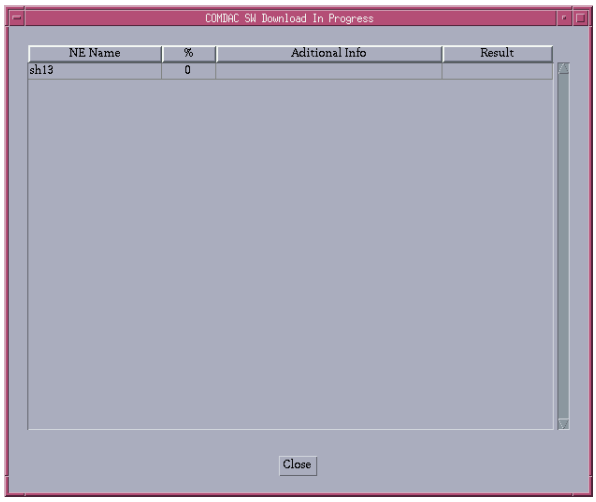


Figure 5-49 COMDAC SW Download In Progress window

This window provides the following information: NE Name, percent of the software download (FTP) operation executed, feedback (Additional information such as write-software, FTP, copy-memory) and the result of the software download operation (successful or unsuccessful).
This information is shown for each NE for which the software download is being performed.

NOTE:
The software download process cannot be cancelled.

8. After the download process is finished click on ***Close*** to exit the *COMDAC Software Download* window.
This button is disabled while the SW download process is being executed.

NOTE:
The following errors will stop the download process:

- NE does not match login and password. The AEM returns operation failed to the AEM.
- NE detects that the side switch to the standby COMDAC is not possible (e.g. 2nd COMDAC not present) and rejects the SW download operation.
- If the download of the data fails an alarm is issued and manual intervention will be required to:
  - restart the download procedure from the beginning, or
  - write from the active COMDAC to the standby COMDAC to back out the partial load (duplex configuration) - see Chapter 5.5.15, page 5-159.
- If the software program is not installed successfully on the standby COMDAC:

  In duplex configuration, an alarm will be sent to the AEM and manual intervention will be required to:
  - restart the download procedure from the beginning, or
  - write from the active COMDAC to the standby COMDAC to remove the downloaded copy - see Chapter 5.5.15, page 5-159.
- The TCP connection between AEM and NE is lost.

5.5.14.4 AFM Software Download window

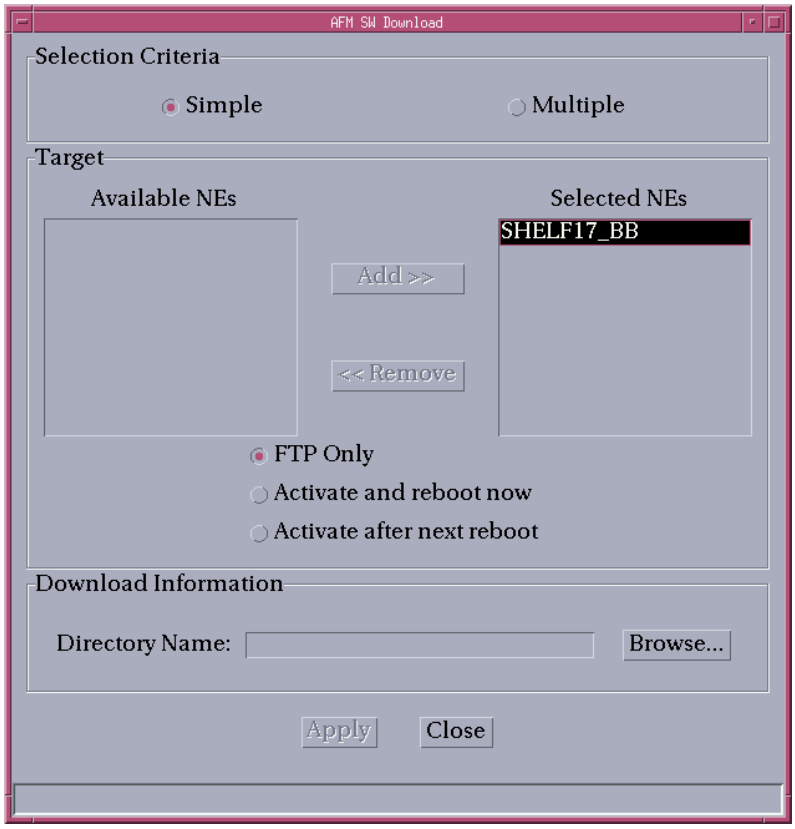


Figure 5-50 AFM Software Download window

This window provides the functionality needed to download files to an NE or to a set of NEs with data agent. The following table shows the parameters of this window:

Parameters/ Buttons	Description
Selection Criteria	Two radio buttons are used to define the target of the download file. **Single**: The target is the pre-selected NE, only its name is in the **Selected NEs** list (see below). The **Add** and **Remove** buttons are disabled. **Multiple**: The **Available NEs** list shows all existing NEs. By means of the ***Add*** button the NEs can be moved to the **Selected NEs** list.

Parameters/ Buttons	Description
Target	The **Available NEs** list shows all existing NEs (with data agents) sorted alphabetically. The **Selected NEs** list shows all NEs to which the download is being done. The ***Add >>*** button can be used to move the selected NE from the **Available NEs** list to the **Selected NEs** list. The ***<< Remove*** button can be used to remove domains from the **Selected NEs** list. (The ***Add >>*** button and the ***<< Remove*** button are available only after having selected an NE in the corresponding list.) Three radio buttons can be used to define the download procedure: ■ **FTP only** (only download) ■ **Activate after next reboot** (download and automatic activation after the next reboot) ■ **Activate and reboot now** (download and automatic activation immediately).
Download Information	**Directory name:** This text field shows the name of the file which will be downloaded. The ***Browse...*** button opens the *File Browser* window where the directory can be selected.
Apply	This button is used to start the software download.

5.5.14.5 Software download to data agent

Procedure Complete the following procedure to start the software download:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Software Download -> Data*** via the cursor menu. The *AFM Software Download* window pops up.
2.	Use the radio buttons in the field **Selection Criteria** to define single or multiple download. For single download proceed with step 4, for multiple download proceed with step 3.
3.	Use the ***Add >>*** button in the field **Target** to move the desired NEs to the **Available NEs** list.

4. Use the radio buttons **FTP only**, **Activate after next reboot** or **Activate and reboot now** in the **Target** field to define the desired download manner. (Please note that the copying and activation can also be done later by means of the *AFM Program Copy & Validation* window - cf. Chapter 5.5.16, page 5-161.)

5. Click on the ***Browse...*** button in the **Download Information** field to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select the directory (example of the file structure: NE Files/NVPS/AFM R1...) that should be downloaded.

6. Click on ***OK*** to confirm. The chosen file name appears in the field **Directory name** in the *AFM Software Download* window.

7. Click on ***Apply*** to initiate the download process. A *Warning* window pops up (the *Software Download* window remains on the screen after the download is finished):

   SW Download is service affecting and the command can not be cancelled while its execution. Continue anyway?

   If you decide to continue the AEM starts the download process. An *AFM SW Download In Progress* window pops up:

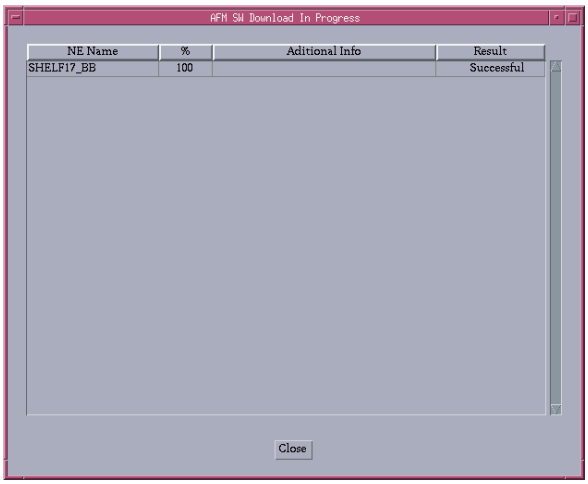


Figure 5-51 AFM SW Download In Progress window

This window provides the following information: NE Name, percent of the software download (FTP) operation executed, feedback (additional Information such as write-software, FTP, copy-memory) and the result of the software download operation (successful or unsuccessful).
This information is shown for each NE to the software download is being performed.

NOTE:
The software download process cannot be cancelled.

8. After the download process is finished click on ***Close*** to exit the *AFM Software Download* window.
This button is disabled while the SW download process is being executed.

5.5.15 COMDAC program copy

Overview

This function is used to copy a newly loaded software from the currently active COMDAC to the standby COMDAC. During normal operation both COMDACs should have the same software version. Therefore the software copying should always be the next step after software download except when software copying is started automatically after software download (cf. Chapter 5.5.14.2, page 5-152).

Duplex Configuration

For the following description it is assumed that the NE is configured in duplex configuration.

Procedure

Complete the following procedure to copy the new software from the active COMDAC to the standby COMDAC:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Program Copy -> Telephony*** via cursor menu. The *COMDAC Program Copy* window pops up:

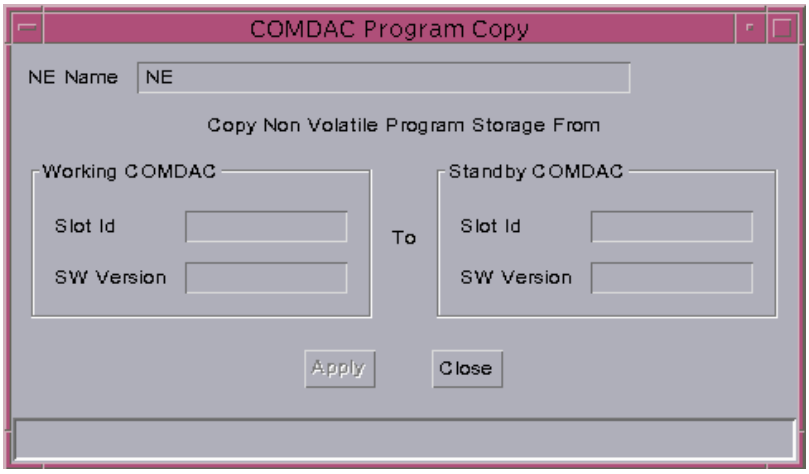


Figure 5-52 COMDAC Program Copy window

This is a dialogue window requesting information from the user to continue. There are two fields (titled **Working COMDAC** and **Standby COMDAC**) showing the corresponding slot number and software versions used in each of the COMDACs.

— **Slot_Id**

Identifies which COMDAC is where (e.g. Working COMDAC in slot 1 and Standby COMDAC in slot 2).

— **SW Version**

Obtained from the NE. The SW version of the working COMDAC will be taken as the NE SW version.

2. Press ***Apply*** to start the software copying. An *In Progress* window pops up:

`Program Copy from COMDAC 1 to COMDAC 2 on <NE NAME> in Progress`

After finishing the copying process successfully the *In Progress* window disappears.

3. Press ***Close*** to exit the *COMDAC Program Copy* window.

5.5.16 AFM program copy and validation

Overview

This function is used to exchange the newly loaded software with the currently active version in the flash memory and reboot the AFM to activate the new software. This should always be the next step after software download except when the copying and validation is started automatically after software download (cf. Chapter 5.5.14.4, page 5-156).

Procedure

Complete the following procedure to exchange the new software with the currently active version:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Program Copy -> Data*** via cursor menu. The *AFM Program Copy & Validation* window pops up:

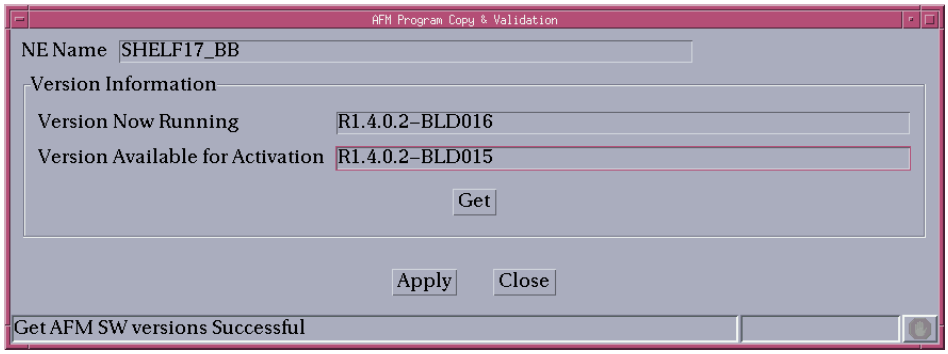


Figure 5-53 AFM Program Copy & Validation window

The fields **Version Now Running** (currently running NE software) and **Version Available for Activation** (standby software, downloaded via FTP) display the corresponding versions.

2. Click on ***Get*** to retrieve the current version information.

3. Click on ***Apply*** to initiate the validation of the new software, the exchange of the software versions and the reboot to make the changes valid. A *Warning* window pops up:

   AFM Program Copy & Validation is service affecting and the command can not be cancelled while its execution. Continue anyway?

   After confirmation an In Progress window pops up:

   AFM Program Copy and Validation from active version to standby version on <NE NAME> in Progress

After finishing the process successfully the *In Progress* window disappears.

4. Press ***Close*** to exit the *AFM Program Copy & Validation* window.

5.5.17 Nonvolatile data storage (NVDS)

Overview

This section describes the backup and restore processes. The backup procedure uploads the data from the NE's COMDAC (or AFM) to the AEM. The restore function deals with the downloading of a previous backup NVDS from the AEM to the NE. Both functions apply to both simplex and duplex NE configurations.

Backup/restore data

For database backup and restoration the AEM is able to create/maintain a copy of provisioning data from the active COMDAC or AFM (NVDS). When a loss of data occurs in the NE (due to factors such as human error, power failure or hardware and software failures), the restoration features enable the AEM to restore a previous backup to one NE.

Backup media

The AEM is able to store the backup copy in diverse storage media that can include HDD (hard disk drive), tapes, removable disk cartridges and any other available mass-storage medium.

FTP

For database backup and restoration operations the AEM uses an FTP (file transfer protocol) connection within the NE. FTP allows the AEM to overwrite or copy information residing on the NE.

The AEM can open only one FTP session per NE at a time where the AEM will support the client role of the FTP session, and the *AnyMedia* Access System will play the server part.

Failing backup/restore

The backup and restore processes will fail if the time period during which the connection is lost exceeds the time-out defined in the AEM or the NE time-out; otherwise the process will continue after the connection is recovered.

5.5.17.1 Data backup (telephony agent)

Procedure Complete the following procedure to initiate data backup for a telephony agent:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Backups -> Telephony*** via the cursor menu. The *COMDAC NVDS Backup* window pops up:

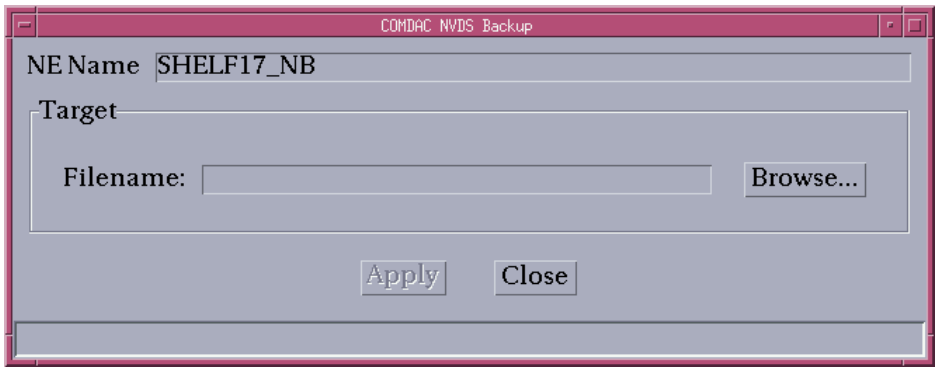


Figure 5-54 COMDAC NVDS Backup window

2. Click on the ***Browse...*** button to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select/create the directory (example of the file structure: NE Files/NVDS/<NE_Name>/COMDAC/R1...) and the file name of the backup file.

NOTE:
Do not insert any blank in the backup file name. Such a file cannot be restored.

3. Click on ***OK*** to confirm. The chosen file name appears in the field **Filename** in the *COMDAC NVDS Backup* window.

4. Click on ***Apply*** (this command button is available only after having selected the file name) to start the backup. An *In Progress* window pops up:

   `NVDS Backup on <NE NAME> in progress.`

   After finishing the backup process successfully the *In Progress* window disappears.

5. Press ***Close*** to exit the *COMDAC NVDS Backup* window.

NOTE:
Pressing the ***Close*** button during the backup execution will cancel the backup operation.

5.5.17.2 Data backup (data agent)

Procedure

Complete the following procedure to initiate data backup for a data agent:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Backups -> Data*** via the cursor menu. The *AFM NVDS Backup* window pops up:

Figure 5-55 AFM NVDS Backup window

2. Click on the ***Browse...*** button to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select/create the directory (example of the file structure: NE Files/NVDS/<NE_Name>/AFM) and the file name of the backup file.

NOTE:
Do not insert any blank in the backup file name. Such a file cannot be restored.

3. Click on ***OK*** to confirm. The chosen file name appears in the field **Filename** in the *AFM NVDS Backup* window.

4. Click on ***Apply*** (this command button is available only after having selected the file name) to start the backup. An *In Progress* window pops up:

   `NVDS Backup on <NE NAME> in progress.`

   After finishing the backup process successfully the *In Progress* window disappears.

5. Press ***Close*** to exit the *AFM NVDS Backup* window.

NOTE:
Pressing the ***Close*** button during the backup execution will cancel the backup operation.

5.5.17.3 Data restore (telephony agent)

Procedure Complete the following procedure to initiate data restore from a telephony agent:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Restore -> Telephony*** via cursor menu. The *COMDAC NVDS Restore* window pops up:

Figure 5-56 COMDAC NVDS Restore window

2. Click on the ***Browse...*** button to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select the directory (example of the file structure: NE Files/NVDS/<NE_Name>/COMDAC/R1...) and file name of the restore file.

3. Click on ***OK*** to confirm. The chosen file name appears in the field **Filename** in the *COMDAC NVDS Restore* window.

4. Click on ***Apply*** (this command button is available only after having selected the file name) to start the restore. A *Warning* window pops up:

. **NVDS Restore may be service affecting and the command can not be cancelled while the execution. Continue anyway?**

5. Press ***Yes*** to confirm this message. An *In Progress* window pops up:

`NVDS restore on <NE Name> in progress`

After finishing the backup process successfully the *In Progress* window disappears.

6. Press ***Close*** to exit the *COMDAC Restore* window.

NOTE:
When an NVDS restore process is started, all AEM variables are set to their initial values to provoke a FULL synchronization. The NE synchronization state goes to ASYNC.
The association between AEM and NE is lost and recovered. The FULL synchronization is launched for that NE.
Finally, the NE is connected and perfectly synchronized.

5.5.17.4 Data restore (data agent)

Procedure Complete the following procedure to initiate data restore from a data agent:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Restore -> Data*** via cursor menu. The *AFM NVDS Restore* window pops up:

Figure 5-57 AFM NVDS Restore window

2. Click on the ***Browse...*** button to open the *File Browser* window (cf. Chapter 5.5.17.5, page 5-168) to select the directory (example of the file structure: NE Files/NVDS/<NE_Name>/AFM) an the file name of the restore file.

3. Click on ***OK*** to confirm. The chosen file name appears in the field **Filename** in the *AFM NVDS Restore* window.

4. Click on ***Apply*** (this command button is available only after having selected the file name) to start the restore. A *Warning* window pops up:

. **NVDS Restore may be service affecting and the command can not be cancelled while the execution. Continue anyway?**

5. Press ***Yes*** to confirm this message. An *In Progress* window pops up:

NVDS restore on <NE Name> in progress

After finishing the backup process successfully the *In Progress* window disappears.

6. Press ***Close*** to exit the *AFM Restore* window.

5.5.17.5 File Browser window

This window is composed of a list where all files and/or subdirectories are shown included in the selected directory. The File Browser can be launched from

- the *Software Download* windows
- the *Backup* windows
- the *Restore* windows and
- the *Groups & NEs* window.

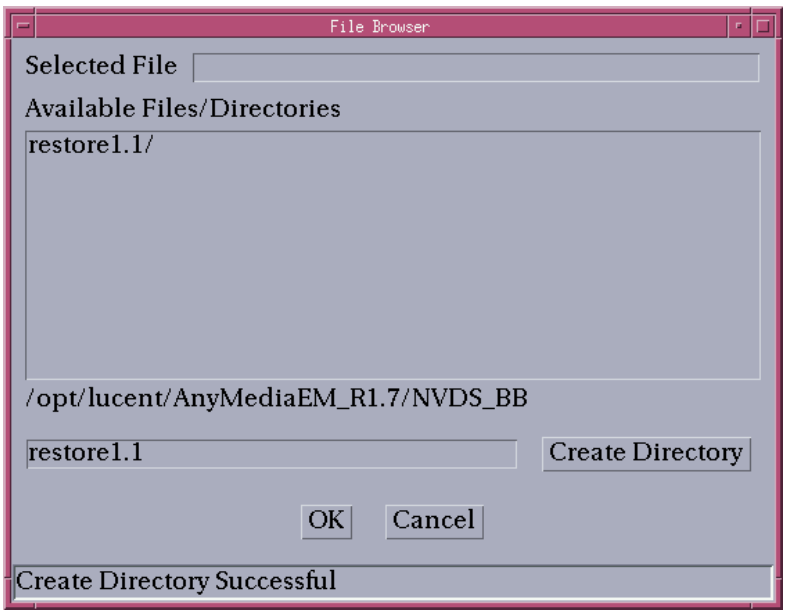


Figure 5-58 File Browser window

The following table shows the parameter of this window:

Parameters/ Buttons	Description
Selected File	This text field displays the selected file. The field is editable only if the file browser has been accessed from a backup window. In this case the **Available Files/Directories** list is used to select the corresponding path (directory/subdirectories).
Available Files/Directories	This list box contains all the existing files or subdirectories contained in the selected directory. If a file is selected this file name will be displayed in the **Selected File** field.
Label	This field displays the current relative path selected in the list above. A different path is shown depending on the window the File Browser has been accessed from.
Create Directory	This button can be used to create a directory. The directory name can be specified by use of the text field on the right-hand side.
OK	This button is used to confirm the selection of the file or directory. If the File Browser has been accessed from a *Backup* window and a new file name has been entered, this file will be created in the selected directory.

5.5.18 TL1 cut-through (telephony agent)

Overview

The AEM provides the user with a command line to a TL1 (transaction language 1) session with any NE. Using this command line, the user can type any TL1 command, send these commands to a selected NE and get the responses to the requests as well as all the autonomous outputs sent by the NE.

TL1 used for the provisioning, maintenance and administration of the *AnyMedia* Access System is an ASCII-based command language.

This cut-through interface is used by remote AEM craft personal when the GUI does not support certain TL1 commands. The AEM will provide the independence between the cut-through interface and the GUI interface.

To open a cut-through interface with an NE the operator must provide the connection information (Login and Password) defined in the NE Name Information window (cf. Chapter 5.5.1, page 5-37).

When the AEM receives the request to open a cut-through session, it opens a telnet connection with the selected NE, to avoid conflicts with the current AEM GUI session. Then the operator will manage the cut-through session through the use of TL1 commands.

Cut-through / GUI independence

The AEM GUI behaviour (but not necessarily the performance) is not affected by any simultaneous cut-through connection running on the platform.

The operator using the AEM GUI does not used to know about any cut-through session running on the AEM platform. The performance of the system could be affected by the load of the hardware, but the behaviour of the GUI is the same in both cases.

Procedure

Complete the following procedure to start a TL1 session:

1. Select ***NE*** in Network Element Browser.

2. Select ***Cut-through -> Telephony*** via the menu bar to start a TL1 session. The *Cut through* window pops up.

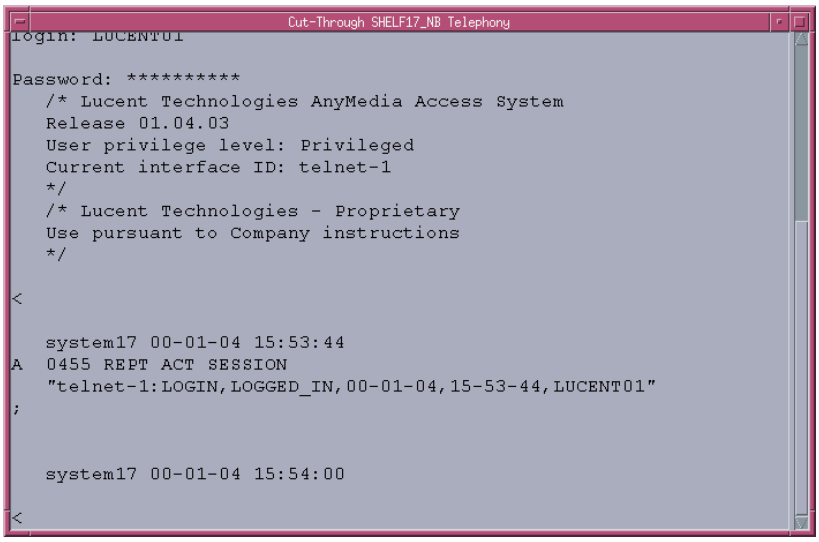


Figure 5-59 Cut-Through window

3. Enter the **Login** and **Password** as defined in the *NE Management* window (cf. Figure 5-15, page 5-39).

Now you are able to enter the appropriate TL1 commands.

The TL1 descriptions (syntax, formats, parameters, ...) are available on-line using the GSI help on *AnyMedia* Access System.

5.5.19 Delete network element

If the NE is not to be managed by the AEM any longer, it can be deleted from the AEM database.

Procedure

Complete the following procedure to delete an NE.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Remove*** via the cursor menu
or select ***File -> Remove*** via the menu bar. A *Warning* window pops up:

   `You are about to delete <NE Name>. Do you want to continue?`

   If you select **No**, the deletion of the NE is rejected. Otherwise, the NE will be deleted.

NOTE:
When an NE is deleted from the AEM database, it is still fully functional. The TL1 and TCP/IP links between the AEM and the NE will be closed and the management access via the AEM is finished until the NE is created and connected again.

Service provisioning

6

Contents

6.1 Introduction 6-1

6.2 Service provisioning (telephony) 6-1

6.2.1 V5 network interfaces 6-9

6.2.1.1 V5 Interface List window 6-9

6.2.1.2 V5 Interface window 6-11

6.2.1.2.1 V5 Interface Data window 6-11

6.2.1.2.2 V5 Link Data window 6-14

6.2.1.3 Create a V5 network interface 6-16

6.2.1.4 Modify a V5.1 network interface 6-16

6.2.1.5 Modify a V5.2 network interface 6-18

6.2.2 Add V5 links to V5 interface 6-20

6.2.2.1 V5.1 Set Feeder window 6-20

6.2.2.2 Add a V5.1 Feeder 6-21

6.2.2.3 V5.2 Add/Remove Links window 6-22

6.2.2.4 Add a V5.2 link 6-24

6.2.3 Physical Feeders List window 6-24

6.2.4 Leased Line Link window 6-26

6.2.4.1 Create a leased line link 6-28

6.2.4.2 Modify a leased line link 6-29

6.2.5 V5 Link window 6-30

6.2.5.1 Create a V5 link 6-33

6.2.5.2 Modify a V5 link 6-33

6.2.6 Primary and secondary V5.2 links 6-35

6.2.6.1 Primary Link window 6-35

6.2.6.2 Modify primary V5.2 link 6-36

6.2.6.3 Secondary Link window 6-37

6.2.6.4 Modify secondary V5.2 link 6-38

Contents

6.2.7 HDSL interface 6-39
6.2.7.1 HDSL Logical Interface List window 6-39
6.2.7.2 HDSL Logical Interface window 6-41
6.2.7.3 Add an HDSL logical interface 6-45
6.2.7.4 Modify an HDSL logical interface 6-46
6.2.8 User ports 6-48
6.2.8.1 User Port List window 6-48
6.2.8.2 ALL user ports 6-52
6.2.8.2.1 ALL User Port window 6-52
6.2.8.2.2 Add an ALL user port 6-55
6.2.8.2.3 Modify an ALL user port 6-56
6.2.8.3 V5 PSTN user ports 6-58
6.2.8.3.1 V5 PSTN User Port window 6-59
6.2.8.3.2 Add a V5 PSTN user port 6-63
6.2.8.3.3 Modify a V5 PSTN user port 6-64
6.2.8.4 DLL user ports 6-66
6.2.8.4.1 DLL User Port window 6-67
6.2.8.4.2 Add a DLL user port 6-71
6.2.8.4.3 Modify a DLL user port 6-72
6.2.8.5 V5 ISDN BRA user port 6-74
6.2.8.5.1 V5 ISDN BA User Port window 6-75
6.2.8.5.2 Add an ISDN BRA user port 6-80
6.2.8.5.3 Modify a V5 ISDN BRA user port 6-81
6.2.8.6 V5 ISDN PRA user port 6-83
6.2.8.6.1 V5 ISDN PRA User Port window 6-84
6.2.8.6.2 Add a V5 ISDN PRA user port 6-87
6.2.8.6.3 Modify a V5 ISDN PRA user port 6-88
6.2.8.7 V/G leased line user port 6-90
6.2.8.7.1 VLL User Port window 6-91
6.2.8.7.2 Add a VLL user port 6-95
6.2.8.7.3 Modify a VLL user port 6-96
6.2.8.7.4 GLL User Port window 6-98
6.2.8.7.5 Add a GLL user port 6-101
6.2.8.7.6 Modify a GLL user port 6-102
6.2.8.8 Edit Timeslots window 6-104

Contents

6.2.8.8.1 Add/remove cross-connection between GLL/VLL user port and LL link timeslot 6-105
6.2.8.9 V5 ISDN User Port Signalling Configuration window 6-106
6.2.8.9.1 Modify the V5 user port signalling data 6-108
6.2.8.10 V5 Signalling window 6-109
6.2.8.10.1 Using the V5 Signalling window 6-113
6.2.8.10.2 Add Timeslot window 6-114
6.2.8.10.3 Add a timeslot 6-115
6.2.8.10.4 Add Communication Channel window 6-116
6.2.8.10.5 Add a communication channel 6-117
6.2.8.10.6 Add Communication Path window 6-118
6.2.8.10.7 Add a communication path 6-118
6.2.8.10.8 Crossconnect Communication Channel with Timeslot window 6-120
6.2.8.10.9 Add a cross-connection between CC and TS 6-121
6.2.8.10.10 Crossconnect CP with CC window 6-122
6.2.8.10.11 Add a cross-connection between CC and CP 6-122
6.2.8.10.12 Edit Communication Channel window 6-124
6.2.8.10.13 Edit a communication channel 6-124
6.2.8.11 V5.2 group 2 protection 6-124
6.2.8.11.1 V5.2 Group 2 Protection window 6-125
6.2.8.11.2 Modify V5.2 group 2 protections 6-127
6.2.8.11.3 Add V5.2 Group 2 Protection window 6-128
6.2.8.11.4 Add a V5.2 group 2 protection 6-129
6.2.8.11.5 Switch V5.2 Group 2 Protection window 6-130
6.2.8.11.6 Switch a V5.2 group 2 protection 6-130
6.2.9 Move a V5 interface in service 6-132
6.2.10 Move a V5 link in service 6-132
6.2.11 Move a V5 user port in service 6-133
6.2.12 Move a ALL/DLL user port in service 6-133
6.2.13 Move a VLL/GLL user port in service 6-134
6.2.14 Delete a VLL/GLL user port 6-134
6.2.15 Delete an ALL/DLL user port 6-135
6.2.16 Delete a V5 user port 6-135
6.2.17 Delete a V5 link 6-136
6.2.18 Remove a communication channel 6-137
6.2.19 Remove a communication path 6-137

Contents

6.2.20 Remove a primary link 6-138
6.2.21 Remove a secondary link 6-139
6.2.22 Remove a V5 protection group 2 6-139
6.2.23 Delete a V5 interface 6-140

6.3 Service provisioning (data) 6-141

6.3.1 ATM Cross Connections List window 6-141
6.3.2 ATM Cross-Connection window 6-144
6.3.3 Add an ATM cross-connection 6-147
6.3.4 Modify an ATM cross-connection 6-148
6.3.5 Remove an ATM cross-connection 6-148

Service provisioning

6

6.1 Introduction

This chapter describes the service provisioning possibilities of the *AnyMedia*® Element Manager - 30 Channel (AEM), R1.7. It addresses the following topics:

- Screen navigation
- Service provisioning (telephony)
- Service provisioning (data).

6.2 Service provisioning (telephony)

Provisioning summary

Prior to service activation on the AEM several data items need to be provisioned. It is necessary to configure cross-connections between ports and logical and physical entities and vice versa. In addition it is necessary to specify the service type (PSTN, ISDN BA, ISDN PRA or permanent leased lines (PLL)).

Supported interfaces

Figure 6-1, page 6-3 is a functional diagram of the cross-connections between the physical (E1 and subscriber) ports of the system and the logical entities. The AEM supports

- up to 16 V5.1
- up to 16 V5.2
- up to 16 PLL interfaces

in any combination not exceeding the maximum of 16 E1 feeders in the system.

2-Mbps cross-connections

E1 logical cross-connections provide 2-Mbps bandwidth to the interfaces. A maximum of 16 E1 cross-connections can be created; they are limited by the maximum number of E1 feeder ports in the system.

64-kbps cross-connections

64-kbps cross-connections bind a subscriber port / bearer channel to a V5.1, a V5.2 or to an LL Interface.
A maximum of 769 64-kbps cross-connections can be created; they are limited by the maximum number of subscriber lines in the system (768, for V5 PSTN), plus the one remote operations channel (ROC).

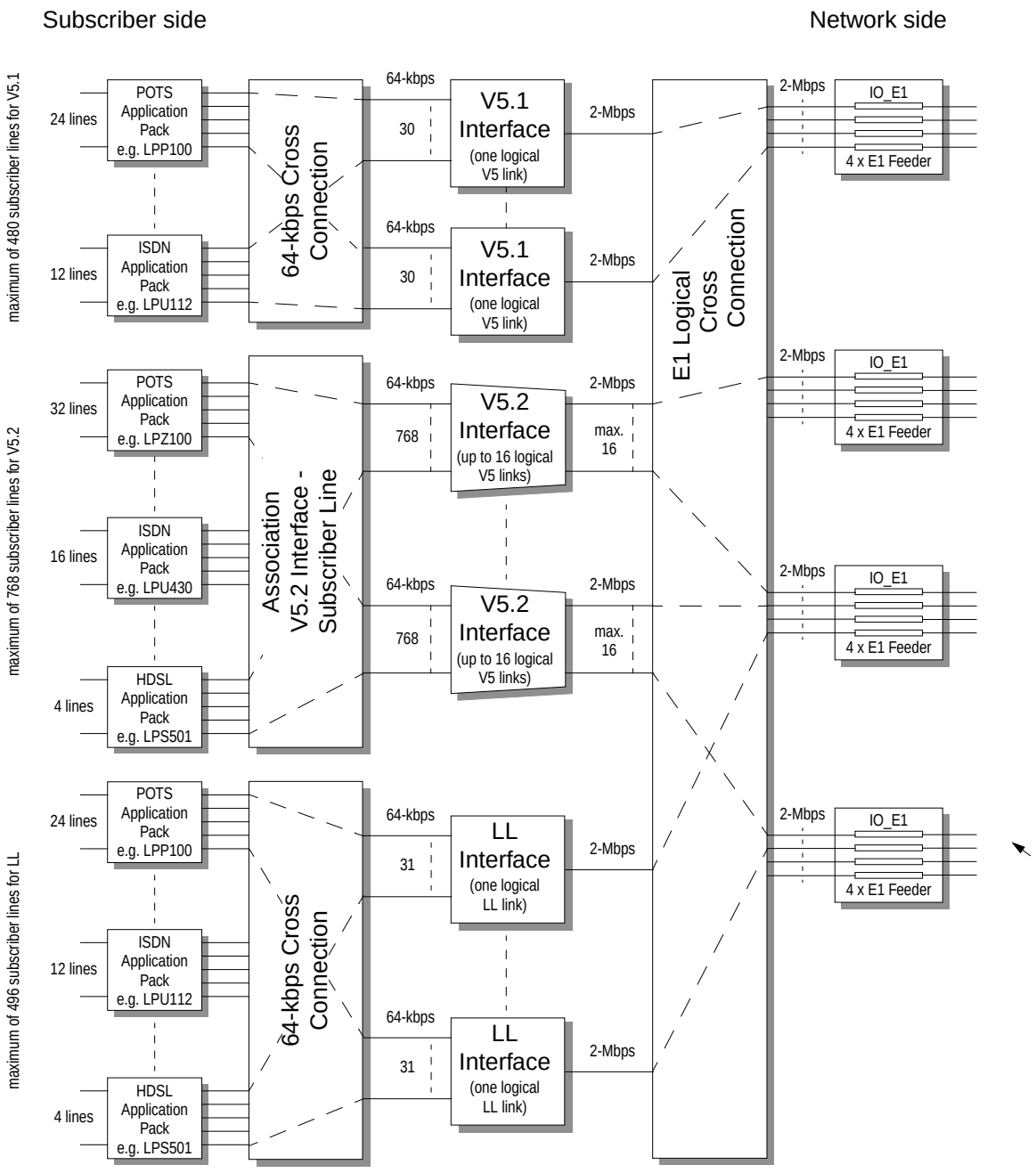


Figure 6-1 Functional diagram of cross-connections within the *AnyMedia* Access System

Ports/Lines Each interface contains the provisioning data for its E1 ports. 64-kbps and E1 cross-connections provide the linkage between the used protocol and the corresponding physical interfaces.

Each V5.1 interface supports one E1 port (2-Mbps) and 30 subscriber lines (64-kbps).

Each V5.2 interface supports up to 16 E1 ports (2-Mbps) and up to 768 subscriber lines (64-kbps).

Each leased line interface supports one E1 port (2-Mbps) and up to 31 analog leased lines (64-kbps) or digital leased lines channels.

NOTE:
A mix of services (V5.x and leased lines) on one E1 feeder is not possible.

V5 protocol

The V5 protocol is a European Telecommunication Standards Institute (ETSI) defined interface protocol between a Local Exchange (LE) and an NE for the support of the following access types:

- Analog telephone access: plain old telephone service (POTS)
- ISDN basic rate access (ISDN BRA)
- ISDN primary rate access (ISDN PRA)

with provisionable information channel allocation or flexible concentration capability within the NE.

Supported subscribers

In principle the V5 protocol is intended to connect public switched telephone network (PSTN) and ISDN subscribers (via V5 interface). ETSI distinguishes between V5.1 interfaces which only allow PSTN and ISDN BRA subscribers to be connected and V5.2 interfaces which allow ISDN PRA subscribers to be connected as well.

POTS subscriber

A POTS subscriber can be connected to the network via a V5.1 or V5.2 interface. In the case of V5.1 it is associated with a specific 64-kbps timeslot of a V5.1 interface. In the case of V5.2 it is associated with a V5.2 interface where the current 64-kbps timeslot is selected on a per call basis.

ISDN BRA subscriber

An ISDN BRA subscriber has the transmission capability of two B-channels (2×64-kbps) and one D-channel (16 kbps). The B-channels are transported in the bearer channels of the V5.x interface; the D-channel is transported in the communication channels of the V5.x interface. An ISDN BRA subscriber can be connected to the network via a V5.1 or V5.2 interface. In the case of V5.1 up to two B-channels are associated with up to two 64-kbps timeslots of a V5.1 interface. In the case of V5.2 the current 64-kbps timeslots are selected on a per call basis.

ISDN PRA subscriber

An ISDN PRA subscriber has the transmission capability of up to 30 B-channels (30×64 kbps) and one D-channel (64-kbps). The B-channels are transported in the bearer channels of the V5.2 interface; the D-channel is transported in the communication channels of the V5.2 interface. An ISDN PRA subscriber can only be connected to the network via a V5.2 interface. It is associated to a V5.2 interface where the current 64-kbps timeslots are selected on a per call basis.

Analog leased line

An analog leased line (ALL) service is used for purposes other than telephony - for example, data transmission with modems. The AEM supports ALL according to ITU M.1020, M.1025, and M.1040.
An ALL subscriber is connected to the network via a leased line interface which is associated with a specific 64-kbps timeslot. ALLs are provided by cross-connecting a Z port on the subscriber side (located at a POTS AP) with one timeslot of an E1 feeder on the network side (located on an IO_E1).

Digital leased line

The *AnyMedia* Access System supports digital leased lines (DLL) with a transmission capability of

- one B-channel (64-kbps) or
- one B-channel (64-kbps) and one D-channel (16-kbps) or
- two B-channels (2 × 64-kbps) or
- two B-channels (2 × 64-kbps) and one D-channel (16-kbps)

on one U interface.

The DLLs are provided by connecting a U port located at an ISDN AP with an E1 feeder located on an IO_E1. The U port has to be provisioned to support DLL and the E1 feeder has to be provisioned to be used for permanent leased line purposes. In this way the subscriber's terminal equipment (TE) is connected to the network provider's digital leased line service node (DLLSN) for routing permanent leased line service circuits. A DLL subscriber is connected to the network via a leased line interface using up to three 64-kbps timeslots, two for the B-channels and one for the D-channel. Only one 16-kbps D-channel can be allocated in one 64-kbps timeslot.

N x 64-kbps leased line

The *AnyMedia* Access System supports two kinds of n × 64-kbps digital leased line services over HDSL interface:

- VLL

  A digital leased line via a data interface is supported, which can be either V.35, V.36 or X.21.

- GLL

  A leased line according to ETS 300 419 is supported via a G.703 interface.

In both cases the particular interface is provided by means of an NTU which is the far end of an HDSL transmission system.
Nx64-kbps DLL services are provided by connecting a number of bearer channels supplied by a VLL or GLL entity with the same number of timeslots of an E1 feeder located on an IO_E1. The n × 64-kbps DLL is provisioned on top of an HDSL logical interface located at an HDSL AP. The HDSL AP can be located in the *AnyMedia* mainshelf as well as in the ONU (subshelf).

Cross-connections

A single NE can contain a number of V5 user ports, a number of V5 interfaces and a number of V5 links (which represent 2.048-Mbps links). There is a bi-directional association (cross-connection) between each V5 interface and all of its related V5 user ports. Likewise there is a bi-directional relationship between each V5 interface and all its related V5 links.

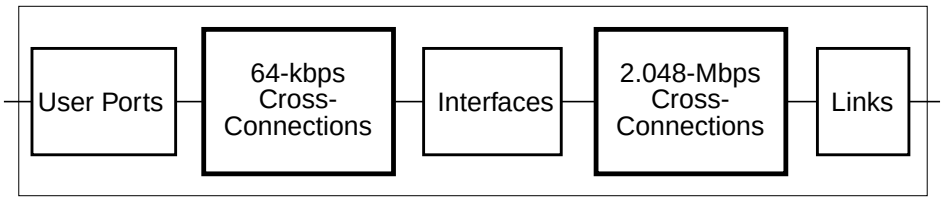


Figure 6-2 Cross-connections

From the management point of view, a V5 interface can be represented by a set of logical manageable entities with their own configuration data and relations (cross-connections) that are established by provisioning.

Interfaces - Links

The NE may contains up to 16 V5 interfaces and up to 16 V5 links (16 E1 physical feeders limitation). On the other hand, for the *AnyMedia* Access System a limitation of 768 subscribers (V5 user ports) arises from the 32-channel POTS APs.

Communication channels, paths and timeslots

Only one V5 link can be associated to a V5.1 interface and up to 16 V5 links can be associated to a V5.2 interface. For both V5.1 and V5.2 interfaces, the association of user signalling with communication paths (CP) and the association between CPs and logical communication channels (CC) have to be provisioned. The association of CCs with physical communication timeslots (TS) is initially provisioned (configured) but can be changed within V5.2 interfaces by the V5.2 protection protocol.

For more information refer to the NE documentation for R1.7.

Screen navigation

Figure 6-3, page 6-7 shows an overview of the screen navigation for service provisioning via AEM.

The arrows represent the order in which the windows can be opened.

Example

To edit the *V5.1 Interface* window go the way through *V5 Interface List* window and the button *Add V5 Interface* (cf. Chapter 6.2.1.1, page 6-9).

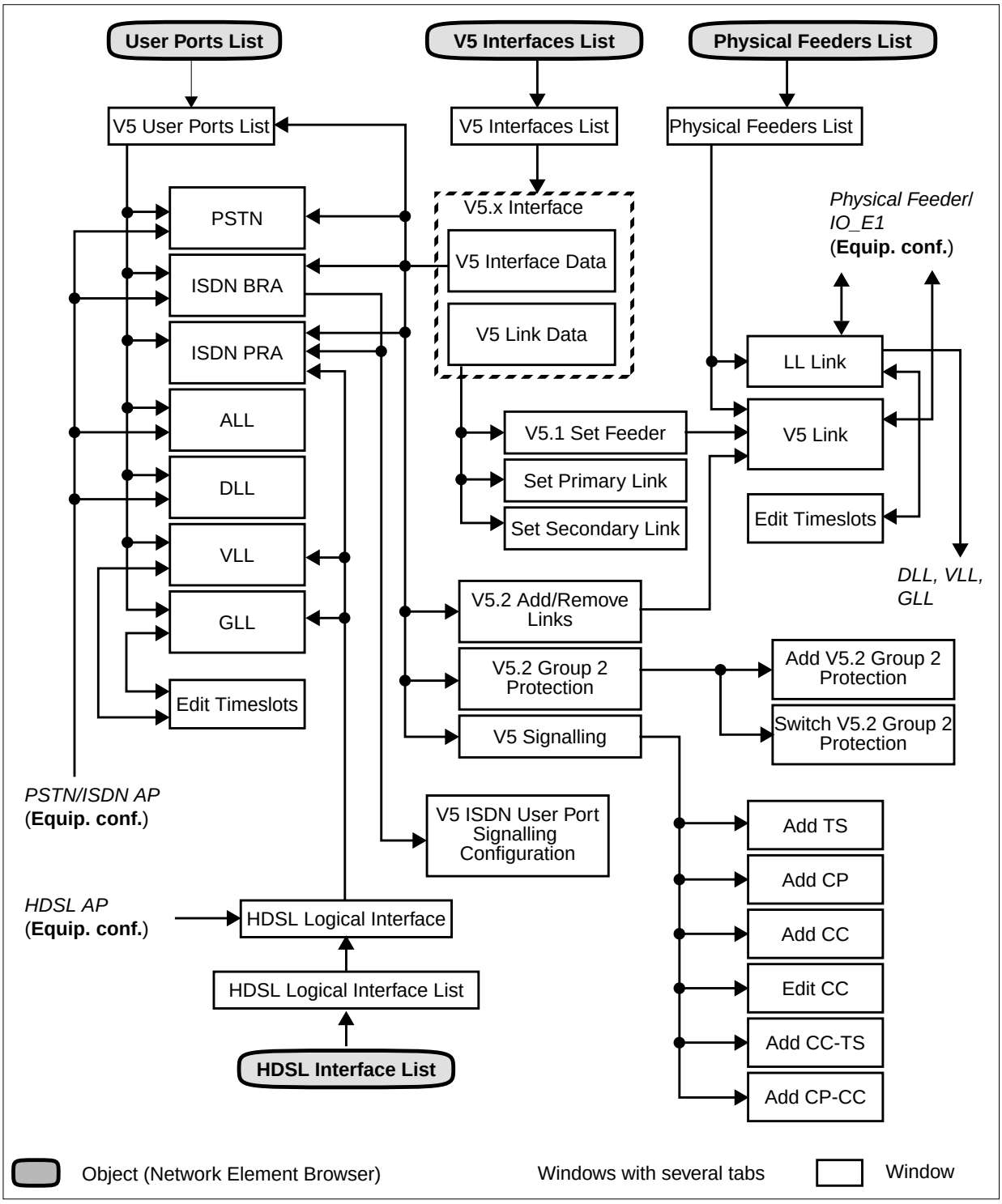


Figure 6-3 Screen navigation for service provisioning (telephony services)

The next sections describe the most common way for provisioning a V5 Interface and the related services:

- Create V5 interface.
- Add V5 links.
- Define primary V5 links (V5.2 interfaces only).
- Define secondary V5 links (V5.2 interfaces only).
- Create communication channels.
- Define communication channels for ISDN signalling protocol.
- Create communication channels to be protected and timeslots to protect them.
- Create ISDN communication paths (subscriber groups).

6.2.1 V5 network interfaces

Overview

The maximum number of V5 interfaces that can be supported by the *AnyMedia* Access System is 16. The AEM rejects at GUI level a V5 interface creation operation if this number is exceeded or if provisioning information is not correct (V5.2 interface identifier must be unique within the managed access network).

NOTE:
NE R1.4 supports V5.2 protocol version "type first edition" and "type second edition". The corresponding parameters can be selected via TL1 command and via GSI but not via AEM R1.7.

6.2.1.1 V5 Interface List window

This window lists all available V5 interface ids. It provides access to the *V5.1 Interface* window and the *V5.2 Interface* window to create or modify a V5 interface.

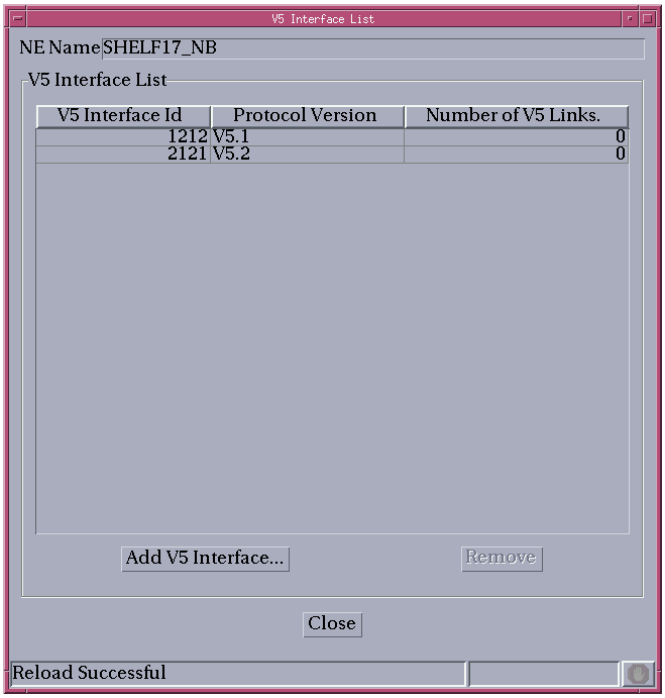


Figure 6-4 V5 Interface List window

The following table shows the view/edit option of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
V5 Interface List	**V5 Interface Id**: The list displays all available V5 interface ids. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. Upon selection of any entry, the ***Edit V5 Interface...*** button becomes available. **Protocol Version**: This text field shows the protocol version of the selected V5 interface. Possible values: V5.1 and V5.2. **Number of V5 Links**: Shows the number of Links cross-connected to the V5 Interface. **Label button**: This button provides access to the *V5.x Interface* window. ***Add V5 Interface...***, if no row is selected in the list. ***Edit V5 Interface...***, if the desired interface id has been selected. ***Remove***: This button can be used to remove a V5 interface from the list

6.2.1.2 V5 Interface window

This window is used to add/modify a V5 interface. When coming from the *V5 Interface List* window (cf. Chapter 6.2.1.1, page 6-9) for modifying the title of the window is *V5.1 Interface* or *V5.2 Interface* (depending on the selected protocol version).

This window consists of two tabs: **V5 Interface Data** and **V5 Link Data**.

6.2.1.2.1 V5 Interface Data window

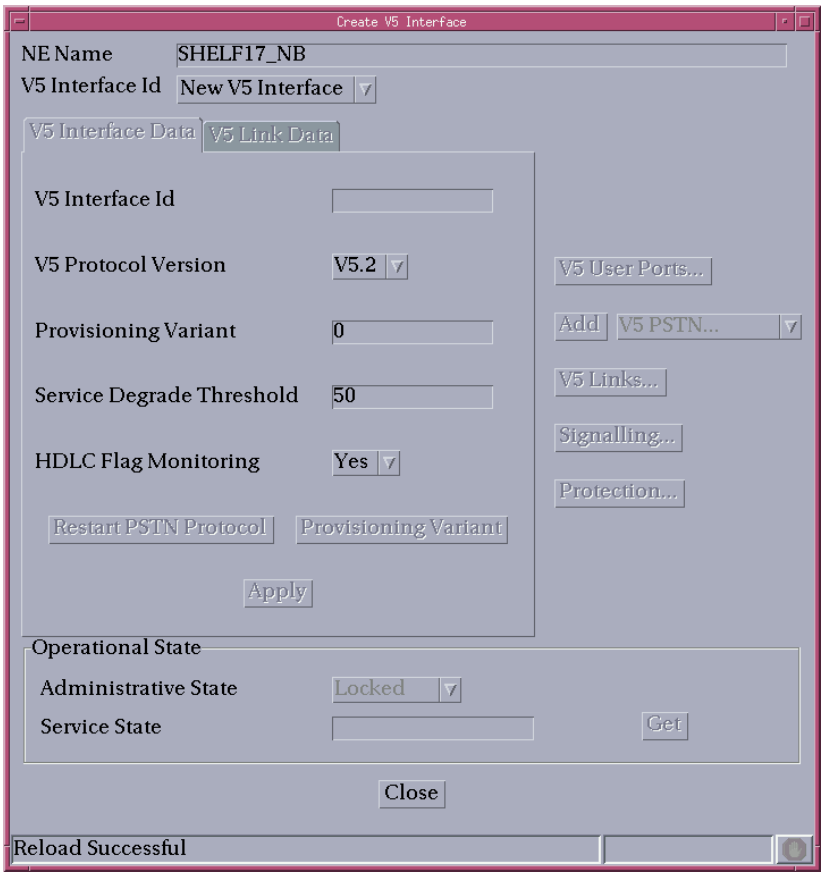


Figure 6-5 V5 Interface window (tab V5 Interface Data)

The following table shows the view/edit option of this window
(please note that the command buttons on the right-hand side are the same for both tabs):

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
V5 Interface Id	This option menu is used to select the interface to edit. The list contains all interfaces in the NE and the entry New V5 Interface (add mode). In add mode the tab V5 Link Data and the navigation buttons are disabled and all parameters in this window are set to the default values.
V5.x Interface Information (the title of this field depends on the protocol version of the interface: V5.1 or V5.2)	**V5 Interface Id**: This text field is used to enter a new interface id (add mode) or to change the current interface id (edit mode). Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. This field can only be changed if the administrative state is "Locked". **V5 Protocol Version**: This option menu is used to select the protocol version for this V5 interface. Possible values: V5.1 and V5.2. This parameter can be modified only if the administrative state is "Locked". **Provisioning Variant**: This text field is used to enter a short integer for the provisioning variant. Possible values: {0, 127}. This parameter can be modified only if the administrative state is "Locked". **Service Degrading Threshold**: This text field is used to enter a short integer for the service degrade threshold. Possible values: {5, 95}. This parameter can be modified only if the administrative state is "Locked". **HDLC Flag Monitoring**: This option menu can be used to define the HDLC Flag Monitoring condition. Possible values: Yes or No. This parameter can be modified only if the administrative state is "Locked". The ***Restart PSTN Protocol*** button and the ***Provisioning Variant*** button can be used to start the corresponding test. For more information refer to Chapter 7.4. The ***Apply*** button is used to confirm the changes in the **V5 Interface Information** field.

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled and the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State**.
Command buttons	The ***V5 User Ports...*** button provides access to the *User Port List* window. It is enabled only in edit mode. The ***Add*** button is can be used to add a user port. It provides access to the following windows dependent on the selected entry in the corresponding option menu: *V5 PSTN User Port* *V5 ISDN BA User Port* *V5 ISDN PRA User Port*. This button is enabled only in edit mode. The ***V5 Links...*** button provides access to the *V5.2 Add/Remove Link* window. The button is enabled only in edit mode for V5.2. The ***Signalling...*** button provides access to the *V5 Signalling* window. The button is enabled only in edit mode. The ***Protection...*** button provides access to the *V5.2 Group 2 Protection* window. The button is enabled only in edit mode for V5.2. It is disabled if the Protection Group 1 is not yet created (no defined secondary link).

6.2.1.2.2 V5 Link Data window

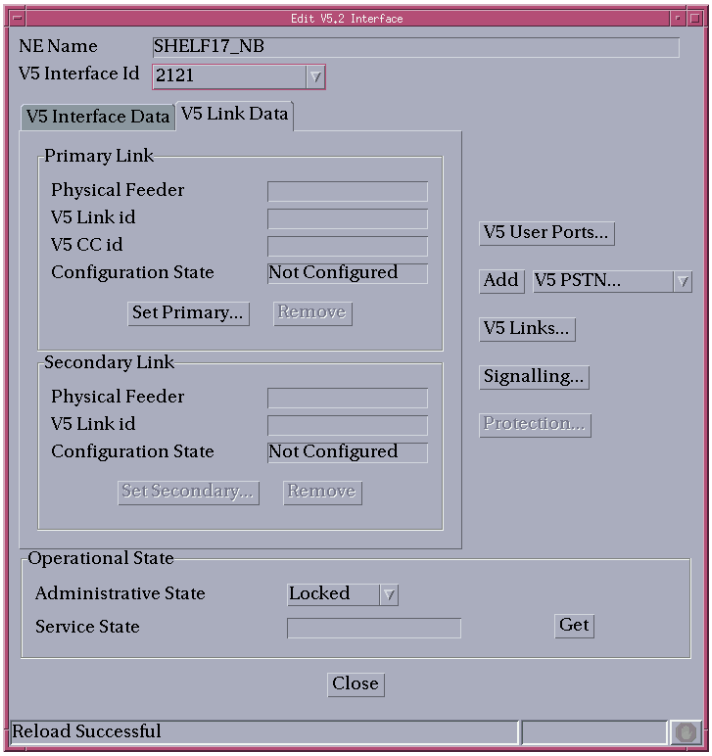


Figure 6-6 V5 Interface window (tab V5 Link Data)

The following table shows the view/edit option of this window (please note that the command buttons on the right-hand side are the same for both tabs):

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This option menu displays the selected interface id. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Link (this field is visible only for V5.1 interfaces)	**Physical Feeder**: This field shows the id that is linked to this V5.1 interface, if there is one. The ***Set Feeder...*** button provides access to the *V5.1 Set Feeder* window. This button is enabled only when the **Administrative State** is "Locked". The ***Remove Feeder*** button can be used to delete the selected feeder. This button is only available if there is a feeder already set and the V5 interface state is "Locked".

Parameters/ Buttons	Description
Primary Link (this field is visible only for V5.2 interfaces)	If a primary feeder is not yet configured all fields remain empty except the field **Configuration State**. The **Physical Feeder** shows the id that is configured as primary feeder, if there is one. The **V5 Link id** shows the link id that is configured as primary feeder, if there is one. Possible values: {0, 255}. The **V5 CC id** shows the id of the communication channel that is cross-connected to timeslot 16 of the primary feeder, if there is one. Possible values: {0, 65503}. The field **Configuration State** indicates whether the primary link is correctly configured or not. Possible values: Not Configured, Partially Configured, Configured. The ***Set Primary...*** button provides access to the *Primary Link* window. It is enabled only when the **Administrative State** is "Locked" and the **Configuration State** for the primary link and the secondary link is "Not Configured". The ***Remove*** button can be used to delete the primary link. It is enabled only when the **Administrative State** is "Locked" and the **Configuration State** for the primary link is "Partially Configured" or "Configured" and the **Configuration State** for the secondary link is "Not Configured".
Secondary Link (this field is visible only for V5.2 interfaces)	If a secondary feeder is not yet configured all fields remain empty except the field **Configuration State**. The **Physical Feeder** shows the id that is configured as secondary feeder, if there is one. The **V5 Link id** shows the id that is configured as secondary feeder, if there is one. The field **Configuration State** indicates whether the primary link is correctly configured or not. Possible values: Not Configured, Partially Configured, Configured. The ***Set Secondary...*** button provides access to the *Secondary Link* window. It is enabled only when the **Administrative State** is "Locked" and the **Configuration State** for the primary link is "Configured" and the **Configuration State** for the secondary link is **"**Not Configured". The ***Remove*** button can be used to delete the secondary link. It is enabled only when the **Administrative State** is "Locked" and the **Configuration State** for the secondary link is "Partially Configured" or "Configured".

6.2.1.3 Create a V5 network interface

Procedure Complete the following procedure to create a V5 interface.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Click on ***Add V5 Interface***. The *V5 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2, page 6-11).
3.	Use the option menu **V5 Interface Id** to select New V5 Interface.
4.	Enter an appropriate value in the text field **V5 Interface Id**.
5.	Define **Protocol Version**, **Provisioning Variant**, **Service Degrading Threshold** and **HDLC Flag Monitoring** and click on ***Apply***.
6.	Click on ***Close*** to exit the window.

6.2.1.4 Modify a V5.1 network interface

Procedure Complete the following procedure to modify a V5.1 interface.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the desired V5.1 interface in the **V5 Interface List** field and click on ***Edit V5 Interface...*** or double click on a row entry. The *V5.1 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2, page 6-11).

If you want to ...	then ...
edit the V5.1 interface parameters	change the parameters in the field **V5.1 Interface Information** and click on ***Apply*** to confirm. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?`**

If you want to ...	then ...
open the *V5 User Port List*	click on ***V5 User Ports...***. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
add a PSTN user port	use the option menu near the ***Add*** button to select ***PSTN...*** and click on ***Add***. The *V5 PSTN User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59).
add an ISDN BRA user port	use the option menu near the ***Add*** button to select ***ISDN BA...*** and click on ***Add***. The *V5 ISDN BA User Port* window pops up (cf. Chapter 6.2.8.5.1, page 6-75).
modify the signalling parameters	click on ***Signalling...***. The *V5 Signalling* window pops up (cf. Chapter 6.2.8.10, page 6-109).
set a feeder	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Set Feeder...***. The *V5.1 Set Feeder* window pops up (cf. Chapter 6.2.2.1, page 6-20).
remove the physical feeder	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Remove Feeder***.
exit the window	click on ***Close***.

6.2.1.5 Modify a V5.2 network interface

Procedure Complete the following procedure to modify a V5.2 interface.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.

2. Select the desired V5.2 interface in the **V5 Interface List** field and click on ***Edit V5 Interface*** or double click on a row entry. The *V5.2 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2, page 6-11).

If you want to ...	then ...
edit the V5.2 interface parameters	change the parameters in the field **V5.2 Interface Information** an click on ***Apply*** to confirm. If the administrative state has been changed from "Unlocked" to "Locked" a *Warning* window pops up: **`Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?`**
open the *V5 User Port List*	click on ***V5 User Ports...***. The *V5 User Port List* window pops up (cf. Figure 6-16, page 6-48).
add a PSTN user port	use the option menu near the ***Add*** button to select ***PSTN...*** and click on ***Add***. The *V5 PSTN User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59).
add an ISDN BRA user port	use the option menu near the ***Add*** button to select ***ISDN BA...*** and click on ***Add***. The *V5 ISDN BA User Port* window pops up (cf. Chapter 6.2.8.5.1, page 6-75).
add an ISDN PRA user port	use the option menu near the ***Add*** button to select ***ISDN PRA...*** and click on ***Add***. The *V5 ISDN PRA User Port* window pops up (cf. Chapter 6.2.8.6.1, page 6-84).
add a V5.2 link	click on ***V5 Links...***. The *V5.2 Add/Remove Link* window pops up (cf. Chapter 6.2.2.3, page 6-22).

If you want to ...	then ...
modify the signalling parameters	click on ***Signalling...***. The *V5 Signalling* window pops up (cf. Chapter 6.2.8.10, page 6-109).
modify the group 2 protection	click on ***Protection...***. The *V5.2 Group 2 Protection* window pops up (cf. Chapter 6.2.8.11, page 6-124).
set a primary link	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Set Primary...*** in the **Primary Link** field. The *Primary Link* window pops up (cf. Chapter 6.2.6, page 6-35)
remove a primary link	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Remove***.
set a secondary link	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Set Secondary...*** in the **Secondary Link** field. The *Secondary Link* window pops up (cf. Chapter 6.2.6.3, page 6-37)
remove a secondary link	switch to tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14) and click on ***Remove***.
exit the window	click on ***Close***.

6.2.2 Add V5 links to V5 interface

This section is divided into two subsections:

- V5.1 Set Feeder
- V5.2 Add Link.

Assumptions

To add a V5 link to a V5 interface the following assumptions must be fulfilled:

- The NE is connected.
- The V5 interface administrative primary service state is OOS (Out of Service) (only for V5.1).
- The physical feeder is not used by any other V5 interface or leased line link.
- The V5 link identifier must be unique within the V5 interface (only forV5.2).

6.2.2.1 V5.1 Set Feeder window

This window displays the current feeder status of the V5.1 interface and provides the opportunity to modify this status.

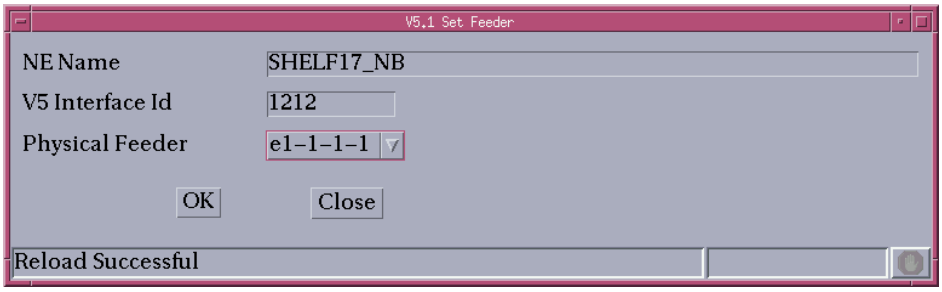


Figure 6-7 V5.1 Set Feeder window

The following table shows the view/edit option of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
V5 Interface Id	This field displays the selected interface id. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex fromat.
Physical Feeder	This option menu can be used to select the desired feeder. It shows the list of physical feeders that are not linked to V5 interfaces (i.e. they are not related to V5 links which are cross-connected to V5 interfaces) or used in leased line groups. Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}.
OK	This button can be used to set the cross-connection between the V5 interface and the selected feeder. If the selected feeder has no associated V5 link, the *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30) for that physical feeder.

6.2.2.2 Add a V5.1 Feeder

The *Set V5.1 Feeder* window is reached from the *V5.1 Interface* window (tab V5 Link Data) by clicking on ***Set Feeder...*** (cf. Chapter 6.2.1.2.2, page 6-14).

Procedure

Complete the following procedure to add a link to the V5.1 interface (only one link is possible).

Step	Procedure
1.	Use the option menu **E1 Feeder** to select an appropriate feeder.
2.	Click on ***OK*** to confirm the selection. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30) where the link can be modified so that cross-connecting is possible. After that the *V5.1 Set Feeder* window is available again and the V5 link and the related cross-connection will be added. Additional the following is added: ■ V5 communication path (CP) *Control* ■ V5 communication channel (CC) ■ Cross-connection between CP *Control* and CC ■ Cross-connection between CC and V5 Link's timeslot 16.
	NOTE: A V5.1 link can be created by setting a V5.1 feeder and then cross-connecting it to a V5.1 interface.
3.	Click on ***Close*** to exit the window.

6.2.2.3 V5.2 Add/Remove Links window

This window displays the current feeder status of the V5.2 interface and provides the opportunity to add and remove V5 links to/from the V5.2 interface.

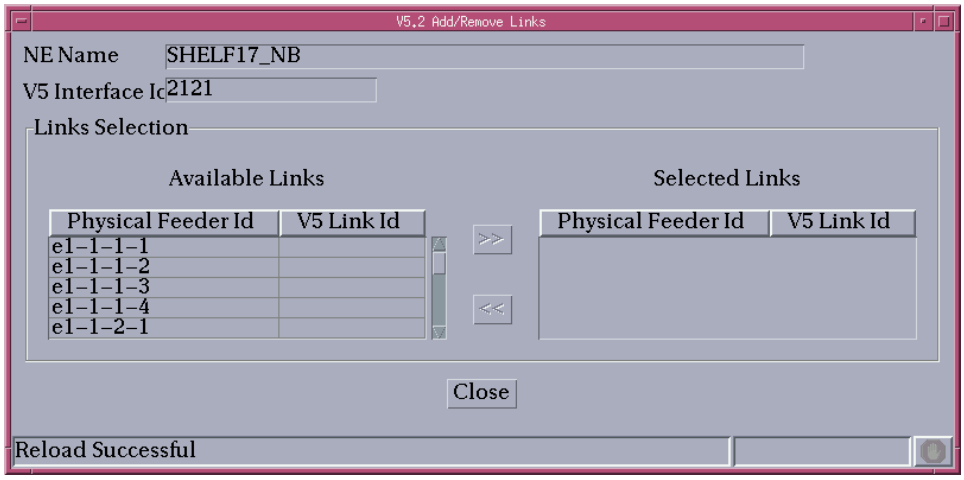


Figure 6-8 V5.2 Add/Remove Links window

The following table shows the view/edit options of the *V5.2 Add/Remove Links* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field displays the selected interface id. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.

Parameters/ Buttons	Description
Links Selection	This field is subdivided into two parts: **Available Links** and **Selected Links**. The **Available Links** list contains all the feeders that are neither associated to a V5 link which is cross-connected to a V5 interface, nor used in a leased line group. Selecting a row in this list activates the ***Add (>>)*** button (see below). The **Selected Links** list contains all the links that are cross-connected to this V5 interface. Selecting a row in this list activates the ***Remove (<<)*** button (see below). **Physical Feeder**: Identifies the physical feeder. Double-clicking on any row of the **Available Links** table causes the same effect as clicking on the ***Add*** button. Double-clicking on any row of the **Selected Links** table causes the same effect as clicking on the ***Remove*** button. **V5 Link id**: Shows the link id of the corresponding feeder. If a V5 link is not yet available this field is empty.
>> (Add)	This button is used to add a link to the V5.2 interface (cross-connection). It is active only if a feeder in the **Available Links** list has been selected. If the feeder already carries a V5 link, and the **V5 Link id** is not present in the V5.2 interface yet, the feeder will be cross-connected to the V5.2 interface (if the **V5 Link id** is already in use in this V5.2 interface the command will be rejected). In case the V5 link is not yet defined, the *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30) for that link, permitting the modification of the link in a way that cross-connecting is possible. The *V5.2 Add/Remove Links* window is locked until the *V5 Link* window is closed. After that the value of the V5 link id is checked. If this is a valid value and the number of V5 links cross-connected to the V5.2 interface is less than or equal to 16, the feeder will be cross-connected. If not, it remains in the available list, and the cross- connection operation is cancelled.
<< (Remove)	This button is active only if a feeder in the **Selected Links** list has been selected. It is used to remove a cross-connection between a V5 link and the V5.2 interface. If the V5 interface is unlocked, and the selected feeder is the primary or secondary feeder (protection group 1 - cf. Chapter 6.2.6, page 6-35), the remove function is not available.

6.2.2.4 Add a V5.2 link

The *V5.2 Add/Remove Links* window is reached from the *V5.2 Interface* window (tab V5 Interface Data) by clicking on ***V5 Links...*** (cf. Chapter 6.2.1.2.1, page 6-11).

Procedure

Complete the following procedure to add a link (links) to the V5.2 interface. Up to 16 V5.2 links are possible.

Step	Procedure
1.	Select an appropriate feeder in the **Available Links** list and click on **>> *(Add)*** or double-click on the feeder. The *V5 Link* window pops up to modify the link in a way that cross-connecting is possible (cf. Chapter 6.2.5.2, page 6-33). After that the *V5.2 Add/Remove Link* window is available again and the V5 link and the related cross-connection are added.
2.	Repeat step 1 to add another **Available Link(s)** or proceed with step 3.
3.	Click on ***Close*** to exit the window.

6.2.3 Physical Feeders List window

This window shows all available physical feeders and provides access to the *V5 Link* window for link parameter modification and to the *Physical Feeder* window (cf. Equipment configuration - Chapter 5.5.5.4, page 5-60) for feeder information.

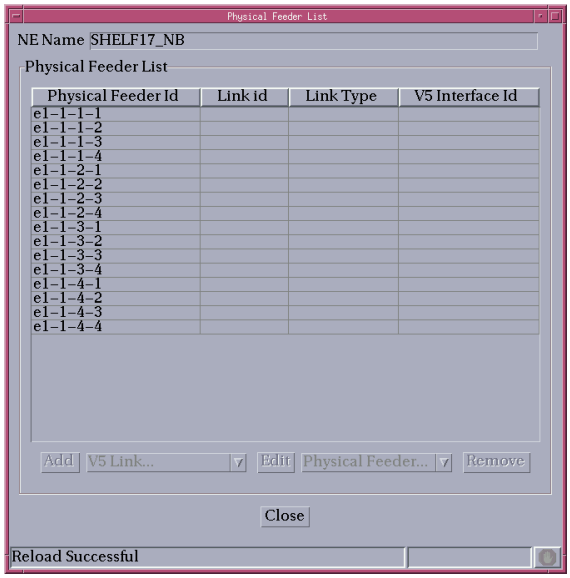


Figure 6-9 Physical Feeders List window

The following table shows the view/edit options of the *E1 Feeders List* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Feeders List	This scrolling list contains physical feeders related to the NE. Selecting a row enables the ***Edit*** and ***Remove*** buttons (see below). **Physical Feeder Id**: Displays the id of the physical feeders. **V5 Link id**: Indicates the value of the V5 Link id, if applicable. If this feeder has no associated V5 Link id, the field is left empty. Possible values: {0, 255} for V5 links, {1, 16} for LL links. **Link Type**: Displays the link type: V5 Link or LL Link. **V5 Interface id**: If the physical feeder is associated with a V5 link and the V5 link is cross-connected to a V5 interface, the value of the V5 interface id is displayed here. Possible values: Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. If there is no cross-connection or if the link is LL link the value is left empty. The ***Add*** button is used to add a link. It provides access to the following windows dependent on the selected entry in the corresponding option menu: *V5 Link* *Leased Line Link*. This button is enabled only if a feeder in the list has been selected with no associated links. The ***Edit*** button provides access to the following windows dependent on the selected entry in the corresponding option menu: *Physical Feeder* *Leased Line Link* (available if the selected feeder has an LL link already associated) *V5 Link* (available if the selected feeder has a V5 link already associated). The ***Remove*** button is used to remove a logical link. It is available only if there is a link associated to the physical feeder.

6.2.4 Leased Line Link window

This window displays the leased line link information and provides the possibility to change it.

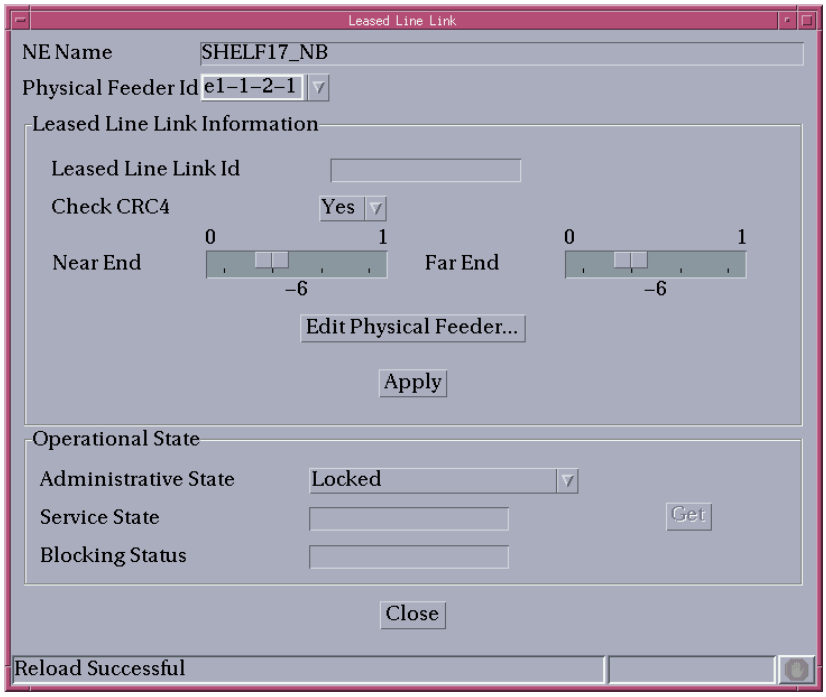


Figure 6-10 Leased Line Link window

The following table shows the view/edit options of the *Leased Line Link* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Feeder Id	This option menu lists all physical feeders. Feeders that carry a leased line link are shown with a light-grey background, if such a feeder is selected the edit mode is active. Free feeders are shown with a white background, if such a feeder is selected the add mode is active.

Parameters/ Buttons	Description
Leased Line Link Information	**Leased Line Link Id**: This text field specifies the LL Link Id. It is left empty at creation time. **Check CRC4**: This option is used to define whether the cyclic redundancy check shall be executed or not. Possible values: Yes, No. Modification is enabled only if the administrative state of the link is "Locked". **Near End**: This slider can be used to define the threshold value for the near-end bit error ratio detection on the related physical feeder. Possible values: {-7, -4}, step 1. The slider is enabled only if CRC4 is set. Modification is enabled only if the administrative state of the link is "Locked". **Far End**: This slider can be used to define the threshold value for the far-end bit error ratio detection on the related physical feeder. Possible values: {-7, -4}, step 1. The slider is enabled only if CRC4 is set. Modification is enabled only if the administrative state of the link is "Locked". The ***Edit Physical Feeder...*** button provides access to the *Physical Feeder* window (cf. Chapter 5.5.5.4, page 5-60). The ***Apply*** button is used to confirm the changes (creation of a new link or changing the available link).
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled and the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The field **Blocking Status** contains the current blocking status obtained (on demand) by the user. The ***Get*** button is used to update the display of the **Operational State**.
Timeslots Information	This table shows the timeslot information for the selected LL link in edit mode: ■ **LL Timeslot** ■ **LL Id** (leased line cross-connected to the timeslot). ■ **LL Type** (possible values: ALL, DLL, VLL (only for NE R1.4), GLL (only for NE R1.4), ROC (only for NE R1.4).).

Parameters/ Buttons	Description
Timeslots Information (continued)	The ***Add*** enables provisioning of a new user port. It provides access to the following windows dependent on the selected entry in the corresponding option menu: *ALL User Port* *DLL User Port* *GLL User Port* (only for NE R1.4) *VLL User Port* (only for NE R1.4). This button is disabled if a row is selected in the time slot list. The ***Edit User Port...*** provides access to the following windows dependent on the selected entry in the time slot list: *ALL User Port* *DLL User Port* *GLL User Port* (only for NE R1.4) *VLL User Port* (only for NE R1.4). This button is enabled only if a row is selected in the time slot list. The ***Edit TSs*** button provides access to the *Edit Timeslots* window (only for LL types VLL and GLL).

6.2.4.1 Create a leased line link

Procedure Complete the following procedure to create an leased line link:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).
2.	Select an appropriate feeder (without an associated LL link) in the list, use the option menu near the ***Add*** button to select **Leased Line Link** and click on ***Add***. The *Leased Line Link* window pops up (cf. Chapter 6.2.4, page 6-26).
3.	Enter a **Leased Line Link id** as prerequisite for adding an LL link.
4.	Press ***Apply*** to confirm.
5.	Click on ***Close*** to exit the window.

6.2.4.2 Modify a leased line link

Procedure Complete the following procedure to modify an LL link:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).

2. Select an appropriate feeder (with an associated LL link) in the list, use the option menu near the ***Edit*** button to select **Leased Line Link** and click on ***Edit***. The *Leased Line Link* window pops up (cf. Chapter 6.2.4, page 6-26).

   This window can also be reached from the *IO_E1* and *Physical Feeder* window via ***Add/Edit Leased Line Link...***.

If you want to ...	then ...
edit the LL link parameters	edit the parameters in the field **Leased Line Link Information** and click on ***Apply*** to confirm.
edit the physical feeder	click on ***Edit Physical Feeder...***. The *Physical Feeder* window pops up (cf. Chapter 5.5.5.4, page 5-60).
change the administrative state	use the corresponding option menu in the field **Operational State** to select the desired state. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?`**
add an user port	use the option menu near the ***Add*** button in the **Timeslot Information** field to select the desired user port and click on ***Add***. The corresponding user port window pops up.
edit an user port	select a time slot in the time slot list an click on ***Edit User Port...***. The corresponding user port window pops up.

3. Click on ***Close*** to exit the window.

6.2.5 V5 Link window

This window displays the V5 link information and provides the possibility to change it.

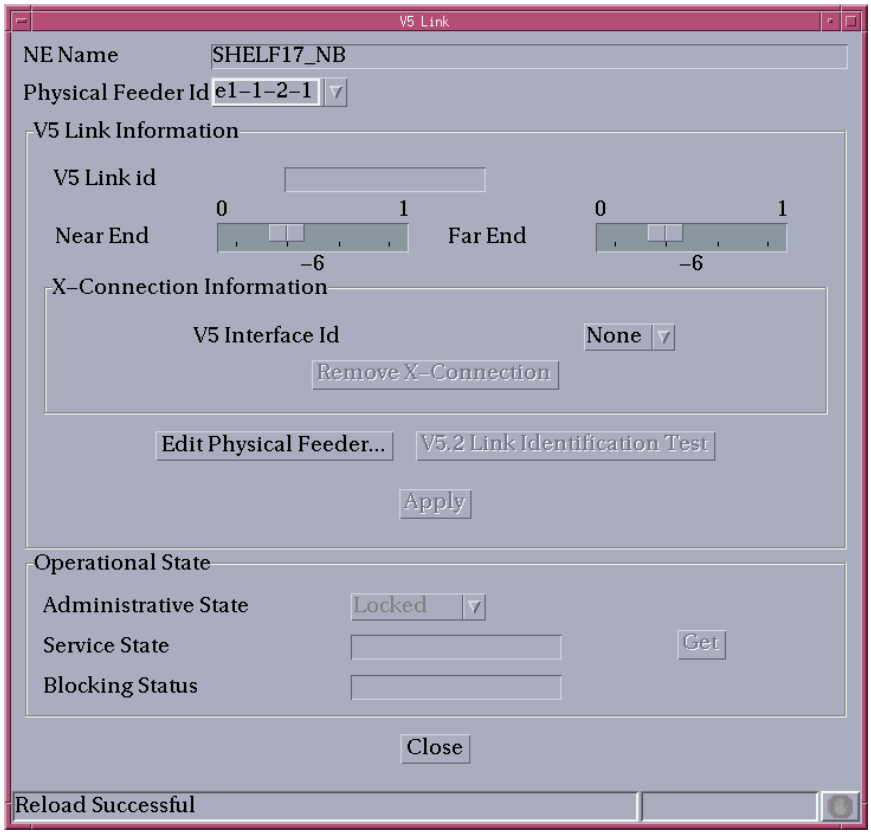


Figure 6-11 V5 Link window

The following table shows the view/edit options of the *V5 Link* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Feeder Id	This option menu lists all physical feeders. Feeders that carry a V5 link are shown with a light-grey background, if such a feeder is selected the edit mode is active. Free feeders are shown with a white background, if such a feeder is selected the add mode is active.

Parameters/ Buttons	Description
V5 Link Information	**V5 Link Id**: This text field specifies the V5 Link Id. Modification is enabled, if the V5 link is not cross-connection to a V5 interface or the V5 link is cross-connection to a V5 interface that is locked or the add mode is active. Modification is enabled only if the administrative state of the link is "Locked". **Near End**: This slider can be used to define the threshold value for the near-end bit error ratio detection on the related physical feeder. Possible values: {-7, -4}, step 1. Modification is enabled only if the administrative state of the link is "Locked". **Far End**: This slider can be used to define the threshold value for the far-end bit error ratio detection on the related physical feeder. Possible values: {-7, -4}, step 1. Modification is enabled only if the administrative state of the link is "Locked". **X-Connection Information:** **V5 Interface id**: This option menu indicates the V5 interface id the link is cross-connected to. If the link has no V5 interface cross-connected all possible V5 interfaces (all V5.2 and all V5.1 without links) are displayed. Possible values: Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. The ***Remove X-Connection*** button is used to remove a cross-connection. It is available only if a cross-connection already exists. The ***Edit Physical Feeder...*** button provides access to the *Physical Feeder* window (cf. Chapter 5.5.5.4, page 5-60). The ***V5.2 Link Identification Test*** button can be used to start the corresponding test. For more information refer to Chapter 7.4.1.12. The ***Apply*** button is used to confirm the changes (creation of a new link or changing the available link).

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Shutdown (Non Deferred), Shutdown (Deferred), Unlocked. The values Shutdown (Non Deferred and Deferred) are available only when the current state is "Unlocked" and the link is already cross-connected to a V5.2 interface. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-Stae - Sec. Serv. State). The field **Blocking Status** contains the current blocking status obtained (on demand) by the user. Possible values if the link is cross-connected to a V5.1 interface: None. Possible values if the link is cross-connected to a V5.2 interface: None, Local, Local and Remote. The ***Get*** button is to update the display of the **Operational State** and the **Blocking Status**.
Communication Channels Information	The information in this table is only available if there is a V5 interface cross-connected. The first column contains the timeslot id, the second the channel type, the third the communication channel id if a communication channel is cross-connected. There are three rows, one for timeslot 16, one for timeslot 31 and one for timeslot 15, in that order. The values in this field cannot be edited here, but only via the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109). **Timeslot**: Displays a timeslot of 64-kbps within the 2.048-Mbps V5 link. Possible values: 16, 31, 15. These values are arranged in this order because of the assignment order in V5. **Channel Type**: Possible values: B, C. Bearer channels (B) are used to transport bearer information. Communication channels (C) are used to transport all other information. All V5 timeslots are initially provisioned for bearer service (B). **CC ID**: Displays the identifier of the cross-connected communication channel. There is no value if the type of channel is B type, nor if no communication channel is cross-connected. Possible values: {0, 65503} valid only for V5.2.

6.2.5.1 Create a V5 link

Procedure Complete the following procedure to create a V5 link.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).
2.	Select an appropriate feeder (without an associated V5 link) in the list, use the option menu near the ***Add*** button to select **V5 Link** and click on ***Add***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30).
3.	Enter a **V5 Link id** as prerequisite for adding a V5 link.
4.	Use the option menu **V5 Interface id** to select a V5 interface (this step is optional).
5.	Press ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.5.2 Modify a V5 link

Procedure Complete the following procedure to modify a V5 link:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).
2.	Select an appropriate feeder (with an associated V5 link) in the list, use the option menu near the ***Edit...*** button to select **V5 Link** and click on ***Edit...***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30). This window can also be reached from the *IO_E1* and *Physical Feeder* window via ***Add/Edit V5 Link...***.

If you want to ...	then ...
edit the V5 link parameters	edit the parameters in the field **V5 Link Information** and click on ***Apply*** to confirm.
add a cross-connection to the V5 interface	use the option menu **V5 Interface** Id to select the desired V5 interface and click on ***Apply***.

If you want to ...	then ...
remove a cross-connection from the V5 interface	use the option menu **V5 Interface** Id to select the desired V5 interface and click on ***Remove Cross-Connection***. A *Warning* window pops up: **`Removing cross-connection between V5 Link id and V5 Interface id may be service affecting. Do you want to continue?`**
edit the physical feeder	click on ***Edit Physical Feeder...***. The *Physical Feeder* window pops up (cf. Chapter 5.5.5.4, page 5-60).
change the administrative state	use the corresponding option menu in the field **Operational State** to select the desired state and click on ***Apply***. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?`**

3. Click on ***Close*** to exit the window.

6.2.6 Primary and secondary V5.2 links

Protection groups

A V5.2 interface supports two protection groups:

- Protection Group 1
  which is handled by setting the primary feeder and secondary feeder (cf. this section and Chapter 6.2.6.4, page 6-38).

  If the primary feeder becomes faulty a protection switch to the secondary feeder takes place.
- Protection Group 2
  which can have up to 43 working communication channels protected and up to three standby timeslots.The handling of protection group 2 is described in Chapter 6.2.8.11, page 6-124.

NOTE:
Only a primary link can be cross-connected to a communication channel.

NOTE:
Protection switching is possible only for the V5.2 protocol.

6.2.6.1 Primary Link window

The *Primary Link* window displays the V5 primary link information. The primary link configuration of a V5.2 interface identifies the V5 link and the V5 communication channel that are selected to carry the signalling which is not related to on-demand services (Control, Link Control and BCC protocol).

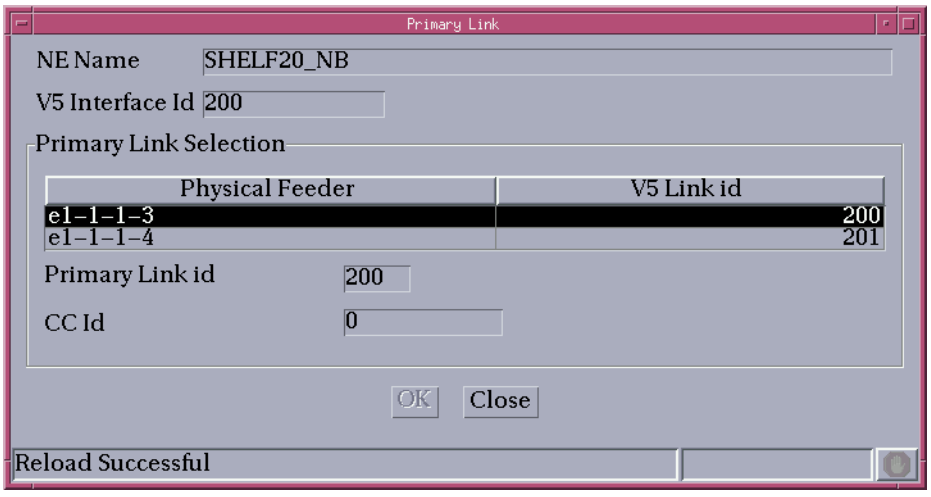


Figure 6-12 Primary Link window

The following table shows the view/edit options of the *Primary Link* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field displays the selected interface id. Possible values: Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Primary Link Selection	This list contains all the links that are cross-connected to this V5 interface. **Physical Feeder**: Displays the physical address of the physical feeder. **V5 Link id**: Displays all the links that are cross-connected to this V5 interface. Possible values: {0, 255}. **Primary Link id**: This value corresponds either to the current primary feeder link id, or to the selected item in the available links list, or is empty if there is no valid primary feeder configured and no selection was made. **CC id**: This field either shows the id of the current communication channel (CC) used for the primary feeder (possible values:{0, 65503}), or the value the user has entered, or is empty if no correctly configured CC is available. NOTE: Although 65503 is the maximum value, only 47 communication channels can exist for a V5.2 interface.
OK	This button is available only if a change was made, i.e. either a CC id was entered, or a feeder was selected, or both. It will use the current data to modify the configuration such that the selected feeder and CC id will identify the primary feeder.

6.2.6.2 Modify primary V5.2 link

This *Primary Link* window can only be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***Set Primary...***.

Procedure

Complete the following procedure to modify a primary V5.2 link.

Step	Procedure
1.	Select an appropriate feeder in the **Primary Link Selection** list.
2.	Enter/change the **CC id**.
3.	Click on ***OK*** to confirm and click on ***Close*** to exit the window.

NOTE:
When a primary link is created the following entities are automatically created: timeslot 16 is set to CC type, a CC with the defined CC id is created and cross-connected to that slot, communication paths *Control*, *Link Control* and *BCC* are created and cross-connected to that CC.

6.2.6.3 Secondary Link window

The *Secondary Link* window displays V5 secondary link information. The secondary link configuration of a V5.2 interface identifies the V5 link that is selected to carry protection group number 1 (protection protocol).

NOTE:
The configuration of a secondary link is only possible if a primary link is already configured.

The *Secondary Link* window can only be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***Set Secondary...***.

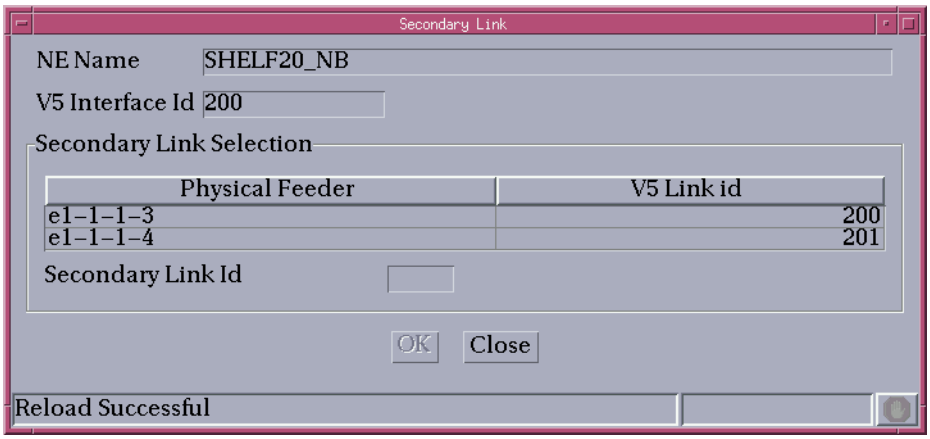


Figure 6-13 Secondary Link window

The following table shows the view/edit options of the *Secondary Link* window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field displays the selected interface id. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Secondary Link Selection	This list contains all the links that are cross-connected to this V5 interface, except the one that is configured as primary link. **Physical Feeder**: Displays the physical address of the physical feeder. Format: e1-shelf-slot-feeder. Possible values: e1-{1}-{1, 4}-{1, 4}. **V5 Link id**: Displays the link id of the shown feeder. Possible values: {0, 255}. **Secondary Link Id**: This value corresponds either to the current secondary feeder link id, or to the selected item in the available link list, or is empty if there is no valid secondary feeder configured and no selection was made.
OK	This button is available only if a change was made, i.e. a feeder has been selected. It will use the current data to modify the configuration such that the selected feeder will identify the secondary feeder.

6.2.6.4 Modify secondary V5.2 link

This *Secondary Link* window can only be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***Set Secondary...***.

Procedure

Complete the following procedure to modify a secondary V5.2 link.

Step	Procedure
1.	Select an appropriate feeder in the **Secondary Link Selection** list.
2.	Click on ***OK*** to confirm and click on ***Close*** to exit the window.

NOTE:
When a secondary link is created the following entities are automatically created: protection group 1, timeslot 16 is set to CC type and cross-connected with that protection group, the CC related to the primary link in that interface is cross-connected also with that protection group, a protection protocol communication path is created and cross-connected with protection group 1.

6.2.7 HDSL interface

6.2.7.1 HDSL Logical Interface List window

This window is available only for NE R1.4. It lists the existing HDSL interfaces and provides access to the *HDSL Interface* window to modify HDSL interface-specific parameters (when applicable) and access to creation of HDSL interfaces.

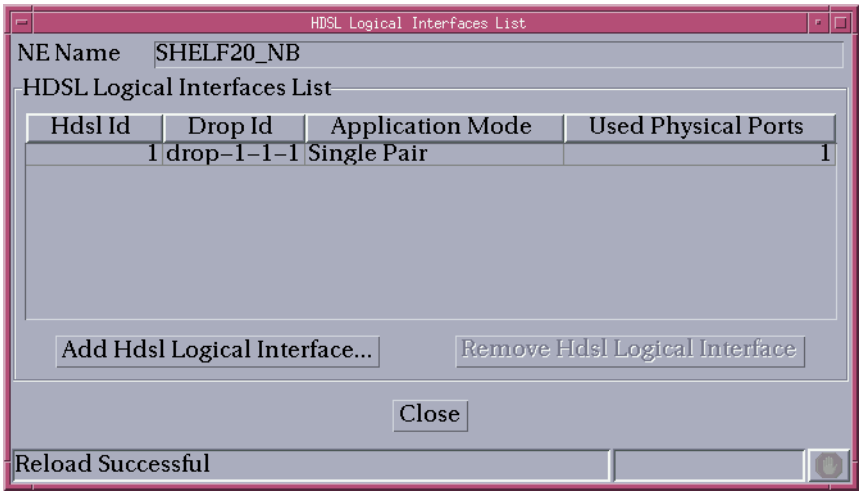


Figure 6-14 HDSL Logical Interfaces List window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
HDSL Logical Interface List	This list displays all available HDSL interface ids and the related parameters. Upon selection of any entry, the ***Edit HDSL Logical Interface...*** button becomes available. **HDSL Id**: Possible values: {0, 128}. **Drop Id**: Possible values: ap1-{1, 16} / subap-{1, 8}-{1, 8}. **Application Mode**: Possible values: Single Pair, Point to Point, Point to Multipoint. **Used Physical Ports**: Number of drops used by this interface: {1, 2}. The ***Label*** button provides access to the *HDSL Logical Interface* window. ***Add HDSL Logical Interface...*** if no selection has been made (add mode). ***Edit HDSL Logical Interface...*** if a physical drop has been selected which is already used in any HDSL logical interface and is an odd one (edit mode). The ***Remove HDSL Logical Interface*** button is used to remove an HDSL interface. This button is available only if an HDSL interface has been selected.

6.2.7.2 HDSL Logical Interface window

This window is used to add/modify an HDSL interface.

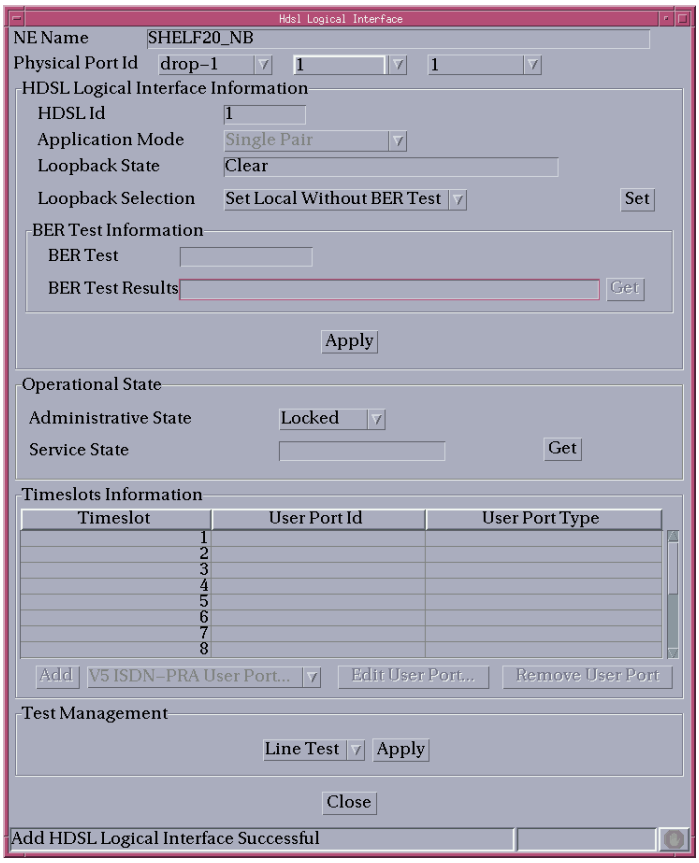


Figure 6-15 HDSL Logical Interface window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Physical Port Id	This information is presented by means of three option menus: The first option menu shows the drop-shelf id: drop-1 or sub-drop-{1, 8}. The second option menu displays the slot number: ap1-{1, 16} or subap-{1, 8}-{1, 8}. The third option menu shows the drop number inside the slot. Already used drops will be shown with a grey background, free drops with a white background.

Parameters/ Buttons	Description
HDSL Logical Interface Information	**HDSL Id**: Indicates the HDSL logical interface id. Possible values: {1, 128}. At creation time this field is empty. **Application Mode**: Shows the application mode of this logical interface. Possible values: Single Pair, Point to Point, Point to Multipoint (see also Table 6-1, page 6-45). **Loopback State**: This field shows the current loopback state. Possible values: Clear, Local with BER test, Local without BER test, NT with BER test, NT without BER test. **Loopback Selection**: This option menu contains all types of loopback states. It is enabled only if a drop has been selected. Possible values: Set Local with BER test: Loopback switched locally on AP (default value), Set Local without BER test: Loopback switched locally on AP (default value), Set NT with BER test: Loopback switched at Network Termination, Set NT without BER test: Loopback switched at Network Termination. Clear: Clear the loopback. The ***Set*** button is used to change the loopback state and to retrieve the current BER test state. Pressing this button confirms the selection made in the option menu **Loopback Selection**. **BER Test**: This field shows the current BER test state: Yes, No, Finished. The display of this value can be updated via ***Set*** or ***Get*** button. **BER Test Results**: This field displays the current BER test result (TL1 string). The display of this value can be updated via the ***Get*** button. The ***Get*** button can be used to retrieve the current loopback state, the current BER test state and the current BER test result from the NE. This button is enabled only if a drop has been selected and the drop has a loopback. The ***Apply*** button is used to confirm the changes of the HDSL logical interface.

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State**.
Timeslots Information	The following fields are enabled only if the HDSL already exists (edit mode). The table is sorted by timeslots. **User Port Id**: Shows the user port associated to the timeslot. **User Port type**: Shows the user port type contained in the timeslot. Possible values: V5 ISDN PRA, GLL, VLL. The ***Add*** button is used to add a user port (see also Table 6-1, page 6-45). It provides access to the following windows dependent on the selected entry in the corresponding option menu: *V5 ISDN PRA User Port* *G Leased Line* *V Leased Line*. This button is enabled only if a timeslot in the list has been selected with no associated user port. The ***Edit User Port...*** button is used to edit a user port. It provides access to the following windows dependent on the selected entry in the corresponding option menu: *V5 ISDN PRA User Port* *G Leased Line* *V Leased Line*. This button is enabled only if a timeslot in the list has been selected with an already associated user port. The ***Remove User Port*** button is used to remove a user port. It is available only if a selection has been made.
Test Management	The ***Apply*** button is used, together with the option menu beside it, to execute one of the following tests: Line test, Port test. For more information refer to Chapter 7.4.

The following table shows the provisionable services depending on the application mode.

Table 6-1 Application mode - Provisionable services

Application mode	Max. provisionable services	Allocatable HDSL timeslots	Number of allocatable timeslots
Single Pair	(1xGLL or 1xPRA) + 1x VLL	1-16 (1-15, if PRA is provisioned)	16 (15 if PRA is provisioned)
Point to Point	(1xGLL or 1xPRA) + 1x VLL	1-31 (without 16, if PRA is provisioned)	31 (30, if PRA is provisioned)
Point to Multipoint	2xGLL + 2xVLL	1-15/17-31	30

6.2.7.3 Add an HDSL logical interface

Procedure

Complete the following procedure to create an HDSL logical interface.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> HDSL Interface*** via the cursor menu. The *HDSL Logical Interfaces List* window pops up (cf. Chapter 6.2.7.1, page 6-39).
2.	Click on ***Add HDSL Logical Interface...***. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).
3.	Use the option menus **Physical Port Id** to select the desired port.
4.	Use the option menu **Application Mode** to select an appropriate mode and click on ***Apply***.
5.	Click on ***Close*** to exit the window.

6.2.7.4 Modify an HDSL logical interface

Procedure Complete the following procedure to modify an HDSL logical interface.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> HDSL Interface*** via the cursor menu. The *HDSL Logical Interfaces List* window pops up (cf. Chapter 6.2.7.1, page 6-39).

2. Select the desired row in the table and click on ***Add HDSL Logical Interface...*** or double click on the row entry. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).

   This window can also be reached via the *HDSL AP* window (cf. Chapter 5.5.5.16, page 5-84) via ***Add*** or ***Edit HDSL...***.

If you want to ...	then ...
get the current loopback state, BER test state and BER test results	click on ***Get*** in the **HDSL Logical Interface Information** field**.**
change the type of the port loopback	use the option menu **Loopback Selection** to chose the loopback state and click on ***Set*** to confirm. If the change is service affecting a *Warning* window pops up: **`Setting Loopback for a feeder can be service affecting. Do you want to continue?`**
change the administrative state	use the corresponding option menu in the field **Operational State**. NOTE: If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of HDSL logical Interface may be service affecting. Do you want to continue?`**.

If you want to ...	then ...
add a V5 ISDN PRA user port	select an empty timeslot in the **Timeslots Information** list, use the option menu beside the ***Add*** button to select **V5 ISDN PRA User Port** and click on ***Add***. The *V5 ISD PRA User Port* window pops up (cf. Chapter 6.2.8.6.1, page 6-84).
add a V or a G leased line user port	select an empty timeslot in the **Timeslots Information** list, use the option menu beside the ***Add*** button to select **G Leased Line** or **V Leased Line** and click on ***Add***. The *GLL User Port* window (cf. Chapter 6.2.8.7.4, page 6-98) or the *VLL* User Port window pops up (cf. Chapter 6.2.8.7.1, page 6-91).
edit an user port	select the desired timeslot in the **Timeslots Information** list and click on ***Edit User Port...*** or double click on the row entry. The corresponding user port window pops up: *V5 ISDN PRA User Port* (cf. Chapter 6.2.8.6.1, page 6-84) *GLL User Port* (cf. Chapter 6.2.8.7.4, page 6-98) *VLL User Port* (cf. Chapter 6.2.8.7.1, page 6-91).
remove an user port	select the desired timeslot in the **Timeslots Information** list and click on ***Remove User Port***.
exit the window	click on ***Close***.

6.2.8 User ports

6.2.8.1 User Port List window

This window displays the user port list based on the selection criteria.

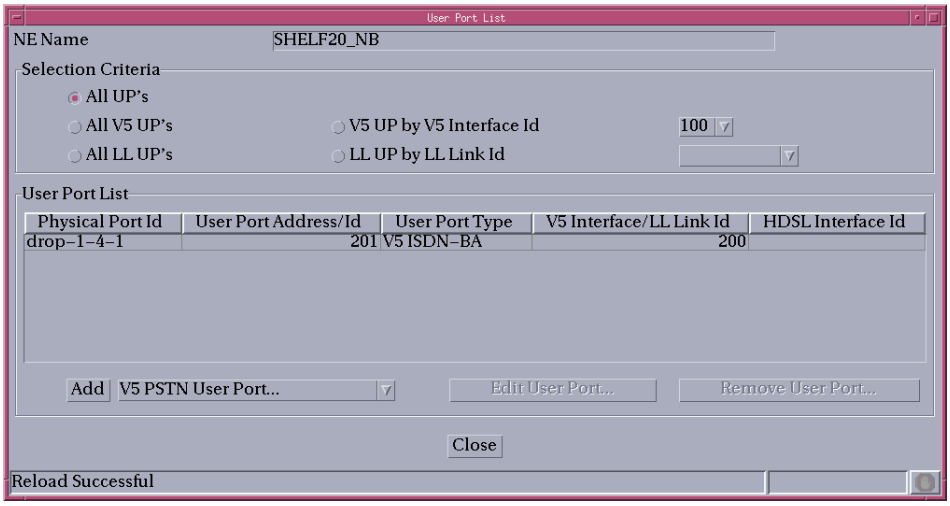


Figure 6-16 User Port List window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Selection Criteria	Radio buttons are used to define the list that will be displayed in the table **User Ports List** (see below). **All Userports**: Displays all the V5 user ports (PSTN, ISDN BA, ISDN PRA), all the leased lines (ALL, DLL, VLL, GLL) user ports and the ROC channel (only for NE R1.4) currently present in the NE. **All V5 Userports**: Displays all the V5 user ports (PSTN, ISDN BA, ISDN PRA) and the ROC channel (only for NE R1.4) currently present in the NE. **All Leased Line Userports**: Displays all the leased lines (ALL, DLL, VLL, GLL) user ports currently present in the NE. **V5 UP by V5 Interface Id**: If this radio button is selected the user port list below displays all the V5 user ports and the ROC channel cross-connected with the V5 interface id present in the related option menu, if applicable. If the value in this option menu is None this radio button cannot be selected. The option menu is used to select a V5 interface id. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. Selecting one id (except None) activates the **V5 Interface Id** radio button. **LL UP by Leased Line Link Id**: If this radio button is selected the user port list below displays all the LL user ports cross-connected with the LL link id present in the related option menu. If the value present in this option menu is None this radio button cannot be selected. The option menu is used to select a LL link id. Possible values: {1, 16} and None. Selecting one id (except None) activates the **Leased Line Link Id** radio button.

Parameters/ Buttons	Description
User Port List	The information in this field is displayed in a 5-column table: **Physical Port Id**: Displays the physical port id associated to the V5 user port shown in the row. Format: drop type-shelf-slot-port Possible values: drop-1-{1, 16}-{1, 32}. **User Port Address/Id**: Indicates the V5 user port address or the LL id within the V5 interface. Possible values: V5 Layer 3 Port Address {0, 32767} for PSTN V5 user port and ROC, Envelope Function Address {0, 8175} for ISDN BA/PRA V5 user port, {1, 768} for LL. **User Port Type**: Displays the type of service provided. Possible values; PSTN, ISDN BA, ISDN PRA, ALL, DLL, VLL, GLL and ROC. NOTE: PSTN **and** ISDN is not possible within the same AP. **V5 Interface/LL Link Id**: Displays the V5 interface id/LL link id cross-connected to the user port. Possible values for V5 Interfaces Id: {0, 16777215} in dec format or {0, FFFFFF} in hex format. Possible values for LL links: {1, 16}. **HDSL Interface Id**: Displays the HDSL logical interface id associated to the user port shown in the row, if applicable. Possible values: {1, 128}.

Parameters/ Buttons	Description
Command Buttons	The ***Edit User Port...*** button is enabled only when a row is selected (except ROC). It provides access to the following windows: *V5 PSTN User Port,* *V5 ISDN BA User Port,* *V5 ISDN PRA User Port,* *ALL User Port,* *DLL User Port,* *GLL User Port,* *VLL User Port* to edit the V5/LL user port parameters (whenever this is possible) or even create, change or remove cross-connections with other V5 entities: V5 interface, V5 communication paths (ISDN) and V5 timeslots (V5.1 protocol). The ***Add*** button is enabled when no row is selected. It provides access to the following windows: *V5 PSTN User Port,* *V5 ISDN BA User Port,* *V5 ISDN PRA User Port,* *ALL User Port,* *DLL User Port,* *GLL User Port,* *VLL User Port* depending on the selection in the related option menu. The list of the possible values depends on the type of selected drop/HDSL. The ***Remove User Port...*** button is enabled only when a row is selected. It can be used to delete all the existing cross-connections between user port and other V5/LL entities and the user port entity.

6.2.8.2 ALL user ports

An ALL service is provided connecting a Z-port located on a POTS AP with one timeslot of an E1 physical feeder located on an IO_E1 pack (leased line link).

In order to provide an analog leased line service the Z-port has to be provisioned to support ALL and the E1 physical feeder has to be provisioned to be used for permanent leased line services connecting the subscriber terminal equipment to either a data multiplexer or an interoffice special services network (note that analog leased line services are totally independent of the V5 protocol).

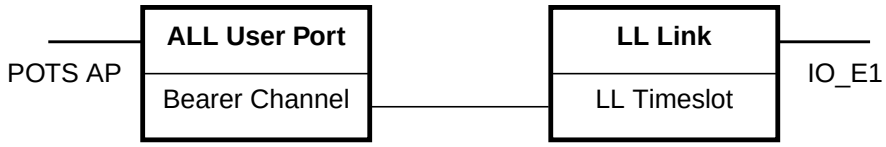


Figure 6-17 Functional model of ALL user port configuration

6.2.8.2.1 ALL User Port window

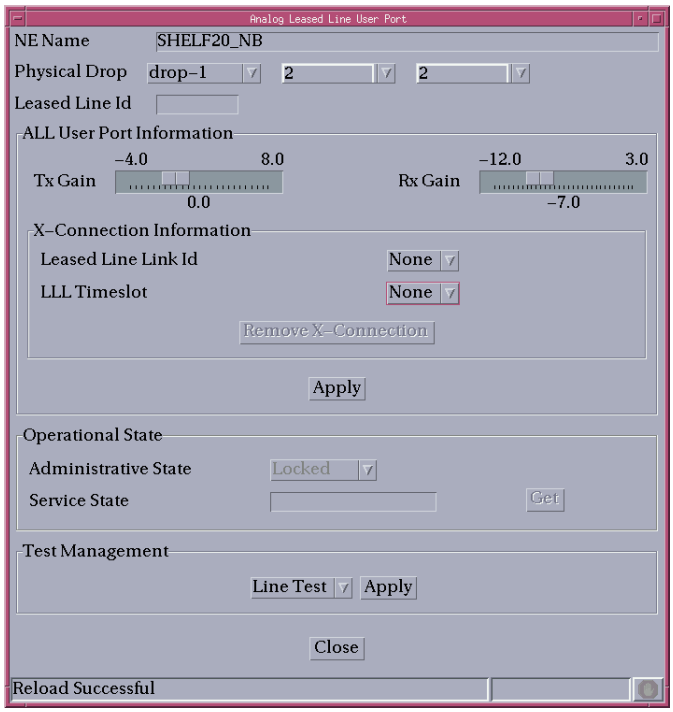


Figure 6-18 ALL User Port window

This window is used to add a new ALL user port and to modify or remove a created ALL user port.

It allows the operator to create/remove the cross-connection between an ALL user port and an LL Link interface, to create/change/remove the cross-connection between an ALL user port bearer channel and an LL Link timeslot as well as to configure and modify ALL user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new ALL user port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Port, Leased Line id), it is not possible to change these parameters here at all, or only insignificantly.

NOTE:
The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop	This field displays the physical port id associated to the ALL user port shown in this window by means of three option menus: ■ The first one contains drop-shelf. Possible values: drop-1 or subdrop-{1, 8}. ■ The second one contains the slot number inside the NE. Possible values: ap1-{1, 16} or subap-{1, 8}-{1, 8}. ■ The third one contains the drop number inside the slot indicated in the previous list {1, 32}. Possible values: drop-1-{1, 16}-{1, 32} or subdrop-{1, 8}-{1, 8}-{1, 32}. If the selected drop is already used by a user port it is shown with a grey background, otherwise a white background is shown. Selecting a free drop activates add mode; selecting a used drop activates edit mode.
Leased Line Id	This field displays the id of the ALL (edit mode) or is left empty (add mode).

Parameters/ Buttons	Description
ALL User Port Information	**Tx Gain**: This slider can be used to define the transmission gain in decibels relative to the digital reference point. Possible values: {-4, 8}. Step 0.5. Modification is enabled only if the administrative state is "Locked". **Rx Gain**: This slider can be used to define the reception gain in decibels relative to the digital reference point. Possible values: {-12, 3}. Step 0.5. Modification is enabled only if the administrative state is "Locked". **X-Connection Information**: This field provides the cross-connection information: ■ **Leased Line Link Id**: This option menu shows the LL link id (if the LL is already cross-connected) or provides the list of all LL links and the value None (if the user port is not cross-connected). ■ **LLL Timeslot**: This option menu displays the LL link timeslot id cross-connected to the ALL user port bearer channel. It allows the timeslot to be created/changed /removed (value None). ■ ***Remove X-Connection***: This button can be used to remove LL-LL link cross-connection. It is enabled only if the administrative state is "Locked". ***Apply***: This button is used to confirm the changes in the **ALL User Port Information** field.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State**.
Test Management	The ***Apply*** button is used, together with the option menu near it, to execute one of the following tests: Line test, Port test. For more information refer to Chapter 7.4.

6.2.8.2.2 Add an ALL user port

Assumptions

For the following description it is assumed that

- the NE is connected
- and the physical drop is provisioned and is not used for any other line
- leased line timeslots are free.

Procedure

Complete the following procedure to add an ALL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **ALL User Port** and click on ***Add***. The *ALL User Port* window pops up (cf. Chapter 6.2.8.2.1, page 6-52).
3.	Use the option menus **Physical Drop** to select a free drop.
4.	Edit all the other parameters of this window as described in Chapter 6.2.8.2.3, page 6-56 (Modify an ALL user port).
5.	Click on ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.8.2.3 Modify an ALL user port

Procedure Complete the following procedure to modify an ALL user port.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).

   This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.

2. Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.

3. Select the desired row in the **User Port List**.

4. Click on ***Edit User Port...***. The *ALL User Port* window pops up (cf. Chapter 6.2.8.2.1, page 6-52).

   This window can also be reached from the *PSTN AP* window (cf. Chapter 5.5.5.13, page 5-77) or from the *Leased Line Link* window (cf. Chapter 6.2.4, page 6-26) via ***Add/Edit User Port.***

If you want to ...	then ...
change the gain parameters	use the sliders **Tx Gain** and **Rx Gain** in the **ALL User Port Information** field to define the desired gain values and click on ***Apply***.
modify the cross-connection	use the option menus **Leased Line Link Id** and **LLL Timeslot**in the **X-Connection Information** field to select the corresponding values and click on ***Apply***.

If you want to ...	then ...
delete a cross-connection	use the option menus **Leased Line Link Id** and **LLL Timeslot**in the **X-Connection Information** field to select the corresponding values and click on ***Remove X-Connection***.
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of ALL user port may be service affecting. Do you want to continue?`**
exit the window	click on ***Close***.

6.2.8.3 V5 PSTN user ports

Overview

The PSTN entity represents a PSTN user port which can be associated to a V5 interface. It contains only one user port bearer channel.

The PSTN protocol information for all the POTS User Ports associated to a specific V5 interface (V5.1 / V5.2) is carried by the PSTN V5 Communication Path, and no provisioning action is needed for this subscriber information allocation.

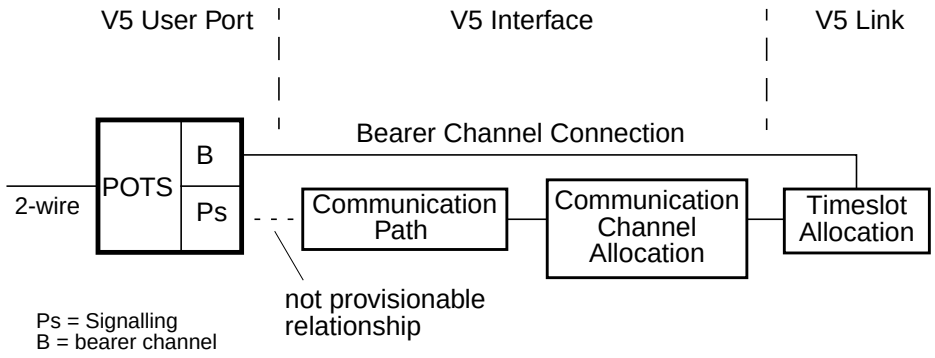


Figure 6-19 Functional model of PSTN user port configuration

6.2.8.3.1 V5 PSTN User Port window

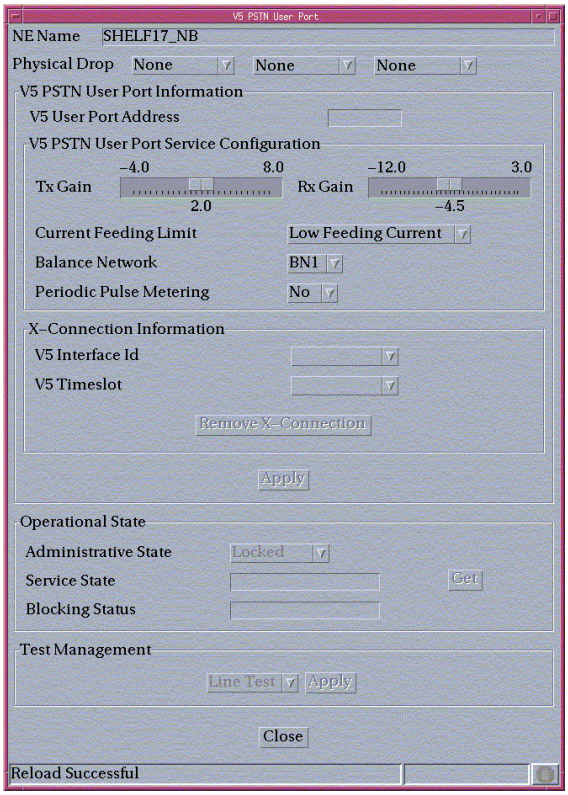


Figure 6-20 V5 PSTN User Port window

This window is used to add a new V5 PSTN user port, or modify an existing V5 PSTN user port.

It allows the operator to create/remove the cross-connection between a V5 PSTN user port and a V5 interface, to create/change/remove the cross-connection between a V5 PSTN user port bearer channel and a V5 timeslot (only for V5.1 protocol) as well as to configure and modify V5 PSTN user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new V5 PSTN user port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Drop, V5 User Port Address and V5 Interface id), it is not possible to change these parameters here at all, or only insignificantly.

NOTE:
The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop	This field displays the physical port id associated to the V5 PSTN user port shown in this window by means of three option menus: ■ The first one contains drop-shelf. Possible values: drop-1 or subdrop-{1, 8}. ■ The second one contains the slot number inside the NE. Possible values: ap1-{1, 16} or subap-{1, 8}-{1, 8}. ■ The third one contains the drop number inside the slot indicated in the previous list {1, 32}. Possible values: drop-1-{1, 16}-{1, 32} or subdrop-{1, 8}-{1, 8}-{1, 32}. If the selected drop is already used by a user port it is shown with a grey background, otherwise a white background is shown. Selecting a free drop activates add mode; selecting a used drop activates edit mode.

Parameters/ Buttons	Description
V5 PSTN User Port Information	**V5 User Port Address**: This field displays the Layer 3 Port Address which identifies the V5 PSTN user port inside the V5 interface. This field is enabled if the user port is not cross-connected to a V5 interface. **V5 PSTN User Port Service Configuration**: This field provides the service configuration information. Modification of the parameters is enabled only if the administrative state is "Locked". ■ **Tx Gain**: This slider can be used to define the transmission gain in decibels relative to the digital reference point. Possible values: {-4, 8}. Step 0.5. ■ **Rx Gain**: This slider can be used to define the reception gain in decibels relative to the digital reference point. Possible values: {-12, 3}. Step 0.5. ■ **Current Feeding Limit**: This option menu can be used to select a desired Current Feeding Limit. Possible Values: High Feeding Current, Low Feeding Current. ■ **Balance Network**: This option menu can be used to select a desired Balance Network (BN). Possible values: BN1, BN2, BN3, BN4, BN5. ■ **Periodic Pulse Metering**: This option menu can be used to request periodic pulse metering. Possible values: Yes, No. **X-Connection Information**: This field provides the cross-connection information: ■ **V5 Interface Id**: This option menu displays the V5 interface id (if the V5 user port is already cross-connected) or provides the list of all V5 interfaces and the value None (if the user port is not cross-connected). ■ **V5 Timeslot**: This option menu displays the V5 timeslot id cross-connected to the V5 user port bearer channel. It allows the timeslot to be created/changed /removed (value None). A selection is enabled only if the selected V5 interface identifies a V5.2 protocol which has a V5 link already cross-connected. ■ ***Remove X-Connection***: This button can be used to remove an LL-LL link cross-connection. It is enabled only if the administrative state is "Locked". ***Apply***: This button is used to confirm the changes in the **V5 PSTN User Port Information** field.

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The field **Blocking Status** displays the current V5 PSTN blocking status obtained (on demand) by the user. Possible values: Local and Remote, None. The ***Get*** button is used to update the display of the **Operational State** an the **Blocking Status**.
Test Management	The ***Apply*** button is used, together with the option menu near to it, to execute one of the following tests: Line test, Port test. For more information refer to Chapter 7.4.

6.2.8.3.2 Add a V5 PSTN user port

Assumptions

For the following description it is assumed that

- the NE is connected
- the physical drop is provisioned and is not used for any other V5 user port or leased line subscriber
- the V5 Layer 3 Port Address (PSTN user ports) is unique within the V5 interface
- and the V5 timeslot is configured as bearer channel and is not in use (only for V5.1).

Procedure

Complete the following procedure to add a V5 PSTN user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **PSTN** and click on ***Add***. The *V5 PSTN User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59).
3.	Use the option menus **Physical Drop** to select a free drop.
4.	Edit all the other parameters of this window as described in Chapter 6.2.8.3.3, page 6-64 (Modify a V5 PSTN port).
5.	Click on ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.8.3.3 Modify a V5 PSTN user port

Procedure

Complete the following procedure to modify a V5 PSTN user port.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).

   This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.

2. Use the radio button **All Userports** or **All V5 Userports** to define the list that will be displayed.

3. Select the desired row in the **User Port List**.

4. Click on ***Edit User Port...***. The *V5 PSTN User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59).

   This window can also be reached from the *PSTN AP* window (cf. Chapter 5.5.5.13, page 5-77) or from the *V5 Interface* window (cf. Chapter 6.2.1.2, page 6-11) via ***Add/Edit User Port.***

If you want to ...	then ...
change the service configuration parameters	use the sliders and the option menus in the **V5 PSTN User Port Information** field to define the desired values and click on ***Apply***.
modify the cross-connection	use the option menus **V5 Interface Id** and **V5 Timeslot** in the **X-Connection Information** field to select the corresponding cross-connection and click on ***Apply***.
delete a cross-connection	use the option menus **V5 Interface Id** and **V5 Timeslot**in the**X-Connection Information** field to select the corresponding cross-connection and click on ***Remove X-Connection***.

If you want to ...	then ...
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **Changing the administrative state of V5 user port may be service affecting. Do you want to continue?**
exit the window	click on ***Close***.

6.2.8.4 DLL user ports

A digital leased line service is provided by connecting a U-port located on an ISDN AP with a number of timeslots of an E1 physical feeder located on an IO_E1 pack (leased line link).

In order to provide a digital leased line service the U-port has to be provisioned to support DLL and the E1 physical feeder has to be provisioned to be used for permanent leased line services connecting the subscriber terminal equipment to the network provider's leased line service. The number of timeslots depends on the type of the requested service.

AnyMedia Access System network digital leased line services offer various transmission capabilities:

- one B channel (64-kbps)
- one B channel and one signalling D channel (16-kbps)
- two B channels
- two B channels and one D channel (16-kbps).

Please note that all the timeslots which provide service for a unique DLL service shall be allocated (cross-connected) to the same leased line link, while only one 16-kbps D channel can be allocated in one 64-kbps timeslot.

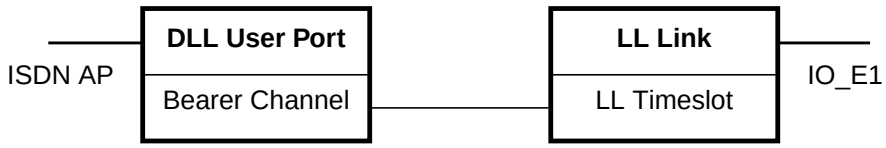


Figure 6-21 Functional model of DLL user port configuration

6.2.8.4.1 DLL User Port window

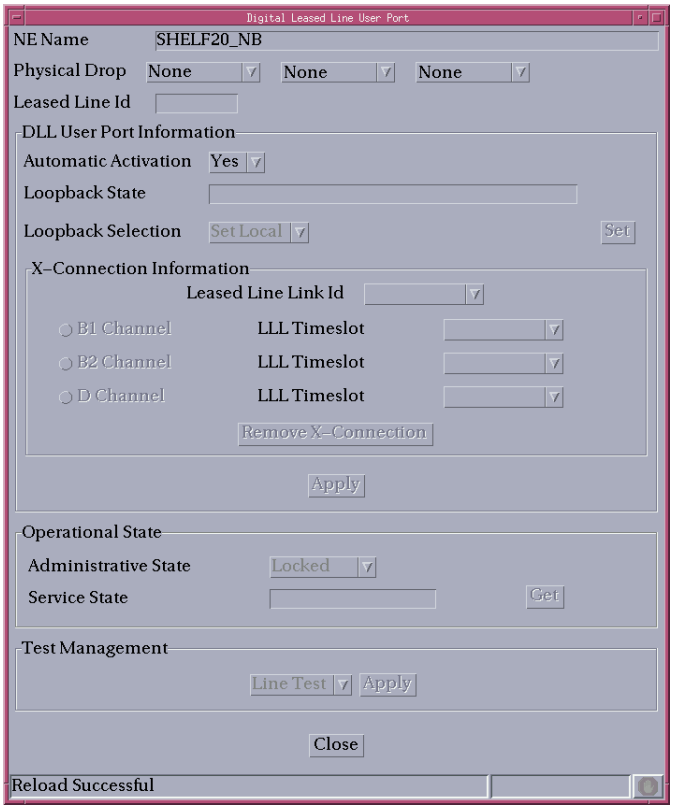


Figure 6-22 DLL User Port window

This window is used to add a new DLL user port and to modify or remove a created DLL user port.

It allows the operator to create/remove the cross-connection between a DLL user port and an LL Link interface, to create/change/remove the cross-connection between a DLL user port bearer channel and an LL Link timeslot as well as to configure and modify DLL user port service parameters configuration and modification.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new DLL user port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Port, Leased Line id), it is not possible to change these parameters here at all, or only insignificantly.

NOTE:
The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop	This field displays the physical port id associated to the DLL user port shown in this window by means of three option menus: ■ The first one contains drop-shelf. Possible values: drop-1 or subdrop-{1, 8}. ■ The second one contains the slot number inside the NE. Possible values: ap1-{1, 16} or subap-{1, 8}-{1, 8}. ■ The third one contains the drop number inside the slot indicated in the previous list {1, 32}. Possible values: drop-1-{1, 16}-{1, 32} or subdrop-{1, 8}-{1, 8}-{1, 32}. If the selected drop is already used by a user port it is shown with a grey background, otherwise a white background is shown. Selecting a free drop activates add mode; selecting a used drop activates edit mode.
Leased Line Id	This field displays the id of the DLL (edit mode) or is left empty (add mode).

Parameters/ Buttons	Description
DLL User Port Information	■ **Automatic Activation**: This option menu provides the possible values Yes and No. Modification is enabled only if the administrative state is "Locked". ■ **Loopback State**: This field displays the current loop-back state (Clear or Local, Regenerator, NT). This state can be changed via the ***Set*** button (see below). ■ **Loopback Selection**: This option menu is used to de-fine the DLL port loopback. It is only enabled if a drop is selected. Possible values: Set Local (loopback switched locally on AP), Set Reg (loopback switched at regenerator), Set NT (loopback switched at network termination), Clear (clear the loopback). ■ The ***Set*** button is used to perform the requested opera-tion (option menu Loopback Selection). **X-Connection Information**: This field provides the cross-connection information: ■ **Leased Line Link Id**: This option menu shows the LL Link id (if the LL is already cross-connected) or pro-vides the list of all LL links and the value None (if the user port is not cross-connected). ■ **B1 Channel**: This check box indicates whether DLL user port bearer channel 1 shall be used for DLL data. ■ **LLL Timeslot Id (B1)**: This option menu displays the LL link timeslot id cross-connected to DLL user port bearer channel 1. It allows the timeslot to be created /changed/removed (value None). ■ **B2 Channel**: This check box indicates whether DLL user port bearer channel 2 shall be used for DLL data. ■ **LLL Timeslot Id (B2)**: This option menu displays the LL link timeslot id cross-connected to DLL user port bearer channel 2. It allows the timeslot to be created /changed/removed (value None). ■ **D Channel**: This check box indicates whether the DLL user port D channel shall be used for DLL data. ■ **LLL Timeslot Id (D)**: This option menu displays the LL link timeslot id cross-connected to the DLL user port D channel. It allows the timeslot to be created /changed/removed (value None).

Parameters/ Buttons	Description
DLL Userport Information (continued)	***Remove X-Connection***: This button can be used to remove an LL-LL link cross-connection. It is enabled only if the administrative state is "Locked". The ***Apply*** button is used to confirm the changes in the **DLL Userport Information** field.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State**.
Test Management	The ***Apply*** button is used, together with the option menu near it, to execute one of the following tests: Line test, Port test, Single Pulse test. For more information refer to Chapter 7.4.

6.2.8.4.2 Add a DLL user port

Assumptions

For the following description it is assumed that

- the NE is connected
- and the physical drop is provisioned and is not used for any other line.

Procedure

Complete the following procedure to add a DLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **DLL User Port** and click on ***Add***. The *DLL User Port* window pops up (cf. Chapter 6.2.8.4.1, page 6-67).
3.	Use the option menus **Physical Drop** to select a free drop.
4.	Edit all the other parameters of this window as described in Chapter 6.2.8.4.3, page 6-72 (Modify a DLL port).
5.	Click on ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.8.4.3 Modify a DLL user port

Procedure Complete the following procedure to modify a DLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Port...***. The *DLL User Port* window pops up (cf. Chapter 6.2.8.4.1, page 6-67). This window can also be reached from the *ISDN AP* window (cf. Chapter 5.5.5.13, page 5-77) or from the *Leased Line Link* window (cf. Chapter 6.2.4, page 6-26) via ***Add/Edit User Port.***

If you want to ...	then ...
change the DLL user port service configuration	use the option menus **Automatic Activation** and **Loopback Selection** in the **DLL User Port Service Configuration** field to define the desired values and click on ***Set***. NOTE: If the loopback state has been changed to "Set" a *Warning* window pops up: **`Setting Loopback for a DLL user port can be service affecting. Do you want to continue?`**
modify the cross-connection	use the option menus and check boxes in the **X-Connection Information** field to define the appropriate values and click on ***Apply***.

If you want to ...	then ...
delete a cross-connection	use the option menus in the **X-Connection Information** field to select the desired cross-connection and click on ***Remove X-Connection***.
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of DLL user port may be service affecting. Do you want to continue?`**
exit the window	click on ***Close***.

6.2.8.5 V5 ISDN BRA user port

Overview

The ISDN BRA entity represents an ISDN BRA user port which can be associated to a V5 interface. It contains up to two user port bearer channels (64-kbps) for the communication signal and a 16-kbps D-channel for protocol information.

The ISDN BRA user port can have up to three different types of data (data signalling, packet and frame) to be carried over any of the communication channels within the V5 interface. On the other hand, an ISDN communication path (CP) represents an information type (Ds, p and f) for one or more ISDN BRA user ports associated to a V5 interface.

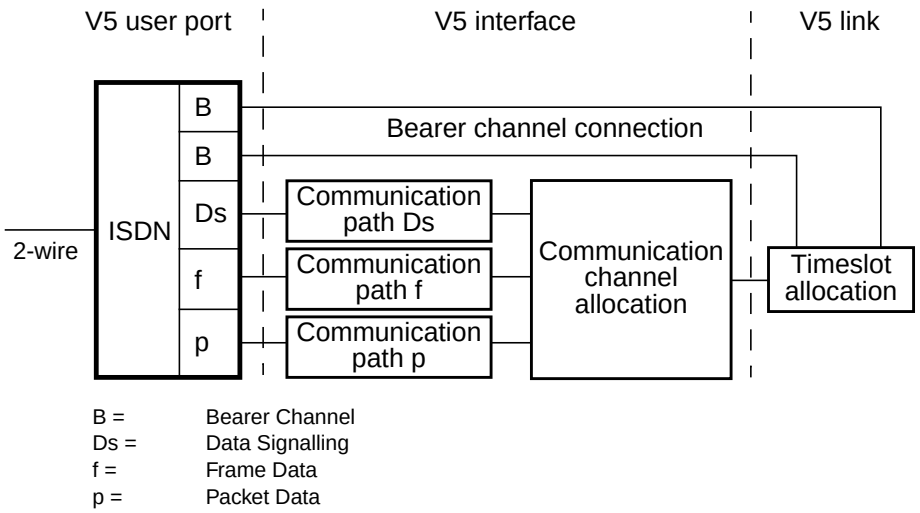


Figure 6-23 Functional model of ISDN BRA user port configuration

6.2.8.5.1 V5 ISDN BA User Port window

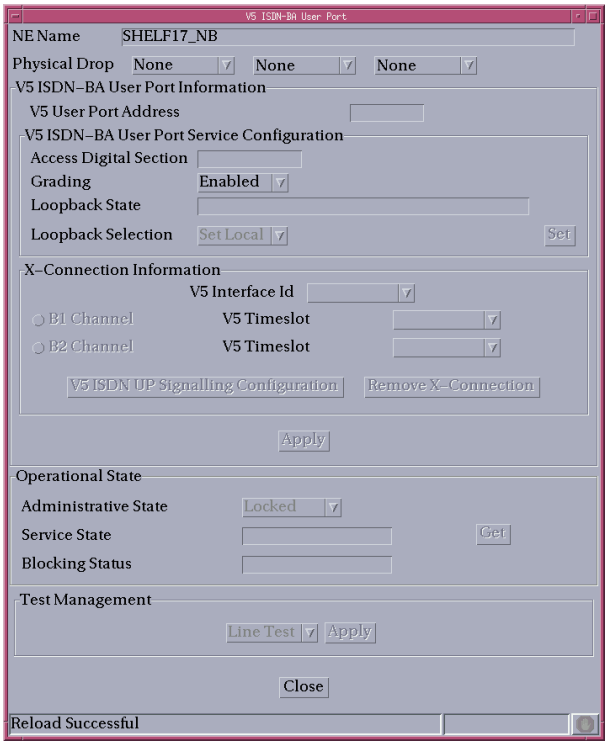


Figure 6-24 V5 ISDN BA User Port window

This window is used to add a new V5 ISDN BRA user port or remove or modify an existing V5 ISDN BRA user port (please note that the GUI uses BA instead of BRA).

It allows the operator to create/remove the cross-connection between a V5 ISDN BRA user port and a V5 interface, to create/modify/remove the cross-connection between a V5 ISDN BRA user port bearer channel(s) and a V5 timeslot (only for V5.1 protocol), to create/change/remove the cross-connection(s) between a V5 ISDN BRA user port and V5 communication path(s) (frame, packet or signalling) as well as to configure and modify V5 ISDN BRA user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new V5 ISDN BRA user port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Drop, V5 User Port Address and

V5 Interface id), it is not possible to change these parameters here at all, or only insignificantly.

NOTE:
The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop	This field displays the physical port id associated to the V5 ISDN BRA user port shown in this window by means of three option menus: ■ The first one contains drop-shelf. Possible values: drop-1 or subdrop-{1, 8}. ■ The second one contains the slot number inside the NE. Possible values: ap1-{1, 16} or subap-{1, 8}-{1, 8}. ■ The third one contains the drop number inside the slot indicated in the previous list {1, 32}. Possible values: drop-1-{1, 16}-{1, 32} or subdrop-{1, 8}-{1, 8}-{1, 32}. If the selected drop is already used by a user port it is shown with a grey background, otherwise a white background is shown. Selecting a free drop activates add mode; selecting a used drop activates edit mode.

Parameters/ Buttons	Description
V5 ISDN BA User Port Information	**V5 Userport Address**: This V5 Envelope Function Address identifies a V5 ISDN BRA user port within a V5 interface. Possible values: {0, 8175}. If the user port is already created and cross-connected to a V5 interface, the corresponding value is displayed and can not be changed. If the user port is created and not cross-connected the displayed value is editable. In all the other cases this field is empty and editable. **V5 ISDN BA Userport Service Configuration**: This field provides the service configuration information: ■ **Access Digital Section**: This text field indicates whether or not there is an access digital section at the ISDN BRA port (present). Modification is enabled only if the administrative state is "Locked". ■ **Grading**: This option menu can be used to define whether performance measurement grading messages should be sent to the connected LE. Possible values: Enabled, Disabled. Modification is enabled only if the administrative state is "Locked". ■ **Loopback State**: This field displays the current loopback state (Clear or Set). This state can be changed via the ***Set*** button on the right-hand side (see below). ■ **Loopback Selection**: This option menu is used to define the ISDN BRA port loopback. It is only enabled if a drop is selected. Possible values: Set Local (loopback switched locally on AP), Set Reg (loopback switched at regenerator), Set NT (loopback switched at network termination), Clear (clear the loopback). ■ The ***Set*** button is used to perform the requested operation (option menu Loopback Selection).

Parameters/ Buttons	Description
V5 ISDN BA User Port Information (continued)	**X-Connection Information**: This field provides the cross-connection information: ■ **V5 Interface id**: This field displays the V5 interface id to which this user port is cross-connected. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. When coming from *V5 Interface* window via ***Add ISDN*** this field is non-editable. If the V5 ISDN BRA user port is cross-connected to a V5 interface this field is editable; however the field can only be changed to the value "None" to delete a cross-connection. In all the other cases an option menu with all V5 interface ids is offered for selection. ■ **B1 Channel**: This check box indicates whether V5 ISDN BRA user port bearer channel 1 shall be used for ISDN data. ■ **V5 Timeslot (B1)**: This field displays the V5 timeslot id cross-connected to V5 ISDN BRA user port bearer channel 1 shown in this window (this field is only available for V5.1). Possible values: None, {1, 31}. This option menu (value "None" is allowed) is available for selection only when the selected V5 interface id identifies a V5.1 interface which has a V5 link already cross-connected and V5 ISDN BRA user port bearer channel 1 is enabled. This option menu is used to create/change/remove (set value "None") the cross-connection between bearer channel 1 and the timeslot. ■ **B2 Channel**: This check box indicates whether V5 ISDN BRA User Port bearer channel 2 shall be used for ISDN data. ■ **V5 Timeslot (B2)**: This field displays the V5 timeslot id cross-connected to V5 ISDN BRA user port bearer channel 2 shown in this window. Possible values: None, {1, 31}. This option menu (value "None" is allowed) is available for selection only when the selected V5 interface id identifies a V5.1 interface which has a V5 link already cross-connected and V5 ISDN BRA user port bearer channel 2 is enabled. This option menu is used to create/change/remove (set "None" value) the cross-connection between bearer channel 2 and the timeslot.

Parameters/ Buttons	Description
V5 ISDN BA User Port Information (continued)	■ The ***V5 ISDN UP Signalling Configuration*** button provides access to the *V5 ISDN User Port Signalling Configuration* window where you are able to create, change or remove cross-connection(s) between V5 ISDN BRA user port and V5 ISDN communication path(s) (packet, frame and signalling). The button is enabled only if the V5 ISDN user port is created and cross-connected to the V5 interface identified in this window. ■ The ***Remove X-Connection*** button can be used to remove a V5 user port - V5 interface cross-connection. This button is enabled only if the administrative state is "Locked". The ***Apply*** button is used to confirm the changes in the **ISDN BA User Port Information** field.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked, Shutdown. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The field **Blocking Status** displays the current V5 ISDN BRA blocking status obtained (on demand) by the user. Possible values: Local, Remote, None. The ***Get*** button is used to update the display of the **Operational State** and the **Blocking Status**.
Test Management	The ***Apply*** button is used, together with the option menu near it, to execute one of the following tests: Line test, Port test, CRC test (only for ISDN BA). For more information refer to Chapter 7.4.

6.2.8.5.2 Add an ISDN BRA user port

Assumptions

For the following description it is assumed that

- the NE is connected
- the physical drop is provisioned and is not used for any other V5 user port or leased line subscriber
- the Envelope Function Address is unique within the V5 interface
- and the V5 timeslot is configured as bearer channel and is not in use (only for V5.1).

Procedure

Complete the following procedure to add a V5 ISDN BRA user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **V5 ISDN BA User Port** and click on ***Add***. The *V5 ISDN BA User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59).
3.	Use the option menus **Physical Drop** to select a free drop.
4.	Edit all the other parameters of this window as described in Chapter 6.2.8.5.3, page 6-81 (Modify a V5 ISDN BRA user port).
5.	Click on ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.8.5.3 Modify a V5 ISDN BRA user port

Procedure

Complete the following procedure to modify a V5 ISDN BRA user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.x Interface* windows (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the radio button **All Userports** or **All V5 Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Port...***. The *V5 ISDN BA User Port* window pops up (cf. Chapter 6.2.8.3.1, page 6-59). This window can also be reached from the *ISDN AP* window (cf. Chapter 5.5.5.13, page 5-77) or from the *V5 Interface* window (cf. Chapter 6.2.1.2, page 6-11) via ***Add/Edit User Port***.

If you want to ...	then ...
change the ISDN BRA user port service configuration	use the option menus **Grading** and **Loopback Selection** in the **V5 ISDN BA User Port Service Configuration** field to define the desired values and click on ***Set***. NOTE: If the loopback state has been changed to "Set" a *Warning* window pops up: **`Setting Loopback for a V5 ISDN BRA user port can be service affecting. Do you want to continue?`**
modify a cross-connection between user port and V5 interface	use the option menus and check boxes in the **X-Connection Information** field to select the appropriate values and click on ***Apply***.

If you want to ...	then ...
delete a cross-connection between user port and V5 interface	use the option menus and check boxes in the **X-Connection Information** field to select the desired values and click on ***Remove X-Connection***.
modify the V5 ISDN user port signalling configuration (cross-connection between V5 ISDN BRA user port and V5 ISDN communication path(s) (packet, frame and signalling))	use the option menus and check boxes in the **X-Connection Information** field to select a user port with a cross-connected V5 interface and click on ***V5 ISDN UP Signalling Configuration***. The *V5 ISDN BA User Port Signalling Configuration* window pops up (cf. Chapter 6.2.8.9, page 6-106).
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of V5 user port may be service affecting. Do you want to continue?`**
exit the window	click on the ***Close*** button.

6.2.8.6 V5 ISDN PRA user port

Overview

The ISDN PRA entity represents an ISDN PRA user port which can be associated to a V5.2 interface. PRA (primary rate access) for ISDN contains up to thirty 64-kbps B channels for communication signal and a 64-kbps D channel for protocol information. The B-channels are transported in the bearer channels of the V5.2 interface (BCC protocol) and the D-channel is transported in the communication paths of the V5.2 interface.

The ISDN PRA user port can have up to three different types of data (data signalling, packet and frame) to be carried over any of the logical communication channels within the V5.2 interface.

On the other hand, an ISDN communication path (CP) represents an information type (Ds, p and f) for one or more ISDN PRA user ports associated to a V5.2 interface.

The association of an ISDN PRA subscriber D channel to V5 ISDN communication paths is done by provisioning within the V5.2 interface.

The ISDN PRA service is provisioned on top of HDSL transmission equipment. This transmission equipment can operate in several modes which have to be selected by HDSL configuration management (cf. Chapter 5.5.5.16, page 5-84).

NOTE:
An ISDN PRA subscriber can be provisioned only if its related HDSL logical interface is already provisioned (cf. Chapter 6.2.7.1, page 6-39).

6.2.8.6.1 V5 ISDN PRA User Port window

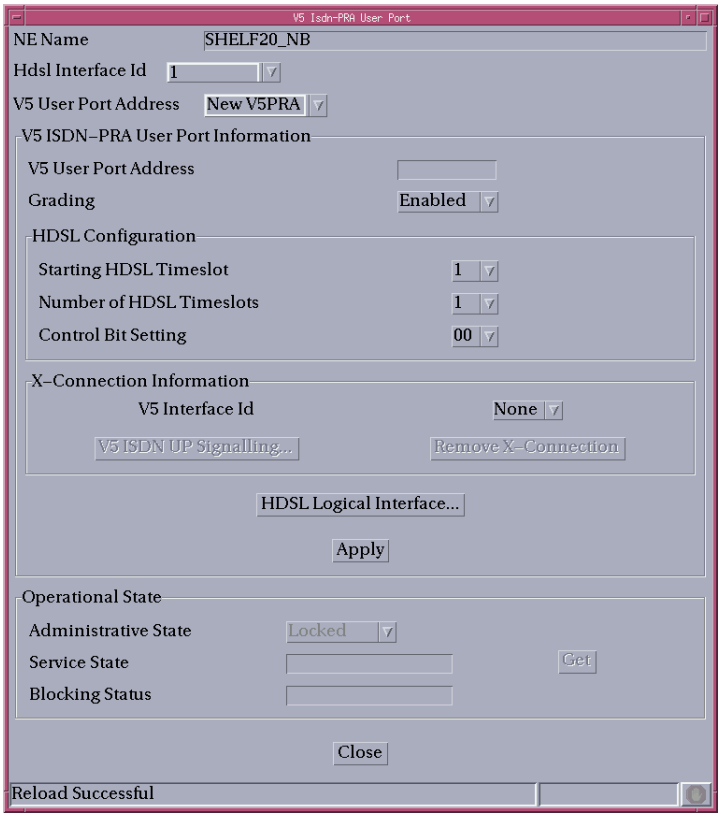


Figure 6-25 V5 ISDN PRA User Port window

This window is used to add a new V5 ISDN PRA user port or remove or modify an existing V5 ISDN PRA user port.

It allows the operator to create/remove the cross-connection between a V5 ISDN PRA user port and a V5.2 interface as well as to configure and modify V5 ISDN PRA user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new V5 ISDN PRA user port is created, all editable parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as HDSL Logical Interface id, V5 User Port Ad-

dress and V5 Interface id), it is not possible to change these parameters here at all, or only insignificantly.

The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
HDSL Interface Id	This option menu displays the HDSL logical interface id associated to the V5 user port shown in this window. If the interface is already used by a V5 user port it is shown with a grey background, otherwise a white background is shown. Selecting a free interface activates add mode; selecting a used interface activates edit mode.
V5 ISDN PRA User Port Information	**V5 User Port Address**: This V5 Envelope Function Address identifies a V5 ISDN PRA user port within a V5.2 interface. Possible values: {0, 8175}. If the user port is already created and cross-connected to a V5 interface, the corresponding value is displayed and can not be changed. If the user port is created and not cross-connected the displayed value is editable. In all the other cases this field is empty and editable. **Grading**: This option menu can be used to define whether performance measurement grading messages should be sent to the connected LE. Possible values: Enabled, Disabled. **HDSL Configuration**: This field provides the service configuration information. The option menus are enabled only if the administrative state is "Locked". ■ **Starting HDSL Timeslot**: This option menu can be used to select the starting timeslot on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. ■ **Number of HDSL Timeslots**: This option menu can be used to select the number of timeslots on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. ■ **Control Bit Setting**: This option menu can be used to define the setting of the SA57SA6 control bits. Possible values: {0, 1}.

Parameters/ Buttons	Description
V5 ISDN PRA User Port Information (continued)	**X-Connection Information**: This field provides the cross-connection information: ■ **V5 Interface id**: This field displays the V5.2 interface id to which this user port is cross-connected. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format. When coming from the *V5.2 Interface* window via ***Add ISDN PRA*** this field is non-editable. In all the other cases an option menu with all V5.2 interface ids is offered for selection. ■ The ***V5 ISDN UP Signalling...*** button provides access to the *V5 ISDN User Port Signalling Configuration* window where you are able to create, change or remove cross-connection(s) between V5 ISDN PRA user port and V5 ISDN communication path(s) (packet, frame and signalling). The button is enabled only if the V5 ISDN user port is created and cross-connected to the V5.2 interface identified in this window. ■ The ***Remove X-Connection*** button can be used to remove a V5 user port - V5 interface cross-connection. This button is enabled only if the administrative state is "Locked". The ***HDSL Logical Interface...*** button provides access to the *HDSL Logical Interface* window. The ***Apply*** button is used to confirm the changes in the V5 **ISDN PRA User Port Information** field.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked, Shutdown. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The field **Blocking Status** displays the current V5 ISDN PRA blocking status obtained (on demand) by the user. Possible values: Local, Remote, None. The ***Get*** button is used to update the display of the **Operational State** and the **Blocking Status**.

6.2.8.6.2 Add a V5 ISDN PRA user port

Assumptions

For the following description it is assumed that

- the NE is connected
- the HDSL interface is already provisioned on the physical drop
- the application mode must be either "single pair" or “point to point”
- the required HDSL logical timeslots (including timeslot 16) must be free and available
- the primary service state of the HDSL interface must be OOS
- the HDSL AP is provisioned with enough PCMH timeslots to support the ISDN PRA user port.

Procedure

Complete the following procedure to add a V5 ISDN PRA user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **ISDN PRA** and click on ***Add***. The *V5 ISDN PRA User Port* window pops up (cf. Chapter 6.2.8.6.1, page 6-84).
3.	Use the option menus **HDSL Interface Id** to select a free interface.
4.	Edit all the other parameters of this window as described in Chapter 6.2.8.6.3, page 6-88 (Modify a V5 ISDN PRA user port).
5.	Click on ***Apply*** to confirm.
6.	Click on ***Close*** to exit the window.

6.2.8.6.3 Modify a V5 ISDN PRA user port

Procedure

Complete the following procedure to configure a V5 ISDN PRA user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the radio button **All Userports** or **All V5 Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Port...***. The *V5 ISDN PRA User Port* window pops up (cf. Chapter 6.2.8.6.1, page 6-84). This window can also be reached from the *HDSL Logical Interface* window (cf. Chapter 6.2.7.2, page 6-41) or from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) via ***Add/Edit User Port***.

If you want to ...	then ...
change the ISDN PRA user port HDSL configuration	use the option menus **Starting HDSL Timeslot**, **Number of HDSL Timeslot** and **Control Bit Setting** in the **HDSL Configuration** field to define the desired values and click on ***Apply***.
change the grading adjustment	use the option menu **Grading** to select the desired entry and click on ***Apply***.
add a cross-connection	enter the V5 Envelope Function Address into the text field **V5 Userport Address**, use the option menu **V5 Interface Id** in the field **X-Connection Information** to select the interface id and click on ***Apply***.
modify the V5 ISDN user port signalling configuration (cross-connection between V5 ISDN PRA user port and V5 ISDN communication path(s) (packet, frame and signalling))	click on ***V5 ISDN UP Signalling...***. The *V5 ISDN BA User Port Signalling Configuration* window pops up (cf. Chapter 6.2.8.9, page 6-106).
delete the existing cross-connection between user port and V5.2 interface	click on ***Remove X-Connection***.

If you want to ...	then ...
modify the HDSL logical interface parameters	click on ***HDSL Logical Interface...***. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of V5 user port may be service affecting. Do you want to continue?`**
exit the window	click on the ***Close*** button.

6.2.8.7 V/G leased line user port

Overview

The *AnyMedia* NE supports two kinds of N64 DLL services: GLL, which comprises on n64 digital leased line services via a G.703 interface, and VLL, which supports a digital leased line service via a data interface which can be either V.35, V.36, or X.21. Note that for both services (VLL and GLL) the HDSL transmission system is implemented and has to be provisioned.

N64 DLL services are provided by connecting a number of bearer channels supplied by a GLL or VLL with the same number of timeslots of an E1 physical feeder located on an IO_E1 pack. The n64 digital leased line services have to be provisioned on top of a logical HDSL interface (note that the HDSL AP can be located in the mainshelf as well as in the subshelf). The number of timeslots depends on the type of the requested service and all of these timeslots need to be allocated (cross-connected) in the same leased line link.

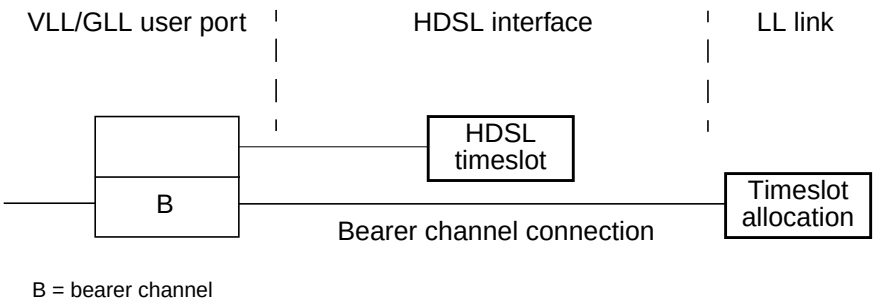


Figure 6-26 Functional model of VLL user port configuration

Note that the bearer channel entities associated to a VLL/GLL user port are automatically created/removed by the *AnyMedia* Access System when the VLL/GLL user port is created/removed. Note that the number of bearer channels created in ascending order will depend on the specified number of HDSL timeslots to be used and all of them must be cross-connected to timeslots of the same leased line link.

The *AnyMedia* Access System limitation on the number of n64 digital leased line user ports which can be created is given by the capacity of the feeder side with 16 links * 31 timeslots = 496 leased line timeslots to be used for bearer channel traffic (there is no restriction on the ONU side).

6.2.8.7.1 VLL User Port window

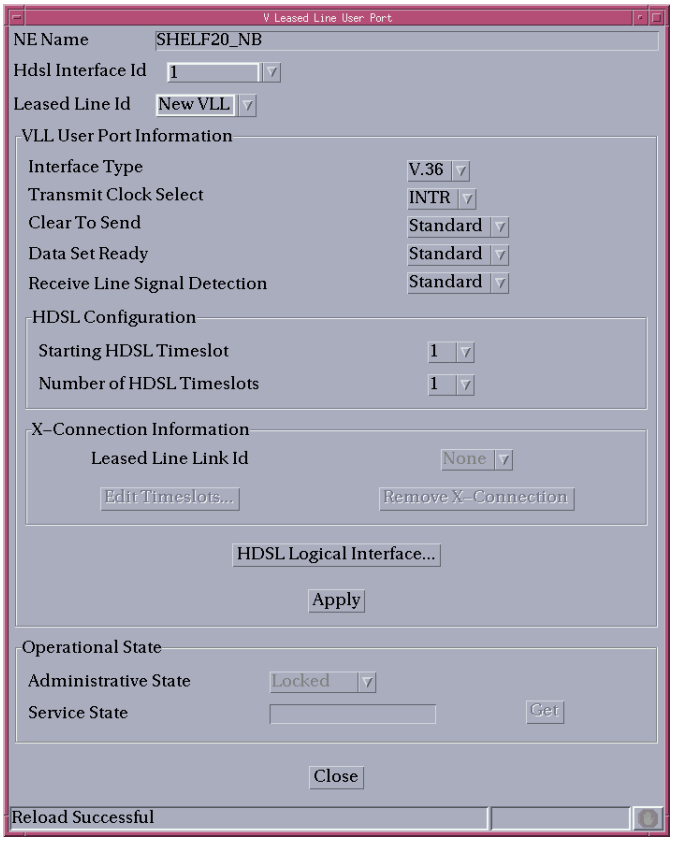


Figure 6-27 VLL User Port window

This window is used to add a new VLL user port or remove or modify an existing VLL user port.

It allows the operator to create/remove the cross-connection between a VLL user port and an LL interface as well as configure and modify VLL user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
HDSL Interface Id	This option menu displays the HDSL logical interface id associated to the VLL user port shown in this window. If the interface is already used by a VLL user port it is shown with a grey background, otherwise a white background is shown. Selecting a free interface activates add mode; selecting a used interface activates edit mode.
Leased Line Id	This option menu shows the VLLs in the HDSL interface and the value New VLL. Selecting New VLL activates add mode; selecting a used interface activates edit mode.
VLL User Port Information	**Interface Type**: This option menu lists the possible interface types. Possible values: V.35, V.36, X.21. Selection is possible only in add mode. **Transmit Clock Select:** This option menu is used to define the synchronization source of the transmit clock. Possible values: EXT, INTF, INTR. Modification is enabled only if the administrative state is "Locked". **Clear to Send**: This option menu can be used to define the method of generation of the CTS control signal. Possible values: ON, OFF, Standard. Only applicable for V.35 and V.36 interfaces. Modification is enabled only if the administrative state is "Locked". **Data Set Ready**: This option menu can be used to define the method of generation of the DSR control signal Possible values: ON, OFF, Standard. Only applicable for V.35 and V.36 interfaces. Modification is enabled only if the administrative state is "Locked". **Receive Line Signal Detection**: This option menu can be used to define the method of generation of the RLSD control signal Possible values: ON, OFF, Standard. Modification is enabled only if the administrative state is "Locked".

Parameters/ Buttons	Description
VLL User Port Information (continued)	**HDSL Configuration**: This field provides the HDSL configuration information. The option menus are enabled only if the administrative state is "Locked". ■ **Starting HDSL Timeslot**: This option menu can be used to select the starting timeslot on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. ■ **Number of HDSL Timeslots**: This option menu can be used to select the number of timeslots on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. **X-Connection Information**: This field provides the cross-connection information: ■ **Leased Line Link id**: This field displays the LL link interface id to which this user port is cross-connected. Possible values: None, {0, 16}. When coming from the *Leased Line Link* window via ***Add VLL*** this field is non-editable. In all the other cases an option menu with all LL link interface ids is offered for selection. ■ The ***Edit Timeslots...*** button provides access to the *Edit timeslots* window where you are able to create, change or remove cross-connection(s) between VLL user port and LL link timeslots. The button is enabled only if the VLL user port is created and cross-connected to the LL link interface identified in this window. ■ The ***Remove X-Connection*** button can be used to remove a VLL user port - LL link interface cross-connection. This button is enabled only if the administrative state is "Locked". The ***HDSL Logical Interface...*** button provides access to the *HDSL Logical Interface* window. The ***Apply*** button is used to confirm the changes in the **VLL User Port Information** field.

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the Secondary Service State Acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State** and the **Blocking Status**.

6.2.8.7.2 Add a VLL user port

Assumptions

For the following description it is assumed that

- the NE is connected
- the HDSL interface is already provisioned on the physical drop
- the HDSL logical interface service state must be OOS
- the HDSL logical interface supports VLL service and the specified HDSL logical timeslots are available
- the number of timeslots on the PCM highway provisioned for the HDSL AP concerned is not exceeded.

Procedure

Complete the following procedure to add a VLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **VLL User Port** and click on ***Add***. The *VLL User Port* window pops up (cf. Chapter 6.2.8.7.1, page 6-91). This window can also be reached from the *Leased Line Link* window (cf. Chapter 6.2.4, page 6-26) via ***Add VLL***.
3.	Use the option menu **HDSL Interface Id** to select a free interface.
4.	Use the option menu **Leased Line Id** to select **New VLL**.
5.	Use the option menu **Interface Type** to select the desired type.
6.	Edit all the other parameters of this window as described in Chapter 6.2.8.7.3, page 6-96 (Modify a VLL user port).
7.	Click on ***Apply*** to confirm.
8.	Click on ***Close*** to exit the window.

6.2.8.7.3 Modify a VLL user port

Procedure Complete the following procedure to modify a VLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Port...*** The *VLL User Port* window pops up (cf. Chapter 6.2.8.7.1, page 6-91). This window can also be reached from the *HDSL Logical Interface* window (cf. Chapter 6.2.7.2, page 6-41).
5.	Use the option menu **HDSL Interface Id** to select the desired interface.
6.	Use the option menu **Leased Line Id** to select a VLL.

If you want to ...	then ...
change the VLL user port HDSL configuration	use the option menus **Starting HDSL Timeslot** and **Number of HDSL** in the **HDSL Configuration** field to define the desired values and click on ***Apply***.
change the VLL user port service configuration	use the option menus **Clear to Send**, **Data Set Ready** and **Receive Line Signal Detection** in the **VLL User Port Service Configuration** field to set the corresponding values and click on ***Apply***.
add a cross-connection	use the option menu **Leased Line Link Id** in the field **X-Connection Information** to select the LL link interface id and click on ***Apply***.
modify the cross-connection between VLL user port and LL link timeslot	click on ***Edit Timeslots***. The *Edit Timeslots* window pops up (cf. Chapter 6.2.8.8, page 6-104).

If you want to ...	then ...
delete the existing cross-connection between VLL user port and LL link interface	select the desired LL link id and click on ***Remove X-Connection***.
modify the HDSL logical interface parameters	click on ***HDSL Logical Interface...***. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of VLL user port may be service affecting. Do you want to continue?`**
exit the window	click on the ***Close*** button.

6.2.8.7.4 GLL User Port window

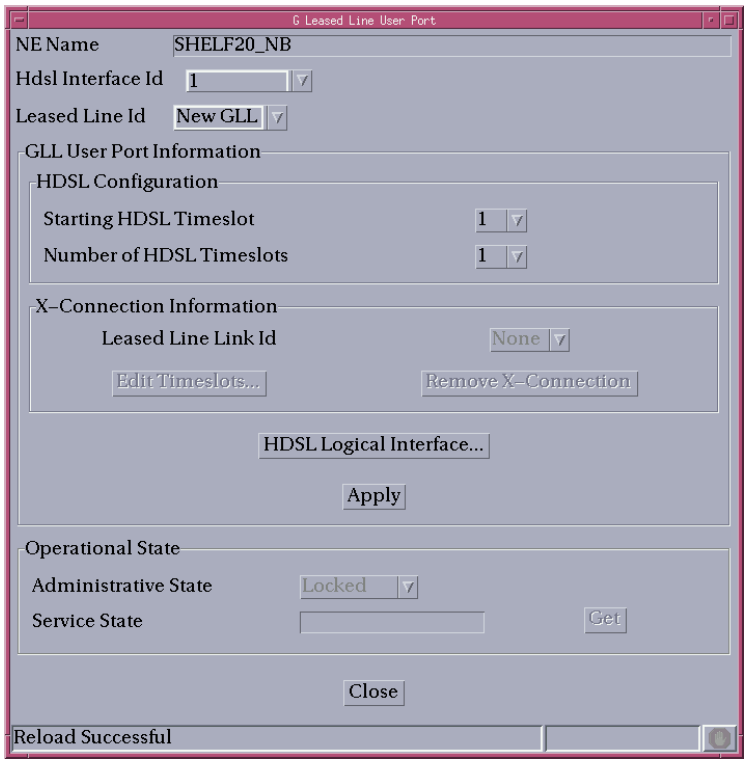


Figure 6-28 GLL User Port window

This window is used to add a new GLL user port, or remove or modify an existing VLL user port.

It allows the operator to create/remove the cross-connection between a GLL user port and an LL interface as well as configure and modify GLL user port service parameters.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
HDSL Interface Id	This option menu displays the HDSL logical interface id associated to the GLL user port shown in this window. If the interface is already used by a GLL user port it is shown with a grey background, otherwise a white background is shown. Selecting a free interface activates add mode; selecting a used interface activates edit mode.
Leased Line Id	This option menu shows the GLLs in the HDSL interface and the value New GLL. Selecting New GLL activates add mode; selecting a used interface activates edit mode.
GLL User Port Information	**HDSL Configuration**: This field provides the HDSL configuration information: ■ **Starting HDSL Timeslot**: This option menu can be used to select the starting timeslot on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. Modification is enabled only if the administrative state is "Locked". ■ **Number of HDSL Timeslots**: This option menu can be used to select the number of timeslots on the HDSL interface. Possible values: cf. Table 6-1, page 6-45. Modification is enabled only if the administrative state is "Locked". **X-Connection Information**: This field provides the cross-connection information: ■ **Leased Line Link id**: This field displays the LL link interface id to which this user port is cross-connected. Possible values: None, {0, 16}. When coming from the *Leased Line Link* window via ***Add GLL*** this field is non-editable. In all the other cases an option menu with all LL link interface ids is offered for selection.

Parameters/ Buttons	Description
GLL UserPort Information (continued)	■ The ***Edit Timeslots...*** button provides access to the *Edit timeslots* window where you are able to create, change or remove cross-connection(s) between GLL user port and LL link timeslots. The button is enabled only if the GLL user port is created and cross-connected to the LL link interface identified in this window. ■ The ***Remove X-Connection*** button can be used to remove a GLL user port - LL link interface cross-connection. This button is enabled only if the administrative state is "Locked". The ***HDSL Logical Interface...*** button provides access to the *HDSL Logical Interface* window. The ***Apply*** button is used to confirm the changes in the **VLL Userport Information** field.
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked, Unlocked. The field **Service State** shows the current operational state obtained (on demand) by the user. Possible values: Enabled, Disabled + the secondary service state acronym (OP.-State - Sec. Serv. State). The ***Get*** button is used to update the display of the **Operational State** an the **Blocking Status**.

6.2.8.7.5 Add a GLL user port

Assumptions

For the following description it is assumed that

- the NE is connected
- the HDSL interface is already provisioned on the physical drop
- the HDSL logical interface service state must be OOS
- the HDSL logical interface supports GLL service and the specified HDSL logical timeslots are available
- the number of timeslots on the PCM highway provisioned for the HDSL AP concerned is not exceeded.

Procedure

Complete the following procedure to add a GLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the option menu beside the ***Add*** button to select **GLL User Port** and click on ***Add***. The *GLL User Port* window pops up (cf. Chapter 6.2.8.7.4, page 6-98). This window can also be reached from the *Leased Line Link* window (cf. Chapter 6.2.4, page 6-26) via ***Add GLL***.
3.	Use the option menu **HDSL Interface Id** to select a free interface.
4.	Use the option menu **Leased Line Id** to select **New VLL**.
5.	Edit all the other parameters of this window as described in Chapter 6.2.8.7.6, page 6-102 (Modify a GLL user port).
6.	Click on ***Apply*** to confirm.
7.	Click on ***Close*** to exit the window.

6.2.8.7.6 Modify a GLL user port

Procedure Complete the following procedure to modify a GLL user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48). This window can also be reached from the *V5.2 Interface* window (cf. Chapter 6.2.1.2, page 6-11) by clicking on ***V5 User Ports...***.
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Port...***. The *GLL User Port* window pops up (cf. Chapter 6.2.8.7.4, page 6-98). This window can also be reached from the *HDSL Logical Interface* window (cf. Chapter 6.2.7.2, page 6-41).
5.	Use the option menu **HDSL Interface Id** to select the desired interface.
6.	Use the option menu **Leased Line Id** to select a GLL.

If you want to ...	then ...
change the GLL user port HDSL configuration	use the option menus **Starting HDSL Timeslot** and **Number of HDSL** in the **GLL User Port Configuration** field to define the desired values and click on ***Apply***.
add a cross-connection	use the option menu **Leased Line Link Id** in the field **X-Connection Information** to select the LL link interface id and click on ***Apply***.
modify the cross-connection between GLL user port and LL link timeslot	click on ***Edit Timeslots***. The *Edit Timeslots* window pops up (cf. Chapter 6.2.8.8, page 6-104).
delete the existing cross-connection between GLL user port and LL link interface	select the desired LL link id and click on ***Remove X-Connection***.

If you want to ...	then ...
modify the HDSL logical interface parameters	click on ***HDSL Logical Interface...***. The *HDSL Logical Interface* window pops up (cf. Chapter 6.2.7.2, page 6-41).
change the administrative state	use the corresponding option menu in the field **Operational State**. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **`Changing the administrative state of VLL user port may be service affecting. Do you want to continue?`**
exit the window	click on the ***Close*** button.

6.2.8.8 Edit Timeslots window

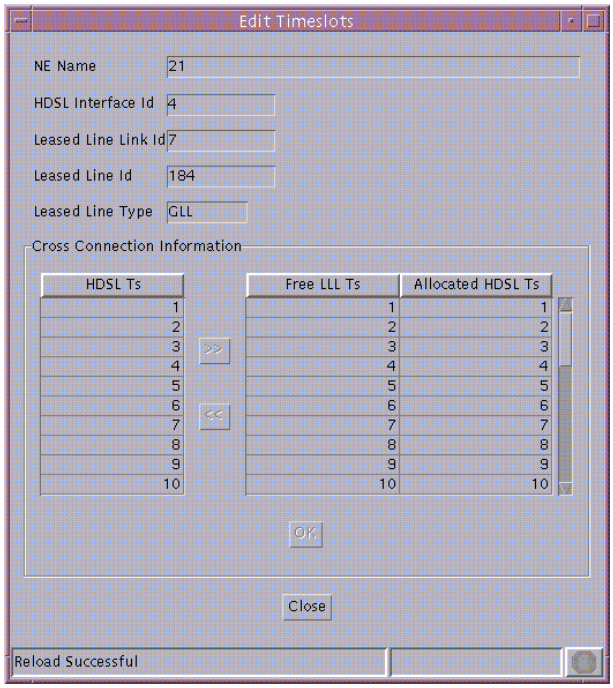


Figure 6-29 Edit Timeslots window

This window displays the cross-connection timeslot information of both HDSL timeslots and leased line link timeslots. It is used to add/remove cross-connections between GLL/VLL user port and LL link timeslot.

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
HDSL Interface Id	This field shows the HDSL logical interface id of the leased line.
Leased Line Link Id	This field shows the leased line link id which is cross-connected to the leased line.
Leased Line Id	This field displays the leased line id which is cross-connected to the leased line link.
Leased Line Type	This text field shows the leased line type: VLL or GLL.

Parameters/ Buttons	Description
Cross Connection Information	**HDSL Ts**: This list shows all the timeslots of the HDSL logical interface used by the selected leased line. The **>> (Add)** button can be used to move the selected HDSL timeslot into the **LLL Timeslots** table (see below). The background of the selected list entry changes from white to grey. The LLL timeslots need not to be selected in consecutive order but always in ascending order. The **<< (Remove)** button can be used to de-allocate the HDSL timeslots from the **LLL Timeslots** table and to move it back to the **HDSL Timeslots** list. **LLL Timeslots**: This table contains the leased line link timeslots and the already allocated HDSL timeslots for this leased line. The table consists of two columns: ■ **Free LLL Ts** and **Allocated HDSL Ts.** The ***Ok*** button is used to confirm the changes.

6.2.8.8.1 Add/remove cross-connection between GLL/VLL user port and LL link timeslot

Procedure

The corresponding window (*Edit Timeslots*) can be reached from the *Leased Line Link* window (cf. Chapter 6.2.4, page 6-26), *VLL User Port* window (cf. Chapter 6.2.8.7.1, page 6-91) or the *GLL User Port* window (cf. Chapter 6.2.8.7.4, page 6-98).

If you want to ...	then ...
add a cross-connection	select a timeslot in the list **HDSL Ts,** click on **>>** to move the selected timeslot into the **LLL Timeslots** table and press ***Ok*** to confirm.
remove a cross-connection	select an already allocated timeslot in the list **LLL Timeslots,** click on **<<** to move the timeslot into the **HDSL Timeslots** table and press ***Ok*** to confirm.
exit the window without changes	click on the ***Close*** button.

6.2.8.9 V5 ISDN User Port Signalling Configuration window

This window is used to configure the V5 ISDN BA/PRA user port signalling data. It allows the creating, changing or removing of cross-connection(s) between V5 ISDN BA/PRA user port and V5 ISDN communication path(s) (packet, frame and data signalling).

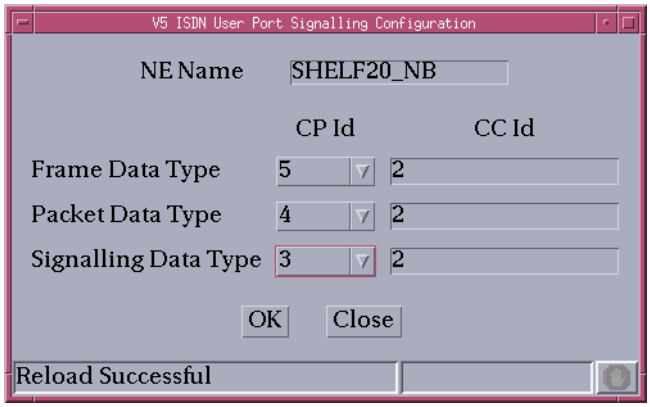


Figure 6-30 V5 ISDN User Port Signalling Configuration window

This window displays the V5 communication path ids (frame, packet and signalling) associated to the V5 ISDN BA/PRA user port.

Parameters/ Buttons	Description
Frame Data Type (f)-CP id	This option menu shows the frame communication paths (CPs) present in the V5 interface to which the user port is cross-connected. If no CP is cross-connected "null" value is displayed in this field. This option menu is available only when the selected V5 interface id (*V5 ISDN BA User Port* window - cf. Chapter 6.2.8.5.1, page 6-75 or *V5 ISDN PRA User Port* window - cf. Chapter 6.2.8.6.1, page 6-84) identifies a V5 interface which contains V5 CPs of frame type (f) already configured. Possible values: {0, 9} for V5.1, {0, 145} for V5.2.
CC Id	This non-editable text field shows the communication channel (CC) id, if the selected CP (f) is already cross-connected to a CC. Possible values: {1, 3} for V5.1, {0, 65503} for V5.2.

Parameters/ Buttons	Description
Packet Data Type (p)-CP id	This option menu shows the packet communication paths (CPs) present in the V5 interface to which the user port is cross-connected. If no CP is cross-connected "null" value is displayed in this field. This option menu is available only when the selected V5 interface id (*V5 ISDN BA User Port* window - cf. Chapter 6.2.8.5.1, page 6-75 or *V5 ISDN PRA User Port* window - cf. Chapter 6.2.8.6.1, page 6-84) identifies a V5 interface which contains V5 CPs of frame type (p) already configured. Possible values: {0, 9} for V5.1, {0, 145} for V5.2.
CC Id	This non-editable text field shows the communication channel (CC) id, if the selected CP (p) is already cross-connected to a CC. Possible values: {1, 3} for V5.1, {0, 65503} for V5.2.
Signalling Data Type (Ds)-CP id	This option menu shows the signalling communication paths (CPs) present in the V5 interface to which the user port is cross-connected. If no CP is cross-connected "null" value is displayed in this field. This option menu is available only when the selected V5 interface id (*V5 ISDN BA User Port* window - cf. Chapter 6.2.8.5.1, page 6-75 or *V5 ISDN PRA User Port* window - cf. Chapter 6.2.8.6.1, page 6-84) identifies a V5 interface which contains V5 CPs of frame type (Ds) already configured. Possible values: {0, 9} for V5.1, {0, 145} for V5.2.
CC Id	This non-editable text field shows the communication channel (CC) id, if the selected CP (Ds) is already cross-connected to a CC. Possible values: {1, 3} for V5.1, {0, 65503} for V5.2.
OK	This button is used to confirm the changes.

6.2.8.9.1 Modify the V5 user port signalling data

Procedure

The corresponding window (*V5 ISDN User Port Signalling Configuration*) can be reached from the *V5 ISDN BA User Port* window (cf. Chapter 6.2.8.5.1, page 6-75) or the *V5 ISDN PRA User Port* window (cf. Chapter 6.2.8.6.1, page 6-84).

If you want to ...	**then ...**
add a cross-connection	use the option menu(s) **CP Id** to select a CP and click on ***OK***.
change a cross-connection	use the option menu(s) **CP Id** to select another CP and click on ***OK***.
remove a cross-connection	use the option menu(s) **CP Id** to select 0 and click on ***OK***.
exit the window without changes	click on the ***Close*** button.

6.2.8.10 V5 Signalling window

Overview

This window displays the signalling structure of a V5 interface. It shows the communication channel timeslots (TSs), the communication channels (CCs), communication paths (CPs), links between TS and CC and links between CP and CC. It allows creation, edition and deletion of these.

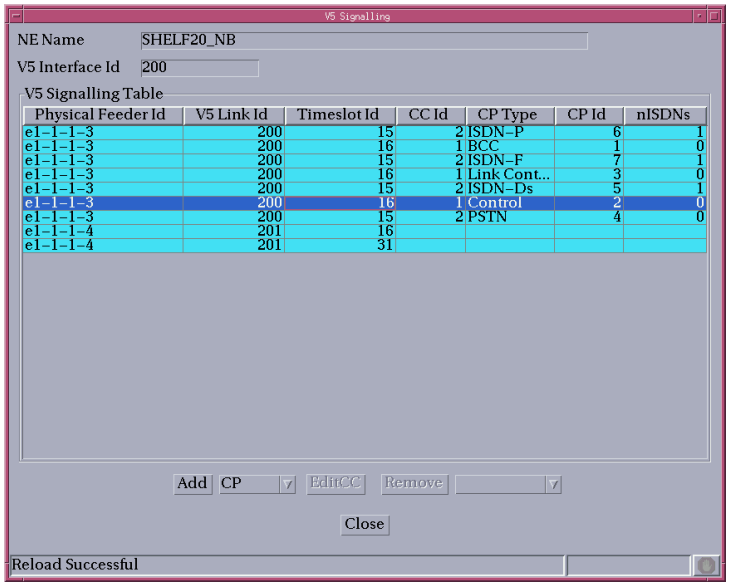
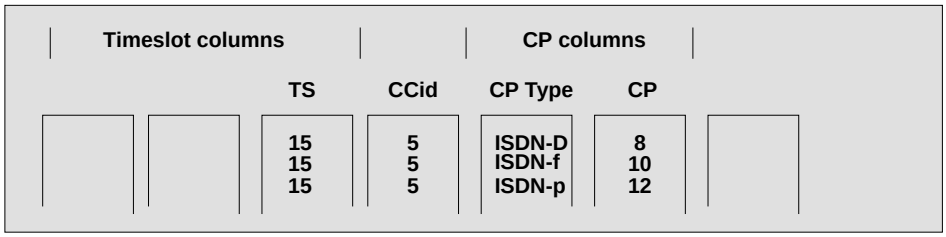


Figure 6-31 V5 Signalling window

V5 signalling table

The V5 Signalling table consists of 4 fields: Timeslot columns, CC id, CP columns and Number of ISDNs.

Several lines can share a TS and CC, as several CPs can be linked to the same CC (e.g. see below).



Absence of an entry (TS, CC or CP) indicates that the link between this entry and the non-absent item does not exist yet. In these cases the ***Add...*** buttons can be used to establish the desired links.

Each line can be selected separately. Selecting any CP line also selects the related CC and TS fields (if available). Operations allowed on a selection are the delete operations, according to the criteria listed below.

Protected items

The protected items are also displayed (V5.2 group 2 protection). A row that is subject to protection is marked visibly (e.g. different background colour or different text colour), as not all editing operations can be performed on it. The operations that are not available on these rows are: Remove CC-TS and Add CC-TS. Protections are set and removed from the protection window (cf. Chapter 6.2.8.11, page 6-124).

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Timeslot columns	This column defines a single timeslot in the V5 interface. The shown timeslot associated to a V5 CC is the current cross-connection and does not correspond with the configured one in the event of a protection switch. **Physical Feeder Id**: This column contains the physical feeder that carries the concerned timeslot. **V5 Link id**: This column contains the V5 link id of the link that is concerned. **Timeslot Id**: This column contains the timeslot number that corresponds to the concerned timeslot. Possible values: 15, 16, 31 (only C-type CCs).
Communication Channel (CC Id)	The entry in this column identifies the communication channel.
CP columns	**CP Type**: This column specifies the type of communication path that is concerned. Possible values: Control, Link control (only for V5.2), BCC (only for V5.2), PSTN, ISDN - p, ISDN - f, ISDN - Ds. **CP Id**: This column specifies an identifier that determines the communication path in a unique way inside the V5 interface. It is constructed by taking the CP id, and stripping all except the last number. Possible values: {1, 145}.
Number of ISDNs	This column specifies, for ISDN communication paths, the number of ISDN user ports that are cross-connected to it. It is used only as reference so the user can estimate the importance and traffic on that CP.

Parameters/ Buttons	Description
Command Buttons	The command buttons are only available when the administrative state of the selected V5 interface is "Locked". The ***Add...*** button provides access to the following windows dependent on the selected entry in the **V5 Signalling Table**: *Add Timeslot, Add Communication Channel, Add Communication Path, Add Communication Channel with Timeslot, Add Communication Path with Communication Channel*. ⇛ NOTE: For *Add Timeslot*: The chosen timeslot is not created, but changed to C-channel. *Add Communication Channel* and *Add Communication Path with Communication Channel* is always possible regardless of the administrative state of the V5 interface. *Add Communication Channel with Timeslot* is not possible for protected items. When the called window is closed the *V5 Signalling* window will be updated with the changes made. The ***Edit CC...*** button provides access to the *Edit Communication Channel* window (enabled only for V5.2). The button is available when the selected row contains only a TS. When the called window is closed the *V5 Signalling* window will be updated with the changes made. The label button ***Remove...*** can be used to delete a TS, a CC, a CP, a CC-TS cross-connection or a CP-CC cross-connection depending on the selected entry in the **V5 Signalling Table**:

Parameters/ Buttons	Description
Command Buttons (continued)	■ ***Remove TS***, ***Remove CC***, ***Remove CP***: The button is available only, if the selected row contains just a TS, CC or CP. NOTE: This button is disabled if the selected TS belongs to a protection group. ISDN CPs can only be deleted if there are no user ports linked to them. These must be deleted from the user port windows. A TS is never really removed, but marked as B-channel (C-channel -> B-channel). ■ ***Remove CC-TS***: The button is available only if the selected row contains both CC and TS. After removing the cross-connection the row is split in two, one column for TS without CC and one for CC without TS. NOTE: This button is disabled if the selected TS belongs to a protection group. ■ ***Remove CP-CC***: The button is available only if the selected row contains both CP and CC. After removing the cross-connection the row is split in two, one column for CP without CC and one for CC without CP.

NOTE:
This window displays all CPs, CCs and TSs as well as those used for the primary and secondary link. The available operations (in the subordinate windows) cannot fully reconstruct a full signalling system from scratch, only the ISDN and PSTN signalling is intended to be managed from this window. The primary and secondary feeder configuration are managed from the primary and secondary feeder fields in the *V5.2 Interface* window, tab V5 Link Data (cf. Chapter 6.2.1.2.2, page 6-14).

6.2.8.10.1 Using the V5 Signalling window

Procedure

The *V5 Signalling* window is reached from the *V5.x Interface* window (cf. Chapter 6.2.1.2, page 6-11).

If you want to ...	then ...
add a timeslot	select a row without TS and click on ***Add TS***. The *Add Timeslot* window pops up (cf. Chapter 6.2.8.10.2, page 6-114).
add a communication channel	select a row without CC and click on ***Add CC***. The *Add Communication Channel* window pops up (cf. Chapter 6.2.8.10.4, page 6-116).
add a communication path	select a row without CP and click on ***Add CP***. The *Add Communication Path* window pops up (cf. Chapter 6.2.8.10.6, page 6-118).
add a cross-connection between CC and TS	select the CC and TS to be cross-connected and click on ***Add CC-TS***. The *Add Communication Channel with Timeslot* window pops up (cf. Chapter 6.2.8.10.8, page 6-120).
add a cross-connection between CP and CC	select the CP and CC to be cross-connected and click on ***Add CP-CC***. The *Add Communication Path with Communication Channel* window pops up (cf. Chapter 6.2.8.10.10, page 6-122).
edit a communication channel	select a row which contains only a TS and click on ***Edit CC...***. The *Edit Communication Channel* window pops up (cf. Chapter 6.2.8.10.12, page 6-124).
remove a timeslot, a communication channel or a communication path	select a timeslot, a communication channel or a communication path and click on ***Remove***.
remove a cross-connection between CC and TS	select the corresponding row and click on ***Remove CC-TS***.
remove a cross-connection between CP and CC	select the corresponding row and click on ***Remove CP-CC***.
exit the window	click on ***Close***.

6.2.8.10.2 Add Timeslot window

This window is used to allocate a timeslot, linked to the V5 interface, to the set of CC timeslots.

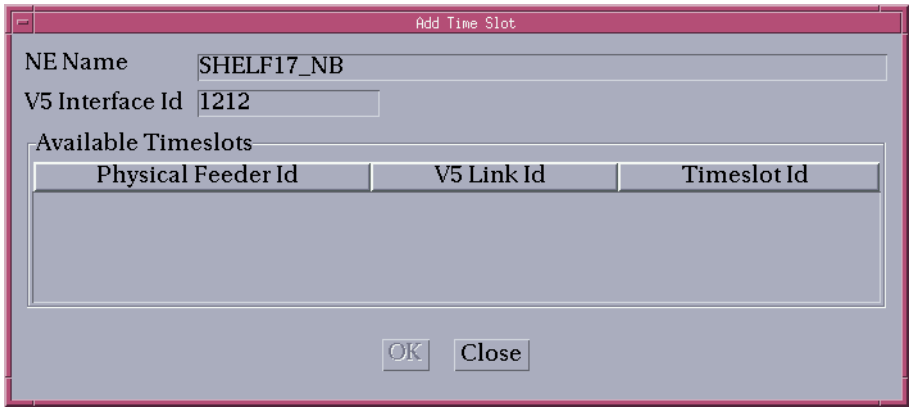


Figure 6-32 Add Timeslot window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Available Timeslots	The scrolling list contains the identification of available timeslots for addition to the C-channel list. The list contains only those timeslots that are currently B-channels. Candidate timeslots are limited to timeslots 15, 16 and 31 of each linked feeder. A single row of this list can be selected. **Physical Feeder Id**: This column indicates the physical feeder a timeslot belongs to. **V5 Link Id**: This column contains the V5 link id of the physical feeder. **Timeslot Id**: This column shows the number of the timeslots within this feeder.
OK	This button is used to allocate a timeslot. The button is enabled only when a timeslot is selected.

6.2.8.10.3 Add a timeslot

The *Add Timeslot* window can be reached only via ***Add TS*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to add a timeslot.

Step	Procedure
1.	Select a row in the **Available Timeslots** list.
2.	Click on ***OK***. The timeslot will be modified to become a C-channel.
3.	Click on ***Close*** to exit the window.

6.2.8.10.4 Add Communication Channel window

This window is used to create a CC. When creating a CC it is also possible to cross-connect it to a timeslot (optional).

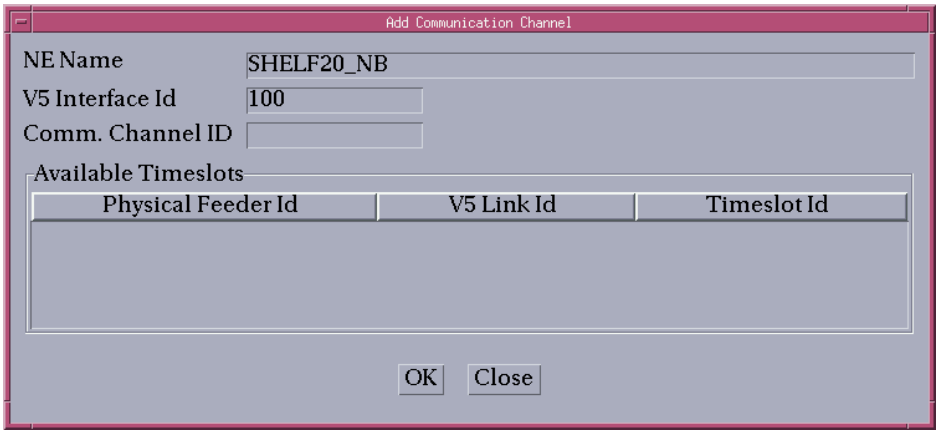


Figure 6-33 Add Communication Channel window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Communication Channel Id	This field is used to enter the id of the CC that is to be created. This value is only taken into account for V5.2. Possible values: {0, 65503}.
Available Timeslots	This scrolling list contains the C-channel timeslots that are not in protection mode, and have no CC linked yet and the value None. **Physical Feeder Id**: Displays the physical feeder a timeslot belongs to. **V5 Link id**: Displays the V5 Link id associated to the feeder shown in the previous field. **Timeslot Id**: Displays the CC timeslots that are not in protection mode and have no CC linked yet. Possible values: None, 15, 16, 31.
OK	This button is used to create a CC with the given id. It is only enabled when a CC id is specified.

6.2.8.10.5 Add a communication channel

The *Add Communication Channel* window can be reached only via ***Add CC*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to add a communication channel.

Step	Procedure
1.	Enter an appropriate **CC id** (only for V5.2).
2.	Select a row in the **Available Timeslots** list.
3.	Click on ***OK*** to add a CC. If this is successful and a timeslot is specified the new CC will be cross-connected to that timeslot.
4.	Click on ***Close*** to exit the window.

6.2.8.10.6 Add Communication Path window

This window is used to create a CP. When creating a CP it is also possible to cross-connect it to a CC (optional).

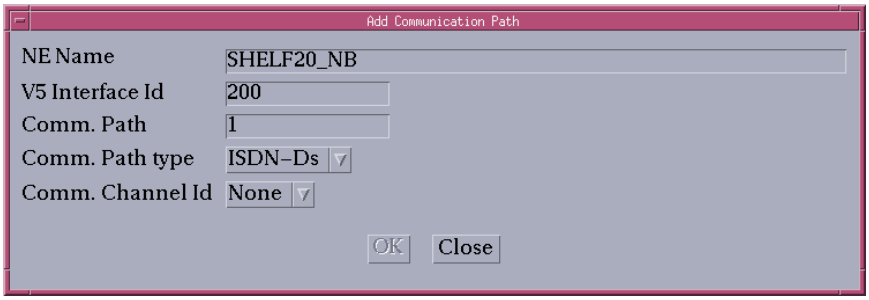


Figure 6-34 Add Communication Path window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Communication Path	This field is used to enter the identification number of the CP that to be created. Possible values: {1, 9} for V5.1, {1, 145} for V5.2.
Communication Path Type	This option menu contains the possible types of CP. Possible values: PSTN, ISDN-Ds, ISDN-p, ISDN-f. NOTE: *Control*, *Link control* and *BCC* communication paths are automatically created when a V5 interface is created (cf. Chapter 6.2.1, page 6-9).
Communication Channel Id	This option menu contains the communication channels that are already created and the value None. Possible values: None, {0, 65503}.
OK	This button is used to create a CP of the specified type with the given id. The button is enabled only when the identification number is specified.

6.2.8.10.7 Add a communication path

The *Add Communication Path* window can be reached only via ***Add CP*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to add a communication path.

Step	Procedure
1.	Use the option menu **Communication Path Type** to select an appropriate CP type.
2.	Enter the **CP Id**.
3.	Optionally: Use the option menu **Communication Channel id** to select a CC id.
4.	Click on ***OK*** to add a CP. If this is successful and a CC is specified the new CP is cross-connected to that CC, if there is not yet a CP of that type cross-connected.
5.	Click on ***Close*** to exit the window.

6.2.8.10.8 Crossconnect Communication Channel with Timeslot window

This window is used to create a cross-connection between a CC and a timeslot.

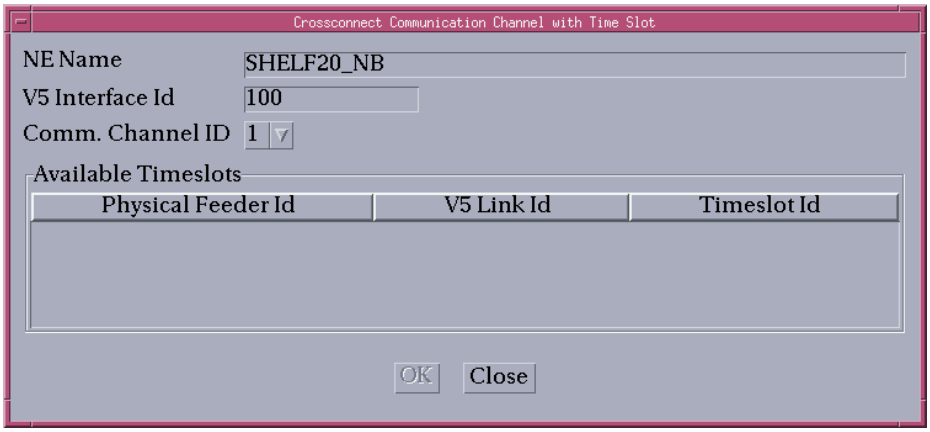


Figure 6-35 Crossconnect Communication Channel with Time Slot window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Communication Channel Id	This option menu contains the list of all CCs that are not yet cross-connected to a timeslot and the value None (not available CC).
Available Timeslots	**Physical Feeder Id**: Displays the physical feeder a timeslot belongs to. **V5 Link id**: Displays the V5 Link id associated to the feeder shown in the previous field. **Timeslot**: IdDisplays the CC timeslots that are not in protection mode and have no CC linked yet. Possible values: None, 15, 16, 31.
OK	This button is used to cross-connect the CC to the timeslot (if there is no other timeslot of the same type linked to that CC). This button is enabled only when both previous data entries have been specified.

6.2.8.10.9 Add a cross-connection between CC and TS

The *Crossconnect Communication Channel to Timeslot* window can be reached only via ***Add CC-TS*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to add a cross-connection between a communication channel and a timeslot.

Step	Procedure
1.	Use the option menu **Communication Channel Id** to select an appropriate CC.
2.	Select a row in the **Available Timeslots** list.
3.	Click on ***OK*** to cross-connect the selected CC to the selected timeslot.
4.	Click on ***Close*** to exit the window.

6.2.8.10.10 Crossconnect CP with CC window

This window is used to create a cross-connection between a CP and a CC.

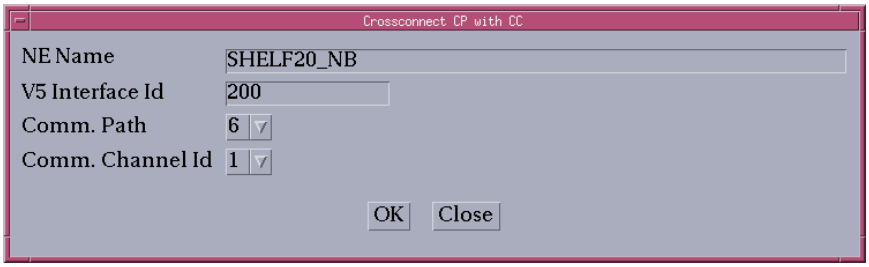


Figure 6-36 Crossconnect CP with CC window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format
Comm. Path	This option menu contains the list of all CPs that are not yet cross-connected to the CC and the value None (not available CP). Possible values:{1, 9} for V5.1 {1, 146} for V5.2.
Comm. Channel Id	This option menu contains all the CCs. Possible values: {0, 65503}.
OK	This button is used to cross-connect the CP to the CC if there is no other CP of the same type linked to that CC. This button is enabled only when both previous data entries have been specified.

6.2.8.10.11 Add a cross-connection between CC and CP

The *Crossconnect CP with CC* window can be reached only via ***Add CP-CC*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to add a cross-connection between a communication path and made communication channel.

Step	Procedure
1.	Use the option menu **Comm. Path** to select an appropriate CP.
2.	Use the option menu **Comm. Channel Id** to select an appropriate CC.
3.	Click on ***OK*** to cross-connect the selected CP to the selected CC.
4.	Click on ***Close*** to exit the window.

6.2.8.10.12 Edit Communication Channel window

This window is used to modify a CC id.

Figure 6-37 Edit Communication Channel window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Comm. Channel Id	This field is used to enter the new value for the CC. This value is only taken into account for V5.2. Possible values: {0, 65503}.
OK	This button is used to modify a CC to the given id. It is only enabled when a CC id is modified.

6.2.8.10.13 Edit a communication channel

The *Edit Communication Channel* window can be reached only via ***Edit CC*** from the *V5 Signalling* window (cf. Chapter 6.2.8.10, page 6-109).

Procedure

Complete the following procedure to modify a communication channel.

Step	Procedure
1.	Enter a new **Comm. Channel id**.
2.	Click on ***OK*** to confirm.
3.	Click on ***Close*** to exit the window.

6.2.8.11 V5.2 group 2 protection

Protection Groups

A protection group is used for defining a protection switching relationship where one or more standby timeslots provide protection for one or more working communication channels. The working (protected) channels and the standby (protecting)

ones have to be provisioned. If a working timeslot, carrying a protected communication channel, becomes faulty a protection switch takes place. In this case a standby timeslot is selected for replacing the faulty one. If the faulty timeslot becomes operational again, it will be added to the protection group as a standby timeslot (non-revertible switch). After recovering the V5.2 interface, its initial provisioned configuration is re-established by the NE.

A V5.2 interface supports two protection groups:

- Protection group 1
  which can only have one working communication channel and only one standby timeslot associated. Protection group 1 is automatically created if primary and secondary link are configured.
- Protection group 2
  which can have up to 43 working communication channels protected and up to three standby timeslots. Protection group 2 is automatically created if a protection or protection unit related to group 2 is created.

Protection group 1 is handled via the *Primary Link* window (cf. Chapter 6.2.6.1, page 6-35) and *Secondary Link* window (cf. Chapter 6.2.6.3, page 6-37).

The following section describes the handling of protection group 2.

6.2.8.11.1 V5.2 Group 2 Protection window

This window is used to create/show/remove the V5.2 group 2 protection structure of a V5.2 interface. It shows the communication channel timeslots (TSs) as well as the current CC and the configured CC. The main part is a table. Each row in the table presents a protection unit, with its timeslot.

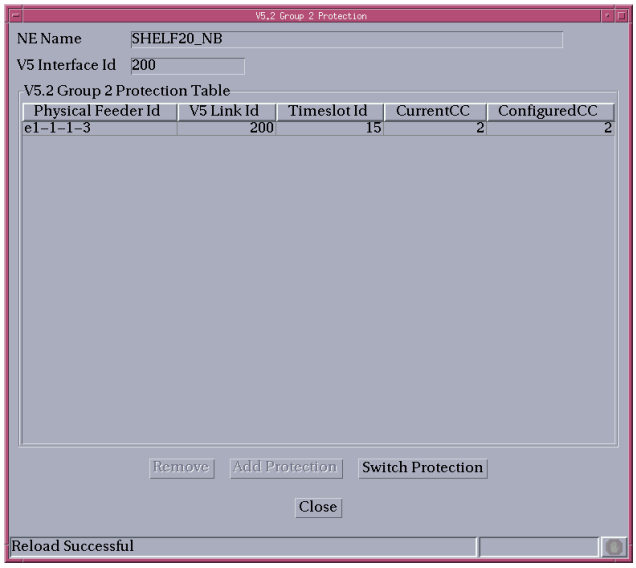


Figure 6-38 V5.2 Group 2 Protection window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
V5.2 Group 2 Protection Table	This table contains the V5.2 Group 2 Protection structure for the selected V5 interface. Each line contains a timeslot, current CC and configured CC field. Each line can be selected separately. The operation that applies to a selected row is the remove operation (see below). Operations are possible only if the administrative state of the V5 interface is "Locked". In this case the **Current CC (see below)** displays no value, as it is not applicable. It only represents relevant data when the interface is running. **Timeslot columns:** ■ **Physical Feeder Id**: This column contains the physical feeder that carries the concerned timeslot. ■ **V5 Link id**: This column contains the V5 Link id of the link that is concerned. ■ **Timeslot Id**: This column contains the timeslot number that corresponds to the concerned timeslot. Possible values: 15, 16, 31.

Parameters/ Buttons	Description
V5.2 Group 2 Protection Table (continued)	**Current CC**: This column identifies the communication channel via its CC id carried on this timeslot at this time. Only valid when the V5 interface is "Unlocked". **Configured CC**: This column defines the CC id of the communication channel that is carried on this timeslot on start-up of the interface.
Command buttons	***Add Protection***: This button provides access to the *Add V5.2 Group 2 Protection* window (cf. Chapter 6.2.8.11.3, page 6-128). This button is only available when the V5 interface is "Locked". ***Remove***: This button is only enabled when a row in the table is selected and the V5 interface is "Locked". If the selected row contains a timeslot and a configured CC, the result is that the CC remains configured over that timeslot, but is no longer protected. If the selected row contains no configured CC, the timeslot is no longer available for protection. ***Switch Protection***: This button provides access to the *Switch V5.2 Group 2 Protection* window (cf. Chapter 6.2.8.11.5, page 6-130). This button is only available when the V5 interface is "Unlocked".

6.2.8.11.2 Modify V5.2 group 2 protections

The *V5.2 Group 2 Protection* window can be reached only from the *V5.2 Interface* window (cf. Chapter 6.2.1.2.1, page 6-11) via ***Protection...***.

Procedure

Complete the following procedure to modify the V5.2 group 2 protection:

If you want to ...	then ...
add a group 2 protection	click on ***Add Protection***. The *Add V5.2 Group 2 Protection* window pops up (cf. Chapter 6.2.8.11.3, page 6-128).
make a protection switch for a communication channel	click on ***Switch Protection***. The *Switch V5.2 Group 2 Protection* window pops up (cf. Chapter 6.2.8.11.5, page 6-130).
remove (delete) an already defined protection structure	select the desired row in the **V5.2 Group 2 Protection Table** and click on ***Remove***.
exit the window	click on the ***Close*** button.

6.2.8.11.3 Add V5.2 Group 2 Protection window

This window is used to add either a timeslot (protecting) or communication channel (protected) to protection group 2 (i.e. to create a protection unit).

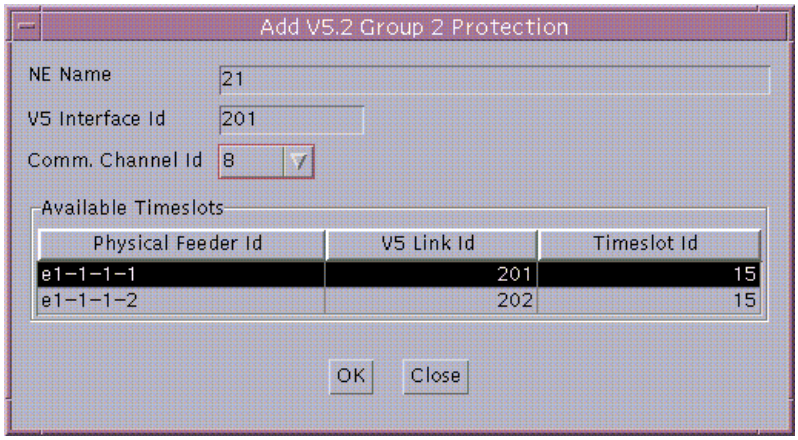


Figure 6-39 Add V5.2 Group 2 Protection window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Comm. Channel Id	This option menu contains the list of all CCs that are linked to a timeslot and not yet in the protection mode. When a value is selected, the corresponding timeslot is displayed in the timeslot field. The value "None" cannot be selected, but it can be obtained when a timeslot is selected that has no CC linked.
Available Timeslots	**Physical Feeder Id**: Displays the physical feeder a timeslot belongs to. **V5 Link id**: Displays the V5 Link id associated to the feeder shown in the previous field. **Timeslot Id**: Displays the timeslots within the feeder.

Parameters/ Buttons	Description
OK	This button is enabled when data entries have been selected in one of the above fields. If the selected value concerns a timeslot without CC, a protection unit is created for that timeslot which protects the other timeslots. If a timeslot is selected that carries a CC, a protection unit is defined for that timeslot and the CC is configured to it. That CC is then protected.

6.2.8.11.4 Add a V5.2 group 2 protection

The *Add V5.2 Group 2 Protection* window can be reached only from *V5.2 Group 2 Protection* window (cf. Chapter 6.2.8.11.1, page 6-125) via ***Add Protection***.

Procedure

Complete the following procedure to add a group 2 protection.

Step	Procedure
1.	Use the option menu **Comm. Channel id** to select an appropriate CC id.
2.	Select a row in the **Available Timeslots** list.
3.	Click on ***OK*** to create a group 2 protection.
4.	Click on ***Close*** to exit the window.

6.2.8.11.5 Switch V5.2 Group 2 Protection window

This window is used to switch timeslot/CC selection within protection group 2.

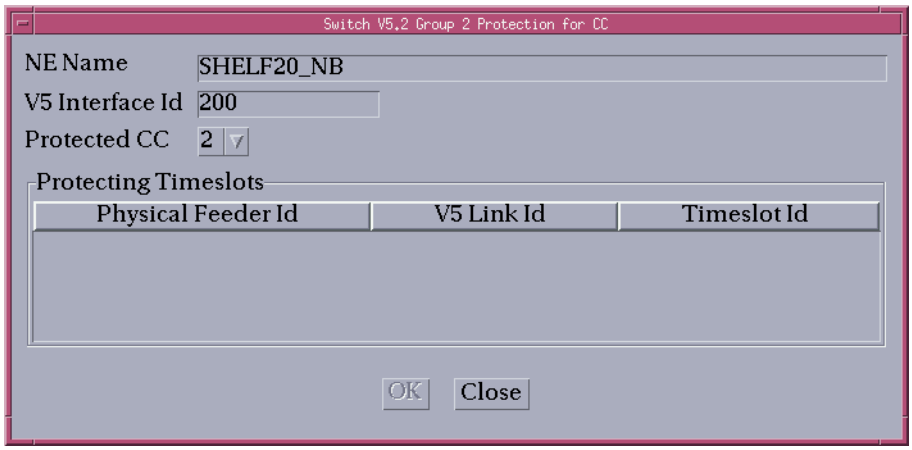


Figure 6-40 Switch V5.2 Group 2 Protection window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
V5 Interface Id	This field shows the id of the selected V5 interface. Possible values: {0, 16777215} in dec format or {0, FFFFFF} in hex format.
Protected CC	This option menu contains the list of all CCs that are in the V5.2 group 2 protection mode.
Protecting Timeslots	This option menu contains the timeslots that have no current CC and that are in protection group 2 of this V5.2 interface. **Physical Feeder Id**: Displays the physical feeder a timeslot belongs to. **V5 Link id**: Displays the V5 Link id associated to the feeder shown in the previous field. **Timeslot Id**: Displays the timeslots within this feeder.
OK	This button is enabled only when data entries have been selected in the above fields. The V5.2 group 2 protection switch of the selected CC to the selected timeslot is executed.

6.2.8.11.6 Switch a V5.2 group 2 protection

The *Switch V5.2 Group 2 Protection* window can be reached only from the *V5.2 Group 2 Protection* window (cf. Chapter 6.2.8.11, page 6-124) via ***Switch Protection***.

Procedure

Complete the following procedure to execute a protection switch:

Step	Procedure
1.	Use the option menu **Protected CC** to select an appropriate CC id.
2.	Select a row in the **Protection Timeslots** list.
3.	Click on ***OK***. The protection switch is executed.
4.	Click on ***Close*** to exit the window.

6.2.9 Move a V5 interface in service

Procedure Complete the following procedure to move a V5 interface in service:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the desired V5 interface in the V5 Interface List and click on ***Edit V5 Interface***. The *V5 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2, page 6-11).
3.	Use the option menu ***Administrative State*** to change this parameter from "Locked" to "Unlocked".
4.	Click on ***Close*** to exit the window.

6.2.10 Move a V5 link in service

Procedure Complete the following procedure to move a V5 link in service:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).
2.	Select an appropriate feeder (with an associated V5 link) in the list, use the option menu beside the ***Edit*** button to select V5 Link and click on ***Edit***. The *V5 Link* window pops up (cf. Chapter 6.2.5, page 6-30).
3.	Use the option menu ***Administrative State*** to change this parameter from "Locked" to "Unlocked".
4.	Click on ***Close*** to exit the window.

6.2.11 Move a V5 user port in service

Procedure Complete the following procedure to move a V5 user port in service:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **All V5 Userports** to define the list that will be displayed.

NOTE:
Do the following for all V5 user ports which should be moved in service.

3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Ports...***. The corresponding *V5 User Port* window pops up.
5.	Use the option menu ***Administrative State*** to change this parameter from "Locked" to "Unlocked".
6.	Click on ***Close*** to exit the window.

6.2.12 Move a ALL/DLL user port in service

Procedure Complete the following procedure to move an ALL/DLL user port in service:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Ports...***. The *ALL/DLL User Port* window pops up.
5.	Use the option menu ***Administrative State*** to change this parameter from "Locked" to "Unlocked".

6. Click on ***Close*** to exit the window.

6.2.13 Move a VLL/GLL user port in service

Procedure Complete the following procedure to move a VLL/GLL user port in service:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Edit User Ports...***. The *VLL/GLL User Port* window pops up.
5.	Use the option menu **HDSL Interface Id** to select the desired interface.
6.	Use the option menu **Leased Line Id** to select a VLL/GLL.
7.	Use the option menu ***Administrative State*** to change this parameter from "Locked" to "Unlocked".
8.	Click on ***Close*** to exit the window.

6.2.14 Delete a VLL/GLL user port

Procedure Complete the following procedure to delete a VLL/GLL user port:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Remove User Port...***. A warning window pops up: **Removing *VLL/GLL User Port* may be service affecting. Do you want to continue?**

If you decide to continue, the AEM will send a delete message to the NE:

- delete cross-connection between bearer channel and a leased line-timeslot.
- delete VLL/GLL.

6.2.15 Delete an ALL/DLL user port

Procedure Complete the following procedure to delete an ALL/DLL user port:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **All Leased Line Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List**.
4.	Click on ***Remove User Port...***. A warning window pops up: **Removing *ALL/DLL User Port* may be service affecting. Do you want to continue?** If you decide to continue, the AEM will send a delete message to the NE: ■ delete cross-connection between bearer channel and a leased line-timeslot. ■ delete ALL/DLL.

6.2.16 Delete a V5 user port

Procedure Complete the following procedure to delete a V5 user port.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> User Port*** via the cursor menu. The *User Port List* window pops up (cf. Chapter 6.2.8.1, page 6-48).
2.	Use the radio button **All Userports** or **V5 Userports** to define the list that will be displayed.
3.	Select the desired row in the **User Port List** and click on ***Remove User Port...***. A *Warning* message pops up:

Removing *V5 User Port* may be service affecting. Do you want to continue?

If you decide to continue, the AEM will send a delete message to the NE:

- delete cross-connection between bearer channel and a V5 timeslot (for V5.1 protocol).
- delete cross-connection between V5 user port and V5 interface.

6.2.17 Delete a V5 link

Procedure Complete the following procedure to delete a V5 link.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3, page 6-24).

2. Select the desired V5 link id and click on ***Remove***. A *Warning* message pops up:

   Removing *V5 Link id* may be service affecting. Do you want to continue?

   If you decide to continue, the AEM will send a delete message to the NE:

   - delete cross-connection between V5 communication channels and V5 protection group (V5.2).
   - delete cross-connection between V5 communication channels and V5 timeslot (V5.2).
   - delete cross-connection between V5 protection group and V5 link's timeslots (V5.2).
   - delete cross-connection between V5 link and V5 interface (V5.2).
   - delete cross-connection between V5 communication channels and V5 link's timeslots (V5.1).
   - delete cross-connection between V5 user port bearer channels and V5 link's timeslots (V5.1).
   - delete cross-connection between V5 communication path (control) and V5 communication channel (basic) (V5.1).
   - delete V5 communication path (control), if provisioned (V5.1).
   - delete V5 communication channel (basic), if provisioned and not cross-connected to any other V5 communication path (V5.1).
   - delete cross-connection between V5 link and V5 interface (V5.1).

6.2.18 Remove a communication channel

Procedure Complete the following procedure to remove a communication channel.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
1.	Select the desired V5.1 interface in the V5 Interface List and click on ***Edit V5 Interface***. The *V5.1 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2.1, page 6-11).
2.	Click on ***Signalling...***. The *V5 Signalling* window pops up
3.	Select the CC to be deleted and click on ***Remove***. The AEM will send a delete message to the NE: ■ delete cross-connection between V5 communication channel and a V5 timeslot. ■ delete cross-connection between V5 communication path and V5 communication channel.

6.2.19 Remove a communication path

Procedure Complete the following procedure to remove a communication path.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu, select the desired **V5 Interface id** in the *V5 Interfaces List* window and click on ***Edit V5 Interface...***. The *V5.x Interface* window pops up.
2.	Click on ***Signalling...***. The *V5 Signalling* window pops up
3.	Select a CP to be deleted in the list and click on ***Remove***. The AEM will send a delete message to the NE: ■ delete cross-connection between V5 communication path and V5 communication channel.

6.2.20 Remove a primary link

NOTE:
A secondary link has to be removed (cf. Chapter 6.2.21, page 6-139) before a primary link can be removed.

Procedure

Complete the following procedure to remove a primary link.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the desired V5.2 interface in the V5 Interface List and click on ***Edit V5 Interface***. The *V5.2 Interface* window (tab V5 Interface Data) pops up.
3.	Select tab V5 Link Data.
4.	Click on ***Remove***in the **Primary Link** field to remove the primary link. After removing the primary link all automatically created entities are automatically removed: ■ cross-connection between V5 protection group 1 and V5 communication channel. ■ cross-connection between V5 communication channel (basic) and V5 primary link's timeslot 16. ■ cross-connection between V5 communication path (control) and V5 communication channel. ■ V5 communication path (control), if it is provisioned. ■ cross-connection between V5 communication path (link control) and V5 communication channel. ■ V5 communication path (link control), if it is provisioned. ■ cross-connection between V5 communication path (BCC) and V5 communication channel. ■ V5 communication path (BCC), if it is provisioned. ■ cross-connection between V5 communication path and V5 communication channel (basic). ■ cross-connection between V5 protection group 1 and a V5 link's timeslot. ■ V5 protection group 1, if it is provisioned.

6.2.21 Remove a secondary link

Procedure Complete the following procedure to remove a secondary link.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the desired V5.2 interface in the V5 Interface List and click on ***Edit V5 Interface***. The *V5.2 Interface* window (tab V5 Interface Data) pops up.
3.	Select tab V5 Link Data.
4.	Click on ***Remove*** in the **Secondary Link** field to remove the secondary link. After removing the secondary link all automatically created entities are automatically removed.

6.2.22 Remove a V5 protection group 2

Procedure Complete the following procedure to remove a V5 protection group 2.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the desired V5.2 interface in the V5 Interface List and click on ***Edit V5 Interface***. The *V5.2 Interface* window (tab V5 Interface Data) pops up.
3.	Click on ***Protection...***. The *V5.2 Group 2 Protection* window pops up (cf. Chapter 6.2.8.11.1, page 6-125).
4.	Select the entry in the table to be removed and click on ***Remove***. The AEM will send a delete message to the NE: ■ delete cross-connection between V5 protection group 2 and V5 communication channel. ■ delete cross-connection between V5 protection group 2 and V5 timeslot. ■ delete cross-connection between V5 protection group 2 and V5 communication channel or V5 timeslot.

NOTE:
If all protecting and protected units are deleted the protection group is also deleted.

6.2.23 Delete a V5 interface

To be able to delete a V5 interface it is necessary beforehand to perform the following:

- remove V5 protection group 2, if it is configured (cf. Chapter 6.2.22, page 6-139).
- remove secondary link, if it is configured (cf. Chapter 6.2.21, page 6-139).
- remove primary link, if it is configured (cf. Chapter 6.2.20, page 6-138).
- delete all V5 communication paths contained in the V5 interface (cf. Chapter 6.2.19, page 6-137).
- delete all V5 communication channels contained in the V5 interface (cf. Chapter 6.2.18, page 6-137).
- delete all cross-connections between V5 user ports an V5 interface (cf. Chapter 6.2.16, page 6-135).
- delete all cross-connections between V5 links and V5 interface (cf. Chapter 6.2.17, page 6-136).

Procedure

Complete the following procedure to delete a V5 interface.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu. The *V5 Interfaces List* window pops up.
2.	Select the V5 interface id to be deleted and click on ***Remove***. The AEM will send a delete message to the NE.

6.3 Service provisioning (data)

The data service functionality covers the connection establishment process between an ADSL subscriber interface and an E3 network interface.

This functionality is performed in the same way for all the AFM releases managed by AEM R1.7.

Pre-provisioning of ATM links and cross-connections is possible (i.e. if the packs and ports are pre-provisioned the ATM links and cross-connections can also be pre-provisioned even if the related card is not inserted).

This chapter describes the creation, modification and deletion of ATM virtual path/channel links and cross-connections in an NE.

6.3.1 ATM Cross Connections List window

This window displays all ATM cross-connections within the NE. It can also be used to add/edit/remove cross-connections.

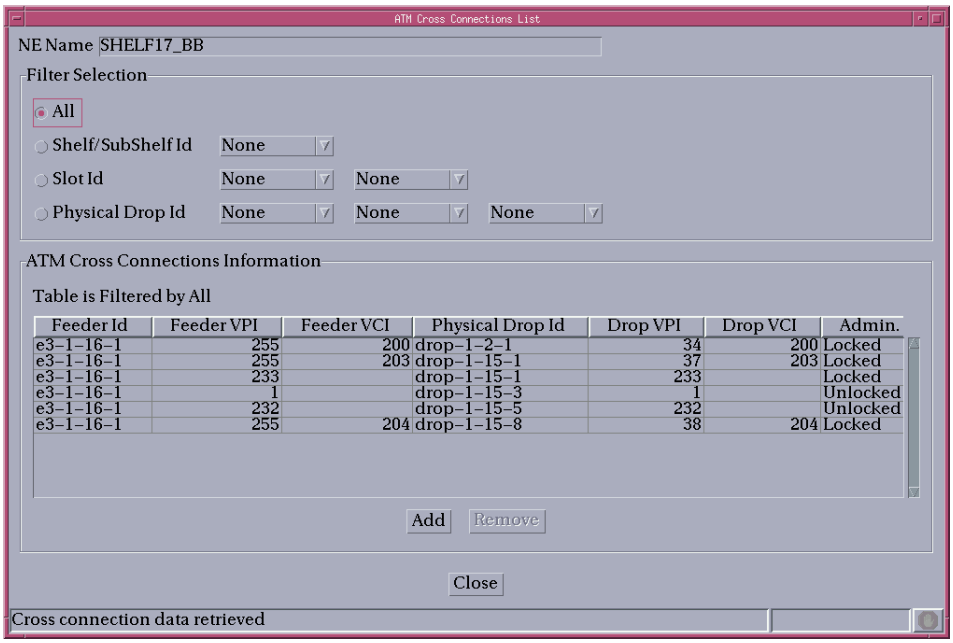


Figure 6-41 ATM Cross Connections List window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Filter Selection	Four radio buttons and six related option menus can be used to select the filter for displaying the cross-connections in the list below. ■ **All**: This button can be used to list all cross-connections within the NE. ■ **Shelf/Subshelf Id**: This button can be used to list all cross-connections within a shelf or subshelf. The related option menu provides the following values: main shelf id, ids of all created subshelves, None. ■ **Slot Id**: This button can be used to list all cross-connections within a slot. The related two option menus provide the following values: first menu: main shelf id, ids of all created subshelves, None. second menu: ADSL slots related to the selection in the first option menu, None. ■ **Physical Drop Id**: This button can be used to list all cross-connections of a drop. The related three option menus provide the following values: first menu: main shelf id, ids of all created subshelves, None. second menu: ADSL slots related to the selection in the first option menu, None. third menu: drop numbers inside the selected slot, None. Selecting a radio button updates the cross-connection table except None is selected in one of the related option menus. The same will happen when a value (except None) is selected in the right-most option menu: the corresponding radio button is activated and the cross-connection list is updated. Please note the following relation between the associated option menus: Physical drop can be selected only if a slot id has been selected beforehand and a slot id can be selected only if a shelf/subshelf id has been selected beforehand.

Parameters/ Buttons	Description
ATM Cross-Connections Information	This list shows the cross-connection parameters. The number of displayed cross-connections depends on the selected filter (see radio buttons above). **Feeder Id**: Shows the feeder involved in the ATM cross-connection (e.g. ds-1-15-1). **Feeder VPI**: Shows the VPI used to create the cross-connection on the feeder side. **Feeder VCI**: Shows the VCI used to create the cross-connection on the feeder side. This field is empty if the row represents a VP cross-connection. **Physical Drop Id**: Indicates the VCI used to create the cross-connection on the feeder side. It will be the drop selected in this window (e.g. drop-1-5-4). NOTE: If no drop is created "not defined" will be displayed. In this case the ***Add/Edit*** operation is disabled. **Drop VPI**: Shows the VPI used to create the cross-connection on the drop side. **Drop VCI:** Shows the VCI used to create the cross-connection on the drop side. This field can be empty if the row is a VP cross-connection. **Administrative State:** This field shows the current administrative state of the cross-connection. The button (***Add***/***Edit***) provides access to the *ATM Cross-Connection* window (cf. Chapter 6.3.2, page 6-144). If a cross-connection has been selected: ***Edit*** if no cross-connection has been selected: ***Add***. NOTE: This button is disabled if the selected cross-connection is not associated with a drop. The ***Remove*** button can be used to remove a selected cross-connection. This button is enabled only if a cross-connection is selected.

6.3.2 ATM Cross-Connection window

This window is used to create, remove or edit ATM cross-connections over an ADSL drop.

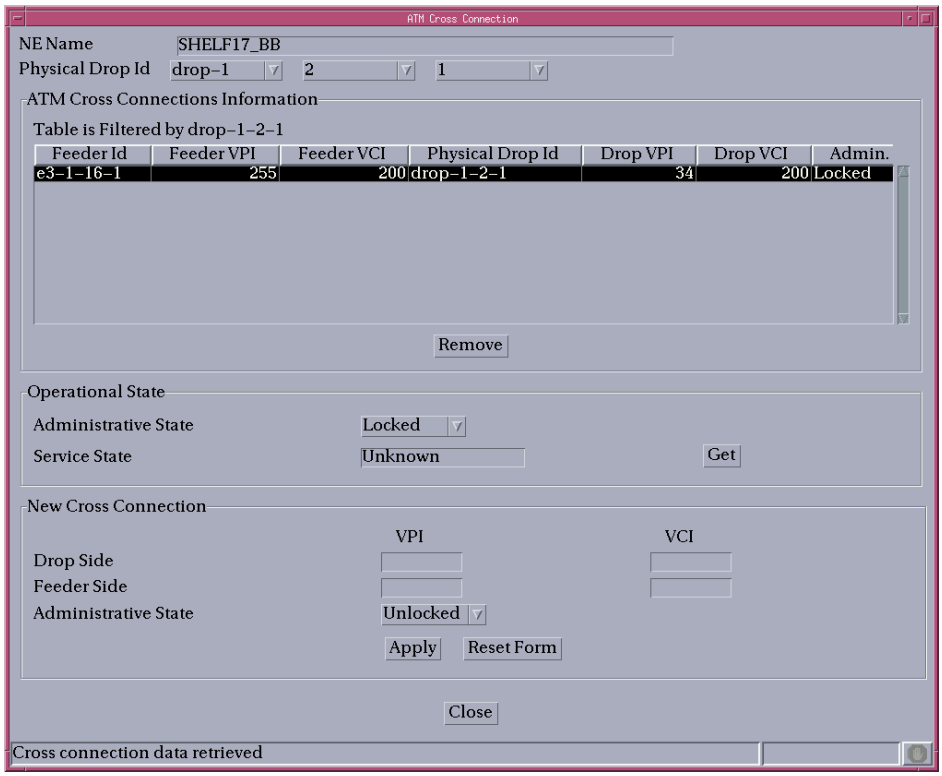


Figure 6-42 ATM Cross-Connection window

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Physical Drop Id	The ADSL drop id is shown by means of three option menus: ■ The first one contains the drop-shelf Format: drop-1 or subdrop-{1, 8}.None is also allowed. ■ The second one contains the slot number inside the NE, but only for slots in which an ADSL pack is provisioned. Format: {1, 16} for main shelf or {1, 8} for subshelf. None is also allowed. ■ The third one contains the drop number inside the slot indicated in the previous list {1, x}. Format: drop-shelf-slot-port. Possible values: drop-1-{1, 16}-{1, x} or subdrop-{1, 8}-{1, 8}-{1, x}. (depending on the ADSL type x can be 4 or 8). These option menus show the drop selected in the previous window. The option menus can also be used to select another drop.
ATM Cross-Connections Information	This list shows the cross-connection parameters. The number of displayed cross-connections depends on the selected filter (see option menus above). **Feeder Id**: Shows the feeder involved in the ATM cross-connection. **Feeder VPI**: Shows the VPI used to create the cross-connection on the feeder side. **Feeder VCI**: Shows the VCI used to create the cross-connection on the feeder side. This field is empty if the row represents a VP cross-connection. **Physical Drop Id**: Indicates the physical drop used to create the cross-connection on the feeder side. It will be the drop selected in this window. **Drop VPI**: Shows the VPI used to create the cross-connection on the drop side. **Drop VCI:** Shows the drop VCI used to create the cross-connection on the drop side. This field can be empty if the row is a VP cross-connection. **Administrative State:** This field shows the current administrative state of the cross-connection. The ***Remove*** button can be used to remove a selected cross-connection. This button is enabled only if a cross-connection is selected.

Parameters/ Buttons	Description
Operational State	The option menu **Administrative State** provides the possible states that can be used: Locked and Unlocked. NOTE: The NE rejects the change from "Locked" to "Locked" or from "Unlocked" to "Unlocked". Trying to do this provokes a command unsuccessful answer. The field **Service State** shows the state of the ADSL drop obtained (on demand) by the user. Possible values: Enabled, Disabled, Dormant (NE R1.4). The ***Get*** button can be used to update the display of the Operational State.
New Cross Connection	**Drop Side (VPI)**: This field is used to define the VPI used to create the cross-connection on the drop side. Possible values: {0, 255}. **Drop Side (VCI)**: This field is used to define the VCI used to create the cross-connection on the drop side. Possible values: {1, 1023}. This field can be empty if the cross-connection is at VCI level. **Feeder Side (VPI)**: This field is used to define the VPI used to create the cross-connection on the feeder side. Possible values: {1, 255}. **Feeder Side (VCI)**: This field is used to define the VCI used to create the cross-connection on the feeder side. Possible values: {33, 1023}. **Administrative State:** This option menu is used to define the administrative state for the NE cross-connection. Possible values: Locked, Unlocked (default). The ***Reset Form*** button can be used to reset all values in this field. The ***Apply*** button is used to create a new cross-connection.

6.3.3 Add an ATM cross-connection

Overview

The field New Cross Connection in the *ATM Cross Connection* window is used to define the parameters for new cross-connections over an ADSL drop.

There are four possibilities to launch the *ATM Cross Connection* window:

- via *ATM Cross Connection List* window (***Add***) - see below
- via *ATM Cross Connection List* window (***Edit***)
- via *ADSL AP* window (***ATM Cross-Connections***)
- via *ADSL AP* window (***Edit Drop***) and *ADSL Drop* window (***ATM Cross-Connections***).

Procedure

Complete the following procedure to add an ATM cross-connection.

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***List -> ATM Cross-Connections*** via the cursor menu. The *ATM Cross Connection List* window pops up (cf. Chapter 6.3.1, page 6-141).

2. Click on ***Add***. The *ATM Cross Connection* window pops up (cf. Chapter 6.3.2, page 6-144).

3. Use the option menus **Physical Drop Id** to select the ADSL drop in which you want to create a new ATM cross-connection.
(If the *ATM Cross Connection* window has been launched in another way (see above) a ADSL Drop is already selected.)
The list **ATM Cross-Connection Information** displays all cross-connections for the selected ADSL drop.

If you want to ...	then ...
add a VP cross-connection	define the **Feeder VPI** and the **Drop VPI** in the field **New Cross Connection**, change the administrative state to "Unlocked" (if required) and click on ***Apply***.
add a VC cross-connection	define the **Feeder VPI, Feeder VCI, Drop VPI** and **Drop VCI** in the field **New Cross Connection**, change the administrative state to "Unlocked" (if required) and click on ***Apply***.

4. Click on ***Close*** to exit the window

6.3.4 Modify an ATM cross-connection

Procedure Complete the following procedure to modify an ATM cross-connection.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> ATM Cross-Connections*** via the cursor menu. The *ATM Cross Connection List* window pops up (cf. Chapter 6.3.1, page 6-141).
2.	Use the radio buttons and the related option menus to select the filter for the display of the cross-connection table.
3.	Click on the cross-connection to be changed and press ***Edit***. The *ATM Cross Connection* window pops up (cf. Chapter 6.3.2, page 6-144). This window can also be reached from the *ADSL AP* window (cf. Chapter 5.5.5.27, page 5-105) or from the *ADSL Drop* window (cf. Chapter 5.5.5.29, page 5-110) via ***ATM Cross-Connections***.
4.	Use the option menu **Administrative State** to change this state. If the administrative state has been changed from “Unlocked” to “Locked” a *Warning* window pops up: **Changing the administrative state of an ATM cross connection may be service affecting. Do you want to continue?**
5.	Click on ***Close*** to exit the window.

6.3.5 Remove an ATM cross-connection

Procedure Complete the following procedure to remove an ATM cross-connection.

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> ATM Cross-Connections*** via the cursor menu. The *ATM Cross Connection List* window pops up (cf. Chapter 6.3.1, page 6-141).
2.	Use the radio buttons and the related option menus to select the filter for the display of the cross-connection table.
3.	Click on the cross-connection to be removed and press ***Remove***. If the cross-connection is in service a *Warning* window pops up: **Removing an ATM cross connection may be service affecting. Do you want to continue?**

If you decide to continue, the AEM will send a delete message to the NE.

4. Click on ***Close*** to exit the window.

Fault management and maintenance

7

Contents

7.1 Overview 7-1

7.2 Alarm management 7-1

7.2.1 Overview 7-1

7.2.2 Maintain up-to-date alarm information 7-2

7.2.3 Alarm notification to the user 7-3

7.2.4 Provide access to the current alarm data 7-7

7.2.5 Managing the raising of alarms 7-7

7.2.6 Manage alarm acknowledgment 7-8

7.2.7 Managing the clearing of alarms 7-8

7.2.8 Alarm data synchronization 7-8

7.2.9 AEM alarm log handling 7-9

7.2.10 Periodical deletion of cleared alarms 7-9

7.3 Alarm monitoring 7-10

7.3.1 General 7-10

7.3.2 Starting and terminating the alarm viewer 7-10

7.3.2.1 Starting the Alarm Viewer 7-10

7.3.2.2 Terminating the Alarm Viewer 7-11

7.3.3 Performing Alarm Viewer functions 7-11

7.3.3.1 Menu bar 7-12

7.3.3.2 Toolbar 7-14

7.3.3.3 General Information 7-14

7.3.3.4 Alarm table 7-15

7.3.3.4.1 Alarm parameters 7-15

7.3.3.4.2 Sorting alarms 7-17

7.3.4 System management functions 7-18

7.3.4.1 File 7-18

7.3.4.2 Views 7-18

Contents

7.3.4.3 Filters 7-19
7.3.4.4 Administrator defined filters 7-21
7.3.4.4.1 Syntax rules 7-21
7.3.4.4.2 Example for filter file 7-23
7.3.4.5 Help 7-23
7.3.5 Alarm Viewer functions 7-24
7.4 Test management 7-25
7.4.1 Telephony tests 7-26
7.4.1.1 User line test 7-26
7.4.1.1.1 User line test via GUI 7-27
7.4.1.2 User port test 7-30
7.4.1.2.1 User port test via GUI 7-30
7.4.1.3 Stand-by card test scheduling 7-32
7.4.1.3.1 Test scheduling via TL1 commands 7-32
7.4.1.4 Built-in self-test 7-33
7.4.1.5 TAP test 7-33
7.4.1.5.1 TAP test via GUI 7-33
7.4.1.6 CRC test (ISDN drop) 7-34
7.4.1.6.1 CRC test via GUI 7-35
7.4.1.7 Single pulse test 7-37
7.4.1.7.1 Single pulse test via TL1 command 7-37
7.4.1.8 Loopback test on the feeder side 7-38
7.4.1.9 Loopback test on the ISDN user port side 7-39
7.4.1.9.1 Loopback test on the ISDN user port side via GUI 7-39
7.4.1.10 Restart PSTN protocol 7-40
7.4.1.11 Provisioning variant test 7-41
7.4.1.12 V5.2 link identification test 7-42
7.4.2 Data tests 7-43
7.4.2.1 ADSL test list 7-43
7.4.2.2 ADSL corrupted CRC test 7-45
7.4.2.3 ADSL BIST test 7-47
7.5 Alarms 7-49
7.5.1 Overview 7-49
7.5.2 Alarm types 7-49
7.5.3 Network element alarms 7-51
7.5.4 General element manager platform alarms 7-51

Contents

7.5.4.1 LOG_DEL_FULL 7-51
7.5.4.2 LOG_DEL_PART 7-52
7.5.4.3 PRINT_ALARM 7-52
7.5.5 Element manager alarms concerning network element 7-53
7.5.5.1 ALARM_AO_NOT_PROCESS 7-53
7.5.5.2 ALARM_EVENT_NOT_PROCESS 7-54
7.5.5.3 COMM_DENIED 7-54
7.5.5.4 COMMUNICATION_LOST 7-55
7.5.5.5 COMM_PROBLEM 7-55
7.5.5.6 COMM_RES_NOT_AVAILABLE 7-56
7.5.5.7 CONFIG_AO_NOT_PROCESS 7-56
7.5.5.8 CONFIG_EVENT_NOT_PROCESS 7-57
7.5.5.9 CX_CONN_NOT_VISIBLE 7-58
7.5.5.10 INVALID_MIB_IDENTIFIER 7-58
7.5.5.11 NB_ASSOC_FAILED 7-59
7.5.5.12 NB_ASSOC_LOST 7-59
7.5.5.13 SW_VR_ILLEGAL 7-60
7.5.5.14 TCP_IP_CON_REFUSED 7-61
7.5.5.15 TL1_COMM_DENIED 7-62
7.5.5.16 UNABLE_TO_SYNC_ALARM 7-62
7.5.5.17 UNABLE_TO_SYNC_CONFIG 7-63
7.5.5.18 UPLOAD_PROBLEM 7-64
7.5.6 Correlated alarms 7-65

Contents

Fault management and maintenance

7

7.1 Overview

This chapter provides you with information about

- basics on the alarm management
- basics on alarms
- maintenance actions if certain alarms are pending
- using the Alarm Viewer
- performing test actions with test management
- basics on information management (e.g. connection states).

7.2 Alarm management

7.2.1 Overview

The main function of the alarm management is to manage the *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7 and network element (NE) related alarms that are registered in the element manager system (EMS). For the list of the alarms generated by the management system refer to Chapter 7.5.4, page 7-51. For the list of alarms concerning network element refer to Chapter 7.5.5, page 7-53.

Once the communication connection between the AEM and an NE is established, the AEM clears the "not-connected" NE alarm indication (if it exists) and starts an alarms and environment alarms synchronization process between the AEM alarm database and active NE alarms. Finally the AEM will try to update its view of NE configuration data and will start a synchronization process between the AEM data set and the NE configuration information (NE NVDS). The NE database is always the master.

The database does not maintain the alarm history, it only stores the current alarm statuses. An alarm can be in one of the following states:

- Severity states:
  - raised
  - cleared
- Acknowledgment states:
  - acknowledged
  - not acknowledged.

The main responsibilities of the alarm management subsystem (AMS) are the following:

- maintain up-to-date alarm information
- notify alarm changes to alarm clients
- provide access to the current alarm data
- manage alarm raising
- manage cleared alarms
- manage acknowledgment of alarms
- synchronization of the alarm data per NE
- AEM alarm log handling
- periodical deletion of cleared alarms.

7.2.2 Maintain up-to-date alarm information

During the alarm life time, the AEM updates the following information:

- the date and time of the last severity change (Date&Time Last Change)
- the last alarm severity change (Perceived Severity)
- the last alarm acknowledge status change (Acknowledge State)
- the last user id which has acknowledged an alarm (Acknowledge User)
- the number of raises the alarm has been raised between the first raised time and the actual time (Number Raises)
- the last alarm correlation state change (Correlation State).

During an alarm life the severity status can change from raised to cleared and vice versa.

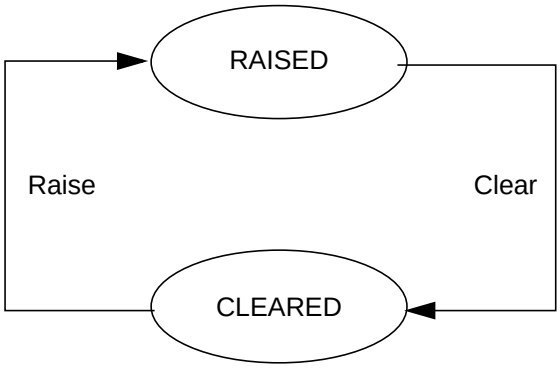


Figure 7-1 Life cycle of an alarm

7.2.3 Alarm notification to the user

Whenever incorrect data (out-of-range values, inappropriate value types, etc.) is entered at the graphical user interface (GUI), a new alarm occurs or the status of any alarm changes to raised again, an alarm message is reported to the AEM. The alarms are indicated, if defined, visually.

Visual alarm indication

The occurrence of a new alarm of a defined severity (default value: critical) is visually indicated in different ways:

- Notification icon displayed in the AEM access bar.

  This icon consists of a flag. If new alarms are received the flag is raised and an audible signal is issued. If the user clicks on the icon the flag goes down.

- Via the Network Browser

  The Network Browser displays all groups and NEs created in the AEM by the use of icons (cf. Figure 7-8, page 7-26).

  The icons change their color to reflect the highest severity alarm (critical, major, minor, indeterminate or warning alarms). The highest severity alarm of a group is the highest severity alarm of all the alarms of its child groups and NEs. The alarm status color is in accordance with the alarm viewer color set (red for critical and major; yellow for minor; white for indeterminate and warning).

  — Select ***Group*** in the Network Browser and ***Alarm Monitoring*** in the cursor menu to look at the group-specific alarms.

  — Select ***NE*** in the Network Browser and ***Alarm Monitoring*** in the cursor menu to look at the NE-specific alarms.

- Shelf view window

  This window (cf. Figure 7-2, page 7-6) provides general inventory, provisioning and alarm information (through the plug-in LEDs). Each slot shows the card type inserted and its alarms (via a red FLT LED, if available). If the slot is empty, no card will be shown.

  See the table below for the list of LEDs provided on each plug-in. The table describes the colors used when the LED is ON or blinking. If the LED is OFF the color black is used.

Table 7-1 LED meanings

Pack	LED	Color	Meanings
IO_E1	FLT	red	■ Lit during pack failure. ■ Flashes when the pack executes off-line self-test.
	ACT	green	Lit when the pack is service-active.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 4.
COMDAC	FLT	red	■ Lit when a fault is detected on the pack. ■ Flashes during software download and turn-up.
	ACT	green	Indicates that this COMDAC is active.
	CR	red	Lit when the highest severity alarm is critical.
	MJ	red	Lit when the highest severity alarm is major.
	MN	yellow	Lit when the highest severity alarm is minor.
	NE	yellow	Lit when the source of the fault or abnormal condition is near-end.
	FE	yellow	Lit when the source of the fault or abnormal condition is far-end.

Table 7-1 LED meanings

Pack	LED	Color	Meanings
CIU	FLT	red	Lit when a fault is detected on the pack.
	ACT	green	Lit when a test is in progress. Pack id in operation.
	POW1	green	Lit when -48V power supply A is in operation.
	POW2	green	Lit when -48V power supply B is in operation.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	ACO	green	Alarm cut-off reminder.
IO_HDLC	FLT	red	■ Lit when a fault is detected on the pack. ■ Flashes when the pack executes off-line shelf-test.
	ACT	green	Lit when the pack is service-active.
APs	FLT	red	■ Lit when a fault is detected on the AP. ■ Flashes when the AP executes off-line shelf-tests.
HDSL	FLT	red	Lit when a fault is detected on the pack.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 4.
OAP	FLT	red	Lit when a fault is detected on the pack.
	CFL	yellow	Lit when a fault or facility alarm occurs.
OCP	FLT	red	Lit when a fault is detected on the pack.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	CLF	yellow	Lit when a fault or facility alarm occurs.

Table 7-1 LED meanings

Pack	LED	Color	Meanings
AFM	FLT	red	Lit when a fault is detected on the pack.
	ACT	green	Indicates that this AFM is active.
	CR-MJ	red	Lit when the highest severity alarm is critical or major.
	MN	yellow	Lit when the highest severity alarm is minor.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in-service received E1 port 2.

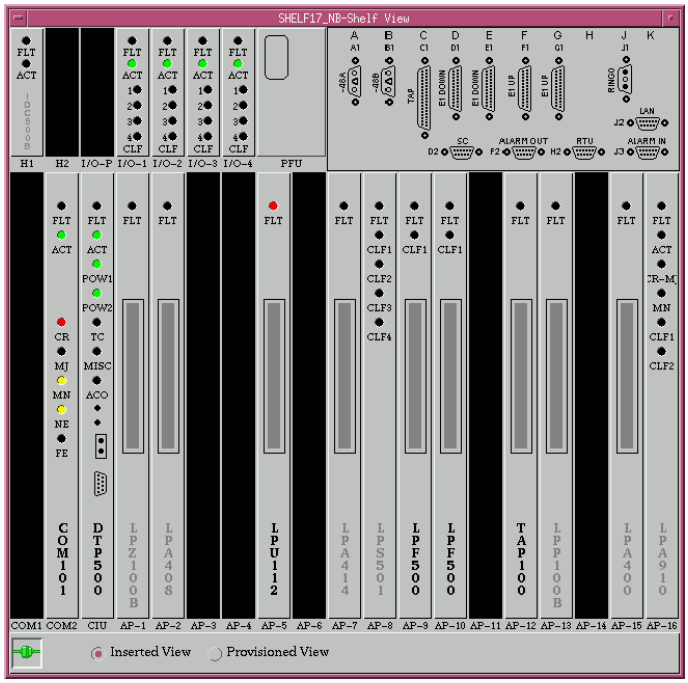


Figure 7-2 Example of a shelf view

Alarm information

For more information on the reported alarm open the Alarm Viewer (cf. Chapter 7.3, page 7-10).

Alarm acknowledgment/clearance

Acknowledging alarms and clearing alarms is described in Chapter 7.3.5, page 7-24.

7.2.4 Provide access to the current alarm data

Alarm retrieval

The user can select lists of alarms filtered by several fields. Therefore the user specifies a selection criterion (cf. Chapter 7.3.4.3, page 7-19) that is taken by the AMS to make the appropriate filters. For instance, an user can request all the critical alarms of an NE, or all platform alarms, or all alarms which are service affecting and are raised at the same time.

The number of alarms stored in the alarm database can be retrieved, too. The total number of alarms can be retrieved as well as the number of alarms per severity (number of critical alarms, major, minor and indeterminate).

User domains

The user domain is the list of NEs and/or the AEM the user can manage. The user domains are applicable in the AMS to the alarm retrieval operations and to the alarm notification.

Each user can only request alarms and the number of alarms that are in the user's domain. The client and server security filters fill in this information. When the alarm retrieval operation arrives at the alarm server, in addition to the normal input data it also contains the user domain information added by the user interface.

7.2.5 Managing the raising of alarms

General

An alarm is raised by different types of agents (e.g. telephony and data) or by any object of the AEM. When an alarm is raised its state and the relevant transmitted data (cf. Chapter 7.5.2, page 7-49) are updated. The alarm information provided by these agents can be different and with different formats. The AEM will convert this information to a common format, this common format is based on the ITU-T Recommendation X.733 ITU-T.

Special care has to be taken if the alarm is raised repeatedly (see "Repetitive and fluctuating alarms"). In this case the already existing alarm is put into the raised state. The user acknowledge identification, if available, is removed from the alarm. This way a raised condition of an existing alarm is considered as a new raising (not a new alarm). The number of occurrences is increased every time the same alarm is raised.

Repetitive and fluctuating alarms

A repetitive alarm is an alarm that is raised several times before it is cleared. A fluctuating alarm is an alarm that is raised and cleared alternatively several times in a short period (at least less than the AEM constant for the cleared alarms, see Chapter 7.2.10, page 7-9).

To handle these alarms three fields are defined and maintained for each alarm:

- First Raised Time
- Last Changed Time
- Number of Occurrences.

The alarm viewer can obtain the following information:

- The "Number of Occurrences" is the number of times the alarm has been raised between when it was first raised and the current time (only the raised alarms are counted). In this period the alarm has been raised all the time or it may have been raised/cleared several times (it is not relevant to distinguish both cases).

Correlated/duplicated alarms

Alarms coming from the same NE through telephony and data agents (i.e. the same alarm reported via both controller cards) are correlated into a unique new alarm.

Although the result alarm is generated by the AEM, it is handled as an NE alarm.

The perceived severity of the result alarm is the highest severity value of the received source alarms. The service affecting of the result alarm will be the highest value of the received source alarms (where service affecting (SA) is the highest value and not service affecting (NSA) is the lowest).

7.2.6 Manage alarm acknowledgment

Alarms can only be acknowledged by a user at the user interface. It is possible to acknowledge all alarms types. If an alarm is acknowledged its state is updated accordingly and the user identification is registered. Acknowledging an alarm causes a change to the alarm database. Therefore the alarm was logged before in the alarms log. It is possible to acknowledge an alarm that has already been acknowledged. The user identification and the new acknowledge time are registered as well, overwriting the previous acknowledge data.

7.2.7 Managing the clearing of alarms

General

The NE alarms are cleared by the NE-AMS. Platform alarms are cleared automatically (e.g. NE-AEM association alarms) or by a user at the user interface (e.g. log alarms). Users can only clear specific platform alarms. Users cannot clear the association alarms for the NE alarms. When an alarm is cleared its severity is updated and the time is registered, too. Clearing an alarm causes a change to the alarm database. Therefore the alarm is logged beforehand in the alarms log (if the user clears an alarm this will be logged in the action log; if an alarm is cleared by the NE it will be logged in the action log).

If the raise is newer, then it is a repetitive raise; the alarm state is set to the raised state. If the raise is older, then this message is ignored; the alarm state stays in the cleared state and the relevant data is updated.

7.2.8 Alarm data synchronization

The AMS is responsible for the performance of NE alarm synchronization. To accomplish this, the AMS requests all the current alarms (normal and environment) of the NE that is being synchronized. Once the AMS has received these alarms it compares them with the alarms stored in the AEM alarm database. At the end of the synchronization the alarms stored in the alarm database must be the same as

the alarms retrieved from the NE-AMS. Only one synchronization per NE can be performed at the same time. The AMS rejects any synchronization request for the same NE if the first one has still not finished.

7.2.9 AEM alarm log handling

If the user wants to know the different states throughout the alarm life the user will have to see the Log System (cf. Chapter 3.7, page 3-46) in which all alarm changes are stored.

Seven types of logs are used. The AMS logs the following situations:

- Actions log
  - periodical database deletion of cleared alarm's start and end.
  - alarm's synchronization start and end.
  - periodical deletion of cleared alarms.
  - manual clear, manual acknowledge. The user identification that performs these actions is also logged.
  - automatically clear and acknowledgement.
- System-internal events log
  - exception conditions of the AMS.
- Alarms log
  - all alarms received from the NE.

7.2.10 Periodical deletion of cleared alarms

By default, alarms with *cleared* status are maintained for at least three days (including the current day) in the database. This value can be configured by the user via the system variable "AM.minimumClearPeriod" in the file $ANYMEDIAPATH/cfg/AnyMediaEM.cfg and is an integer multiple in days. The default value is 3 days.

The AEM performs a periodical deletion of the alarms with cleared status that exceed the specified time. This is done during the night-time period in low-load hours.

7.3 Alarm monitoring

7.3.1 General

Overview The AEM provides a process to monitor and display all alarms stored in the database. Using this system, the Alarm Viewer, the user is able to see many different alarm attributes such as Event Type, Severity, Alarm Text, Status, Summary and the date and time when the alarm was raised. Via this tool the user can perform actions (e.g. acknowledge, clear) for some of these alarms.

What you will find In this chapter you will find the following information:

- Instructions for starting and terminating the alarm viewer (Chapter 7.3.2, page 7-10)
- Instructions for handling the alarm viewer (Chapter 7.3.3, page 7-11)
- Structure of the alarm viewer window (Chapter 7.3.3.3, page 7-14 and Chapter 7.3.3.4, page 7-15)
- System management (Chapter 7.3.4, page 7-18)
- Alarm viewer functions (Chapter 7.3.5, page 7-24).

7.3.2 Starting and terminating the alarm viewer

7.3.2.1 Starting the Alarm Viewer

The Alarm Viewer can be started in different ways:

- Clicking on the icon ***Alarm Viewer*** in the access bar (cf. Chapter 3.2.3).
- Clicking on ***Alarms*** in the menu bar of the other Element Manager applications (cf. Chapter 3.3.6). In this case only alarms of the NE which is selected in the Network Browser are shown.
- Selecting ***File -> New*** in the Alarm Viewer.

The displayed window has the title "Alarm Viewer" and maintains similarities with the other AEM windows.

The *Alarm Viewer* window consists of the sections:

- Menu bar (File, Views, Filters, Actions, Help).
- Toolbar (buttons for Acknowledge, Clear, Reload and Print).
- General Information.
- Alarm table.

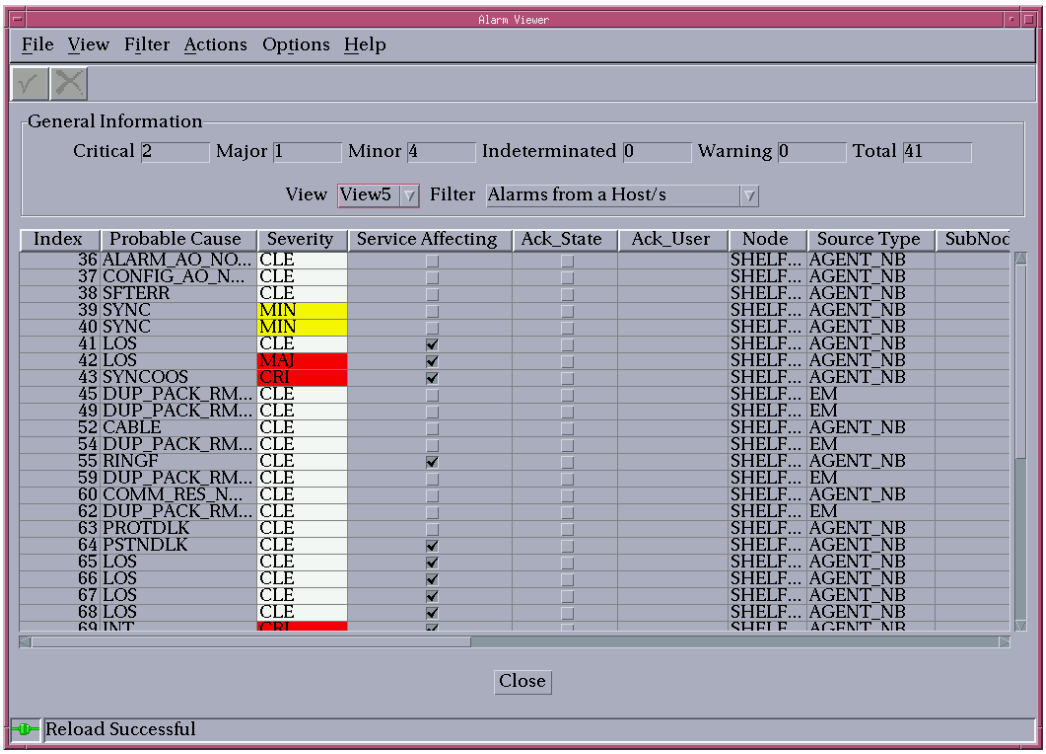


Figure 7-3 Alarm Viewer window

7.3.2.2 Terminating the Alarm Viewer

The Alarm Viewer can be terminated as follows:

- By selecting ***File -> Exit*** in the Alarm Viewer menu to close all Alarm Viewers launched by the user.
- By clicking on the ***Close*** button or ***File -> Close*** to close only the Alarm Viewer in use.

Before quitting the Alarm Viewer the user is prompted for confirmation.

7.3.3 Performing Alarm Viewer functions

The Alarm Viewer provides different possibilities to perform internal functions and alarm management functions.

These functions can be initiated via:

- Menu
- Tool bar

In most cases the choice depends on the user's personal preference.

7.3.3.1 Menu bar

The menu bar is used to activate alarm viewer functions.

NOTE:
The executable functions depend on the respective user privileges.

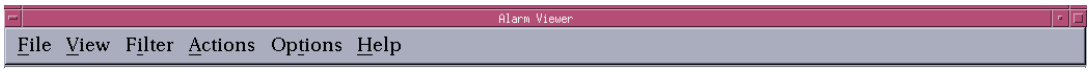


Figure 7-4 Menu bar of the Alarm Viewer

Selection is achieved

- By opening the menu by pressing the left mouse button and dragging the cursor to the desired option in the menu or
- By opening the menu via the keyboard by entering **`Alt`** plus the underlined letter of the relevant menu to open the menu option and then entering the letter underlined in the desired menu option.

Table 7-2 File menu

Menu display	Menu option	Meaning	Information in
New Print Close Exit	New	Launch a new instance of the Alarm Viewer.	Chapter 7.3.4.1, page 7-18
	Print -> Print Table	Print all alarm items displayed in the currently displayed table or save the items into an ASCII file. The Print Dialog window (cf. Chapter 3.5) is opened.	
	Print -> Preview	Show the Preview Frame window (cf. Chapter 3.5).	
	Print -> Print Window	Print a screenshot of the whole window. The Print Dialog is opened (cf. Chapter 3.5).	
	Close	Dismiss this window, but without closing other instances of the Alarm Viewer.	
	Exit	Close all Alarm Viewers opened by the user.	

Table 7-3 Views menu

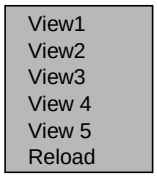
Menu display	Menu option	Meaning	Information in
	View1	Select a view from the predefined views.	Chapter 7.3.4.2, page 7-18
	View2		
	View3		
	View4		
	View5		
	Reload	Display a fresh copy of the current information shown in the window. Only alarms which match the filter criteria will be included.	Chapter 6.3.5, page 6-21

Table 7-4 Filters menu

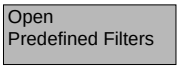
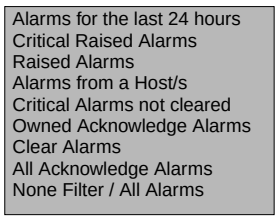
Menu display	Menu option	Meaning	Information in
	Open...	Open a user-defined filter previously stored. No modifications allowed.	
	Predefined Filters 	Selection of filter criteria for displaying alarm information.	Chapter 7.3.4.3, page 7-19

Table 7-5 Actions menu

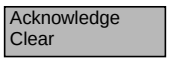
Menu display	Menu option	Meaning	Information in
	Acknowledge	Acknowledge all selected alarms, their status will change to acknowledged.	Chapter 7.3.5, page 7-24
	Clear	Clear all selected alarms, their status will change to cleared.	

Table 7-6 Help menu

Menu display	Menu option	Meaning	Information in
	Index	Display the index help, allowing the user to navigate through the AEM help information.	Chapter 7.3.4.5, page 7-23
	On Window	Display the help information of the window where the user is currently working.	

7.3.3.2 Toolbar

The toolbar contains often used functions and consists of four buttons:

Table 7-7 Toolbar

Function	Icon	Meaning
Acknowledge		Acknowledge all selected alarms. Their acknowledgement states immediately changes to acknowledged. The User_Ack is set to the login of the user who has acknowledged the alarm
Clear		Clear all selected alarms. Their severity states immediately changes to cleared.
Reload		Reload the actual alarm states into the table. Only alarms which match the filter criteria are included.
Print		Open a submenu (Print Table, Print Window, Print Preview) so that one of these items can be selected.

7.3.3.3 General Information

The first section is a frame titled *General Information*, this frame includes controls showing information about the number of alarms of each alarm severity (in the domain where the user is working) related to the active filter and the operator's working domain:

- Critical

  Displays the number of critical (CR) alarms.
- Major

  Displays the number of major (MJ) alarms.
- Minor

  Displays the number of minor (MN) alarms.
- Indeterminate

  Displays the number of indeterminate (IN) alarms.
- Total

  Displays the total number of alarms (all severities).

Additionally the frame contains two option menus, which show the filter (cf. Chapter 7.3.4.3, page 7-19) and view (cf. Chapter 7.3.4.2, page 7-18) currently being used. In these two option menus the user can select filters and views.

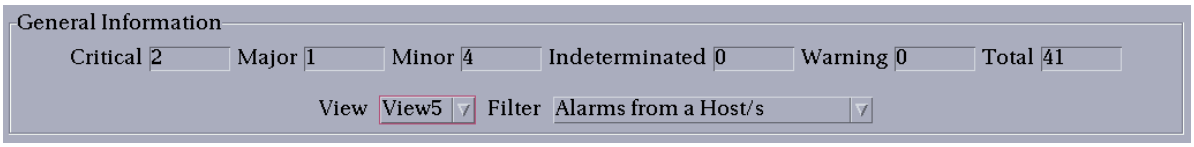
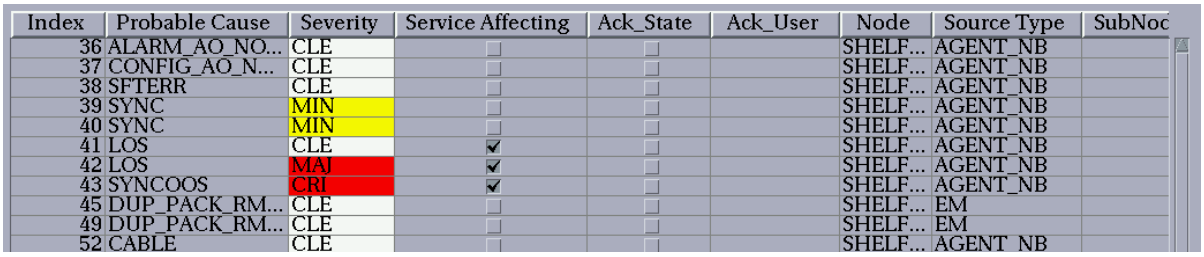


Figure 7-5 General Information frame

7.3.3.4 Alarm table

The last section in the Alarm Viewer window is a table that contains zero or more alarms belonging to a domain. This table allows the user to sort the alarms (cf. Chapter 7.3.3.4.2, page 7-17) by clicking on a specific table header. The user also can select them for acknowledgment or clearance. The mechanism to acknowledge or clear is the same, the user has to select one or more alarms. After selecting the alarms click on ***Acknowledge*** or ***Clear*** in the tool bar
or select ***Actions -> Acknowledge*** or ***Actions -> Clear*** via the menu bar.



Index	Probable Cause	Severity	Service Affecting	Ack_State	Ack_User	Node	Source Type	SubNoc
36	ALARM_AO_NO...	CLE	☐	☐		SHELF...	AGENT_NB	
37	CONFIG_AO_N...	CLE	☐	☐		SHELF...	AGENT_NB	
38	SFTERR	CLE	☐	☐		SHELF...	AGENT_NB	
39	SYNC	MIN	☐	☐		SHELF...	AGENT_NB	
40	SYNC	MIN	☐	☐		SHELF...	AGENT_NB	
41	LOS	CLE	☑	☐		SHELF...	AGENT_NB	
42	LOS	MAJ	☑	☐		SHELF...	AGENT_NB	
43	SYNCOOS	CRI	☑	☐		SHELF...	AGENT_NB	
45	DUP_PACK_RM...	CLE	☐	☐		SHELF...	EM	
49	DUP_PACK_RM...	CLE	☐	☐		SHELF...	EM	
52	CABLE	CLE	☐	☐		SHELF...	AGENT_NB	

Figure 7-6 Alarm list section

7.3.3.4.1 Alarm parameters

For each alarm the following alarm fields (depending on the selected view) can be displayed:

- Index

  Sequence number for each different alarm reported to the AEM (the maximum sequence number is 100 000).

- Probable Cause

  Identifies the probable cause of the alarm. This field contains a unique identification string for each alarm type.

- Severity

  Contains the default severity of the alarm.

  — Critical (*CR*)

  — Major (*MJ*)

  - Minor (*MN*)
  - Indeterminate (*IN*)
  - Warning (*WR*)
  - Cleared (*CL*).

- Service Affecting

  Specifies whether the alarm is subscriber service affecting or not.

  Possible values: Yes, No.

- Acknowledge State

  Reflects if the alarm has been acknowledged by a user.

- Acknowledge User

  The login of the last user who has acknowledged an alarm.

- Node

  A unique text label. For NE alarms, it is the NE-Name of the NE the alarm belongs to. For platform alarms, the string “EM” is used, except for communication alarms.

- Source Type

  Defines the type of alarm reporting source. For NE alarms, the agent type (e.g. NarrowBand, BroadBand, NarrowBand-Broadband) is used. For platform alarms, the string “EM” is used.

- Entity

  Object identifier referring to the alarm. Examples of objects are network elements, "ap-1-1", etc.

- Alarm Text

  Contains text briefly describing the alarm. The summary text is unique in the Element Manager.

- Description

  This field contains a full description of the alarm.

- Agent Description

  For the NE alarms, this field contains the description sent in the TL1 message or in the trap (without internationalizing). For platform alarms, this field is empty.

- Date&Time First Change

  Date and Time of the first severity change.

- Date&Time Last Change

  Date and Time of the last severity change in the life cycle of one alarm.

- Number Raises

  Number of times the alarm has been raised between the first raised time and the current time.

- Correlation State

  This field reflects if one alarm has been correlated or not. In the case of correlated alarms it also identifies if it is a source or a result alarm of the correlation process. For this release only duplicated alarms are considered.

7.3.3.4.2 Sorting alarms

Summary

The user can sort alarms by the different fields by clicking on the respective header. The sort can be in ascending or descending order. The sort order is reversed by clicking on the respective header.

All alarm fields are sorted by alphanumeric order except date and time field.

Effects

The alarms are re-arranged according to the selected criteria.

Sorting alarms

Proceed as follows to sort the alarm display:

Step	Procedure

1. Click on the header according to which the alarms are to be sorted.

   Response: The alarms are sorted according to the selected alarm field in ascending or descending order.

2. Check if the list was sorted as desired.

   Yes: O.K.

   No: Continue with step 3.

3. Click again on the header to sort the list in the reverse order.

   The sort can be in ascending or descending order, each time the user clicks on the same header again the list is sorted the other way.

7.3.4 System management functions

The general system management functions comprise the functions for file management, for defining view options and for getting help. These functions are contained in the following menus:

- File
- Views
- Filters
- Help.

7.3.4.1 File

In the File menu you can start the following actions:

- New

  Launch a new instance of the Alarm Viewer.

- Print

  (cf. Chapter 3.5).

- Close

  Close the active window, but without closing other instances of the Alarm Viewer. Same functionality as the Close button.

- Exit

  Close all Alarm Viewers opened by the user.

7.3.4.2 Views

Summary For displaying alarm lists you can select from five pre-defined views.

- View1:
  Index, Node, Entity, Severity, Date&Time Last Change, Alarm Text.
- View2:
  Index, Node, Entity, Severity, Date&Time Last Change.
- View3:
  Index, Node, Entity, Date&Time First Raise, Date&Time Last Change, Acknowledge User, Number Raises.
- View4:
  Index, Node, Entity, Severity, Date&Time Last Change, Correlation State.
- View5:
  All alarm fields

Effects The alarms are rearranged according to the selected criteria.

Selecting views

Proceed as follows to select the desired view option:

Step	Procedure
1.	Select ***Views -> ViewX*** (X = 1 to 5) in the menu bar. The same view options can be selected via the option menu ***Views*** in the general information section (cf. Chapter 7.3.3.3, page 7-14). *Response:* The alarms are displayed according to the selected view.

7.3.4.3 Filters

Summary

For displaying the alarm lists you can select pre-defined filters. Only those alarms corresponding to the filter criteria are displayed. The alarm set is displayed without modifying the current view.

Pre-defined filters

The pre-defined filters are:

- Alarms for the last 24 hours (all alarms which have been changed in the last 24 hours)
- Critical Raised Alarms
- Raised Alarms
- Alarms from a Host/s
- Critical Alarms not cleared
- Owned Acknowledge Alarms
- Clear Alarms
- All Acknowledge Alarms
- None Filter / All Alarms.

Effects

The alarms are rearranged according to the selected filter criteria.

Selecting filter

Proceed as follows to select the desired filter option:

Step	Procedure

1. Select the desired filter option:

If you want to view ...	then select ***Filters -> Pre-defined Filters...***	Result/Notes
all alarms which have been changed in the last 24 hours	***Alarms for the last 24 hours***	The alarms are displayed according to the selected filter.
all critical raised alarms	***Critical Raised Alarms***	The alarms are displayed according to the selected filter.
all raised alarms	***Raised Alarms***	The alarms are displayed according to the selected filter.
all alarms from a host	***Alarms from a Host/s***	NE selection window will open, see details below.
all not cleared critical alarms	***Critical Alarms not cleared***	The alarms are displayed according to the selected filter.
all owned acknowledge alarms	***Owned Acknowledge Alarms***	The alarms are displayed according to the selected filter.
all cleared alarms	***Clear Alarms***	The alarms are displayed according to the selected filter.
all acknowledge alarms	***All Acknowledge Alarms***	The alarms are displayed according to the selected filter.
all alarms	***None Filter / All Alarms***	The alarms are displayed according to the selected filter.

The same filter option can be selected

— via the option menu ***Filters*** in the general information section (cf. Chapter 7.3.3.3, page 7-14).

If you selected ***Alarms from a Host/s*** the NE selection window is displayed (cf. Figure 7-7, page 7-21) and you have to select one or more NEs and/or the AEM for which the alarms should be displayed. Press ***OK*** in the NE selection window to display the alarms from the selected objects in the Alarm Viewer or press ***Cancel*** to cancel the operation.

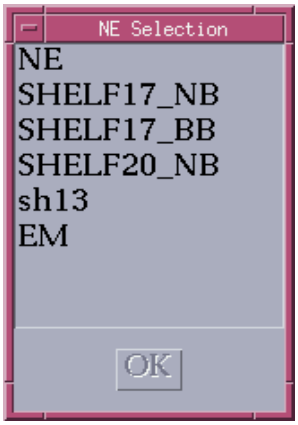


Figure 7-7 NE selection window

7.3.4.4 Administrator defined filters

Administrator privileges required

Only a user with administrator privileges can define own alarm filters in the Alarm Viewer application.

Filter syntax

This filter consist of a combination of logical expressions over the so called field-value tuples of the alarm database. Each logical expression consists of an alarm field, a relational operator (>, <, =, ...) and a value for the specified alarm field. Parenthesis can be used for grouping expressions.

Filter file

If the administrator specifies a logical expression in the filter file the AMS will query the alarm database to return the list of alarms that match this logical expression. For instance, an administrator can request all critical alarms of an NE, or all platform alarms, or all alarms which are service affecting and are raised at the same time.

7.3.4.4.1 Syntax rules

The following rules have to be obeyed for building a filter expression:

- The filter file must contain a single line only.
- A space has to be used between field names, possible values, operators and brackets.
- The expression **`NULL`** has to be used to represent an empty string.

Logical operators

The following symbols for logical operators must be used:

Table 7-8 Logical operators

Operation	Symbol
AND	**&&**
OR	**||**
NOT	**!**

Brackets "( )" must be used to group the expressions if more than one logical expression is needed.

Relational operators

The following symbols for relational operators must be used:

Table 7-9 Relational operators

Operation	Symbol
equal	**==**
less than	**<**
less than or equal	**<=**
greater than	**>**
greater than or equal	**>=**

Alarm field names and values

The alarm field names and their possible values from the following table have to be used.

Table 7-10 Alarm field names and possible values

Field name	Possible values
index	integer > 0
node	integer > 0 (for NE identifiers) or 0 (for AEM)
source_type	**Agent_BB** or **Agent_NB**
object	AID parameter in TL1 REPT-ALAM (e.g. **ap-1-1**)
cause	CONDTYPE parameter in TL1 REPT-ALAM (e.g. **AIS**)
severity	**indeterminate**, **critical**, **major**, **minor**, **warning** or **cleared**
serv_aff	**sa** or **nsa**
event_type	AIDTYPE parameter in TL1 REPT-ALAM (e.g. **COMM**)
ack_state	**ack** or **noack**
ack_user	any string which can be a valid user login
num_raises	integer >= 0
f_c_time	integer (number of seconds since Jan 1 1970 UTC)
l_c_time	integer (number of seconds since Jan 1 1970 UTC)
correlation	**correlated_source**, **no_correlated** or **correlated_result**

7.3.4.4.2 Example for filter file

The following expressions are examples for filters:

- Alarms which are in the state "ack" and do not have the severity "major"

  ```
  ( ack_state == ack ) && ! ( severity == major )
  ```

- Alarms which have the severity "minor" or are not service affecting

  ```
  ( severity == minor ) || ( serv_aff == nsa )
  ```

7.3.4.5 Help

Help is provided for every window. The help text describes the purpose of the window, how to use it and a description of each field of the window is given.

In the menu bar of each AEM application there are two help options:

- Index

  Displays the help index, allowing the user to navigate through the AEM help information.

- On window

  Displays the help information of the window where the user is currently working.

7.3.5 Alarm Viewer functions

Summary The Alarm Viewer provides the user with different functions for managing alarm information:

- Manual reload of alarms
- Acknowledge alarms.

  The user can acknowledge one, several or all reported alarms. The AEM allows different users to acknowledge the same alarm. The name of the last user who has acknowledged the alarm is stored.
- Clear alarms

  The user can clear one, several or all platform alarms (communication alarms are platform alarms that cannot be cleared by the user). If not all selected alarms could be cleared, the user is informed about the alarms for which this action failed.
- Print alarm lists (cf. Chapter 7.3.4.1, page 7-18).

Prerequisites Before performing alarm acknowledgment and alarm clearance select the alarms you want to acknowledge or clear.

Starting actions Select the desired alarm viewer action:

If you want to ...	then select ...	Result/Notes
manually retrieve alarms	***View -> Reload***	Reloads alarms in the table. Only alarms which match the filter criteria are included. The Alarm Viewer is blocked until the reload is finished. Same functionality as ***Reload*** in the tool bar. To customize the displayed alarm list perform the actions described in Chapter 7.3.4.3, page 7-19 and Chapter 7.3.4.2, page 7-18.
acknowledge alarms	***Actions -> Acknowledge***	All selected alarm items are acknowledged. Their status immediately changes to acknowledge. Same functionality as ***Acknowledge*** in the tool bar. For better readability the displayed alarms can be sorted (cf. Chapter 7.3.3.4.2, page 7-17).
clear alarms	***Actions -> Clear***	All selected alarm items are cleared. Their status immediately changes to cleared. Same functionality as ***Clear*** in the tool bar. For better readability the displayed alarms can be sorted (cf. Chapter 7.3.3.4.2, page 7-17).

7.4 Test management

Main functions

Test management provides all the general purpose test functionality. The main functions are:

- Providing the user with different test options (see below)
- Starting the test execution by means of the AEM
- Displaying the test results on the AEM user interface
- Setting and clearing of loopbacks.

Access to the test routines

The test routines are available via the "Groups and NEs Management" application. To start it, click on the Groups and NEs Management icon in the access bar. The menu bar, the Network Browser and the Background Map pop up (cf. Figure 7-8, page 7-26).

The tests can be executed from *AP* windows, *User Port* windows and *TAP AP* window (TAP test).

TL1 commands

Most of the test routines can also be executed via TL1 commands by using the TL1 command line interface (cf. Chapter 5.5.18).

Please refer to the network element documentation for a detailed description of TL1 commands (including an explanation of the input format, restrictions, error conditions etc.).

The test execution via TL1 commands is described in this manual only for the stand-by card test scheduling and the single pulse feeding test because these tests cannot be executed via GUI.

Test options

The following test options are available for telephony application:

- Line test (cf. Chapter 7.4.1.1, page 7-26)
- Port test (cf. Chapter 7.4.1.2, page 7-30)
- Stand-by card test scheduling (cf. Chapter 7.4.1.3, page 7-32)
- Built-in self-test (cf. Chapter 7.4.1.4, page 7-33)
- TAP test (cf. Chapter 7.4.1.5, page 7-33)
- CRC test (cf. Chapter 7.4.1.6, page 7-34)
- Single pulse feeding test (cf. Chapter 7.4.1.7, page 7-37)
- Loopback test on the feeder side (cf. Chapter 7.4.1.8, page 7-38)
- Loopback test on the ISDN user port side (cf. Chapter 7.4.1.9, page 7-39)
- Restart PSTN protocol (cf. Chapter 7.4.1.10, page 7-40)
- Provisioning variant test (cf. Chapter 7.4.1.11, page 7-41)
- V5.2 link identification test (cf. Chapter 7.4.1.12, page 7-42).

The following test options are available for data application:

- ADSL Test List (cf. Chapter 7.4.2.1, page 7-43)
- ADSL corrupted CRC test (cf. Chapter 7.4.2.2, page 7-45)
- ADSL built-in self-test (cf. Chapter 7.4.2.3, page 7-47).

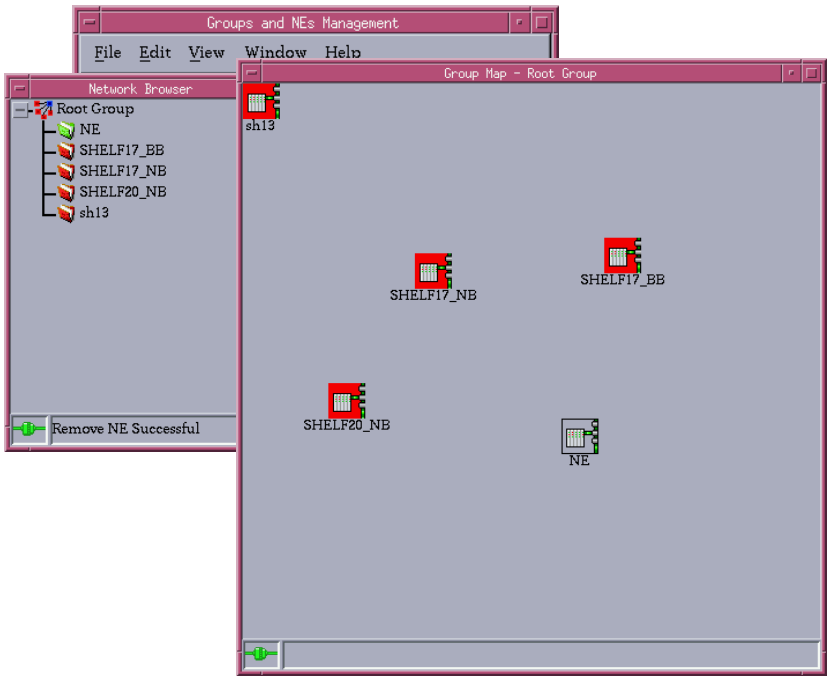


Figure 7-8 Groups and NEs Management window

7.4.1 Telephony tests

7.4.1.1 User line test

Purpose

By means of a line test you are able to run a series of checks for opens, shorts, leakages to ground, foreign voltages, or other faults on the subscriber line that link an AP port circuit to the CPE.

Precondition

Before a line test can be started the following must be done:

- The TAP100 must be equipped and provisioned
- The connection between the TAP100 and the CIU must be established with the correct cable (from the front of the TAP100 to the backplane).

The AEM automatically creates a line test entity when the TAP100 is equipped and provisioned.

NOTE:
The line test can be executed via GUI and via TL1 command.

7.4.1.1.1 User line test via GUI

Procedure

Proceed as follows to start a line test and view the test result:

Step	Procedure
1.	Open one of the following windows: ■ *PSTN/ISDN AP* window (cf. Chapter 5.5.5.13) ■ *HDSL AP* window (cf. Chapter 5.5.5.16) ■ *ALL User Port* window (cf. Chapter 6.2.8.2.1) ■ *V5 PSTN User Port* window (cf. Chapter 6.2.8.3.1) ■ *DLL User Port* window (cf. Chapter 6.2.8.4.1) ■ *V5 ISDN BA User Port* window (cf. Chapter 6.2.8.5.1).
2.	Select the physical port where you intend the test to run.
3.	Use the option menu in the **Test Management** field to select Line Test and click on ***Apply***. After confirming the user line test execution a *Warning* window pops up showing the following message: **Line Test may be service affecting. Do you want do continue?** After confirming this warning the following *In Progress* message pops up: **User Line Test execution in progress on <NE Name>, <Slot ID>, <Provisioned Apparatus Code>, <Port id>.**
4.	Wait until the *Line Test Result* window (cf. Figure 7-9, page 7-28) appears and view the test result.

Test result

The *Line Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

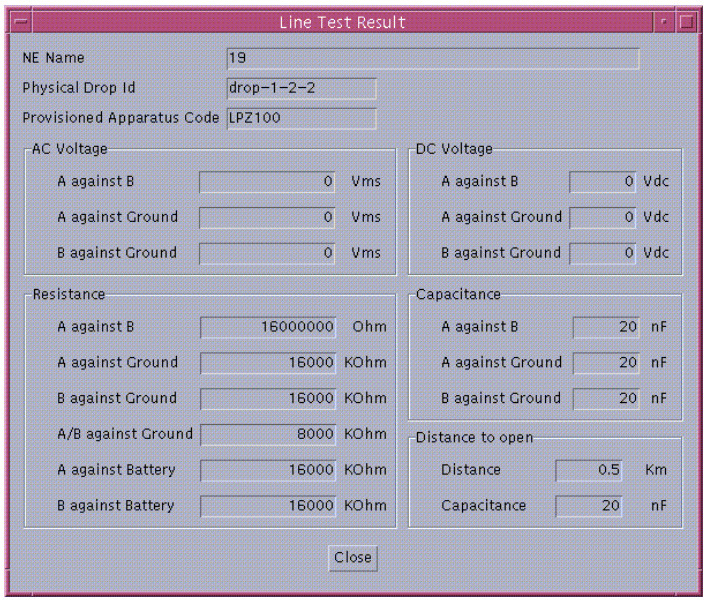


Figure 7-9 Line Test Result window

The text fields are display-only and have the following meaning:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters) as specified at NE creation time.
Slot Id	This field shows the slot number of the AP being used. Possible values: ap-1-{1, 16} or subap-{1, 8}-{1, 8}.
Provisioned Apparatus Code	This code identifies the type of the provisioned card (for example LPZ100, LPS501, etc.).
Port id	This field shows the drop within the provisioned AP.
AC Voltage (Vrms)	These fields display the results of the AC measurements. Possible values: 0 to 200 Vrms.
DC Voltage (Vdc)	These fields display the results of the DC measurements. Possible values: -150 to 150 Vdc.
Resistance (kOhm)	These fields display the results of the insulation resistance measurements. Possible values: 0 to 16000 kOhm (0 to 8000 kOhm for *A/B against Ground*).

Parameters/ Buttons	Description
Capacitance (nF)	These fields display the results of the capacitance measurements. Possible values: 20 to 9000 nF
Distance to open	These fields display the results of the distance measurements. Possible values: 0.5 to 30 km for distance, 20 to 9000 nF for capacitance.

5. Click on ***Close*** to exit the *Line Test Result* window.

7.4.1.2 User port test

Purpose

By means of a port test you are able to run a series of self-diagnostic routines for a particular port on a specified AP (except AFM, ADSL APs).

NOTE:
The user port test can be executed via GUI and via TL1 command.

7.4.1.2.1 User port test via GUI

Procedure

Proceed as follows to start a port test and view the test result:

Step	Procedure
1.	Open one of the following windows: ■ *PSTN/ISDN AP* window (cf. Chapter 5.5.5.13) ■ *HDSL AP* window (cf. Chapter 5.5.5.16) ■ *ALL User Port* window (cf. Chapter 6.2.8.2.1) ■ *V5 PSTN User Port* window (cf. Chapter 6.2.8.3.1) ■ *DLL User Port* window (cf. Chapter 6.2.8.4.1) ■ *V5 ISDN BA User Port* window (cf. Chapter 6.2.8.5.1).
2.	Select the user port where you intend the test to run.
3.	Use the option menu in the **Test Management** field to select Port Test and click on ***Apply***. After confirming the test execution a *Warning* window pops up showing the following message: **Port Test may be service affecting. Do you want do continue?** After confirming this warning the following *In Progress* message pops up: **Port Test execution in progress on <NE Name>, <Slot ID>, <Provisioned Apparatus Code>, <Port id>.**
4.	Wait until the *Port Test Result* window (cf. Figure 7-10, page 7-31) appears and view the test result.

Test result

The *Port Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

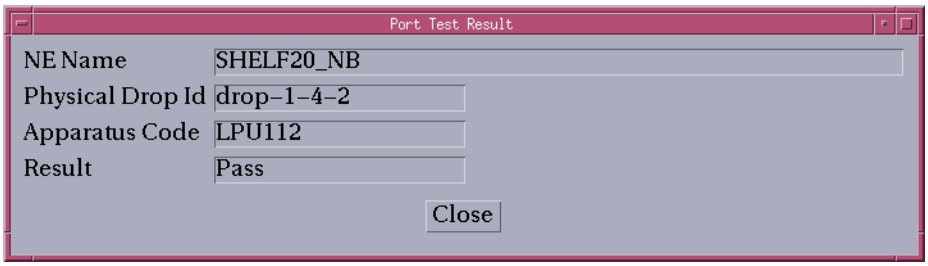


Figure 7-10 Port Test Result window

The text fields are display-only and have the following meaning:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters) as specified at NE creation time.
Physical Drop Id	This field shows the port of the AP affected by the test. Possible values: drop-1-{1,16}-{1,x} / subdrop-{1,8}-{1,8}-{1,x} (“x” depends on the card type.).
Provisioned Apparatus Code	This code identifies the type of the provisioned card (for example LPZ100, LPS501, etc.).
Result	This field displays the result of the test routines. Possible values: PASS or FAIL.

5. Click on ***Close*** to exit the *Port Test Result* window.

7.4.1.3 Stand-by card test scheduling

Side switch and off-line diagnostics

During the execution of stand-by card test scheduling a COMDAC side switch and off-line diagnostics for the stand-by COMDAC are performed.

The AEM provides the opportunity to set up the periodicity and the time of day (cf. Table 7-11) to perform a stand-by card test on:

- the stand-by COMDAC.

NOTE:
Stand-by card test scheduling can be executed only via TL1 command.

7.4.1.3.1 Test scheduling via TL1 commands

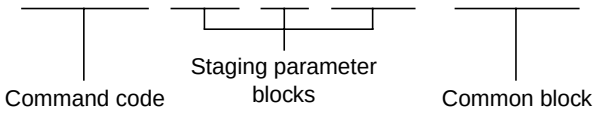
Procedure

Proceed as follows to define the test scheduling via TL1 command:

Step	Procedure

1. Enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.5.18):

```
SCHED-EX:[tid]:AID:[ctag]::INVL,STM
```



The SCHED-EX (Schedule-Exercise) command instructs the system to set up an exercise schedule (exercise interval and start time of the day of exercise) to perform a COMDAC side switch or off-line diagnostics for the stand-by COMDAC.

Parameters in the common block

The parameters in the common block have the following meaning:

Table 7-11 Common block parameters for SCHED-EX

Parameter	Meaning	Format	Possible Values
INVL (Interval)	Periodicity: The number of days between two stand-by card tests.	x-DAY	x=1 ... 365
STM (Start time)	The time of day when stand-by card tests shall be performed.	hh-mm	hh=0 ... 23 (hour-of-day) mm=0 ... 59 (minute-of-hour).

Please refer to the network element documentation for a detailed description of TL1 commands (including an explanation of the input format, restrictions, error conditions etc.).

Result

Depending on the stand-by card test result the following behaviour can be observed:

- If the test is successful the side switch will be performed.
- If the test fails no side switch will be performed. Additionally an alarm will be raised in this case.

7.4.1.4 Built-in self-test

Test request

Each NE performs a built-in self-test of plug-ins periodically.

NOTE:
The built-in self-test is not requested from the AEM, it will always be started from the NE!

Procedure

If a failure occurs, the NE will raise an alarm (*REPT-ALM*) which contains the AID of the failed pack. The alarm is then visible in the Alarm Viewer of the AEM. For more information about possible alarms see Chapter 7.5.5, page 7-53 (describes AEM alarms) or refer to the network element documentation (describes NE alarms).

7.4.1.5 TAP test

This command starts a test access point wiring consistency test which checks the TAP-B I/F and the correct cabling between the CIU and the test AP. This test is only allowed without an active test session.

The AEM automatically creates a line test entity when the TAP100 is equipped and provisioned.

NOTE:
The TAP test can be executed via GUI and via TL1 command.

7.4.1.5.1 TAP test via GUI

Procedure

Proceed as follows to start a TAP test and view the test result:

Step	Procedure
1.	Select ***NE -> Main Shelf -> TAP100*** in the Network Element Browser and ***View*** via the cursor menu or select ***View -> Object*** via the menu bar or single-click on ***TAP*** in the *Shelf View* window. The *TAP AP* window pops up. This window can also be reached from the *Common AP* window by provisioning a slot not yet provisioned (cf. Chapter 5.5.5.11).

2. Click on ***TAP Test...***. An *In Progress* window pops up showing the following message:

   `TAP Test execution in progress on <NE Name>, <Slot Id>, Provisioned Apparatus Code.`

3. Wait until the *TAP Test Result* window (cf. Figure 7-11, page 7-34) appears and view the test result.

Test result

The *TAP Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

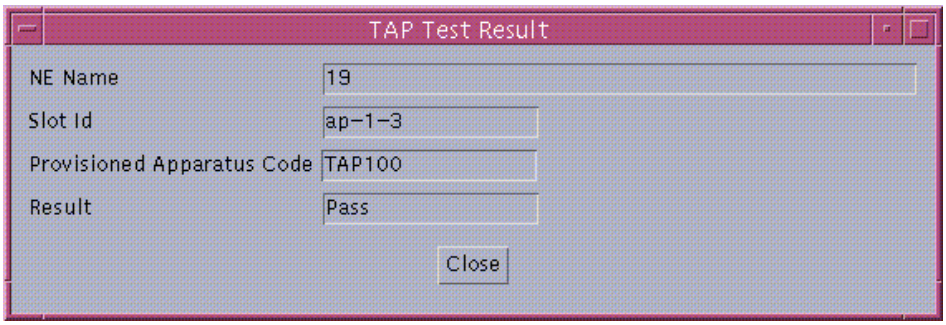


Figure 7-11 TAP Test Result window

The following table describes the parameters of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters) as specified at NE creation time.
Slot Id	This field shows the slot number of the AP being used. Possible values: ap-1-{1, 16}.
Provisioned Apparatus Code	This code identifies the type of the provisioned card (TAP100).
Result	This field displays the result of the test routines. Possible values: PASS or FAIL.

4. Click on **Close** to exit the *TAP Test Result* window.

7.4.1.6 CRC test (ISDN drop)

This command starts a CRC test procedure for the specified ISDN drop (ISDN BRA and DLL). The CRC test procedure checks the proper functionality of the CRC generator and detector for the specified time period.

Precondition

Before the CRC test can be started an ISDN telephone must be connected to the port which shall be tested.

NOTE:
The CRC test can be executed via GUI and via TL1 command.

7.4.1.6.1 CRC test via GUI

Procedure

Proceed as follows to start a CRC test and view the test result:

Step	Procedure
1.	Open one of the following windows: ■ *PSTN/ISDN AP* window (cf. Chapter 5.5.5.13) ■ *DLL User Port* window (cf. Chapter 6.2.8.4.1) ■ *V5 ISDN BA User Port* window (cf. Chapter 6.2.8.5.1).
2.	Select the physical port where you intend the test to run.
3.	Use the option menu in the **Test Management** field to select CRC Test and click on ***Apply***. The *CRC Test* window pops up.

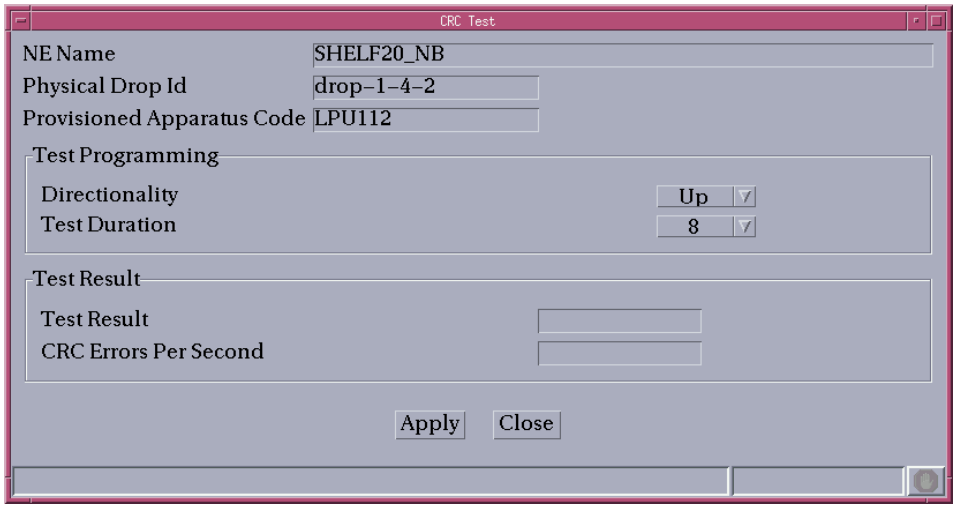


Figure 7-12 CRC Test window

The following table describes the options of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters) as specified at NE creation time.
Slot Id	This field shows the slot number of the AP being used. Possible values: ap-1-{1, 16}.
Provisioned Apparatus Code	This code identifies the type of the provisioned card (LPU112).
Port id	This field shows the drop within the provisioned AP. Possible values: drop-1-{1, 16}-{1, 32}.
Test Programming	The option menu **Directionality** can be used to define the direction of the test. Possible values: Up, Down. The option menu **Test Duration** can be used to define the test duration in seconds. Possible values: {1, 15}.
Test Results	The field **Test Results** shows the test result (FAIL or PASS). The field **CRC Errors Per Second** shows the number of detected CRC errors per second for the selected direction. Possible values: {0, 100}.
Apply	This button is used to confirm the CRC test execution.

4. Use the option menus in the field **Test Programming** to define the test parameters.

5. Click on ***Apply*** to start the CRC test execution.

   After starting the CRC test execution a *Warning* window pops up showing the following message:

   CRC Test may be service affecting. Do you want to continue?

   After confirming this warning the following *In Progress* message pops up:

   CRC Test execution in progress on <NE Name>, <Slot Id>, <Provisioned Apparatus Code>, <Port id>.

6. Wait until the *CRC Test* window appears (cf. Figure 7-12, page 7-35) and view the test result.

7.4.1.7 Single pulse test

Purpose

Used to start and stop a single pulse test procedure for the specified drop (ISDN BRA and DLL). This enables e.g. the craft personal in the field to identify the subscriber line with external measurement equipment.

NOTE:
The single pulse test can be executed only via TL1 command.

7.4.1.7.1 Single pulse test via TL1 command

Procedure

Proceed as follows to start/stop the single pulse test via TL1 command:

Step	Procedure

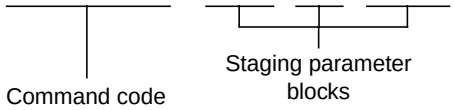
1. Enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.5.18) to start the single pulse test:

```
SND-SP:[tid]:AID:[ctag];
```

The *Warning* window followed by the *In Progress* window pops up as described above.

2. Enter the following TL1 command to stop the single pulse test

```
RMV-SP:[tid]:AID:[ctag];
```



7.4.1.8 Loopback test on the feeder side

It is possible to set or clear a loopback on particular feeders.

NOTE:
Executing a loopback test on an E1 feeder which is used for managing the NE (ROC over PLL) results in loss of the management connection. The connection can be re-established only via GSI using the serial line of the CIU connector (TL1 command: RLS-LPBK-E1::e1-1-{1, 4}-{1, 4}:; where e1-1-{1, 4}-{1, 4} has to be replaced by the corresponding feeder id).

To avoid the loss of the management connection please make sure that the feeder you intend to test is not the feeder of the management interface. Use the TL1 command "RTRV-ROC::[AID]:;" via GSI... or the cut-through connection from the AEM to find out if the feeder is associated to the leased line roc interface.

Procedure

Proceed as follows to set/clear an E1 loopback:

Step	Procedure
1.	Select ***NE -> Main Shelf -> FAC500 -> E1 Feeder*** in the Network Element Browser and ***Edit*** via the cursor menu or select ***View -> Object*** via the menu bar. The *Physical Feeder* window pops up.
2.	Select the physical feeder where you intend the test to run.
3.	Click on ***Set/Clear*** to change the loopback state. If the loopback setting is service affecting a *Warning* window pops up: **`Setting Loopback for a feeder can be service affecting. Do you want to continue?`**
4.	Enter ***y*** and press ***Return*** to confirm.

7.4.1.9 Loopback test on the ISDN user port side

It is possible to set or clear a loopback on an ISDN drop (ISDN BRA and DLL).

7.4.1.9.1 Loopback test on the ISDN user port side via GUI

Procedure Proceed as follows to set/clear a loopback test on the ISDN user port side:

Step	Procedure
1.	Open one of the following windows: ■ *DLL User Port* window (cf. Chapter 6.2.8.4.1) ■ *V5 ISDN BA User Port* window (cf. Chapter 6.2.8.5.1).
2.	Select the drop where you intend the test to run.
3.	Use the option menu **Loopback Selection** to define the desired loopback state and click on ***Set*** to confirm. If the change is service affecting a *Warning* window pops up: **`Setting Loopback for a user port can be service affecting. Do you want to continue?`**
4.	Enter ***y*** and press ***Return*** to confirm.

7.4.1.10 Restart PSTN protocol

Procedure Proceed as follows to restart the PSTN protocol:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu or select ***View -> Network Interface List*** via the menu bar. The *V5 Interfaces List* window pops up.
2.	Select the desired V5 interface in the **V5 Interface List** field and click on ***Edit V5 Interface***. The *V5 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2.1).
3.	Select the V5 interface id and click on ***Restart PSTN Protocol***. A *Warning* window pops up showing the following message: **`Restart PSTN Protocol may be service affecting. Do you want to continue?`**
4.	Enter ***y*** and press ***Return***. The following *In Progress* message pops up: **`Restart PSTN Protocol execution in progress on <NE Name>, <V5 Interface Id>.`**
5.	Wait until the *Restart PSTN Protocol* window appears and view the test result in the field **Operation Results**. Possible values: PASS, FAIL.

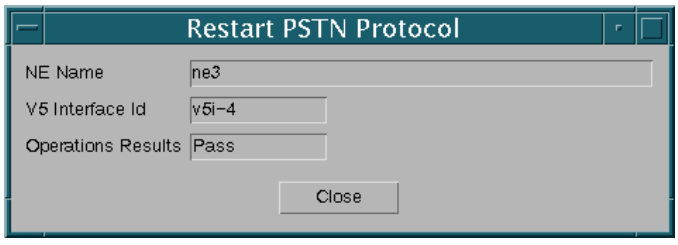


Figure 7-13 Restart PSTN Protocol window

6. Click on **Close** to exit the window.

7.4.1.11 Provisioning variant test

Procedure Proceed as follows to execute the provisioning variant test:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> V5 Interface*** via the cursor menu or select ***View -> Network Interface List*** via the menu bar. The *V5 Interfaces List* window pops up.
2.	Select the desired V5 interface in the **V5 Interface List** field and click on ***Edit V5 Interface***. The *V5 Interface* window (tab V5 Interface Data) pops up (cf. Chapter 6.2.1.2.1).
3.	Select the V5 interface id and click on ***Provisioning Variant Test***. A *Warning* window pops up showing the following message: **`Provisioning Variant Test may be service affecting. Do you want to continue?`**
4.	Enter ***y*** and press ***Return***. The following *In Progress* message pops up: **`Provisioning Variant Test execution in progress on <NE Name>, <V5 Interface Id>.`**
5.	Wait until the *Provisioning Variant Test* window appears and view the test result in the field **Test Results**. Possible values: PASS, FAIL, TIMEOUT.

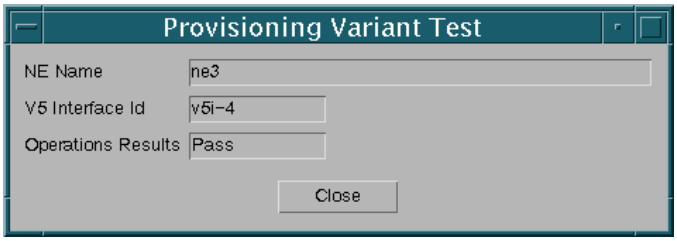


Figure 7-14 Provisioning Variant Test window

6. Click on **Close** to exit the window.

7.4.1.12 V5.2 link identification test

Proceed as follows to execute the V5.2 link identification test:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***List -> Physical Feeder*** via the cursor menu. The *Physical Feeder List* window pops up (cf. Chapter 6.2.3).
2.	Select a feeder (with an associated V5 link) in the list, use the option menu near the ***Edit Logical Link...*** button to select **V5 Link** and click on ***Edit Logical Link...***. The *V5 Link* window pops up (cf. Chapter 6.2.5).
3.	Click on ***V5.2 Link Identification Test*** in the **V5 Link Information** field. A *Warning* window pops up showing the following message: **`V5.2 Link Identification Test may be service affecting. Do you want to continue?`**
4.	Enter ***y*** and press ***Return***. The following *In Progress* message pops up: **`V5.2 Link Identification Test execution in progress on <NE Name>, <V5 Interface Id>.`**
5.	Wait until the *V5.2 Link Identification Test Result* window appears and view the test result in the field **Test Results**. Possible values: PASS, FAIL, TIMEOUT, REJECTED.

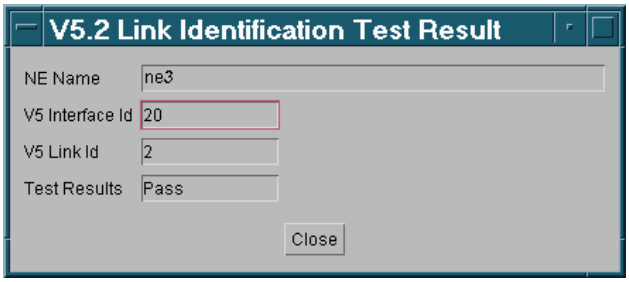


Figure 7-15 V5.2 Link Identification Test Result window

6. Click on **Close** to exit the window.

7.4.2 Data tests

7.4.2.1 ADSL test list

Procedure Proceed as follows to view the ADSL test list:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Lists -> ADSL Test*** via the cursor menu. The *ADSL Test List* window pops up.

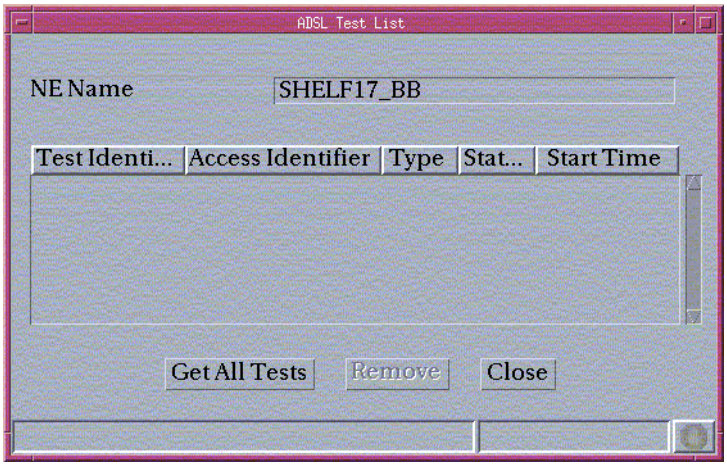


Figure 7-16 ADSL Test List window

This window lists all the tests stored in the data agent. In this window it is possible to delete stored tests.

The following table shows the parameters of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Table	This table shows all tests currently stored in the data agent. The table is sorted by entities. ■ **Test Identifier:** Indicates the test identifier inside the AFM (test number). ■ **Access Identifier**: Indicates the object for which the test has been executed. ■ **Type**: Indicates the test type which has been executed. Possible values: CRC test, BIST (Built-in shelf-test), LED test. ■ **Status (Result)**: Indicates the status of the test. Possible values: In_Progress, Passed, Could not be started, Passed with warning, Aborted. ■ **Start Time**: Indicates the date and time when the test was started.
Command buttons	The ***Get Test List*** button is used to display the list above. The ***Remove*** button can be used to remove a test from the list in the data agent. It is enabled only if a test has been selected.

2. Click on ***Get Test List*** to display the list of the ADSL tests stored in the data agent.

3. Select an entry in the test list and click on ***Remove*** to remove a test from the list or proceed with step 4.

4. Click on ***Close*** to exit the window.

NOTE:
If a test is already running (status In_Progress) a new start (ADSL corrupted CRC test - cf. Chapter 7.4.2.2, page 7-45; ADSL BIST test - Chapter 7.4.2.3, page 7-47) of the same kind of test will provoke a warning:

If the text exists in the table remove it and launch the test again.

7.4.2.2 ADSL corrupted CRC test

Procedure Proceed as follows to set up an ADSL corrupted CRC test:

Step	Procedure
1.	Open one of the following windows: ■ *ADSL AP* window (cf. Chapter 5.5.5.27) ■ *ADSL Drop* window (cf. Chapter 5.5.5.29).
2.	Use the option menu near the ***Apply*** button to select **Corrupted CRC Test** and click on ***Apply***. The *ADSL Corrupted CRC Test* window pops up:

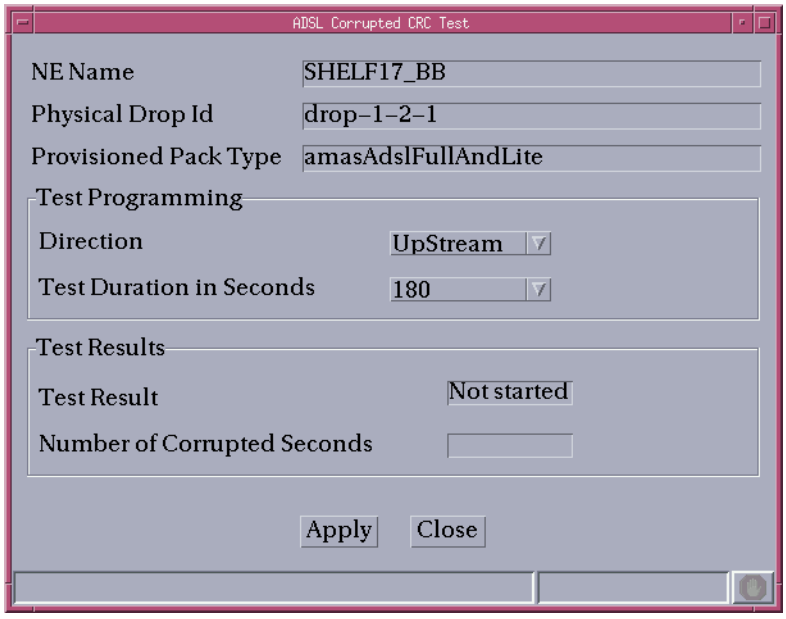


Figure 7-17 ADSL Corrupted CRC Test window

The following table shows the parameters of this window:

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop Id	This field shows the port of the drop affected by the test. Possible values: drop-1-{1, 15}-{1, x}/ subdrop-{1, 8}-{1, 8}-{1, x}. x is the number of drops, supplied by the server.

Parameters/ Buttons	Description
Provisioned Pack Type	This code identifies the type of the provisioned pack. Possible value: ADSL.
Test Programming	**Directionality**: This option menu is used to define the direction of the test. Possible values: Upstream, Downstream. **Test Duration in Seconds**: This option menu is used to define the test duration in seconds. Possible values: {0, 511}.
Test Results	**Test Results**: This field shows the test result. Possible values: PASS, PASS-WARNING, FAIL, IN PROGRESS, ABORTED, NOT STARTED, INVALID TEST. **Additional Information**: This field shows additional information related to the CRC test. If the CRC has been passed the number of the detected CRC is displayed.
Apply	This button is used to execute the corrupted CRC test.

3. Use the option menus in the **Test Programming** field to define the test parameters and click on ***Apply***. The *In Progress* window pops up:

   `ADSL CRC Corrupted CRC Test executed on <NE Name>, <Drop Id> in progress.`

4. Wait until the test is finished and view the test result in the *ADSL Corrupted CRC Test* window (cf. Figure 7-17, page 7-45).

5. Click on ***Close*** to exit the window.

7.4.2.3 ADSL BIST test

Procedure Proceed as follows to set up an ADSL BIST test:

Step	Procedure
1.	Open one of the following windows: ■ *ADSL AP* window (cf. Chapter 5.5.5.27) ■ *ADSL Drop* window (cf. Chapter 5.5.5.29).
2.	Use the option menu near the ***Apply*** button to select **ADSL BIST Test** and click on ***Apply***. If the drop is in the unlocked administrative state a *Warning* window pops up (otherwise the *In Progress* window pops up - see below): **`Performing a BIST Test on ADSL drop may be service affecting. Do you want to continue?`**
3.	Enter ***y*** and press ***Return***. The *In Progress* window pops up: **`BIST Test executed on <NE Name>, <Drop Id> in progress.`**
4.	Wait until the *ADSL BIST Test Result* window appears and view the test result.

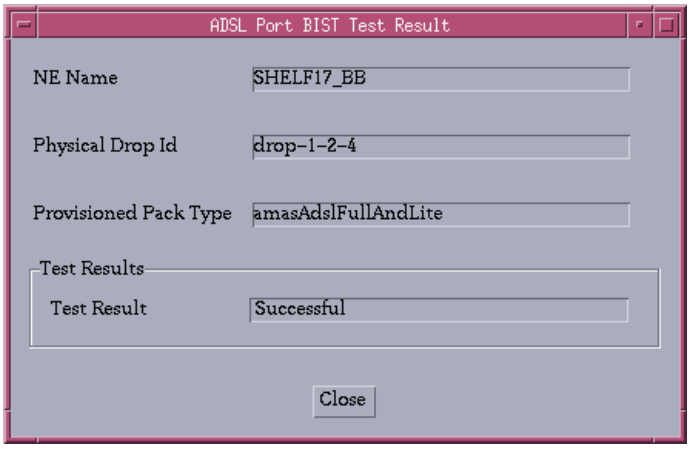


Figure 7-18 ADSL BIST Test Result window

The following table shows the parameters of this window

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Drop Id	This field shows the port of the drop affected by the test. Possible values: drop-1-{1, 15}-{1, x}/ subdrop-{1, 8}-{1, 8}-{1, x} x is the number of drops, supplied by the server.
Provisioned Pack Type	This code identifies the type of the provisioned pack. Possible value: ADSL.
Test Results	**Test Results**: This field shows the test result. Possible values: PASS, PASS-WARNING, FAIL, IN PROGRESS, ABORTED, NOT STARTED, INVALID TEST.

5. Click on ***Close*** to exit the window.

7.5 Alarms

7.5.1 Overview

An alarm is reported for any condition that needs user attention, since it may impact the normal operations of any system under user responsibility (e.g. AEM, NE).

7.5.2 Alarm types

Alarm classification

Detected alarms are classified as one of the following:

- Platform Alarm

  Alarm related to the AEM application or its hardware/software platform. Generated (raised) by any object of the AEM when it detects an abnormal condition to be reported to the user.

  Information provided:

  — Probable Cause

  — Severity

  — Service Affecting

  — AEM Object Identifier

  — Alarm Type Identifier

  — Occurrence Time.

- NE-AM Alarms

  Generated (raised) by the NE-AM. Refer to Chapter 7.2.5, page 7-7 to see how the information comes from the NE-AM to the AEM. The NE-AM alarms are classified in two groups:

  — Normal alarms

  Data provided:
  Access Identifier, Condition Type, Notification Code, Service Affecting, Access Identifier Type, Occurrence Date, Occurrence Time

  — Environment alarms

  Data provided:
  Access Identifier, Alarm Type, Notification Code, Occurrence Date, Occurrence Time.

For all alarm types several alarm data fields are conceptually the same (although they convey different values). For instance, both Condition Type and Alarm Type refer to the type of alarm being raised/cleared (Battery on discharge, Loss of frame, ...).

The following table maps all the equivalent fields to general names that uniquely identify a concept independently of the alarm type.

Table 7-12 General alarm fields

General Name	Platform Alarm	NE Alarm	NE Environment Alarm
Object_Id.	EM Object Identifier	Access Identifier	Access Identifier
Alarm_Type	Alarm Type Identifier	Condition Type	Alarm Type
Severity	Severity	Notification Code	Notification Code
Serv_Affec.	Service Affecting	Service Effect	-
Date_First_Time/ Date_Last_Time[a]	Occurrence Time and Date[a]	Occurrence Time[b]	Occurrence Time[b]
		Occurrence Date[c]	Occurrence Date[c]

a Time and date (YYYY-MM-DD HH-MM-SS)

b Only time (HH-MM-SS)

c Only date (MM-DD)

Alarm severities

For each alarm one of the following alarm severities is defined:

- Critical (CR)
- Major (MJ)
- Minor (MN)
- Warning (WR)
- Indeterminate (IN)
- Cleared (CL)

Alarm identification

The multiple key that uniquely identifies an alarm is:

- Host identifier

  Identifies where the alarm comes from. If it comes from an NE, then this identifier is the NE name. If the alarm is reported by the AEM the host identifier is "EM". For association alarms the host identifier is "NE_name".

- System object identifier

  Identifies the alarm-affected object within the host, which is identified by the host identifier. For association alarms the system object identifier is "ASSOC".

- General alarm identifier

  Unique identifier within each type of alarm.

In order to ease possible communication between different users, an index number is provided as a temporal alarm identification. It is temporal because the index number will be used as a circular sequence (the maximum sequence number is 100 000). It is provided only for user convenience. It will not be used to identify an alarm within the AMS. For this purpose the multiple key defined above has to be used.

7.5.3 Network element alarms

Alarm descriptions Please refer to the network element documentation for detailed alarm descriptions of network element alarms.

7.5.4 General element manager platform alarms

This chapter provides alarm descriptions of general AEM platform alarms including proposals for corrective maintenance actions.

Alphabetical order In the following the AEM platform alarms are listed alphabetically.

7.5.4.1 LOG_DEL_FULL

Meaning All old logs have been deleted. Because more available space was necessary the log type of the current day has been deleted, too. The Object_Id shows which log type has been deleted.

Abbreviation: LOG_DEL_FULL

Severity: Major

Service affecting: No

Effects There are no old logs available, and not all logs of the current day are available to be viewed or stored.

Possible cause(s) There may be a problem or abnormal situation in the AEM, or the selection of the configurable size limits of the log system was too small.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check the AEM for problems or abnormal situations. Have any problems or abnormal situations occurred? **Yes:** Try to resolve these problems or abnormal situations. If this is not possible, continue with step 2. **No:** Continue with step 2.
2.	Check the size limits of the log system. Are the size limits set correctly (cf. Chapter 3.7.2, page 3-46)? **Yes:** Call Lucent Technologies Technical Support. **No:** Set the size limits correctly, i.e. increase the size limits.

7.5.4.2 LOG_DEL_PART

Meaning A log type not yet archived has been deleted due to lack of available space.

Abbreviation: LOG_DEL_PART

Severity: Minor

Service affecting: No

Effects The respective log type can neither be viewed nor archived.

Possible cause(s) There may be a problem or an abnormal situation in the AEM, or the configurable size limits of the log system have not been chosen correctly.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Archive the remaining logs to prevent them from being deleted.
2.	Check the AEM for problems or abnormal situations. Have any problems or abnormal situations occurred? **Yes:** Try to resolve these problems or abnormal situations. If this is not possible, continue with step 3. **No:** Continue with step 3.
3.	Check the size limits of the log system. Are the size limits set correctly (cf. Chapter 3.7.2, page 3-46)? **Yes:** Call Lucent Technologies Technical Support. **No:** Set the size limits correctly, i.e. increase the size limits.

7.5.4.3 PRINT_ALARM

Meaning There are one or more problems blocking the printing jobs.

Abbreviation: PRINT_ALARM

Severity: Major

Service affecting: No

Effects It is not possible to print reports.

Possible cause(s) There may be a problem in the printer, the spoolers, the network or the AEM.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check if a default printer is defined.?
	Yes: Continue with step 2.
	No: Define a default printer.
2.	Check if the printer is working properly.
	Yes: Call Lucent Technologies Technical Support for checking the network or the AEM.
	No: Have the printer repaired.

7.5.5 Element manager alarms concerning network element

This chapter provides alarm descriptions of the AEM platform alarms concerning the data agent including proposals for corrective maintenance actions.

Alphabetical order In the following the AEM platform alarms are listed alphabetically.

7.5.5.1 ALARM_AO_NOT_PROCESS

Meaning The AEM is discarding the Alarm AOs coming from the telephony agent.

Abbreviation: ALARM_AO_NOT_PROCESS

Severity: Major

Service affecting: No

Effects The alarm data of the AEM does not match the alarm data of the telephony agent. The alarm synchronization state is moved to ASYNC.

Possible cause(s) Alarm buffer overflow detection.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Perform a manual alarm synchronization process to upload the alarm data and to start processing AOs.
2.	Is the alarm now cleared?
	Yes: O.K.
	No: Call Lucent Technologies Technical Support.

7.5.5.2 ALARM_EVENT_NOT_PROCESS

Meaning The AEM is discarding the alarm traps coming from the data agent.

Abbreviation: ALARM_EVENT_NOT_PROCESS

Severity: Major

Service affecting: No

Effects The alarm data of the AEM does not match the alarm data of the data agent.

Possible cause(s) Alarm buffer overflow.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Perform a manual alarm synchronization process to upload the alarm data and to start processing traps.
2.	Is the alarm now cleared? **Yes:** O.K. **No:** Call Lucent Technologies Technical Support.

7.5.5.3 COMM_DENIED

Meaning An unsuccessful reply has been detected when the AEM sends the request to establish a connection with the telephony agent.

Abbreviation: COMM_DENIED

Severity: Critical

Service affecting: No

The alarm will be cleared when the connection between the AEM and the telephony agent has been successfully established.

Effects It is not possible to manage the telephony agent.

Possible cause(s) The AEM is trying to establish the connection with an agent while its COMDAC initialization process is in progress.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check if the COMDAC is in the initialization process and wait until this process is finished.

7.5.5.4 COMMUNICATION_LOST

Meaning Communication with data agent lost.

Abbreviation: COMMUNICATION_LOST

Severity: Critical

Service affecting: No

Effects It is not possible to manage the data agent.

Possible cause(s) Heart beat messages are not responded to by the data agent.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct data agent state. **Yes:** Continue with step 2. **No:** Call Lucent Technologies Technical Support.
2.	Check for DCN being in service. **Yes:** Call Lucent Technologies Technical Support. **No:** Put the DCN into service.
3.	Is the alarm now cleared? **Yes:** O.K. **No:** Call Lucent Technologies Technical Support.

7.5.5.5 COMM_PROBLEM

Meaning The data agent does not respond the AEM while trying to establish a communication.

Abbreviation: COMM_PROBLEM

Severity: Critical

Service affecting: No

Effects It is not possible to manage the data agent.

Possible cause(s) Invalid IP address.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for DCN being in service.
	Yes: Continue with step 2.
	No: Put the DCN into service.
2.	Check the IP address of the data agent.
	Yes: Call Lucent Technologies Technical Support.
	No: Correct the IP address.
3.	Is the alarm now cleared?
	Yes: O.K.
	No: Call Lucent Technologies Technical Support.

7.5.5.6 COMM_RES_NOT_AVAILABLE

Meaning The communication between AEM and NE cannot be established.

Abbreviation: COMM_RES_NOT_AVAILABLE

Severity: Critical

Service affecting: No

Effects It is not possible to manage the NE.

Possible cause(s) The limit of connections that the AEM can manage has been reached.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Start new instances of the progress(es) in charge of communication management

7.5.5.7 CONFIG_AO_NOT_PROCESS

Meaning The AEM is discarding the configuration AOs coming from the telephony agent.

Abbreviation: CONFIG_AO_NOT_PROCESS

Severity: Major

Service affecting: No

Effects The configuration data of the AEM does not match the configuration data of the telephony agent. The configuration data synchronization state is moved to ASYNC.

Possible cause(s) Configuration buffer overflow.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Perform a manual configuration synchronization process to upload the configuration data and to start processing AOs.
2.	Is the alarm now cleared? **Yes:** O.K. **No:** Call Lucent Technologies Technical Support.

7.5.5.8 CONFIG_EVENT_NOT_PROCESS

Meaning The AEM is discarding the configuration traps coming from the data agent.

Abbreviation: CONFIG_EVENT_NOT_PROCESS

Severity: Major

Service affecting: No

Effects The configuration data of the AEM does not match the configuration data of the data agent.

Possible cause(s) Configuration buffer overflow.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Perform a manual configuration synchronization process to upload the configuration data and to start processing traps.
2.	Is the alarm now cleared? **Yes:** O.K. **No:** Call Lucent Technologies Technical Support.

7.5.5.9 CX_CONN_NOT_VISIBLE

Meaning Some cross-connections in the AFM are not visible.

Abbreviation: CX_CONN_NOT_VISIBLE

Severity: Minor

Service affecting: No

Effects There are cross-connections in the data agent which cannot be managed by the AEM.

Possible cause(s) There are cross-connections in the AFM associated to non-provisioned ports. This kind of cross-connections are ignored by the AEM upload procedure and therefore they are not visible in the AEM.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Use the CIT or the MIB browser to provision the needed APs or to remove the affected cross-connections.
2.	Request a resynchronization after AP provisioning.

7.5.5.10 INVALID_MIB_IDENTIFIER

Meaning The data agent to communicate with is not a valid data agent.

Abbreviation: INVALID_MIB_IDENTIFIER

Severity: Critical

Service affecting: No

Effects It is not possible to start the communication with the data agent.

Possible cause(s) The sysObjectId MIB variable retrieved from the data agent is not valid.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check the IP address of the data agent.

Yes: Continue with step 2.

No: Correct the IP address.

2. Check for correct sysObjectId MIB variable.

   Yes: Call Lucent Technologies Technical Support.

   No: Correct the IsysObjectId MIB variable.

3. Is the alarm now cleared?

   Yes: O.K.

   No: Call Lucent Technologies Technical Support.

7.5.5.11 NB_ASSOC_FAILED

Meaning The communication association with the telephony agent has failed.

Abbreviation: NE_ASSOC_FAILED

Severity: Critical

Service affecting: No

This alarm covers the following alarms:

- TCP/IP_CON_REFUSED (cf. Chapter 7.5.5.15, page 7-62)
- TL1_COMM_DENIED (cf. Chapter 7.5.5.15, page 7-62)
- NB_ASSOC_LOST (cf. Chapter 7.5.5.12, page 7-59).

NOTE:
This alarm is only used in NBI applications.

7.5.5.12 NB_ASSOC_LOST

Meaning The AEM lost the management association with the telephony agent.

Abbreviation: NEASSOC_LOST

Severity: Critical

Service affecting: No

The alarm will be cleared when the TCP/IP connection and TL1 communication session are available, and the software version currently stored in the NE is supported by the AEM, i.e. when the association process between the AEM and the NE is completed (NE state is **CONNECTED**).

Effects It is not possible to manage the telephony agent. The TL1 communication session and the TCP/IP connection are lost.

Possible cause(s) A loss of the TCP/IP connection has been detected, or the TCP/IP connection has been closed as a consequence of a loss of the TL1 communication session.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure

1. Check the telephony agent state after a waiting period of 1 minute.

   Comment: When the NE state is CONNECTED and the TCP/IP connection is lost or closed, the NE state is moved to TRYING and the loop process to re-establish the connection with the NE is started by the AEM.

   Is the state CONNECTED?

   Yes: O.K.

   No: Continue with step 2.

2. Check for Data Communication Network (DCN) being in service.

   Is the DCN in service?

   Yes: Call Lucent Technologies Technical Support.

   No: Put the DCN into service.

7.5.5.13 SW_VR_ILLEGAL

Meaning The software version currently stored in the agent is not supported by the AEM.

Abbreviation: ILLEGAL_SW_VERSION

Severity: Critical

Service affecting: No

Effects It is not possible to manage the agent. Agent software version is not supported.

Possible cause(s) The software version currently stored in the agent is not supported by the AEM, or the AEM is trying to establish the communication with a agent while its COMDAC/AFM initialization process is in progress.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure

1. Check that the correct version of software is installed on the agent's system controller card.

   Yes: Continue with step 2.

   No: Install the correct SW version.

2. Check if the COMDAC/AFM is in the initialization process, and wait until this process has finished.

3. Is the alarm now cleared?

Yes: O.K.

No: Call Lucent Technologies Technical Support.

7.5.5.14 TCP_IP_CON_REFUSED

Meaning

The TCP/IP connection establishment could not be completed successfully for port numbers 11002, 11004, 11006 and 11008.

Abbreviation: TCP_IP_CON_REFUSED

Severity: Critical

Service affecting: No

Effects

It is not possible to manage the telephony agent.

Possible cause(s)

Some TCP/IP protocol errors stopped the connection establishment process between the AEM and the telephony agent.

Corrective actions

Proceed as follows to clear the alarm:

Step	Procedure

1. Check the TCP/IP communication addresses.

   Are the TCP/IP communication addresses correct?

   Yes: Continue with step 2.

   No: Correct the addresses. Continue with step 4.

2. Check the gateway telephony agent identification.

   Is the gateway telephony agent identification correct?

   Yes: Continue with step 3.

   No: Correct the identification. Continue with step 4.

3. Check the DCN.

   Is the DCN in service?

   Yes: Continue with step 4.

   No: Bring the DCN into service.

4. Is the alarm now cleared?

   Yes: O.K.

   No: Call Lucent Technologies Technical Support.

7.5.5.15 TL1_COMM_DENIED

Meaning User login for a TL1 communication session was denied by the telephony agent for all TCP/IP connections opened.

Abbreviation: TL1_COMM_DENIED

Severity: Critical

Service affecting: No

The alarm will be cleared when a TL1 communication session between the AEM and the telephony agent has been successfully opened.

Effects It is not possible to manage the telephony agent because there is no TL1 communication session available.

Possible cause(s) A user login error is stopping the TL1 communication session establishment process between the AEM and the telephony agent.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct user identification (user login), password and telephony agent target identifier (TID).
2.	Check with the GSI that the four VCs in the telephony agent are not busy (RTRV-STATUS TL1 command).

7.5.5.16 UNABLE_TO_SYNC_ALARM

Meaning The Alarm Synchronization process has failed "n" times.

Abbreviation: UNABLE_TO_SYNC_ALARM

Severity: Major

Service affecting: No

Effects An updated view of the alarm data of the data agent cannot be uploaded.

Possible cause(s) The communication with the data agent may be interrupted.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct data agent state.
	Yes: Continue with step 2.
	No: Call Lucent Technologies Technical Support.
2.	Check for DCN being in service.
	Yes: Call Lucent Technologies Technical Support.
	No: Put the DCN into service.
3.	Is the alarm now cleared?
	Yes: O.K.
	No: Call Lucent Technologies Technical Support.

7.5.5.17 UNABLE_TO_SYNC_CONFIG

Meaning The Configuration Synchronization process has failed "n" times.

Abbreviation: UNABLE_TO_SYNC_CONFIG

Severity: Major

Service affecting: No

Effects An updated view of the configuration data of the data agent cannot be uploaded.

Possible cause(s) The communication with the data agent may be interrupted.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct data agent state.
	Yes: Continue with step 2.
	No: Call Lucent Technologies Technical Support.
2.	Check for DCN being in service.
	Yes: Call Lucent Technologies Technical Support.
	No: Put the DCN into service.

3. Is the alarm now cleared?

Yes: O.K.

No: Call Lucent Technologies Technical Support.

7.5.5.18 UPLOAD_PROBLEM

Meaning Some configuration data have been lost during synchronization.

Abbreviation: UPLOAD_PROBLEM

Severity: Critical

Service affecting: No

Effects Some configuration data are not available in the AEM database.

Possible cause(s) AFM problem.

Corrective actions Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct AFM configuration.

7.5.6 Correlated alarms

Introduction The following table contains a list of AEM alarms triggered by alarms from the telephony or/and data agent.

Example The **POLL** alarm from the telephony agent as well as the **amasAFMAPNoResponseAlarmCS** alarm from the data agent effects the **DUP_NO_RESP_POLL** alarm in the AEM.

Table 7-13 Correlated alarms

Probable cause	Summary	Severity	Service affecting	Object_Id	Description
POLL	not responding to poll	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
amasAFMAPNoResponseAlarmCS	AP not responding to AFM poll	Major, Minor	yes	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
DUP_NO_RESP_POLL	not responding to poll	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	AP: pack not responding to poll
INT	internal hardware failure	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
amasAFMPackFailAlarmCS	AP self test pack failure reported	Major, Minor	yes	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
amasAFMAPFailAlarmCS	AFM self test pack failure reported	Major, Minor	yes	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
DUP_PACK_FAIL	internal hardware failure	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	AP self test pack failure reported
PRCDERR	procedural error	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	illegal/unknown pack in AP slot
amasUnknownPackType	unknown pack detected	Minor	no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
DUP_PACK_MISMATCH	incompatible pack type	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	illegal pack in AP slot
IMPROPRMVL	improper removal	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	missing pack in AP slot
amasAFMPackRemovedAlarmCS	AP has been removed	Minor	yes	ap-1-{1, 16} subap-{1, 8}-{1, 8}	
DUP_PACK_RMVL	pack removal	Major, Minor	yes, no	ap-1-{1, 16} subap-{1, 8}-{1, 8}	missing pack in AP slot

Table 7-13 Correlated alarms

Probable cause	Summary	Severity	Service affecting	Object_Id	Description
PRCDERR	mismatch of logical sub-shelf number	Critical	yes	subsh-{1, 8}	
amasSubShelfAssocia-tionMismatchAlarm	association mismatch re-ported	Major	yes	subsh-{1, 8}	
DUP_SUBSHELF_MISMATCH	incompatible subshelf type	Critical	yes	subsh-{1, 8}	illegal subshelf type in parent slot

Performance monitoring

8

Contents

8.1 Overview 8-1

8.2 ADSL performance monitoring data 8-1

8.2.1 ADSL Performance Monitoring Data window 8-2

8.2.2 Modify the ADSL performance monitoring 8-5

8.3 AFM feeder performance monitoring 8-6

8.3.1 AFM Performance Monitoring window 8-6

8.3.2 Modify the AFM performance monitoring 8-7

8.4 ATM traffic monitoring 8-9

8.4.1 ATM Traffic Monitoring window 8-9

8.4.2 Modify the ATM traffic monitoring 8-10

Contents

Performance monitoring

8

8.1 Overview

This chapter provides you with informations about

- ADSL performance monitoring
- AFM feeder performance monitoring
- ATM traffic monitoring.

It describes the collection, display, logging and threshold reporting for performance monitoring (PM) and traffic measurements counts.

8.2 ADSL performance monitoring data

The AEM is able to retrieve the ADSL performance monitoring counts from the NE via FTP. The interval data are retrieved and stored every 15 minutes the day data are retrieved and stored every 24 hours from each enabled NE.

The data are stored per day in a separate log file (AdslLineStatisticsLog_YYYYMMDD; where YYYY = year, MM = month and DD = day) located in $ANYMEDIAPATH/log. The file contains also hints about start logging, stop logging and error messages.

8.2.1 ADSL Performance Monitoring Data window

This window is used to display all ADSL performance monitoring parameter. This window also allows to select data collection or clear counters of either the selected ADSL drop or all the ADSL drops in the NE. Because there are performance monitoring data by each ADSL drop there are three option menus to select the ADSL drop.

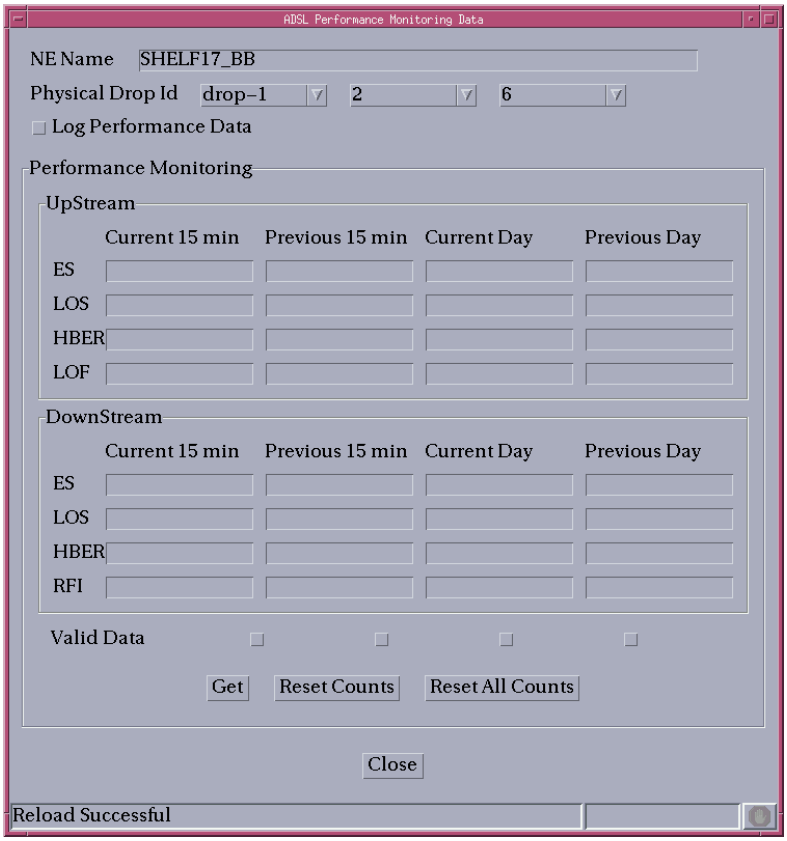


Figure 8-1 ADSL Performance Monitoring Data window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).

Parameters/ Buttons	Description
Physical Drop Id	These fields display the ADSL drop id by means of three option menus: ■ The first one contains the drop shelf Format: drop-1 or subdrop-{1, 8}. None is also allowed. ■ The second one contains the slot number inside the NE, but only for slots in which an ADSL pack is provisioned. Format: {1, 16} for main shelf or {1, 8} for subshelf. None is also allowed. ■ The third one contains the drop number inside the slot indicated in the previous list {1, x}. Format: drop-shelf-slot-port. Possible values: drop-1-{1, 16}-{1, x} or subdrop-{1, 8}-{1, 8}-{1, x}. None is also allowed. (x is the number of drops, supplied by the server).
Log Performance Data	This check box can be used to define whether the AEM is collecting and logging the performance monitoring data for all the ADSL drops in the NE or not.

Parameters/ Buttons	Description
Performance Monitoring	**Upstream**: Four text fields show the values for four different time periods (Current 15 minutes, Previous 15 minutes, Current day, Previous day). ■ **PSES (P-bit Severely Errored Second)**: Possible values: 1... 900 for 15 minutes, 1... 86400 for one day. ■ **LOS (Loss of Signal)**: Possible values: 1 ... 90 for 15 minutes, 1 ... 8640 for one day. ■ **HBER (High Bit Error Rate)**: Possible values: 1... 90 for 15 minutes, 1... 8640 for one day. ■ **LOF (Loss of Frame)**: Possible values: 1... 90 for 15 minutes, 1... 8640 for one day. **Valid Data**: Four check boxes show whether the data for the time period are valid or not. **Downstream**: Four text fields show the values for four different time periods (Current 15 minutes, Previous 15 minutes, Current day, Previous day). ■ **PSES**: Possible values: 1... 900 for 15 minutes, 1... 86400 for one day. ■ **LOS (Loss of Signal)**: Possible values: 1... 90 for 15 minutes, 1... 8640 for one day. ■ **HBER (High Bit Error Rate)**: Possible values: 1... 90 for 15 minutes, 1... 8640 for one day. ■ **RFI (Remote Failure Indication)**: Possible values: 1... 90 for 15 minutes, 1... 8640 for one day. **Valid Data**: Four check boxes show whether the data for the time period are valid or not. The ***Get*** button is used to retrieve the PM data of the selected drop. The ***Reset Counts*** button can be used to restart the performance monitoring of the selected drop. The ***Reset All Drops Counts*** button can be used to restart the performance monitoring of all ADSL drops within the NE.

8.2.2 Modify the ADSL performance monitoring

Procedure

Complete the following procedure to modify the ADSL performance monitoring:

Step	Procedure

1. Select ***NE*** in the Network Element Browser and ***Performance -> ADSL*** via the cursor menu
or click on the ***ADSL PM Data*** button in the *ADSL Drop* window.
The *ADSL Performance Monitoring Data* window pops up.

2. Use the option menus **Physical Drop Id** to select the desired ADSL drop.

3. Use the check box **Log Performance Data** to define whether the monitoring data should be logged or not.

If you want to ...	then ...
retrieve the performance monitoring data	click on ***Get***.
restart the monitoring data counter for the selected drop	click on ***Reset Counts***.
restart the monitoring data counters for all drops within the NE	click on ***Reset ALL Drops Counts***.
exit the window	click on ***Close***.

8.3 AFM feeder performance monitoring

The AFM feeder performance monitoring consists of retrieving, displaying, provisioning and storing DS3/E3 performance measurements detected by the AFM.

The AEM is able to retrieve the DS3/E3 performance monitoring counts from the NE. The interval data are retrieved and stored every 15 minutes the day data are retrieved and stored every 24 hours from each enabled NE. The 24 hour data for feeders is updated every 15 minutes in the AFM.

The data are stored per day in a separate log file (AdslDsxE3StatisticsLog_YYYYMMDD; where YYYY = year, MM = month and DD = day) located in $ANYMEDIAPATH/log. The file contains alsohints about start logging, stop logging and error messages.

8.3.1 AFM Performance Monitoring window

This window displays the AFM performance monitoring parameter of the selected feeder. This window also allows to select data collection (for all the feeders in the NE) or clear counters of one feeder.

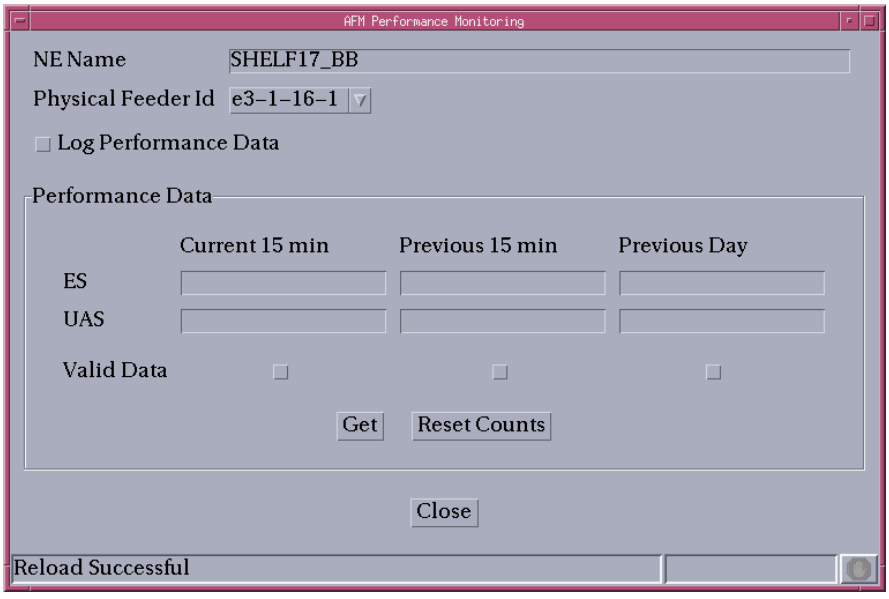


Figure 8-2 AFM Performance Monitoring window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Physical Feeder Id	This option menu can be used to select an appropriate feeder. Possible values: ds3-1-{1, 16}-{1, 2}/e3-1-{1, 16}-{1, 2}.
Log Performance Data	This check box can be used to define whether the AEM is collecting and logging the performance monitoring data for all the feeders in the NE or not.
Performance Data	Three text fields show the values for three different time periods (Current 15 min, Previous 15 min, Previous Day). ■ **ES (Errored Second)**: Possible values: 1 .. 900 for 15 minutes, 1 ... 86400 for one day. ■ **UAS (Unavailable Second)**: Possible values: 1 ... 900 for 15 minutes, 1 ... 86400 for one day. **Valid Data**: Three check boxes show whether the data for the time period are valid or not.
Get	This button is used to retrieve the performance monitoring data of the selected feeder.
Reset Counts	This button can be used to restart the performance monitoring data of the selected feeder.

8.3.2 Modify the AFM performance monitoring

Procedure

Complete the following procedure to modify the AFM performance monitoring:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Performance -> Feeder*** via the cursor menu or click on the ***PM Data*** button in the *AFM Feeder* window. The *AFM Performance Monitoring Data* window pops up.
2.	Use the option menu **Physical Feeder Id** to select the desired feeder.
3.	Use the check box **Log Performance Data** to define whether the monitoring data should be logged or not.

If you want to ...	then ...
retrieve the performance monitoring data	click on ***Get***.

If you want to ...	then ...
restart the monitoring data counter for the selected feeder	click on ***Reset Counts***.
exit the window	click on ***Close***.

8.4 ATM traffic monitoring

Limited ATM traffic measurements for cells received on the ATM feeder are collected by the AFM.

The AEM is able to display/clear the ATM cell traffic data. Interval data are retrieved and stored every 15 minutes from each enabled NE.

The data are stored per day in a separate log file (AdslATMStatisticsLog_YYYYMMDD; where YYYY = year, MM = month and DD = day) located in $ANYMEDIAPATH/log. The file containsalso hints about start logging, stop logging and error messages.

8.4.1 ATM Traffic Monitoring window

This window is used to display all ATM cell traffic data. It also allows to select data collection or to clear the counter.

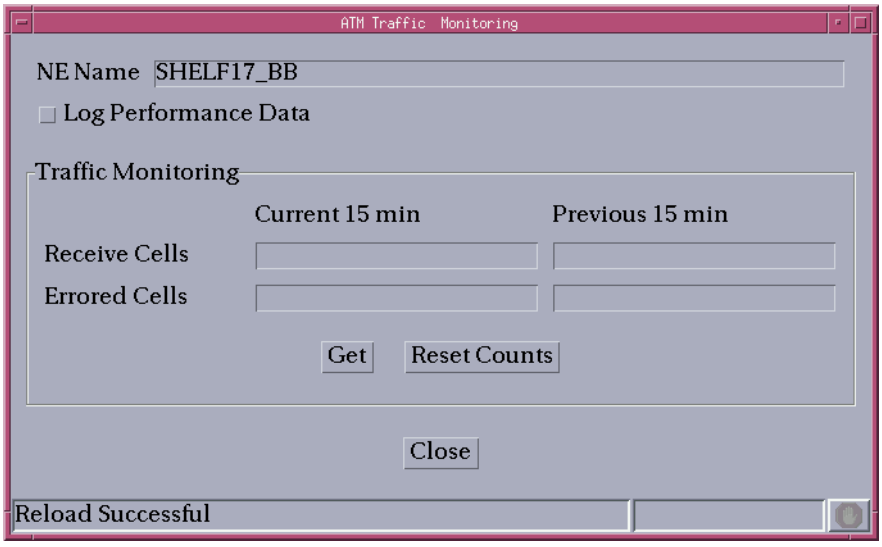


Figure 8-3 ATM Traffic Monitoring window

The following table shows the view/edit options of this window.

Parameters/ Buttons	Description
NE Name	NE name of the selected NE (max. 30 characters).
Log Performance Data	This check box can be used to specify whether the AEM is collecting and logging the traffic monitoring data in the NE or not.

Parameters/ Buttons	Description
Traffic Monitoring	Two text fields show the values for two different time periods (Current 15 min, Previous 15 min). ■ **Receive Cells**: Possible values: 0...800 000 000. ■ **Errored Cells**: Possible values: 0...800 000 000.
Get	This button is used to retrieve the ATM traffic data.
Reset Counts	This button can be used to restart the traffic data of the selected NE.

8.4.2 Modify the ATM traffic monitoring

Procedure

Complete the following procedure to modify the ATM traffic monitoring:

Step	Procedure
1.	Select ***NE*** in the Network Element Browser and ***Performance -> ATM Traffic*** via the cursor menu. The *ATM Traffic Monitoring* window pops up.
2.	Use the check box **Log Performance Data** to define whether the monitoring data should be logged or not.

If you want to ...	then ...
retrieve the traffic monitoring data	click on ***Get***.
restart the traffic monitoring data counter	click on ***Reset Counts***.
exit the window	click on ***Close***.

Data communications network (DCN) configuration

A

Contents

A.1 Overview A-1

A.2 DCN introduction A-1

A.3 Terms used in this chapter A-2

A.4 Network element communication capabilities A-3

A.5 AEM communication capabilities A-5

A.6 Recommended DCN configurations A-5

A.6.1 ROC over permanent leased lines DCN A-6

A.6.1.1 Router configuration A-7

A.6.1.2 *AnyMedia* network element configuration A-7

A.6.1.3 AEM server configuration A-8

A.6.1.4 AEM client configuration A-8

A.6.1.5 Transport elements configuration A-9

A.6.1.6 Connection diagram A-9

A.6.2 Communication with remote NEs using inband ATM PVC A-10

A.6.2.1 Configuration of the router A-11

A.6.2.2 Configuration of *AnyMedia* Access System A-12

A.6.2.2.1 Configuration of COMDAC A-12

A.6.2.2.2 Configuration of AFM A-12

A.6.2.3 AEM server configuration A-12

A.6.2.4 AEM client configuration A-12

A.6.2.5 Transport elements configuration A-12

A.6.2.6 Connection diagram A-13

A.6.3 ROC over semi permanent leased lines (COMDAC R1.4.1 agent) A-14

A.6.3.1 Router configuration A-14

Contents

A.6.3.2	*AnyMedia* network element configuration	A-14
A.6.3.3	Local exchange configuration	A-15
A.6.3.4	Connection diagram	A-16

Data communications network (DCN) configuration

A

A.1 Overview

This appendix provides you with information about

- Data communication network (DCN) introduction,
- general definitions of terms,
- network element management communications,
- AEM management communications,
- recommended DCN configurations.

A.2 DCN introduction

The *AnyMedia*® Access System is designed to provide a full range of telephony access services (like POTS, ISDN and leased lines) and data services.

AEM features

The *AnyMedia* Element Manager - 30 Channel (AEM) R1.7 provides the standard management configuration, equipment configuration, fault and testing, performance and security functions capabilities to do service management, monitoring, generate reports and printouts, do backup and restore functions for example to improve the customer's day to day business.

Communication of AEM and NE

The AEM communicates with the telephony agents by using TL1 commands and file transfer protocol (FTP) over TCP/IP. The AEM communicates with the data agents by using simple network management protocol (SNMP) over UDP/IP and FTP over TCP/IP. The AEM is also prepared to communicate with other legacy OSs by means of TL1 northbound interfaces and via CORBA interface. TL1 is used for request/response and autonomous reports commands and FTP is used for software and database upload/download operations.

DCN

The DCN is the communications infrastructure (routers, WAN links, etc.) needed for communication of the AEM with the NEs it manages. This manual refers to

AEM release 1.7 and the supported NE releases. For these releases many DCN configurations and protocol profiles can be used according to the network operators needs and scenarios. Two sample DCN scenarios are given at the end of this chapter.

A.3 Terms used in this chapter

Data communications network
The DCN consists of the communication media and the interconnected devices which are used to exchange management information between the AEM, the NEs and other management systems.

Remote operations channel
The remote operations channel (ROC) is a bearer channel that conveys management information for a remote system (*AnyMedia* NE). The ROC is expected to be used when the system is installed at locations where no ethernet local area network (LAN) and no separate network (e.g. X.25) exists.

Router
A router is a network layer device that forwards packets from one network to another based on network layer information (OSI layer 3). Data packets are only transferred through the router, if the participant is on another port of the router. The router can keep data traffic certain parts of a LAN. A router is more powerful than a bridge, it reduces the traffic on a LAN more than a bridge, because the IP address is evaluated for traffic control.

Bridge
A bridge is a network layer device that passes packets between two or more network segments that use the same data link communications protocol (OSI layer 2). The network segments appear as one segment to protocol levels higher than the data link layer. The bridge recognizes with the help of the MAC address which LAN component is on which port of the bridge. Data packets are only transferred over the bridge if the participant is on another port of the bridge. With a bridge data traffic can be kept from certain parts of a LAN.

Permanent leased line
A permanent leased line is a permanently established connection between a user port and a separate permanent leased line service network. Leased lines bypass the local exchange (LE).

Semipermanent leased line
A semi-permanent leased line is a V5.x service where bearer channels for certain user ports are pre-connected on provisioning base. Semi-permanent leased lines pass through the V5.x interface and are established under control of the LE by use of the BCC protocol after recovery of the V5.2 interface (V5.1 bearer connections are established anyway). No on-demand signaling is possible. Semi-permanent leased lines are only supported for ROC communication for the COMDAC R1.4.

Inband management channel
The inband management channel is a bearer ATM PVC that conveys management information for a remote BB agent (AFM). It can also be used for carrying NB management information in mixed configurations.

A.4 Network element communication capabilities

In this section the management communication capabilities of an AEM R1.7 are described. The *AnyMedia* Access System provides the following management interfaces for operation, administration, maintenance, and provisioning (OAM&P):

- Craft interface terminal (CIT)

  The CIT port is a local EIA-232D (former RS-232C) interface. It is located on the faceplate of the CIU in the *AnyMedia* Access System for 30-channel market. A PC-based graphical system interface (GSI) can be connected to the CIT port locally. This interface is typically used during initial installation and other maintenance related activities.

  This interface can also be used to remotely manage the NE using the GSI (e.g. POTS dial-up via modem), PPP is implemented on top of the CIT port as to allow this remote management. The protocol profile in the NE for this scenario is shown in Figure A-1.

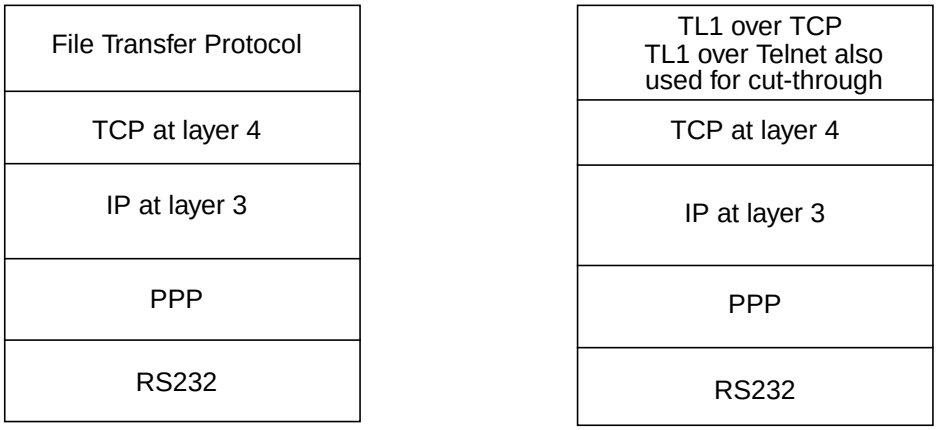


Figure A-1 COMDAC R1.4 remote access to CIT port protocol profiles

- External system LAN interface

  LAN interface is available via the shelf connection panel (SCP) connector on the *AnyMedia* Access System Mainshelf. It provides access to an IEEE 802.3 compliant LAN through a 10BaseT connection. All communications through this interface occur over the transmission control protocol/internet protocol (TCP/IP) to the GSI or AEM. The protocol profile in the NE for this scenario is shown in Figure A-2, page A-4.

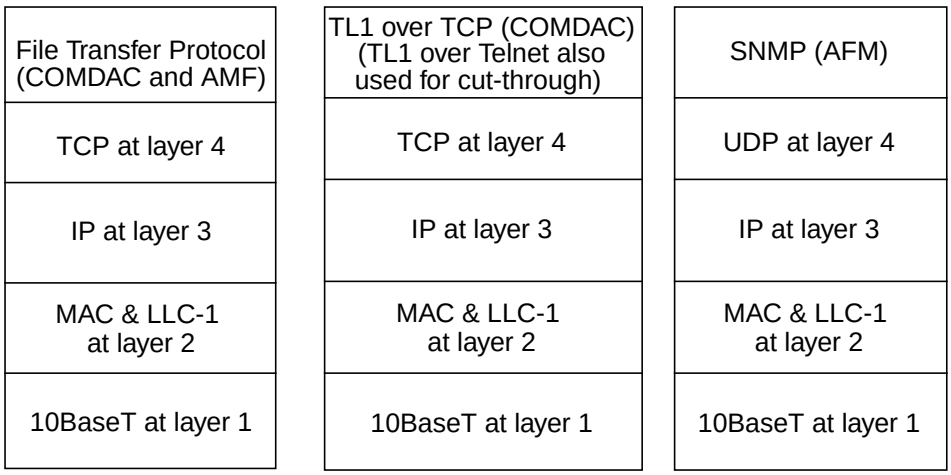


Figure A-2 COMDAC and AFM external LAN interface profiles

- Remote operations channel (ROC)

  ROC is a 64-kbps timeslot within the payload of a E1 link bound to a feeder of the network element. The *AnyMedia* Access System provides access for a remotely located OS if it communicates via TCP. The protocol profile in the NE for this scenario is shown in Figure A-1, page A-3. This alternative can be used if no local ethernet LAN is available or the outside plant (OSP) environment is too severe for a router. It does not need a separate DCN, then it can be a cheaper solution. The protocol profile in the NE for this scenario is shown in Figure A-3.

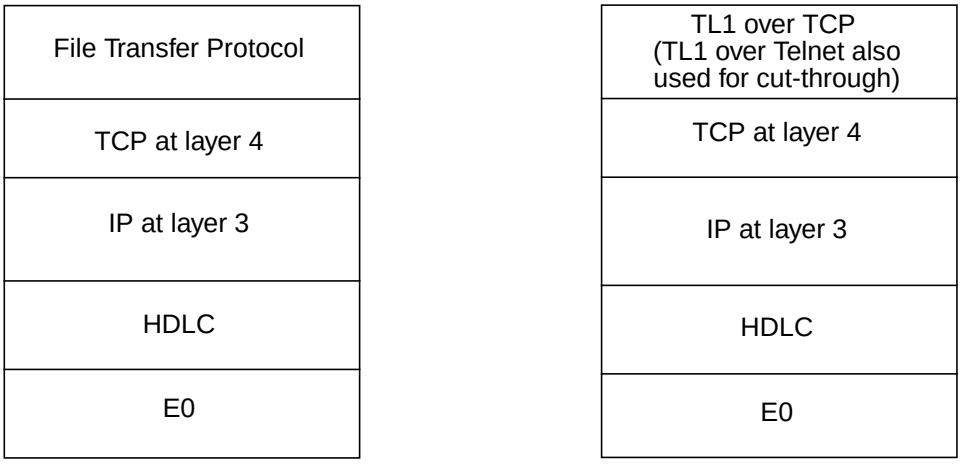


Figure A-3 COMDAC remote operations channel (ROC) protocol profiles

For establishing communication between the AEM and the NE, the NE must be minimally configured with its LAN, ROC or CIT parameters as applicable. This option is the only available, as the *AnyMedia* Access System does not support remote boot and remote TCP/IP configuration. The GSI can be used to provide this initial configuration of the NE using the CIT port.

A.5 AEM communication capabilities

The AEM uses for communicating management data an external system LAN interface. The protocol profile in the AEM for this scenario is shown in Figure A-4.

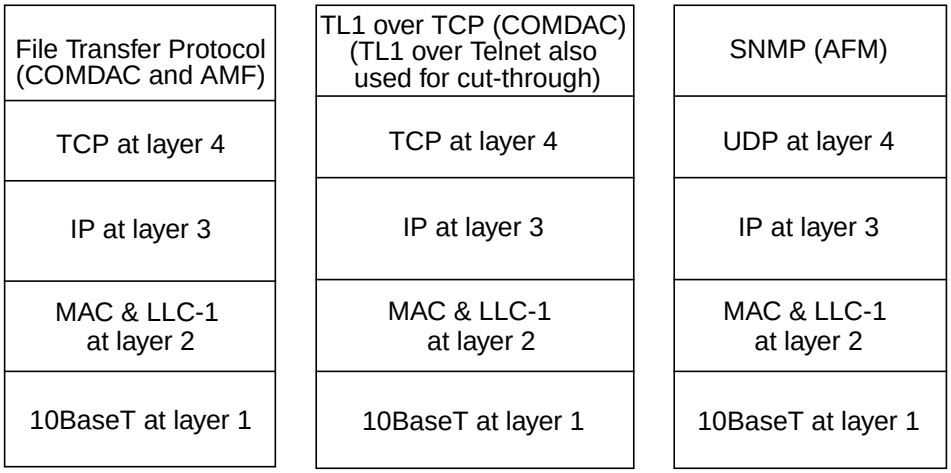


Figure A-4 AEM protocol profiles

A.6 Recommended DCN configurations

If a data network is not yet available between the central site where the AEM is located and the remote site where the NEs are located, the following three configurations are recommended:

- ROC over permanent leased lines DCN, cf. Chapter A.6.1, page A-6
- Communication with remote NEs using inband ATM PVC, cf. Chapter A.6.2, page A-10
- ROC over semi permanent leased lines (COMDAC R1.4.1 agent), cf. Chapter A.6.3, page A-14.

A.6.1 ROC over permanent leased lines DCN

The assumptions for this configuration are:

- The LAN-based V5DLC AEM is located in the central office.
- The V5DLCs NEs are located in remote locations.
- The OAM&P information (mapped in the 64-kbps ROCs) is transported from the AEM in the central office to the remote locations using permanent leased lines (PLLs) which are carried via:
  - SDH equipment in ring or point to point structure. Then a digital cross connect system (e.g. DACS-II) is available in the central office, it extracts the ROCs from each 2-Mbps link and put up to 30 ROCs to one 2-Mbps link.
  - PDH equipment in point to point structure. Then a digital cross connect system (e.g. DACS-II) is available in the central office, it extracts the ROCs from each 2-Mbps link and put up to 30 ROCs to one 2-Mbps link.
  - Using existing data communication network (leased line network). Then a leased line service node is available in the central office, it extracts the 64-kbps ROCs from each 2-Mbps link and concentrates up to 30x64-kbps ROCs into a single 2-Mbps link to the router (channelized E1 I/F).
- The PLLs will be originated at the AEM side by means of routers and DACS equipment and will be terminated at the COMDAC of the NE which extracts the ROC and its associated management information.
- The router at the AEM side will have to make a translation between E0/HDLC/IP/TCP and the AEM protocol stack 10BaseT/MAC&LLC1/IP/TCP. The AEM side router configuration will have channelized E1 interfaces. The Router/Bridge could be delivered by Lucent Technologies.
- One remote operation channel is used per V5DLC (64-kbps ROC carried on a 2-Mbps LL I/F).
- In this scenario one feeder is used in every network element to establish PLLs (instead of using it for V5 links), then if the only information which is carried over the PLL feeder is ROC the bandwidth of the transport network is wasted and a new cable is needed to be inserted in this feeder. If one feeder of the NE already supports other customer LLs no waste is made.
- For layer 2 HDLC raw protocol is used between V5DLC and the router.
- For up to 30 V5DLC connected to the LE, a single E1 interface for the router/bridge is sufficient.

A.6.1.1 Router configuration

The minimal requirements for the router/bridge for supporting this scenario are:

- Minimal WAN interface requirements

  The router/bridge must have one or more channelized 2-Mbps E1 interfaces (ITU G.703/G.704). Both, the symmetrical 120 ohms resistive (balanced) or the coaxial 75 ohms (unbalanced) resistive versions of the E1 interface should be supported depending on the customer needs. An IP address may be assigned to each time-slot or channel group. HDLC framing needs to be supported at the layer 2 of every slot inside the channelized E1 interface.

- Minimal LAN interface requirements

  The router must have one or two (for cascading purpose) ethernet (IEEE 802.3) 10Base T ports. In case of two LAN ports, LAN-to-LAN routing should be supported.

Provisioning needs for the router/bridge are the following:

- E1 interface functionality (line code, framing type etc.)
- timeslot mapping (each needed serial interface related to one ROC will be a channel group mapped on a time slot of the channelized E1)
- protocols and encapsulations
- IP-addresses for IP routing (routing tables)
- ethernet media.

The initial provisioning of a router/bridge is typically performed by a VT100/ANSI terminal, connected to a RS-232C port. When the IP-address of the router is provisioned, the router may be configured via LAN (TELNET, SNMP) but this depends on the router/bridge being used.

A.6.1.2 *AnyMedia* network element configuration

The ROC is the management interface used to access the NE. The initial provisioning has to be done via pre-provisioning (factory settings) or a local GSI (LAN or RS-232C) because the LL interface, carrying the remote operations channel, must be in-service to get remote access to the NE via remote operations channel (ROC). To enable the use of 64-kbps bearer channels for remote operations, the following provisioning needs for the V5DLC (30 channel market NE) are required:

- Create a ROC line (virtual port), which can be addressed as remote LAN interface (same IP-address as the local LAN interface on the V5DLC *(ent-roc TL1 command).*
- Create a leased line link entity *(ENT-LLL TL1 command).*
- create a cross connection between the ROC line entity and a 64-kbps timeslot of leased line link *(ENT-CRS-LLTS TL1 command).*
- Bring ROC channel into service.

On the 30 channel *AnyMedia* NE we must configure the ROC over the non-V.5 PLL service, and the IP characteristics of the NE. We use TL1 commands to configure the NE by means of the GSI craft terminal, the TL1 commands related to this scenario are listed below. Note that the default router address of the NE must be set to 224.0.0.2 (universal router's multicast address) so that the NE points to the router on the other side of the ROC interface.

```
ENT-ROC::roc-1;
ENT-LLL::lll-1::::e1-1-1-1;
ENT-CRS-LLTS::roc-1,llts-1-16;
```

Once communications with the AEM are established via the ROC, we can execute remote operations on the NE as if we are connected via the LAN. We can also use either the GSI or a standard windows FTP/TELNET.

A.6.1.3 AEM server configuration

Server IP parameters

The server on which the AEM application resides must have its IP parameters configured:

- IP address (e.g. 135.88.20.234)
- subnet mask (e.g. 255.255.240.0)
- default router (e.g. 135.88.17.1).

Configuration

In the AEM the following parameters have to be configured to be able to communicate with the NEs.

- TCP/IP configuration related to NEs
  - For every NE the AEM wants to communicate with, its IP address (e.g. 135.88.4.2) must be introduced in the AEM (provisionable with the AEM GUI via cut-through).
- Association configuration related to NEs
  - For every NE with which the AEM has to communicate, the NEs Target Identifier (TID) must be known by the AEM (provisionable with the AEM GUI via cut-through).
  - For every NE with which the AEM wants to communicate, the LOGIN and the PASSWORD information related to that NE must be introduced in the AEM. (provisionable with the AEM GUI via cut-through).

A.6.1.4 AEM client configuration

Client IP parameters

The workstation with the AEM client has the following IP parameters configured. Note that if the client is located at the same machine as the server these parameters are already configured.

- IP address (e.g. 135.88.20.230)
- subnet mask (e.g. 255.255.240.0)
- default router (e.g. 135.88.17.1).

The client workstation has to be configured as a client machine of the server workstation where the AEM server is going to run.

The 'SystemPreferences.ini' file includes the LOGTELNET, PASSTELNET and SERVER variables that have to be configured only it the user wants to open a cut-through session in the AEM client..

A.6.1.5 Transport elements configuration

If transport is achieved by means of SDH equipment in ring or point to point structure, then:

- The paths (i.e. VC-12 paths) used for transporting the E1 links need to be provisioned.
- The digital cross connect system which extracts the ROCs from each 2-Mbps link and put up to 30 ROCs over PLL to one 2-Mbps link need to be configured. For up to seven remote V5DLC the TMN-252 SCX can be used.

If transport is achieved by means of PDH equipment in point to point structure, then:

- The E1 paths used for transporting the ROCs through the PDH network need to be provisioned.
- The digital cross connect system which extracts the ROCs from each 2-Mbps link and put up to 30 ROCs over PLL to one 2-Mbps link need to be configured. For up to 7 remote V5DLCs the TMN-252 SCX can be used.

If transport is achieved by means of leased line networks, then a leased line service needs to be provisioned.

A.6.1.6 Connection diagram

For testing purposes, the E1 interface of the E1 router may be either directly connected to the E1 feeder of the NE or may be connected to this feeder using an intermediate transport network and/or a cross-connect equipment.

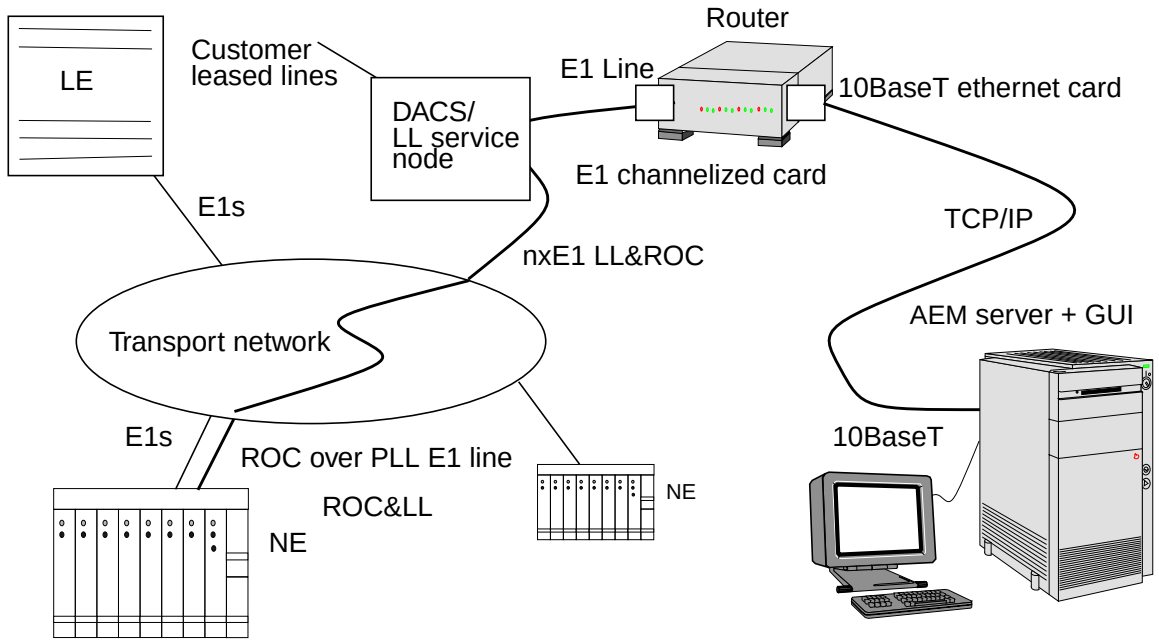


Figure A-5 Configuration of 30 channel permanent leased line access to ROC

A.6.2 Communication with remote NEs using inband ATM PVC

The assumptions for this configuration are:

- There are data and telephony access technologies collocated in the same NE. Data access is oriented to data applications and is based on asynchronous transfer mode (ATM) over asymmetrical digital subscriber line (ADSL) access. The data access consists of ADSL application packs and access feeder multiplexer (AFM) control cards which make the switching between ADSL access traffic and ATM networks using E3 interfaces (30-channel market).
- There is an ATM network between central office and remote *AnyMedia* NEs.
- In this scenario ATM permanent virtual connections (PVCs) are used to communicate telephony (TL1/FTP over TCP based) and data (SNMP over UDP and FTP over TCP based) management traffic between AEM and *AnyMedia* NEs.
- One ATM PVC will be used for every NE to be managed, this ATM PVC carries IP packets related to both COMDAC and AFM management information.
- ATM PVCs carrying management information related to one NE are originated in a LAN environment where AEM is located.

- A DCN device is needed at the Central Office to make the translation between 10BaseT/MAC&LLC1/IP and E3/ATM PVC/AAL5/802.2 LLC/802.2 SNAP/IP interface to the ATM network. The LLC encapsulation method to be supported by that device is that described in RFC 1483, i.e. this method allows multiplexing multiple protocols over a single ATM virtual circuit. Further, this method carries connectionless network traffic over the ATM network. Note that this functionality (if available) can also be performed by the ATM switch connected by means of a LAN connection with the central office (e.g. CBX-500), in these cases there is no need of a separate ATM router at the CO.
- ATM PVC which carries IP management information is carried over an ATM network and finally they are inserted in a related NE by means of E3 data ports, IP packets contained in the ATM PVC are extracted in the data AFM card which also support RFC 1483.
- Part of these IP packets (those with IP address of AFM) which carry BB management information are terminated in AFM.
- Part of these IP packets (those with IP address of COMDAC) which carry telephony management information are forwarded to AFM LAN port which is joined to COMDAC LAN port (located on the SCP of the *AnyMedia* Mainshelf), these IP packets will be terminated in the COMDAC.

A.6.2.1 Configuration of the router

The router at central office need to be configured. The minimal requirements for the router for supporting this scenario are:

- Minimal WAN interface requirements

  The router must have one or more ATM E3s interfaces with the ATM network (or any other physical interface, e.g. STM-1, E1 depending on the edge ATM switch to interface with). It is in charge of mediating from 10BaseT/ MAC&LLC1/ IP to E3/ATM, AAL5, 802.2 LLC, 802.2 SNAP/ IP. The logical WAN interface should be compatible with that of the connected ATM switch (e.g. Support of UNI 3.1 ATM cell switching). This router must support RFC 1483 (multiprotocol over ATM encapsulation) since AFM supports it.
- Minimal LAN interface requirements

  The router must have one or two (for cascading purpose) Ethernet (IEEE 802.3) 10BaseT/100BaseT ports. In case of two LAN ports, LAN-to-LAN routing should be supported.

The configuration tasks to be performed on router are:

- Configure ATM E3 interface
- Configure LAN interface
- Configure ATM PVCs inside the ATM E3 interfaces
- Create routing tables for both AFM and COMDAC (e.g. those IP packets to be sent to COMDAC and AFM addresses should be routed to the IP address of the related PVC).

A.6.2.2 Configuration of *AnyMedia* Access System

A.6.2.2.1 Configuration of COMDAC

On the *AnyMedia* telephony part of NE the user must configure the local LAN port. The initial provisioning has to be done via pre-provisioning (factory settings) or a local GSI (RS-232C). To do so the user must configure the COMDAC LAN port IP address, the default router address (address of AFM LAN port) and the subnet mask of the NE local LAN port. We use TL1 commands to configure the NE as it is shown in the next example.

```
set-ip::::::shelf=135.88.4.2,defrouter=135.88.17.1,submask=255.255.240.0
```

A.6.2.2.2 Configuration of AFM

On the AFM we must configure the in-band ATM permanent virtual connection (PVC) which is carrying telephony and data management information. This ATM PVC will be terminated at AFM and IP packets contained in it will be extracted. For this PVC VPI should be 0 and VCI greater than 31. ATM PVCs may be provisioned in AFM by means of GSI via local CIT altogether with AFM IP addresses (one for E3 interface and another one for LAN port). IP, Net Mask and Gateway addresses for AFM must be provisioned.

On the AFM we must configure a routing table (i.e. so that IP packets related to COMDAC are forwarded to the AFM LAN port and IP packets related to AFM are terminated at AFM)

The user must join AFM LAN port with COMDAC LAN port located on the SCP of the *AnyMedia* Mainshelf by means of a ethernet cross over cable.

A.6.2.3 AEM server configuration

The AEM server configuration is the same as described in Chapter A.6.1.3, page A-8.

A.6.2.4 AEM client configuration

The AEM client configuration is the same as described in Chapter A.6.1.4, page A-8.

A.6.2.5 Transport elements configuration

The ATM switches which will transport the ATM PVCs carrying the IP management traffic need to be provisioned, i.e a table must be provisioned in these switches saying that the cells from a specific VPI/VCI are related to a VPI/VCI pair in another interface. The ATM router and *AnyMedia* Access System must be attached to the ATM network by using E3 links (for the ATM router other links may also be used, e.g. E1/STM-1, etc.). If the switch supports directly rfc1483 a direct LAN connection between the switch and the CO LAN environment must be provisioned, in this case there is no need of ATM router at the CO side.

If SDH ADMs are used the paths which carry the ATM information need to be provisioned.

A.6.2.6 Connection diagram

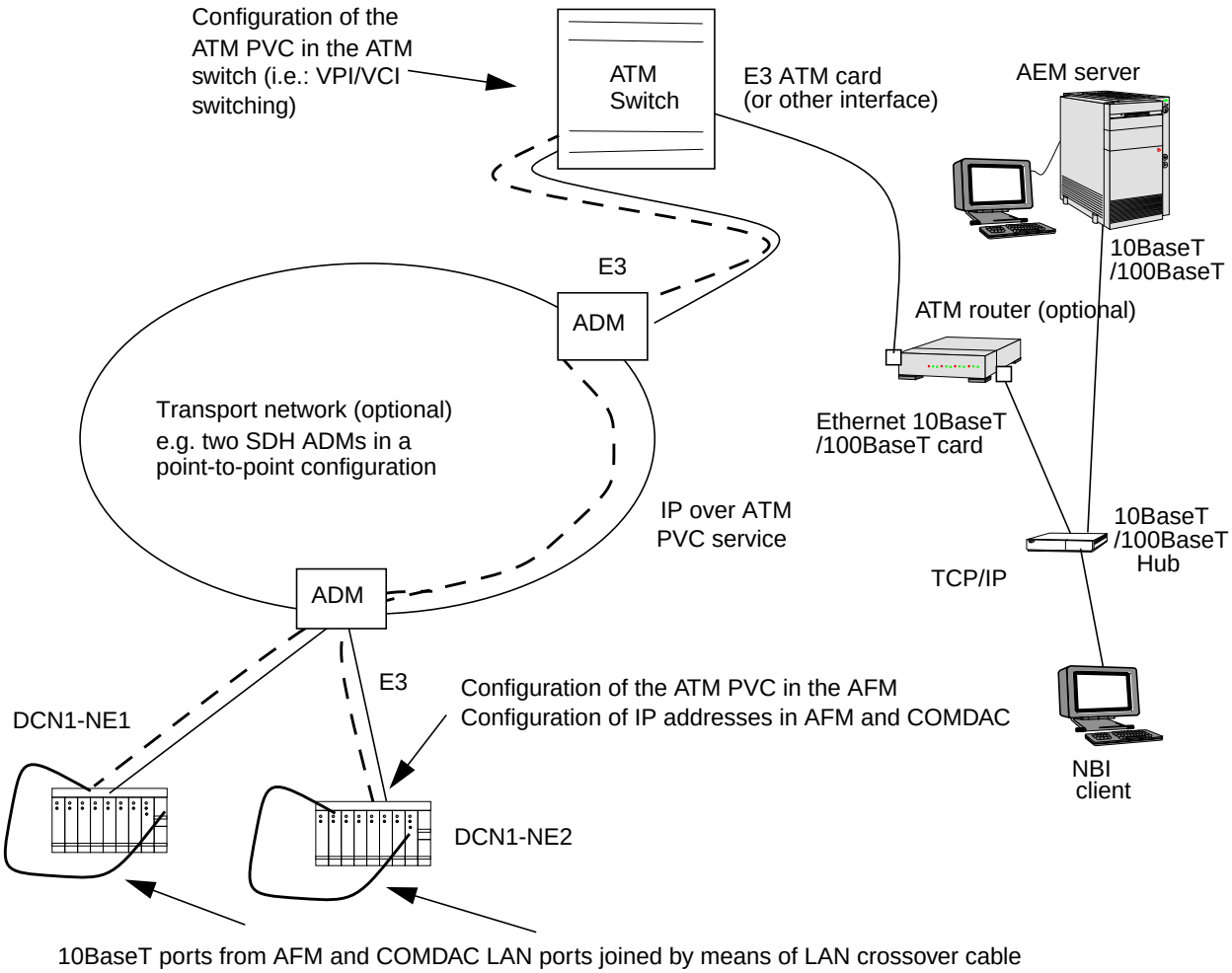


Figure A-6 Communication with remote NEs using in-band ATM PVC

A.6.3 ROC over semi permanent leased lines (COMDAC R1.4.1 agent)

The assumptions for this configuration are:

- The LAN-based V5DLC AEM is located in the central office
- The V5DLCs NEs are located in remote locations.
- The local exchanges connected to V5DLCs NEs support semi permanent leased lines (SPLLs) services for V5.1 and V5.2 access technologies.
- The V5DLCs NEs support SPLL ROCs. This is applicable for R1.4.1 NEs. Note that these NEs will support SPLLs for management communications, not for customer services.
- The OAM&P information (mapped in the 64 kbit/s ROCs) is transported from the AEM in the central office to the V5DLCs in the remote locations using 64-kbps SPLLs.
- The 64-kbps ROCs are originated in an E1 router at the EM location. The router at the AEM side will have to make a translation between E0/HDLC/IP/TCP and the AEM protocol stack 10BaseT/MAC&LLC1/IP/TCP. The AEM side router configuration will have channelized E1 interfaces and will support HDLC protocol at layer 2. Up to 30 NEs will be managed per E1 link originated in the AEM router.
- The channelized E1s carrying the 64-kbps ROCs coming from the router will be inserted (maybe through a transport network) to the LE to which the V5DLCs are connected.
- A SPLL service will be provisioned between the LE and every V5DLC to be managed. This SPLL will be carried inside a V5.1 or V5.2 interface which communicate the LE with every V5DLC to be managed. The LE will nail-up the 64-kbps ROCs to these SPLLs. One remote operation channel is used per V5DLC (64-kbps ROC carried on a 64-kbps SPLL)
- The V5DLC which supports the E0 (SPLL)/HDLC/IP/TCP protocol stack will extract the management information from the SPLL.

A.6.3.1 Router configuration

This section is the same as the equivalent in section A.6.1 ROC over permanent leased lines DCN.

A.6.3.2 *AnyMedia* network element configuration

The ROC is the management interface used to access the NE. The initial provisioning has to be done via pre-provisioning (factory settings) or a local GSI (LAN or RS-232C) because the SPLL interface, carrying the remote operations channel, must be in-service to get remote access to the NE. To enable the use of 64-kbps bearer channels for remote operations, the following provisioning needs for the V5DLC (30 channel market NE) are required. Note that it is assumed that the V5 interfaces, V5 links, V5 communication channels and the other needed entities are previously created and giving service.

- Create a ROC entity (virtual port), which can be addressed as remote LAN interface (same IP-address as the local LAN interface on the V5DLC *(ENT-ROC TL1 command).*
- Create a V5 User Port of single channel SPLL type and associate it to ROC. *(ENT-V5UP TL1 command).*
- Associate the SPLL V5 User Port to the V5.X interface *(ent-crs-up command).*
- If the interface is V5.1 we must create a cross-connection between the v5 line termination bearer channel from the v5 UP and a timeslot of a v5.1 interface *(ENT-CRS-BCTS TL1 command)*
- Configure the ROC interface IP address *(SET-IP TL1 command).*
- Configure the COMDAC routing table *(ENT-ROUTE TL1 command).* For doing that a routing entry, in this entry say that all the IP packets with destination to the AEM IP address are to be forwarded to the ROC interface.

The following TL1 commands are an example of the described process for a V5.2 interface.

```
ENT-V5I::v5i-5::::v52,2000,,,,y,;
ENT-ROC::roc-1;
ENT-V5UP::v5up-5::::ssplL,roc-1,v5l3addr;
ENT-CRS-UPI::v5up-5,v5i-5:;
```

Once communications with the Element Manager are established via the ROC, we can execute remote operations on the NE as if we are connected via the LAN. We can also use either the GSI or a standard windows FTP/TELNET.

A.6.3.3 Local exchange configuration

The 64-kbps SPLLs need to be provisioned between the LE and every NE to be managed. The LE needs to be configured so that it is able to extract the 64-kbps from the E1 (coming from the EM router) and nail them up to the 64-kbps SPLLs going to every NE.

A.6.3.4 Connection diagram

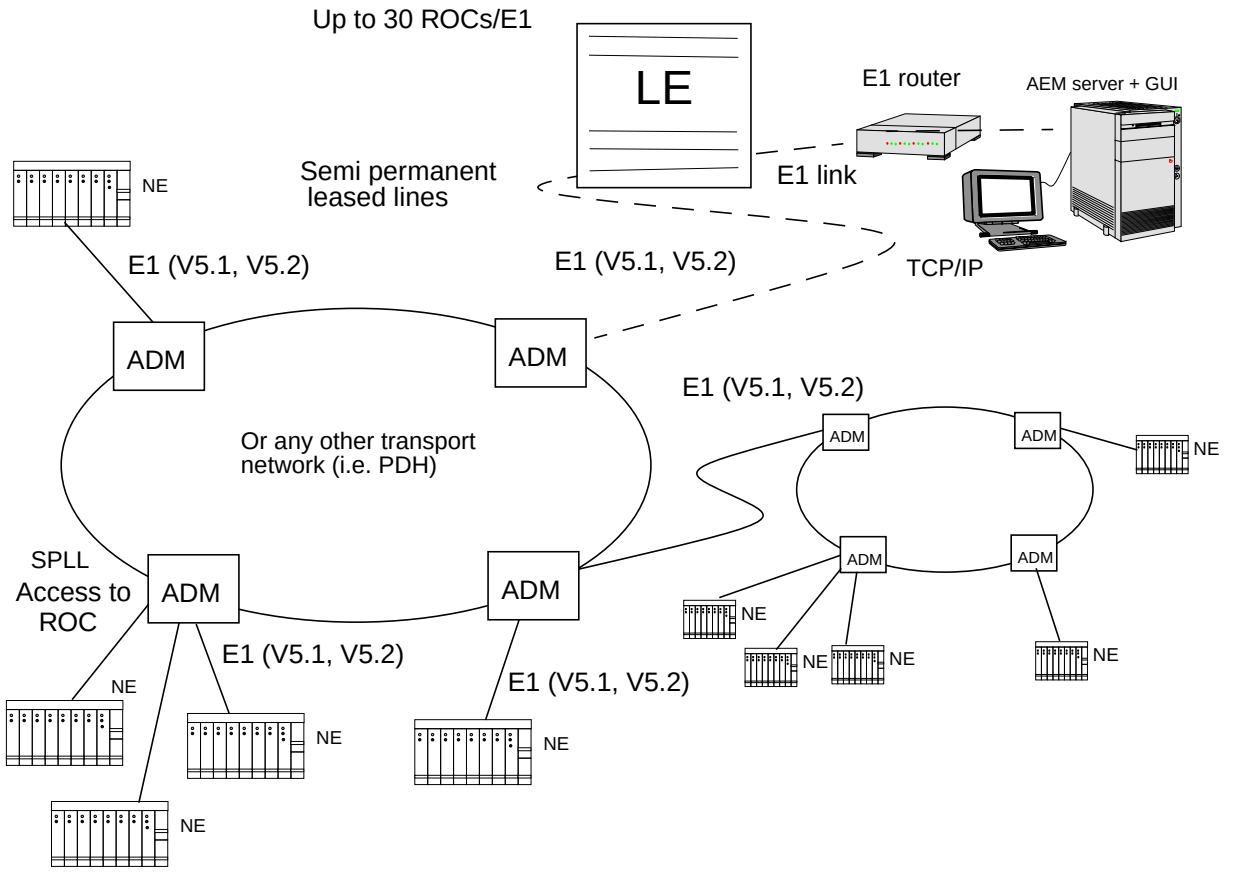


Figure A-7 Semi permanent leased line access to ROC for NE R1.4.1

Configuration parameters

B

Contents

B.1 Overview B-1

B.1.1 *AnyMedia* server configuration variables B-1

B.1.2 *AnyMedia* client GUI configuration variables B-7

Contents

Configuration parameters

B

B.1 Overview

This chapter provides information about all the configuration parameters that are used with *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7 as follows:

- an alphabetical list of all configuration parameters that are used with AEM R1.7.
- a detailed information about each parameter.

These configuration parameters are distributed in three configuration files, as follows:

- **AnyMediaEM.cfg** for variables used by the *AnyMedia* servers.
- **AnyMedia.ini** and **SystemPreferences.ini** for variables used by the GUI.

Only the configuration parameters the *AnyMedia* administrator can modify are explained in this chapter -modify these configuration variables with caution as they may adversely affect the correct operation of the application-. To modify the other configuration parameters stored in the configuration files, please contact with Lucent Technologies TCL.

B.1.1 *AnyMedia* server configuration variables

The following table provide an alphabetical list of the configuration variables for *AnyMedia* servers.

The directories can be defined either absolute or relative to the environment variable **`$ANYMEDIAPATH`**.

Table 2-1 AnyMediaEM.cfg File

Configuration management settings

Name	Description
AM.clearHour	Hour of the day in 24h format at which the removal process of the alarm database is executed every day. It is OPTIONAL. If not present, default value is taken. Possible values: 0 to 23 Default value: 1
AM.clearMinute	Minute within the AM.clearHour at which the removal process of the alarm database is executed every day. It is OPTIONAL. If not present, default value is taken. Possible values: 0 to 59 Default value: 0
AM.correlationRulesPath	AM configuration file location relative to *Anymedia* path. It contains the correlation rules needed for the reduced correlation process in the AM subsystem. It is MANDATORY. It should be present in this file. Default value: AM/cfg/CorrelationRules.cfg.
AM.minimumClearPeriod	Number of days that cleared alarms remain in the database before they are removed. It is optional. If not present, default value is taken. Possible values: 1 to *. Default value: 3.
AM.platformAlarmTablePath	AM configuration file location relative to *Anymedia* path. It contains the static information of the platform alarms. It is MANDATORY. It should be present in this file. Default value: AM/cfg/PlatformAlarmTable.cfg.

NOTE:
All CM variables in this file are mandatory and must be defined here.

Name	Description
CM.directoryNVDS	NVDS files location. This files store information in such a way as to survive indefinite periods of total power failure. The current values for all provisionable parameters are stored in the NVDS directory and hence are the parameter values that will be used on subsequent NE power-up. Default value: CM/nefiles/NVDS. NOTE: The path is relative to the *AnyMedia* installation path.
CM.directoryNVPS	NVPS files location. It keeps software program data. It resides in the NE <COMDAC> Default value: CM/nefiles/NVPS. NOTE: The path is relative to the *AnyMedia* installation path.
CM.FTPtimeOut	Time out in seconds for all FTP commands. The FTP command is aborted if there is no progress of file transfer during the interval. Possible values: 90 to 900 seconds. Default value: 300.
CM.maxTriesCounter	Maximum number of SNMP PDUs retransmissions when time out. Possible values: 0 to (upper limit not defined). Default value: 3.
Gen.directoryTemp	Temporary directory of the AEM application. Default value: tmp.
Gen.orbixTracesInEm	Orbix daemon trace level. Possible values: 0 to 2. Default value: 0
Gen.timeout	Time out in milliseconds for COBRA calls. Possible values: 0 to *. Default value: 480 000 ms.
FB.Root.NVDS_BB	Path associate to the root key used by File Browser. Default value: NVDS_BB.

Name	Description
FB.Root.NVDS_NB	Path associate to the root key used by File Browser. Default value: NVDS_NB.
FB.Root.NVPS_BB	Path associate to the root key used by File Browser. Default value: NVPS_BB.
FB.Root.NVPS_NB	Path associate to the root key used by File Browser. Default value: NVPS_NB.
FB.Root.ALARM_FILTERS	Path associate to the root key used by File Browser. Default value: ALARM_FILTERS.
NEM.association.timeSync	Indicates if the time and date in the agents has to be kept in synchronization with the time and date of the AEM. Possible values: true, false. Default value: true.
NEM.aoHandler.fullSyncInvalidTimes	Maximum number of retries of full synchronizations. Possible values: 0 to 5 times. Default value: 3.
NEM.aoHandler.queueSize	Maximum size of the event's queue. Possible values: 1 to 1000 elements. Default value: 1000.
NEM.association.heartBeatNumber	Maximum number of missing heartbeats to the NE. Possible values: 1 to 5 times. Default value: 3.
NEM.association.heartBeatTime	Time between two heartbeats to the NE. Possible values: 0 to 15 minutes. Default value: 5.
NEM.association.loopTimer	Time to wait after connection to four TCP/IP ports have been tried and failed. Possible values: 0 to 50 minutes. Default value: 5.

Name	Description
NEM.timeSync.delay	Maximal time delay in seconds when a time sync is not needed. Possible value: 0 to 30 seconds. Default value: 30
NEM.association.osContext	TL1 context used as parameter in ENT-OSAC-MAP TL1 command. Default value: TL1OTHER1
NEM.association.tl1Timeout	Time out for all TL1 commands. Possible values: 1 to 5. Default value: 4.
BAM.association.timeSync	Indicates if the time and date in the agents has to be kept in synchronization with the time and date of the AEM. Possible values: true, false. Default value: true.
BAM.association.heartBeat-Number	Maximum number of missing heartbeats to the NE. Possible values: 1 to 5 times. Default value: 3.
BAM.association.heartBeat-Time	Time between two heartbeats to the NE. Possible values: 0 to 15 minutes. Default value: 5.
BAM.association.snmpTimeout	Time out for all SNMP commands. Possible values: 1 to 5. Default value: 4.
BAM.association.snmpRetries	Maximum number of times for a SNMP re-transmission. Possible values: 1 to 10. Default value: 3.
BAM.association.nextAttempt	Time to wait after a new SNMP communication attempt. Possible values: 0 to 50 minutes. Default value: 5.
BAM.alarmSync.period	Time between periodic alarm synchronization. Possible values: 3600 to 86400 seconds. Default value: 21600.
BAM.cfgSync.period	Time between periodic config synchronization.

	Name	Description
	BAM.timeSync.delay	Maximal time delay when a time synchronization is not needed. Possible values: 0 to 30 seconds. Default values: 30.
	BAM.cfgSync.maxRetries	Maximum number of retries of full synchronizations. Possible values: 0 to 5 times. Default value: 3.
	BAM.trapHandler.queueSize	Maximum size of the trap's queue. Possible values: 1 to 1000 elements. Default value: 1000.
OAM settings	OAM.backup.archiveDirectory	Destination of the log files archived by the *AnyMedia* archive script, if it is not specified as command-line parameter. It can be a tape device. Default value: archives.
	OAM.backup.backupDirectory	Destination of the log files and data bases backed up by the *AnyMedia* backup script, if it is not specified as command-line parameter. It can be a tape device. Default value: backups.
	OAM.backup.backupLogDirectory	Location of the log files of the backup/archive/restore scripts execution. Default value: tmp.
	OAM.backup.numberOfLogFiles	Maximum number of log files (per type) allowed in the OAM.backup.backupLogDirectory. Range of values: 1 to *. Default value: 10 files per script file.
	OAM.log.directoryCurrentLogs	Default path where the restored *AnyMedia* logs will be placed from a previous archive. Default value: log.
	OAM.log.directoryRestoredLogs	Location of the *AnyMedia* log files restored from a previous backup or archive. Default value: restored.

Name	Description
OAM.log.minimumDaysKept	Number of days a log file should be kept in the system before being removed. If space is needed and the log file is still within this period, a platform alarm is raised (and the file is removed). Possible values: 1 to *. Default value: 7 days.
OAM.sysadmin.clientIdleTime	Period of inactivity after that a client is forced to log out. Possible values: 60 to *. Default value: 240 seconds.

B.1.2 *AnyMedia* client GUI configuration variables

The following table provides an alphabetical list of the configuration parameters for *AnyMedia* GUI.

Table 2-2 SystemPreferences.ini configuration file

Name	Description
Site settings	
SITE	The city or the location where the AEM is working. This value is used for printing purposes, it is mandatory at installation time.
LOC_LANG=en LOC_COUNTRY=US	Default locale of the application. These value cannot be modified.
The following variable should be used to change the timezone. That should be done only if some problems has been detected by default. In order to notify to the application that the time zone should be change the value of TZ_userDefined should be set to true. In order to set properly the time zone to be used in the AnyMedia application we have to set the following variables: TZ_rawOffset, TZ_ID, TZ_startMonth, TZ_startDay, TZ_startDayOfWeek, TZ_startTime, TZ_endMonth, TZ_endDay, TZ_endDayOfWeek, TZ_endTime.	
TZ_userDefined	Possible values: true, false Default value: false
TZ_rawOffset	Defines the difference in milliseconds between local time and UTC.

	Name	Description
	TZ_ID	The syntax necessary to define a TZ_ID is the following: GMT[+|-]hh[[:]mm]. For example, you might specify GMT+14:00 as a custom time zone ID. The time zone that is returned when you specify a custom time zone ID does not include daylight savings time, then it is necessary to use the rest of variables to set the daylight saving time for this time zone.
	TZ_startMonth	The daylight savings starting month. Month is 0-based. e.g., 0 for January.
	TZ_startDay	The daylight savings starting day-of-month.
	TZ_startDayOfWeek	The daylight savings starting day-of-week-in-month. Day of week are 1-based: 1 is SUNDAY, 2 is MONDAY and so on.
	TZ_startTime	The daylight savings starting time in local wall time, which is standard time in this case.
	TZ_endMonth	The daylight savings ending month. Month is 0-based. e.g., 0 for January.
	TZ_endDay	The daylight savings ending day-of-month.
	TZ_endDayOfWeek	The daylight savings starting day-of-week-in-month. Day of week are 1-based: 1 is SUNDAY, 2 is MONDAY and so on.
	TZ_endTime	The daylight savings ending time in local wall time, which is daylight time in this case.
User view settings	USERVIEW	Default view in User Administration and Profiling application. Possible values: users, user groups, domains or objects. Default value: users.
Alarm viewer settings	ALM_VIEW	Default view of the Alarm Viewer. Range of values: 1 to 5. Default value: 3.
	ALM_FILTER	Default alarm filter of the Alarm Viewer. Possible values: 0:Last 24 hours, 1:Critical raised alarms, 2:Raised alarms, 3:Alarm from a Host/s, 4:Critical alarms not cleared, 5:Owned acknowledge alarms, 6:All acknowledge alarms, 7:None filter/all alarms. Default value: 3.

	Name	Description
	DEFAULT_LOG_TYPE	Default Options Window of Log Viewer. Possible values: Act_TASK, Iee_TASK, Ao_TASK. Default value: Act_TASK.
Cut-through settings	LOGTELNET	Login to connect to AEM server for cut-through purposes. Default value: defined at installation time.
	PASSTELNET	Password to connect to AEM server for Cut-through purposes. Default value: defined at installation time.
	SERVER	Server host where the AEM application is running. Default value: defined at installation time.
Help settings	HELP_URL	Contains the URL where the help files are located.
	HELP_BROWSER	HELP_BROWSER Solaris Setting: this property should contain the name of browser being used (netscape in our case) the full path is not necessary. HELP_BROWSER Windows Setting: however in windows it is necessary to specify the full path where the browser is located (remember that in this case it is needed to use double back slashes). For example: C:\\Program Files\\ Netscape\\Communicator\\Program\\ netscape.exe. Default value: netscape.
Event settings	EVENT_DELAY	This is the delay applied to all events received by the GUI (except those ones managed by the System Events Distributor). That is, the delay between the GUI event reception and the event handler process. Value expressed in milliseconds. Default value: 5000.
V5 settings	V5_RADIX	This is the radix being used to display the v5 id. Default value: 10.

	Name	Description
Market settings	IS_NAR_MARKET	This variables defines if the *AnyMedia* application is being used either in the NAR market (true) or in the international market (false). Default value: false.
Groups & NEs settings	The RELEASE_MAP_X options define a list of key value pairs used to map each release-related object to the corresponding class which implements the functionality for that object. Using this mapping, several releases can be mapped to the same class, if possible, allowing for code reuse.	
	Agent related classes: RELEASE_MAP_0=NB_R13-RT,guinemanage.AgentNB30ch RELEASE_MAP_0=NB_R131-RT,guinemanage.AgentNB30ch RELEASE_MAP_2=NB_R14-RT,guinemanage.AgentNB30chR14 RELEASE_MAP_4=BB_R112,guinemanage.AgentBB RELEASE_MAP_5=BB_R14,guinemanage.AgentBB	
	Shelf related classes: RELEASE_MAP_6=sh,guinemanage.NEsh RELEASE_MAP_7=subsh,guinemanage.NEsubsh	
	Pack related class: RELEASE_MAP_8=TAP100,guinemanage.NEslotTAP	

Table 2-3 AnyMedia.ini configuration file

Name	Description
LV_READLINES	Line number of server log messages read in Log Viewer. Possible values: 1 to 50. Default value: 50.

Northbound interface

C

Contents

C.1 Overview C-1

C.2 Northbound interface basics C-1

C.2.1 Northbound interface description C-1

C.3 Northbound interface specific TL1 messages C-3

C.3.1 REPT ALM (Report Alarm) C-4

C.3.1.1 Purpose C-4

C.3.1.2 Output format C-4

C.3.1.3 Output format parameters C-4

C.3.2 RTRV-ALM (Retrieve-Alarms) C-9

C.3.2.1 Purpose C-9

C.3.2.2 Input format C-9

C.3.2.3 Input format parameters C-9

C.3.2.4 Output format C-10

C.3.2.5 Output format parameters C-10

C.3.2.6 Generic error responses C-14

C.3.3 RTRV-ALM-ENV (Retrieve-Alarm-Environment) C-15

C.3.3.1 Purpose C-15

C.3.3.2 Input format C-15

C.3.3.3 Input format parameters C-15

C.3.3.4 Output format C-16

C.3.3.5 Output format parameters C-16

C.3.3.6 Generic error responses C-18

Contents

Northbound interface

C

C.1 Overview

This appendix provides you with information about the

- Northbound interface basics and
- Northbound interface specific TL1 messages.

C.2 Northbound interface basics

C.2.1 Northbound interface description

General

The *AnyMedia*® Element Manager - 30 Channel (AEM) R1.7 offers to any external OS a straight TL1 connection with the set of NEs in the OS's network. Using this link, any external OS with access rights to open a northbound interface session, can configure, test or monitor a set of NEs using a TL1 interface and can receive the responses to the TL1 commands and the autonomous outputs which are generated by the NE (depending on the northbound interface application type selected).

Two types of northbound interfaces

The AEM provides two different types of northbound interface applications:

- general northbound interface

  all types of autonomous messages received from the NE are send to the OS. None NE autonomous messages will be inhibited.

- alarm only northbound interface

  only alarm and environment alarm autonomous message received from the NE are sent to the OS, the AEM will inhibit the rest of NE autonomous messages (database changes, events, etc...).

Configure terminal for session

Before the telnet session for the northbound interface is opened the **TERM** variable must be set correctly. Set the **TERM** variable either to **dtterm**, **xterm** or **vt100**.

Restrictions with multiple sessions

While a northbound interface session is already open another session of a different type must not be opened for the same NE.

Avoid interference with other EM

When a northbound interface session is opened it is recommendable to send the message **ALW-MSG::vc-all:::,ALL;** to avoid that changes in the configuration of the NE introduced by another manager could interfere with our application.

Start northbound interface session

To start a northbound interface session, the OS must open a TCP/IP connection with the AnyMedia Element Manager. Then a TL1 interface, see *Command and Message Manual*, is used.

Firstly, the OS is authenticated and authorized via the ACT-USER message. The AEM opens a dedicated TL1 virtual circuit with every NE included in the domain of the external OS. When the connections are open, any TL1 command typed by the OS operator, will be sent, to the proper NE, and the responses to these commands, as well as all the available autonomous output messages (AO) will be routed to the proper OS.

Close northbound interface session

To close the northbound interface session, the external OS uses the CANC-USER TL1 message. When this message reaches the AEM, it logs-out the external OS, closes all the TCP/IP connections which are involved in this northbound interface session (both sides, northbound to the OS, and southbound to the NEs managed by the OS) and logs the end of the northbound interface link.

Maintaining authentication information

The OS will be authenticated and authorized by the AEM not by the NE. Using this mechanism, the OS will only have to send one ACT-USER TL1 message, which will be spawned by the AEM to all the NEs in the network managed by the OS. To do that, the AEM will have to maintain some information, e.g. the TIDs and IP addresses of all the NEs managed by the OS, and a UID - PID pair to open a virtual circuit on each NE. The AEM operator will be provided with the required set of script tools to maintain this information easily.

Close virtual circuits with NEs

In the same way, only one CANC-USER message, sent by the OS to the AEM, will be enough to close all the virtual circuits with the NEs, and the northbound interface session.

Routing of TL1 messages

For the routing of the TL1 messages, the NEs TID is used, and from every NE configuration table, the corresponding IP address is determinated. Incoming messages that have no TID (field empty), are sent to all connected NEs.

Messages from NEs

In case the OS will send a TL1 request message, the OS has to support as many completion responses as NEs are connected. Messages coming from the NEs (responses and autonomous output), are queued until they are complete (i.e. received) and then sent to the northbound OS. There are no guarantees about the order in which responses are sent to the OS.

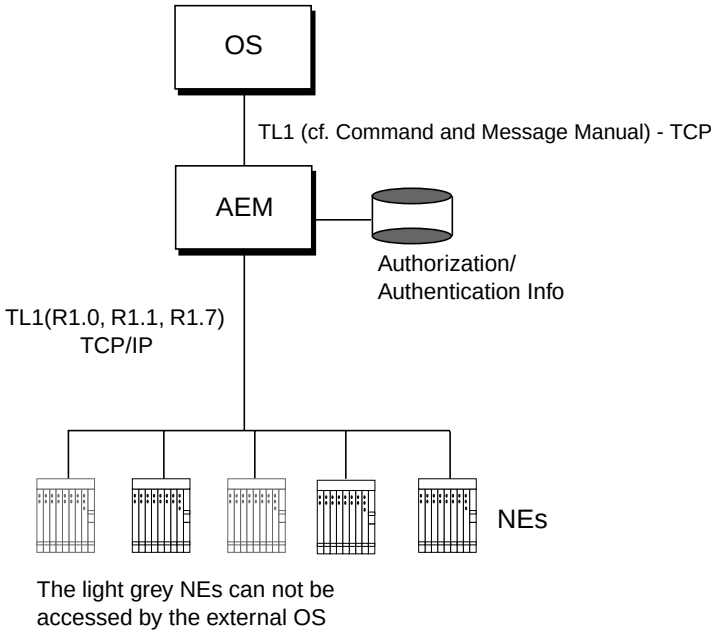


Figure C-1 Northbound interface

The number of concurrent northbound interface sessions supported by a single NE will depend on the number of available virtual circuits on the NE.

The AEM will provide the independence of the northbound interface sessions and the AEM GUI interface, so an operator using the AEM GUI, will not get to know whether a northbound interface session is running or not.

C.3 Northbound interface specific TL1 messages

Some TL1 messages feature more parameters when invoked via AEM. These TL1 messages are described in this section, namely

- REPT ALM (Report Alarm)
- RTRV-ALM (Retrieve-Alarms)
- RTRV-ALM-ENV (Retrieve-Alarm-Environment).

C.3.1 REPT ALM (Report Alarm)

C.3.1.1 Purpose

A REPT ALM (Report Alarm) message is generated autonomously by the NE to report the occurrence of an equipment, facility, or system alarm condition to the OS/AEM and CIT. An alarm condition reported via the REPT ALM message has a corresponding REPT ALM clearance message that is generated when the alarm condition clears.

Abortable	No
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

C.3.1.2 Output format

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
AC atag REPT ALM AIDTYPE

"AID:NTFCNCDE,CONDTYPE,SRVEFF,OCRDAT,OCRTM:CONDDESCR"
;
```

C.3.1.3 Output format parameters

AID Access identifier

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes

AID is the address of the equipment or facility for which an alarm is being reported.

Abbreviation	Meaning
ap-1-{1-16}	Application Pack
ciu-1	Communication interface unit
comdac-1-{1-2}	COMDAC
drop-1-{1-16}-{1-32}	drop

Abbreviation	Meaning
e1-1-{1-4}-{1-4}	E1 physical port (feeder side)
ioe1-1-{1-4}	E1 circuit pack
iohdlc-1-{1-2}	IOHDLC Circuit Pack
pwrsrc-1-{a,b}	Power Source
roc-1	Remote Operations Channel
sclk-1	Station Clock
sh-1	Shelf
subap-{1-8}-{1-8}	Subshelf Application Pack
subdrop-{1-8}-{1-8}-{1-32}	Subshelf drop
subsh-{1-8}	Subshelf
v5i-{1-16}	v5 interface
v5l-{1-16}	v5 Link
v5ts-{1-16}-{1-31}	v5 Time Slot
{string}[a]	NE TID (Target Identifier)

a only available via AEM

NTFCNCDE **Notification code**

This parameter appears in the Common Block

Type	List
Required	Yes

NTFCNCDE is the alarm level.

Abbreviation	Meaning
CL	Cleared Alarm
CR	Critical Alarm
MJ	Major Alarm
MN	Minor Alarm

CONDTYPE **Condition type**

This parameter appears in the Common Block

Type	List
Required	Yes

CONDTYPE is a code denoting the condition type. A message reporting the clearing of an alarm has the same condition type as the one reporting the alarm.

Abbreviation	Meaning
AIS	Alarm indication signal
BKUPMEMP	System data memory mismatch
BCCDLK	BCC protocol data link failed
CABLE	Cable disconnect
CPYMEMF	Copy program memory failed
CTRLDLK	Control protocol data link failed
DATASYSCR	Data system failed critical
DATASYSMJ	Data system failed major
DATASYSMN	Data system failed minor
DBCRRPT	Data memory corrupt
DBMEMTRF	Data memory update abort
EXT	External failure
IMPROPRMVL	Improper removal
INT	Internal hardware failure
LCTRLDLK	Link control protocol data link failed
LOF	Loss of frame
LOS	Loss of signal
NE_ASSOC_FAILED[a]	Assoc with NE failed
PACKM	Pack mismatch
POLL	Not responding to poll
PRCDERR	Procedural error
PROTDLK	Protection protocol data link failed
PSTNDLK	PSTN protocol data link failed
PSTNF	Restart PSTN failed
PWR	Power fault
PWROVLD	Power overload
RAI	Remote alarm indication
RINGF	Ringing source input failed
SERVGRP	Server group maintenance limit exceeded
SFTCRRPT	Software program corrupt
SFTERR	Software version mismatch
SWFTDWNF	Software download failed
SYNC	Synchronization input failed

Abbreviation	Meaning
SYNCOOS	System free running
T-BERL	BER exceeds threshold
T-BERLN	BER exceeds threshold near end
T-FC-CABLE	Cable suspect exceeds failure count threshold
T-FC-INT	Internal pack failure exceeds failure count
UNXPRS	Unexpected reset

a only available via AEM

SRVEFF **Service effect**

This parameter appears in the Common Block

Type	List
Required	Yes

SRVEFF indicates the effect of the reported alarm on service.

Abbreviation	Meaning
NSA	Non Service Affecting
SA	Service Affecting

OCRDAT **Occurrence date**

This parameter appears in the Common Block

Type	Date
Required	Yes

OCRDAT indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

OCRTM **Occurrence time**

This parameter appears in the Common Block

Type	Time
Required	Yes

OCRTM indicates the time of the condition being reported and has the format HH-MM-SS (hours-minutes-seconds).

CONDDESCR **Condition description**

Type	String
Required	Yes
Min # chars	1
Max # chars	68

This is the text description for the reported alarm condition. This information can be found in the Correlations Tables. The 68 characters included a pair of escaped quotes \"\".

AIDTYPE **Access identifier type**

Type	List
Required	Yes

MODIFIER is the message modifier to the REPT ALM message.

Abbreviation	Meaning
COM	Common
E1	E1
EQPT	Equipment

C.3.2 RTRV-ALM (Retrieve-Alarms)

C.3.2.1 Purpose

The RTRV-ALM (Retrieve-Alarms) command instructs the system to retrieve: (1) all currently active alarms, (2) currently active equipment alarms, (3) currently active facility alarms, or (4) currently active system level alarms from the system.

C.3.2.2 Input format

```
RTRV-ALM-[AIDTYPE]:[tid]::[ctag];
```

Abortable	Yes
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

C.3.2.3 Input format parameters

tid **Target ID**

This parameter appears in the TID Block

Type	String
Required	No
Default Type	Dynamic

Target ID is the name of the system to which the command is addressed.

ctag **Correlation tag**

This parameter appears in the CTAG Block

Type	String
Required	No
Default Type	Dynamic

This field is used to associate the command message to the response message.

AIDTYPE **Access identifier type**

Type	List
Required	No
Default Type	Fixed
Default	ALL

Access identifier type

Abbreviation	Meaning
ALL	All
COM	Common
E1	E1
EQPT	Equipment

C.3.2.4 Output format

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
M ctag COMPLD

"AID,AIDTYPE:NTFCNCDE,CONDTYPE,SRVEFF,OCRDAT,OCRTM:CONDDESCR"
;
```

C.3.2.5 Output format parameters

AID **Access identifier**

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes
Default Type	Fixed
Default	lt-all

This is the address of the equipment and/or facility for which an alarm condition is being reported. Note: If the Modifier=COM, the Access ID is null.

Abbreviation	Meaning
ap-1-{1-16}	Application pack
ciu-1	Communication interface unit
comdac-1-{1-2}	COMDAC
drop-1-{1-16}-{1-32}	drop
e1-1-{1-4}-{1-4}	E1 physical port (feeder side)
ioe1-1-{1-4}	E1 circuit pack
iohdlc-1-{1-2}	IO_HDLC Circuit Pack
pwrsrc-1-{a,b}	Power Source
roc-1	Remote operations channel
sclk-1	Station clock
sh-1	Shelf
subap-{1-8}-{1-8}	Subshelf application pack
subdrop-{1-8}-{1-8}-{1-32}	Subshelf drop
subsh-{1-8}	Subshelf
v5i-{1-16}	V5 interface
v5l-{1-16}	V5 link
v5ts-{1-16}-{1-31}	V5 timeslot
{string}[a]	NE TID (Target identifier)

a only available via AEM

AIDTYPE **Access identifier type**

This parameter appears in the Access ID Block

Type	List
Required	Yes

Abbreviation	Meaning
ALL	All
COM	Common
E1	E1
EQPT	Equipment

NTFCNCDE

Notification code

This parameter appears in the Common Block

Type	List
Required	Yes

This is notification code associated with a single alarm condition.

Abbreviation	Meaning
CR	Critical alarm
MJ	Major alarm
MN	Minor alarm

CONDTYPE

Condition type

This parameter appears in the Common Block

Type	List
Required	Yes

Abbreviation	Meaning
AIS	Alarm indication signal
BCCDLK	BCC protocol data link failed
BKUPMEMP	System data memory mismatch
CABLE	Cable disconnect
CPYMEMF	Copy program memory failed
CTRLDLK	Control protocol data link failed
DATASYSCR	Data system failed critical
DATASYSMJ	Data system failed major
DATASYSMN	Data system failed minor
DBCRRPT	Data memory corrupt
DBMEMTRF	Data memory update abort
EXT	External failure
IMPROPRMVL	Improper removal
INT	Internal hardware failure
LCTRLDLK	Link control protocol data link failed
LOF	Loss of frame
LOS	Loss of signal

Abbreviation	Meaning
NE_ASSOC_FAILED[a]	Assoc with NE failed
PACKM	Pack mismatch
POLL	Not responding to poll
PRCDERR	Procedural error
PROTDLK	Protection protocol data link failed
PSTNDLK	PSTN protocol data link failed
PSTNF	Restart PSTN failed
PWR	Power fault
PWROVLD	Power overload
RAI	Remote alarm indication
RINGF	Ringing source input failed
SERVGRP	Server group maintenance limit exceeded
SFTCRRPT	Software program corrupt
SFTERR	Software version mismatch
SWFTDWNF	Software download failed
SYNC	Synchronization input failed
SYNCOOS	System free running
T-BERL	BER exceeds threshold
T-BERLN	BER exceeds threshold near end
T-FC-CABLE	Cable suspect exceeds failure count threshold
T-FC-INT	Internal pack failure exceeds failure count
UNXPRS	Unexpected reset

a only available via AEM

SRVEFF

Service effect

This parameter appears in the Common Block

Type	List
Required	Yes

This indicates the reported alarm condition is service-effecting or non-service effecting.

Abbreviation	Meaning
NSA	Non service affecting
SA	Service affecting

OCRDAT **Occurrence date**

This parameter appears in the Common Block

Type	Date
Required	Yes

This indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

OCRTM **Occurrence time**

This parameter appears in the Common Block

Type	Time
Required	Yes

This indicates the time of the condition being reported and has the format hours:minutes:seconds.

CONDDESCR **Condition description**

Type	String
Required	Yes
Min # chars	1
Max # chars	68

This is the text description for the reported alarm condition. This information can be found in the Correlations Tables. The 68 characters included a pair of escaped quotes \"\".

C.3.2.6 Generic error responses

Code	Definition	Reason for code
CLOS[a]	NE Connection Not Available	Connection with the <NE TID> is not available
IITA	Input, Invalid Target Identifier	TID does not match with SID, has unallowed characters, or string is too long
IICT	Input, Invalid Correlation Tag	Incorrect CTAG
IBNC	Input, Block Not Consistent.	Parameter entered in the wrong block.

a only available via AEM

C.3.3 RTRV-ALM-ENV (Retrieve-Alarm-Environment)

C.3.3.1 Purpose

The RTRV-ALM-ENV (Retrieve-Alarm-Environment) command instructs the system to retrieve all currently active environment alarms.

C.3.3.2 Input format

```
RTRV-ALM-ENV:[tid]::[ctag];
```

Abortable	Yes
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

C.3.3.3 Input format parameters

tid **Target ID**

This parameter appears in the TID Block

Type	String
Required	No
Default Type	Dynamic

Target ID is the name of the system to which the command is addressed.

ctag **Correlation tag**

This parameter appears in the CTAG Block

Type	String
Required	No
Default Type	Dynamic

This field is used to associate the command message to the response message.

C.3.3.4 Output format

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
AC atag REPT ALM ENV

"AID:NTFCNCDE,ALMTYPE,OCRDAT,OCRTM,ALMMSG"
;
```

C.3.3.5 Output format parameters

AID **Access identifier**

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes

AID is the access identifier of the contact closure.

Abbreviation	Meaning
mc-1-{1-8}	Miscellaneous Contact Closure
submc-{1-8}-{1-8}	Subshelf miscellaneous contact closures

NTFCNCDE **Notification code**

This parameter appears in the Common Block

Type	List
Required	Yes

NTFCNCDE is the alarm level.

Abbreviation	Meaning
CR	Critical Alarm
MJ	Major Alarm
MN	Minor Alarm

ALMTYPE

Alarm type

This parameter appears in the Common Block

Type	List
Required	Yes

Alarm Type. Use alarm type instead of condition type for RTRV-ALM-ENV.

Abbreviation	Meaning
ACF	AC Loss (AC Input Power Failure)
BD	Battery on Discharge
FAN	Fan Unit Failed
MISC1	Miscellaneous 1
MISC2	Miscellaneous 2
MISC3	Miscellaneous 3
MISC4	Miscellaneous 4
MISC5	Miscellaneous 5
MISC6	Miscellaneous 6
MISC7	Miscellaneous 7
MISC8	Miscellaneous 8
MJF	Fuse Major
MNF	Fuse Minor
NONE	None
PMJ	Power Major
PMN	Power Minor
TAMPER	Intrusion (Door Open)

OCRDAT

Occurrence date

This parameter appears in the Common Block

Type	Date
Required	Yes

This indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

OCRTM **Occurrence time**

This parameter appears in the Common Block

Type	Time
Required	Yes

This indicates the time of the condition being reported and has the format HH:MM:SS (hours:minutes:seconds).

ALMMSG **Alarm message**

This parameter appears in the Common Block

Type	String
Required	Yes
Min # chars	1
Max # chars	40

Alarm Message. Use alarm message instead of condition description. Refer to the Correlation Tables for the default environmental alarm conditions.

C.3.3.6 Generic error responses

Code	Definition	Reason for code
CLOS[a]	NE Connection Not Available	Connection with the <NE TID> is not available
IITA	Input, Invalid Target Identifier	TID does not match with SID, has unallowed characters, or string is too long
IICT	Input, Invalid Correlation Tag	Incorrect CTAG
IBNC	Input, Block Not Consistent.	Parameter entered in the wrong block.

a only available via AEM

Abbreviations

A

ADSL
Asymmetrical Digital Subscriber Line

AEM
AnyMedia® Element Manager

AFM
Access Feeder Multiplexer

AID
Access Identifier

ALL
Analog Leased Line

AMAS
AnyMedia Access System

AMS
Alarm Management Subsystem

ANSI
American National Standards Institute

AO
Autonomous Output Message

AP
Application Pack

APOG
Applications, Planning, and Ordering Guide

ASCII
American Standard Code for Information Interchange

ATM
Asynchronous Transfer Mode

AUTO
Automatic

B

BAL
Balance

BB
Broadband

BITS
Building Integrated Timing Supply

BRA
Basic Rate Access

C

CD
Compact Disk

CDE
Common Desktop Environment

CFL
Customer Feature List

CIT
Craft Interface Terminal

CIU
Communication Interface Unit

CLEI
Code assigned by Bellcore

CO
Central Office

COBRA
Common Object Request Broker Architecture

CPE
Customer Premises Equipment

CR
Critical (alarm severity)

CRV
Call Reference Value

CTAG
Correlation Tag

CTRL
Control

D

DB
Database

DC
Direct Current

DCN
Data Communication Network

DDS
Digital Data System

DFL
Default

DID
Direct Inward Dial

DLL
Digital Leased Line

DMG
Distributed Module Group

DMT
Discrete Multitone

DPT
Dial Pulse Termination

E

ECI
(Code that corresponds to the bar-coded label on the faceplate of the plug-in)

EIA
Electronic Industries Association

EM
Element Manager

EMS
Element Manager System

ENT
Enter

EOC
Embedded Operations Channel

EQPT
Equipment

ESF
Extended Super Frame

ETO
Equalized Transmission Only

EVT
Event

F

FAF
Facility Failure

FEF
Family of Equipment Failure

FLT
Fault

FS
SuperFrame with Datalink

FTP
File Transfer Protocol

FXO
Foreign Exchange Office

G

GLL
G Leased Line

GSI
Graphical System Interface

GUI
Graphical User Interface

H

HBER
High Bit Error Rate

HDLC
High Level Data Link Control

HDSL
High bit-rate Digital Subscriber Line

HP
Hewlett Packard

HW
Hardware

I

ICC
InterChangeability Code

ICMS
Integrated Configuration Management System

ID
Identifier

IEEE
Institute of Electrical and Electronics Engineers

IIOP
Internet Interoperability Protocol

IN
Information (alarm severity)

IP
Internet Protocol

IS
In Service

ISDN
Integrated Services Digital Network

ITU
International Telecommunication Union

L

LAN
Local Area Network

LBER
Low Bit Error Ratio

LCN
Local Communication Network

LE
Local Exchange

LED
Light Emitting Diode

LIC
License

LL
Leased Line

LLL
Leased Line Link

LLN
Logical Line Number

LPBK
Loop Back

LS
Loop Start

M

MG
Module Group

MHz
Megahertz

MJ
Major (alarm severity)

MLT
Mechanized Loop Testing

MM
Module Manager

MN
Minor (alarm severity)

MON
Degraded Signal

MR
Modification Request

N

NB
Narrowband

NE
Network Element

NEM
Network Element Management / AnyMedia EM subsystem

NFS
Network File Sharing

NM
Network Management

NMA
Network Monitoring and Analysis

NMS
Network Management System

NVDS
Nonvolatile Data Storage

NVPS
Nonvolatile Program Storage

O

OAM
Operations, Administration and Maintenance

OCU
Office Channel Unit

OMG
Object Management Group

OODB
Object Oriented Database

OOS
Out Of Service

OPS
Operations System

ORB
Object Request Broker

OS
Operation System

P

PBX
Private Branch Exchange

PC
Personal Computer

PCM
Pulse Code Modulation

PDN
Public Data Network

PFU
Power Filter Unit

PID
Password Identifier

PLL
Permanent Leased Line

PLN
Physical Line Number

PLR
Pulse Link Repeater

POTS
Plain Old Telephone Service

PPP
Point to Point Protocol

PSTN
Public Switched Telephone Network

PT
Power Test

PVC
Permanent Virtual Channel

R

RAM
Random Access Memory

RCV
Receive

RDLD
Red Lined

REPT
Report

ROC
Remote Operations Channel

ROM
Read Only Memory

RTU
Remote Test Unit

S

SC
Station Clock

SCC
Serial Communication Channel

SCEC
Secondary Channel Error Correction

SCI
Station Clock Interface

SCP
Shelf Connection Panel

SDH
Synchronous Digital Hierarchy

SEO
Supported Entity Outage

SNMP
Simple Network Management Protocol

SPLL
Semi Permanent Leased Line

SVC
Switched Virtual Circuits

SW
Software

T

TA
Terminal Adapter
Test Area

TAP
Test Access Path
Test Application Pack

TCA
Threshold Crossing Alert

TCP
Transmission Control Protocol

TID
Target Identifier

TL1
Transaction Language 1

TMN
Telecommunication Management Network

TNM
Total Network Management

TO
Transmission Only

TS
Test
Timeslot

U

UART
Universal Asynchronous Receiver/Transmitter

UAS
Unassigned

UDP
User Datagram Protocol

UEQ
Unequipped

UI
User Interface

UID
User Id

UPS
Uninterruptable Power Supply

UX
Unix

V

VL
V Leased Line

W

WAN
Wide Area Network

X

XO
Crystal Oscillator

Glossary

10Base T
This is a physical interface used for high speed Ethernet connection. It uses twisted pair cables.

A

a-wire
One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines connected for example with Z interfaces, U interfaces or ADSL interfaces. The a-wire is sometimes called tip-wire.

AEM-NB
AnyMedia Access System Element Manager for Narrowband Services. It may be also named simply EM in some parts of the document.

AID
Access Identifier - AID is the address within a TL1 command that is used to identify the physical or logical entity (or entities) within a network element to which the command applies. It has the format of a unique component identifier followed by hierarchical addresses of components. For example, e1-{1}-{2}-{4} is an object representing E1#4 on IO_E1 plug-in #2 in *AnyMedia* Access System shelf #1.

Active plug-in
Identifies the plug-in which is currently responsible for handling the service in a protected configuration. An active plug-in may also be in a state where no service is possible, for example faulty or moved to OOS by the operator.

ADSL (Full-rate ADSL, Classic)
Asymmetric Digital Subscriber Line - A method of data transmission over unloaded copper loops. The data rate transmitted toward the end user is typically much higher (up to about 6 Mbps) than the data rate transmitted by the end user (up to 640 kbps).

Alarm
Any condition that needs operator attention, since it may impact the normal operations of any system under operator responsibility (for example Element Manager, Network Element).

AMS
Alarm Management Subsystem.

***AnyMedia* Access System**
The *AnyMedia* Access System is an access network element (NE) which supports various narrowband and broadband services, digital as well as analog.

AO
Autonomous output; reports generated by the NEs.

Apparatus code
The apparatus code is an 8-byte item of ASCII information stored in the nonvolatile data storage (NVDS) of a plug-in (for example LPZ100, DTP500,...). It is a unique identifier which specifies the function of the plug-in.

Application
Group of one or more modules that offer related functionality.

Applications Pack (AP)
This is a circuit pack which provides the line-side interface functionality for POTS, SPOTS, ISDN or special service circuits. Each AP handles 24 or 32 lines (POTS, SPOTS, COIN and special services) or 16 lines (ISDN). There can be up to 16 APs in an *AnyMedia* Access System shelf. APs are for example LPZ100, LPU112, TAP100 as well as ADSL and AFM packs for broadband applications.

Archive
Process of copying file systems to removable media (such as tape) and deleting the original files once they have been backed up.

B

b-wire
One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines connected for example with Z interfaces, U interfaces or ADSL interfaces. The b-wire is sometimes called ring-wire.

Backup
Process of copying file systems to removable media (such as tape) to safeguard against loss, damage, or corruption.

BB
Broadband.

BCC protocol
Bearer Channel Connection protocol - This is a V5.2 protocol which allocates bearer channels on demand.

Bearer channel
A 64-kbps timeslot within the V5.x interface allocated for a B-channel of an ISDN user port or a channel from a POTS user port.

Blinking Alarm
An alarm which is continuously changing its status: raised, clear, raised, clear ...

Bridge
A network layer device that passes packets between two or more network segments that use the same data link communications protocol (OSI layer 2). The network segments appear as one segment to protocol levels higher than the data link layer. The bridge recognizes with the help of the MAC address which LAN component is connected at which port of the bridge. Data packets are only transferred over the bridge if the participant is at another port of the bridge. With a bridge, data traffic can be kept from a certain part of a LAN.

Built-in Self Test (BIST)
This is a procedure executed by each plug-in circuit pack either after power-up or on demand. The task is to check the functions of the hardware.

Burst Load
Load that can occur in certain well-known circumstances, where response times are no longer guaranteed, but queues handle excess traffic. After removing the causes of the burst load, and a certain settling time, normal operation is resumed. During burst load there is a graceful degradation, no loss of information, only a queueing occurs to defer the load to a later moment.

Busy Hour Load
Maximum load that is expected to occur in real life that must be handled with normal response times.

C

Circuit
This refers to the devices and functions built on or provided by an AP for one port. In some documents this is also called facility. The subscriber line is not included.

CIT: Craft Interface Terminal
A local RS232 connection on the *AnyMedia* access system to which a PC GUI can be connected.

Client
An entity that initiates requests to a server. For the *AnyMedia* Access System a client could be a PC with a GUI interface, a telnet session or an OS (like the AEM-NB).

Client Application
A group of one or more user modules that offer related functionality.

Client Host
A machine where one or more user modules are installed.

Common Data and Control Pack (COMDAC)
Common Data and Control - Plug-in which provides the central control and transmission fabric for the *AnyMedia* Access System. The COMDAC supports multiple system applications, including V5.x switched services and analog and digital leased lines (ALL and DLL) and a variety of application packs.

Communication channel
A group of one or more communication paths, all of different types. Is associated to a 64-kbps timeslot on a V5.x interface. This association may be changed by a protection switch (only V5.2).

Communication path
A communication path carries any one of the following information types:

- layer 2 data links carrying the control protocol, link control protocol, PSTN protocol, protection protocol and BCC protocol,
- all the ISDN Ds-type data (ISDND) (signaling), ISDN p-type data (ISDNP) and ISDN f-type data (ISDNF) from one or more user ports.

It should be noted that this definition includes the possibility that there is more than one communication path of the same information type, each allocated to a different logical communication channel.

Configuration Management
This consists of a set of functions for controlling the network elements, including initialization, parameter setting, starting and stopping and collecting information about the NE configuration.

Cross-Connection
A term for a logical association between two objects, e.g. between a subscriber port and a network interface. A physical cross-connection may additionnaly be established in the case of a network interface where bandwidth allocation is done on a provisioning basis (V5.1). In the case of V5.2 the bearer channel allocation is done on a per-call basis by the BCC protocol.

D

Date
This refers to the day, month, and year and represents a calendar function that needs to include a calculation for leap years and a capability of determining the day of the week from the date, and must be Y2K compliant.

DCN
Data Communications Network; the communication media and interconnected devices used to exchange management information between the AEM-NB, the NEs and other OSs.

Defaults
Defaults are the parameter values built into the *AnyMedia* Access System when it is shipped from the factory. The sum of all defaults forms the default configuration. (Default values are restored upon execution of an Initialize-System command.) For TL1 commands there are defined defaults for parameter values which are used for parameters not given in the command line.

Device Driver
A program that controls a specific device, such as a cartridge tape (DAT).

Distributed Module Group
Set of module groups of the same type distributed to provide load balancing and protection features.

Distribution Port
The circuitry that provides narrowband access (i.e., up to the 1.544 Mbps DS1 rate) to a single network interface over one (2- or 4-wire) metallic facility and converts between the format seen by this network interface (e.g., analog voice-frequency, ISDN U-interface, etc.) and the internal format (i.e., 4-Mbps timeslots). Distribution Ports are contained in Application Packs / Channel Units for the *AnyMedia* Access System. A maximum of 32 Distribution Ports are supported on POTS/COIN Application Packs (APs) and a maximum of 16 Distribution Ports are supported on ISDN APs.

Download
The process of moving information from a server to a client at the request of a client according to client/server paradigm. Expected applications of this capability are database retrievals.

Drop
This comprises the wire to the customer and customer premises equipment (CPE). In some documents this is also called equipment.

Duplex mode
Two COMDACs are equipped in the *AnyMedia* Access System. One COMDAC is active and controls the whole system, the other is in stand-by mode. During operation the memories (NVPS, NVDS and RAM) of both are mutually consistent. One reason to perform a side switch is if the active COMDAC fails. In this case the COMDAC previously in stand-by mode is now active.

E

E1
E1 is the standard acronym for the 2.048-Mbit/s interface defined in the ITU-T Recommendations G.703/G.704.

EAS Element Access Server
This is a CORBA server developed by Lumos Technologies which provides an interface between TL1 messages and CORBA methods.

EM Domain
An assigned collection of Controlled Objects.

EM Task
This represents a subset of the management functions supported by EM applications.

EM User
An entity defined via login name that can be assigned at least to an AEM user group.

EM User Group
A logical group of EM users enabled to access one or more “domains”. Permissions to access domains, applications and tasks are administered on an EM user group basis.

Embedded Operations Channel (EOC)
A duplicated DS0 data link dedicated for exchange operations messages between the LDS and RDT.

Entity
The term entity or object represents an entry in a TL1 administrative view, i.e. an entity (or object) may be entered, changed, deleted or retrieved by a TL1 command.

F

Far end
Any other network element residing in the network complex away from the AEM (that is the location of the service node is at the opposite end of the feeder E1 for the reported failure).

Fault Case
For some faults (e.g. DCN failure), normal working conditions need to be re-established within certain time limits. These are fault cases that are taken into account.

Fault Management
For detecting, displaying, storing, filtering and routing fault/alarm data.

Flag monitoring
The flag monitoring function requires that flags, sent on V5 communication channels towards the NE by the LE, must be monitored in the NE. Flag monitoring is mandatory for V5.2 interfaces and optional for V5.1 interfaces; flag sending is mandatory in any case for both directions, i.e. NE to LE and LE to NE.

Forced Switch
This refers to an Element Manager-initiated switch command that instructs the NE to perform a switch no matter what the conditions of the protection unit (COMDAC and IO_HDLC circuit packs only) are.

Full Backup
This copies a complete file system or directory.

G

General settings
These are parameters which are valid for all customer-specific configurations (for example loop-start function for all Z ports which are assigned for POTS service or suppression of out-band signalings for Z ports which are assigned for ALL (transmission-only) service).

GSI
Graphical System Interface - A user-friendly front-end for communicating with a system. In the *AnyMedia* Access System the GSI is installed on a Windows 95 personal computer and used for entering and receiving TL1 (Transaction Language 1) messages. The GSI provides support for managing the *AnyMedia* Access System in the following functional areas:

- Configuration management
- Fault management
- Performance management
- Security management
- Inventory management.

GSI-NB
The Graphical System Interface for narrowband services. This is a Windows 95-based PC which uses TL1 commands for the management of *AnyMedia* Network Elements.

GUI
The Graphical User Interface of the AEM-NB.

H

Host
A machine where one or more modules are installed.

Hub or Multiport Repeaters
This have 8, 12, 16 or more ports. With their help multiple devices with 10BASE-T interface can be connected to a single LAN. They have at least one additional port for connecting an additional segment of a LAN.

I

Incremental Backup
This copies new files and files that have changed since a previous backup. The incremental backups are usually given a dump level which determines which files are backed up. A certain level incremental backup will save all the new or changed files since the last backup with a lower level.

Inhibit Switch
This refers to an Element Manager-initiated switch command that instructs the NE to inhibit a side switch irrespective of the conditions of the active unit (COMDAC and IO_DS1 circuit packs only).

Internationalization
This is the process of isolating the language- and customs-dependent code in a computer program from the language-independent code. The term internationalization is often abbreviated as *i18n*.

IP Addresses
These are distributed according to the worldwide or local configuration. The IP address is used in ISO layer 3. A LAN contains tables for making an assignment between MAC address and IP address.

INIT-SYS command
The INIT-SYS command is used to clear the database and to restore the *AnyMedia* Access System to default values set at factory.

Inventory
The inventory is the summary of data stored on a plug-in in the NVDS during manufacturing which is used to identify the plug-in and its functionality.

ISDN BRA service
Integrated Services Digital Network Basic Rate Access Service - Connects ISDN BRA subscribers to the network via dial up connection.

L

Level 1 Applications
The minimum set of server applications that have to run together to provide the minimum functionality of the AEM-NB. These applications must exist before the Level 2 Application can be started. If this group is shut down the AEM-NB is shut down.

Level 2 Applications
Server applications that can be started up and shut down individually without affecting the functioning of other applications.

Line Test
Also called drop test. This checks for open circuits, short circuits, leakages to ground, foreign voltages, or other faults on the subscriber line that connects an AP port circuit to the CPE. The results are used to detect broken or bad quality wires even before the customer realizes a lack of quality.

LL/PLL Permanent Leased Lines
A service in which resources are used permanently for the transmission of data between two points. The switch is not responsible for setting up this service.

Locale
This is a geographic or political region that shares the same language and customs. In this document, a locale is also used to refer to the definition of the subset of a user's information technology environment that depends on language and cultural conventions.

Localization
This is the process of adapting a program for use in a specific locale.

LOG File
This is the file used for listing all actions that have occurred in a system. This information is generated and recorded concurrently and sequentially as transactions and events are processed in the system.

Logical line identity
For logical addressing of an end-customer termination either associated to a V5.1 or a V5.2 interface

Logical link
A logical entity providing 31 64-kbps timeslots which is associated to a 2.048-Mbps interface. One (V5.1) or more links (only V5.2) may be related to a V5.x interface.

M

MAC Address
This is a 6-byte hardware address, which identifies a unique participant worldwide in an Ethernet LAN. A MAC address is used in OSI layer 2.

Manual (normal) Switch
This refers to an Element Manager-initiated switch command that instructs the NE to perform a switch only if the protection unit (COMDAC and IO_HDLC circuit packs only) is in service and not faulty.

Migration
This refers to converting an NE from one software release to another by installing a different software release.

Mixed ISDN/POTS mode
An operation mode of the *AnyMedia* Access System where ISDN and POTS service is possible. Because ISDN subscribers are provisioned, the frame relay function has to be performed. Therefore at least one IO_HDLC plug-in is necessary (optionally a second one for protection). V5 communication channel information is frame relayed on the IO_HDLC plug-in and routed towards ISDN subscribers (for ISDN D-channel information) and to the COMDAC (for V5 layer 3 protocols) respectively.

Module
Executable that provides a subset of services in the AEM and describes a way to handle its process instances.

Module Group
Set of modules with strong functional dependencies that influence the way they are installed and managed.

N

NE
AnyMedia Access System Network Element.

Non-Volatile Data Storage (NVDS)
This refers to a capability of the *AnyMedia* Access System to store information in such a way as to survive indefinite periods of total power failure. The current values for all provisionable parameters are stored in the NVDS and hence are the parameter values that will be used on subsequent NE power-up.

Non-revertive mode
A certain system resource which has become faulty and thus caused a switch to or a replacement by a certain other (standby) resource is NOT reused automatically if the (temporarily) faulty resource returns back to operation. Instead of this the standby resource is used furtheron. A switch back may take place later on, but is independent from the recovery of the (temporarily) faulty resource.

Examples:

a) If a reference clock switch between COMDAC phase locked loop (PLL) reference clock inputs has occurred due to a failure condition, the AEM will not automatically return to the primary reference, even if the failure condition has cleared.

b) V5.2 protection switching of communication channels.

Non-Volatile Program Storage (NVPS)
This keeps software program data. It resides in the COMDAC.

Normal Hour Load
The average load expected during the lifetime of the system.

NVDS
Nonvolatile Data Storage - NVDS refers to that part of the database which can be retained even after a power failure, for example provision parameters.

NVPS
Nonvolatile Program Storage - NVPS refers to nonvolatile memory on the COMDAC used to store the load image.

O

Off-line Backups
These are backups performed automatically via any scheduling mechanisms, e.g. cron file.

On-line Backups
These are backups performed on user demand.

Operator
This refers to the *AnyMedia* Element Manager users.

Operator Mode
Testing initiated by staff from the EM using the NE-integrated capabilities. These tests can last some time, e.g., some measurements can be executed several times during a test session. The results in this mode usually are values (e.g. resistance, voltage, ...) and pass/fail decisions.

Overload
The load that causes the system to take drastic measures to ensure its integrity. During overload normal system function is disrupted and certain inputs (the ones causing the overload) are ignored. After clearing the overload situation, the system is left in asynchronous state for those inputs that generated the overload. Re-synchronization of this input retrieves synchronization.

OS
This is any operations system or Element Manager connected to the *AnyMedia* Access System by some means of communication. For the AEM-NB the communication method is TCP/IP.

P

Package
Logical parts of the AEM which provide specific functionality and can be started up, used and shutdown independently. There are three packages: Narrowband package, Broadband package and Administration package.

Password (PID)
Character string used to authenticate the identity of a user. The password should consist of 6 to 10 case sensitive alphanumeric characters, it should be changed frequently, it is stored and transmitted in an encrypted form.

PCM Highway
The COMDAC pack is connected to each AP by the PCM highway, which consists of two 4.096-Mbps serial links, a 4.096-MHz clock and an 8-kHz sync signal. The *AnyMedia* Access System uses two PCM highways between the COMDAC, the IO_HDLC and each of the 16 AP slots.

Performance Management
For receiving, detecting, time stamping, analyzing, displaying and storing performance data.

Plain Old Telephone Service (POTS)
The conversional 2-wire analog subscriber service.

Platform
The hardware on which any *AnyMedia* EM module, server or client, is running.

Platform Alarm
This is an alarm related to the *AnyMedia* Element Manager application or its hardware/software platform. It usually refers to an Element Manager function or hardware/software platform object.

PLL
Permanent Leased Line - These lines may be analog (ALL) or digital (DLL). They are not switched services and are not carried to the LE through the V5 interface but on special separate 2-Mbps links.

Plug-in
Term that is generally used for circuit pack units (for example LPZ100, IO_E1) which have pre-designated slots with the capability to plug in the circuit pack. Channel units are a subset of circuit packs used for supporting specific telephony functionality as in the case of line termination plug-in.

Port
This is circuitry built on an AP to provide an interface for subscribers. Note that more than one port can be housed on an AP, e.g. the LPZ100 provides 32 Z-ports.

Port Test
Also called circuit test. Verifies the ability of an AP port to provide proper transmission and signaling. It is the testing of the port hardware. The functions of the port test rather depend on the hardware function of the circuit (e.g. POTS, pulse metering, ISDN, ...). These tests are performed on each AP using part of their self-test capabilities.

Primary link
The 2.048-Mbps link in a multi-link V5.2 interface whose physical communication channel in timeslot 16 carries a communication path for the protection protocol and, on V5.2 initialization, also the communication path for the control protocol, link control protocol, and the BCC protocol. Other communication paths may also be carried in the timeslot 16.

Protection group 1
This is the standard group of physical communication channels consisting of the protected logical communication channel on the primary link and the protecting standby channel on the secondary link of a V5.2 interface, each located in timeslot 16.

Protection group 2
This is an optional protection group of a V5.2 interface, consisting of up to 3 standby communication channels, serving as protecting channels for all logical communication channels, not included in protection group 1.

Protection switch
A switch of the service from the service plug-in to the protection plug-in. A protection switch can be requested manually or driven by plug-in fault.

PSTN (user port)
Public Switched Telephone Network - Delivers analog telephony and data services to a POTS subscriber. It is addressed by a logical layer 3 address used in the relevant protocols on the V5.x interface. With respect to the V5.x interface the layer 3 address uniquely identifies one PSTN user port.

R

Response Time
The real elapsed time between detectable start of an action and its completion.

Restore
The process of copying backup files from removable media to a working directory, replacing the original files which could have been damaged.

ROC (Remote Operations Channel)
The bearer channel that conveys management information for a remote system (*AnyMedia* NE). The ROC is intended to be used when the system is installed at locations where no local Ethernet LAN and no separate network (e.g., X.25) exists.

Router
A network layer device that forwards packets from one network to another based on network layer information (OSI layer 3). Data packets are only transferred through the router if the participant is connected to another port of the router. With a router, data traffic can be kept from certain parts of a LAN. A router is more powerful than a bridge, it reduces the traffic on a LAN more than a bridge, because the IP address is evaluated for traffic control.

S

Station Clock
An external 2048 kHz synchronization signal, according to ITU-T G.703.

Security Management
This restricts access based upon the establishment of log-in procedures and an associated set of passwords. Screen locks are used as well.

User access is based upon domain partitioning. Controls the access to the data and capabilities inherent within a fixed partition of the network, including unbundling.

Server
A network element that waits for requests from clients to perform specific tasks. This is the function performed by the *AnyMedia* Access System.

Server Application
This is a set of server processes that perform a certain function.

Server Host
This is the machine where the system server modules are installed.

Server Module
This is the module that provides a subset of the system services.

Service
This is a piece of functionality provided by a server module.

Service State (of an object or entity)
This represents the current availability status of an associated resource or service in the NE from the management point of view (e.g., memory administration, maintenance).

Side Switching
This refers to the operation of deactivating the active core entity and activating the standby core entity (COMDAC and IO_HDLC circuit packs).

Simplex mode
One COMDAC is equipped in the *AnyMedia* Access System and controls the whole system. If this COMDAC fails the system also fails.

Software Download
The transport of the information required to upgrade/update a given NE's generic program.

Software package
At the architectural level, software packages are the primary vehicle for functional partitioning of the system. Software packages are configuration units of the system.

SPLL: Semi Permanent Leased Lines
A service in which resources are used permanently for the transmission of data between two points. The switch is responsible for setting up this service.

System
AEM-NB software. It provides a set of services allowing an operator to manage the *AnyMedia* NE.

System Failure
Any problem that prevents the AEM-NB from continuing to work.

T

TAS (Terminal Access Server)
This adapts local area networks (LAN) to wide area networks (WAN). TASs have the ability to integrate remote network elements in a local network. TASs support different LAN protocols (e.g. Ethernet) and WAN protocols (e.g. PPP).

TCA (Threshold Crossing Alert)
A crossing of a parameter threshold that is generally considered to be a transient condition.

TAP100
Test Application Pack - TAP100 is the internal test head executing the measurements required for the drop.

TELNET
This is a remote terminal interface protocol which allows remote login capability into a system on a network from any other node on that network that is also running TELNET. TELNET is a TCP/IP application.

Test Access Path (TAP)
There are up to two TAPs, one consisting of two pairs (TAP-B) and the other of six pairs (TAP-A), both providing internal and external metallic test access to the circuits.

Test Session
This is the procedure including all necessary functions to test a subscriber. This includes the setup of the test path as well as the release of the test equipment. The test session runs in the NE.

Time
This represents a 24-hour clock function.

TL1 (Transaction Language 1)
This is a bellcore standard message language. It is the primary means of operating and maintaining the V5DLC system. A TL1 message session supports bi-directional message transmission and when a TL1 link is established, the system can initiate autonomous messages to monitor alarms and changes in system status.

TS
Timeslot - Any cyclic time interval that can be recognized and defined uniquely. For example a 64-kbps channel of a V5 interface that can be used either as a bearer channel (carrying subscriber payload information) or as a communication channel (carrying both subscriber and network element signaling information).

U

Upgrade
Is a type of migration where the software release is changed from an earlier release to a later release.

Upload
The process of moving information from a client to a server at the request of a client according to client/server paradigm. Intended applications of this capability are software updates and restoring databases.

User
The operator who will use the EM to provision, maintain and monitor the *AnyMedia* Access System.

User Identifier (UID)
This is a unique user login identifier. This string is required and cannot be null. Grouping of UID string values for this command is not allowed. The valid UID value is a 3 to 10 case-sensitive alphanumeric character string.

V

V5.x interface

An ETSI defined interface between a local exchange and an access network element. A V5.1 interface consists of one single 2-Mbps (E1) link containing communication channels and bearer channels. A V5.2 interface consists of up to sixteen 2-Mbps (E1) links containing communication channels and bearer channels. The term V5.x interface is used for clarification that certain facts, a certain description or requirements are relevant for both V5.1 and V5.2 interface.

W

Workload or Load

A mix of actions and their frequencies from all possible input points that need processing in some way in the system.

Z

Z-port

A Z-port is circuitry built on a POTS AP to provide a Z interface for analog subscribers. Note that more than one Z port is housed on an *AnyMedia* Access System POTS AP, for example the LPZ100 provides 32 Z-ports.

Z-port (for transmission only)

This is a Z-interface normally used for services other than telephony (e.g. data transmission). This type of Z-interface does not support DC feeding and does not support out-band signaling. This interface can support Analog Leased Line (ALL) service.

Index

123...

1:1 protection 5-144
1:N protection 5-144

A

Access bar 3-4
Access protection 1-31
Access to the testroutines 7-25
Actions 1-16 3-46
AEM external system LAN interface A-5
AEM-NB protocol profiles A-5
AFM traffic monitoring 8-9
Alarm
  ~ log 1-28
  Classification 7-49
Alarm cut-off function (ACO) 5-5
Alarm interfaces
  Local alarm and status indicators 5-4
  Miscellaneous alarm closure inputs 5-4
  Office alarm outputs 5-4
Alarm Reporting 7-3
Alarm Severities 7-50
Alarm Viewer
  Alarm Table 7-15
  General Information 7-14
  Menu Bar 7-12
  System management functions 7-18
  Toolbar 7-14
Alarm viewer
  Starting 7-10
ALARM_AO_NOT_PROCESS 7-53
ALARM_EVENT_NOT_PROCESS 7-54
Alarms
  Alarm classification 7-49
  Reporting via EM 7-3
Alternate key 3-5
AnyMedia Access System
  Main components 5-2
AP provisioning 5-74
Applications, start 3-4
Apply (button) 3-14
Archive (database) 3-38
Archive command 3-40
Assign
  ~ controlled objects to domains 4-12
  ~ user groups access to applications 4-21
  ~ user groups access to domains 4-20
  ~ user groups access to tasks 4-22
  ~ users to user groups 4-6
Association (NE-AEM) 5-41
Association state 5-41
Autonomous Reports 1-16 3-46
Available Domains 5-38

B

Background map 5-20
Backspace key 3-5
Backup
  ~ command 3-40
  ~ level 3-43
  ~ schedules 3-43
  ~ types 3-38
Backup (database) 3-38
Bridge (definition) A-2
Built-in self-test 7-33
Buttons, often used
  Apply 3-14
  Cancel 3-14
  Close 3-14
  OK 3-14

C

Cancel (button) 3-14
CD-ROM XIX
Check box 3-13
CIT port protocol profiles A-3
Click (mouse) 3-5
Client application 3-16
Close (button) 3-14
COMDAC protection mode (simplex) 5-141
COMDAC Protection State 5-143
COMM_PROBLEM 7-55
Comments on document XX
COMMUNICATION_LOST 7-55
CONFIG_AO_NOT_PROCESS 7-56
CONFIG_EVENT_NOT_PROCESS 7-57
configuration management
  overview 1-3
Connection states (BB agent-AEM) 5-40 5-44
Control key 3-5
Controlled Objects 4-25
Craft interface terminal A-3

Create
~ domain 4-8
~ user 4-3
~ user group 4-14
Cross-connection
General 6-3
Cursor aspects 3-6
Cursor menu 3-10
CX_CONN_NOT_VISIBLE 7-58

D

Data Communications Network (definition) A-2
Database
Archive 3-38
Backup 3-38
Full backup 3-38
Incremental backup 3-38
Off-line backup 3-38
On-line backup 3-38
Restore 3-38
DCN configurations A-5
DCN introduction A-1
Delete
~ domain 4-12
~ user 4-7
~ user group 4-23
Delete key 3-5
disk space 2-2
Documentation XVIII
Comment procedure XX
Packaging and format XVIII
Domain
Create ~ 4-8
Delete ~ 4-12
Modify ~ 4-10
Double click (mouse) 3-5
Drag (mouse) 3-6
Drop-down list box 3-14

E

Environment Alarms 7-49
Escape key 3-5
External LAN AEM system interface A-5
External LAN interface profiles A-4
External system LAN interface A-3

F

Fault
clearance 1-28
identification 1-27
source 1-28
fault management
overview 1-3
File
Close 7-12 7-18
Exit 7-12 7-18
New 7-12 7-18
Print 7-12 7-18
Reload 7-13
Filr Browser 5-168
Full backup (database) 3-38
Functional diagram
Cross-connections 6-3

H

Help icon 3-4

I

Icon 3-7
Icons, greyed 3-4
ILLEGAL_SW_VERSION 7-60
Incremental backup (database) 3-38
Input focus 3-6
Installation
third-party software 1-24
integrated management mode 1-5
Interfaces
Synchronization interfaces 5-3
INVALID_MIB_IDENTIFIER 7-58
Inventory Management 5-6
IP Address 5-39

K

Keyboard 3-5

Keys, special
Alternate 3-5
Backspace 3-5
Control 3-5
Delete 3-5
Escape 3-5
Return 3-5

L

LAN interface, external system A-3
Life cycles
network 1-23
List box 3-14
Log
alarm ~ 1-28
Log alarms 3-47
Log management 3-46
Log out (workspace menu) 3-12
Log size 3-46
Log type
Actions 1-16 3-46
Autonomous Reports 1-16 3-46
System Internal Events 1-16 3-46
Log Viewer application 3-47
LOG_DEL_FULL 7-51
LOG_DEL_PART 7-52
Login 3-2 5-39
Logout
~ manually from System 3-3
Loopback
Test 7-38
LUMOS Installation 2-10

M

Menu
Actions 7-13
File 7-12 7-18
Filters 7-13 7-19
Help 7-13
Views 7-13
Menu bar 3-10
menu bar 5-18
Menus, often used
File -> Exit 3-15
File -> Print 3-15
Help -> Index 3-15
Help -> On Window 3-15
Metallic Shelf Controller 2-2
Minimize/Restore Front Panel (workspace menu) 3-12
Miscellaneous alarm closure inputs 5-4
Modifying
network 1-29
network element 1-30
Mouse 3-5

N

NE Memory Administration 5-6
NE Software Administration 5-6
NE synchronization 5-123
NE_ASSOC_FAILED 7-59
NE-AM Alarms 7-49
NEASSOC_LOST 7-59
Network
life cycle 1-23
modifying 1-29
normal operation 1-26
physical installation 1-24
Network Browser 5-19
Network element
modifying 1-30
registration 1-25
Network Element Browser 5-20
Network planning 1-24
Normal Alarms 7-49
NVDS
backup (data) 5-165
backup (telephony) 5-164
restore (data) 5-167
restore (telephony) 5-166

O

ObjectStore Configuration 2-18 2-22
ObjectStore Installation 2-17
Office alarm interfaces 5-4
Off-line backup (database) 3-38
OK (button) 3-14
On-line backup (database) 3-38
Option menu 3-14
OrbixMT Installation 2-13
OrbixNames Installation 2-15
Ordering
Document XIX

P

Pass-through interface C-1
Password 5-39
Path-through interface, TL1 messages C-3

Performance
~ monitoring 1-30
Performance management
overview 1-4
Performance monitoring
AFM feeder 8-6
Periodical Alarm Deletion 7-9
Platform Alarm 7-49
Port test 7-30
Port test result 7-28 7-31
Print reports 3-34
PRINT_ALARM 7-52
Product safety
Classification XVII
Programs (workspace menu) 3-12
protection
forced switching 5-144
inhibit switching 5-144
manual switching 5-144
side switching 5-144
Protection mode
COMDAC 5-147
Protection Source 5-129
Protection Switching
COMDAC 5-144 5-146
HDLC 5-147
Provisioning
network 1-25
provisioning model 5-35
Pushbutton 3-13

Q

Quitting the Alarm Viewer 7-11

R

Radio button 3-14
Reaction
to fault identification 1-28
Recovery 1-28
Reference Source 5-129
Refresh (workspace menu) 3-12
Remote Operations Channel (definition) A-2
Remote Operations Channel protocol profiles A-4
Remote Operations Channel, protocol A-4
Repetitive Alarm 7-7
Restart Workspace Manager (workspace menu) 3-12
Restore (database) 3-38
Restore command 3-40
Return key 3-5
RogueWave Installation 2-12
Router (definition) A-2

S

Safety
Classification XVII
SCHED-EX 7-32
Screen navigation
equipment configuration 5-35
Security Id 5-48
security management
overview 1-4
Selected Domains 5-38
Server application
Definition 3-16
Server applications start-up via a command line 3-18
Shelf Layout 5-3
Shelf protection
COMDAC 5-144
Shelf view 5-50
Shuffle Up/Down (workspace menu) 3-12
Software
~ installation 1-24
download 5-151
upgrade 5-151
Software copy
COMDAC 5-159
Sorting Alarms 7-17
Spin box 3-14
sreen navigation
service provisioning (narrowband) 6-6
stand-alone mode 1-5
Standby card test scheduling 7-32
Status Bar 5-18
status bar 5-21
Supported Interfaces 6-1
System
~ security 1-31
System Internal Events 1-16 3-46
System management functions 7-18

T

Tab 3-14
TAP test result 7-34
TAR command 3-41
Target ID 5-39
TCP/IP_CON_REFUSED 7-61
Terminating the Alarm Viewer 7-11
Testing interfaces 5-5

Testroutines
Access to the ~ 7-25
Built-in self-test 7-33
Loopback test 7-38
Port test 7-30
Port test result 7-28 7-31
Result of standby card test scheduling 7-33
Single Pulse Feeding test 7-37
Standby card test scheduling 7-32
TAP test result 7-34
Text box 3-14
timing source 5-129
timing source control
primary source 5-131
secondary source 5-131
timing sync mode 5-131
TL1 messages (Path-through interface) C-3
TL1_COMM_DENIED 7-54 7-56 7-62
tool bar 5-19
Trademarks XIV
Typographical conventions XV

U

UNABLE_TO_SYNC_ALARM 7-62
UNABLE_TO_SYNC_CONFIG 7-63 7-64
Unassign
~ controlled objects from domains 4-12
~ user groups access from applications 4-22
~ user groups access from domains 4-21
~ user groups access from tasks 4-23
~ users from user groups 4-6
User
Create ~ 4-3
Delete ~ 4-7
Modify ~ 4-5
User administration 4-1
User group
Create ~ 4-14
Delete ~ 4-23
Modify ~ 4-19

V

V5 interfaces 6-9
V5 Protocol 6-4

W

Window controls 3-6 3-7
maximize button 3-8
menu bar 3-8
minimize button 3-7
scroll bar 3-8
title bar 3-7
window frame 3-7
window menu 3-8
Window controls, AEM-NB windows 3-12
Window menu 3-9
Close 3-9
Lower 3-9
Maximize 3-9
Minimize 3-9
Move 3-9
Restore 3-9
Size 3-9
Windows, basics 3-6
Workspace manager 3-11
Workspace menu 3-11
Log out 3-12
Minimize/Restore Front Panel 3-12
Programs 3-12
Refresh 3-12
Restart Workspace Manager 3-12
Shuffle Up/Down 3-12