



***LambdaUnite*[™] MultiService Switch (MSS)**

Release 1

User Operations Guide

365-374-021
CC109088567
Issue a
October 2001



Copyright © 2001 Lucent Technologies. All Rights Reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies and the business management owner of the material.

For permission to reproduce or distribute, please contact:

Lucent Learning +49 911 526 3315 or +49 911 526 2455

Notice

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

Mandatory customer information

Trademarks

These trademarks are used in this manual:

LambdaUnite is a trademark of Lucent Technologies.

Ordering information

The order number of this document is 365-374-021 (Issue a).

Support

Technical support

Please contact your Lucent Technologies Local Customer Support Team (LCS) for technical questions about the information in this document.

Information product support

On the following page, we provide a comment form for you to report errors or make suggestions about this document.

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations



LambdaUnite™ MultiService Switch (MSS)
Release 1
User Operations Guide
365-374-021 Issue a October 2001

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve.

1. Was the information product:

	Yes	No	Not applicable
In the language of your choice?	☐	☐	☐
In the desired media (paper, CD-ROM, etc.)?	☐	☐	☐
Available when you needed it?	☐	☐	☐

Please provide any additional comments:

2. Please rate the effectiveness of this information product:

	Excellent	More than satisfactory	Satisfactory	Less than satisfactory	Unsatisfactory	Not applicable
Ease of use	☐	☐	☐	☐	☐	☐
Level of detail	☐	☐	☐	☐	☐	☐
Readability and clarity	☐	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐	☐
Completeness	☐	☐	☐	☐	☐	☐
Technical accuracy	☐	☐	☐	☐	☐	☐
Quality of translation	☐	☐	☐	☐	☐	☐
Appearance	☐	☐	☐	☐	☐	☐

If your response to any of the above questions is "Less than satisfactory" or "Unsatisfactory," please explain your rating.

3. If you could change one thing about this information product, what would it be?

4. Please write any other comments about this information product:

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to <http://www.lucent-info.com/comments>

Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com



Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations



LambdaUnite™ MultiService Switch (MSS)
Release 1
User Operations Guide
365-374-021 Issue a October 2001

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve.

1. Was the information product:

	Yes	No	Not applicable
In the language of your choice?	☐	☐	☐
In the desired media (paper, CD-ROM, etc.)?	☐	☐	☐
Available when you needed it?	☐	☐	☐

Please provide any additional comments:

2. Please rate the effectiveness of this information product:

	Excellent	More than satisfactory	Satisfactory	Less than satisfactory	Unsatisfactory	Not applicable
Ease of use	☐	☐	☐	☐	☐	☐
Level of detail	☐	☐	☐	☐	☐	☐
Readability and clarity	☐	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐	☐
Completeness	☐	☐	☐	☐	☐	☐
Technical accuracy	☐	☐	☐	☐	☐	☐
Quality of translation	☐	☐	☐	☐	☐	☐
Appearance	☐	☐	☐	☐	☐	☐

If your response to any of the above questions is "Less than satisfactory" or "Unsatisfactory," please explain your rating.

3. If you could change one thing about this information product, what would it be?

4. Please write any other comments about this information product:

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to <http://www.lucent-info.com/comments>

Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com





Contents

About this information product

Purpose	<u>xvii</u>
Reason for reissue	<u>xvii</u>
Safety labels	<u>xvii</u>
Conventions used	<u>xix</u>
Related documentation	<u>xx</u>
Documented feature set	<u>xxii</u>
How to comment	<u>xxii</u>
How to order	<u>xxii</u>

1 Safety

Overview	<u>1-1</u>
General notes on safety	
Overview	<u>1-3</u>
Structure of safety instructions	<u>1-4</u>
Basic safety aspects	<u>1-6</u>
Specific safety areas	
Overview	<u>1-10</u>
Laser safety	<u>1-11</u>

Optical circuit pack specifications	<u>1-14</u>
Laser product classification	<u>1-15</u>
Electrostatic discharge	<u>1-18</u>
Safety requirements in specific deployment phases	
Overview	<u>1-20</u>
Transportation	<u>1-21</u>
Storage	<u>1-24</u>
Installation	<u>1-26</u>
Taking into operation	<u>1-29</u>
Operation and maintenance	<u>1-31</u>
Taking out of operation	<u>1-36</u>

2 Security administration

Overview	<u>2-1</u>
Administering user logins	
Overview	<u>2-3</u>
Creating a user login	<u>2-5</u>
Modifying a user login	<u>2-8</u>
Deleting a user login	<u>2-10</u>
Disabling user logins	<u>2-11</u>
Enabling user logins	<u>2-13</u>
Logging out NE users	<u>2-15</u>
Supporting information for “Administering user logins”	<u>2-17</u>
Changing super user ids	
Overview	<u>2-19</u>

Changing super user ids on the *WaveStar*® CIT [2-20](#)

Changing user passwords

Overview [2-22](#)

Changing the user password on the *WaveStar*® CIT [2-23](#)

Changing the user password on the NE [2-25](#)

Modifying user security parameters

Overview [2-27](#)

Modifying a user's own notification list [2-28](#)

Modifying user security parameters by admin [2-30](#)

Supporting information for “Modifying user security parameters by admin” [2-32](#)

Provision global security parameters [2-33](#)

Retrieving security information

Overview [2-35](#)

Displaying a list of all users logged into an NE [2-36](#)

Displaying login information for an NE [2-38](#)

Retrieve security log [2-40](#)

Retrieve system wide security parameters [2-41](#)

Retrieve security info of own user [2-43](#)

Retrieve security info of all or other user [2-45](#)

3 Management communication setup

Overview [3-1](#)

Changing the NE name (TID) [3-3](#)

Configuring the data communication network (high level) [3-6](#)

Configuring the basic DCN parameters for the *WaveStar*® CIT [3-9](#)

Supporting information for “Configuring the basic DCN parameters for the <i>WaveStar</i> [®] CIT”	<u>3-12</u>
Configuring the LDB timers for the <i>WaveStar</i> [®] CIT	<u>3-15</u>
Supporting information for “Configuring the LDB timers for the <i>WaveStar</i> [®] CIT”	<u>3-17</u>
Administering the address list at the <i>WaveStar</i> [®] CIT	<u>3-18</u>
Supporting information for “Administering the address list at the <i>WaveStar</i> [®] CIT”	<u>3-22</u>
Configuring the basic DCN parameters for an NE	<u>3-28</u>
Supporting information for “Configuring the basic DCN parameters for an NE”	<u>3-32</u>
Configuring data communication channels	<u>3-36</u>
Supporting information for “Configuring data communication channels”	<u>3-39</u>
Configuring the TARP parameters for an NE	<u>3-44</u>
Supporting information for “Configuring the TARP parameters for an NE”	<u>3-46</u>
Assigning TARP manual adjacencies	<u>3-47</u>
Supporting information for “Assigning TARP manual adjacencies”	<u>3-52</u>
Setting system parameters	<u>3-53</u>
Supporting information for “Setting system parameters”	<u>3-55</u>
Setting date and time	<u>3-56</u>
Supporting information for “Setting date and time”	<u>3-58</u>

4 Equipment provisioning

Overview	<u>4-1</u>
Initial equipment provisioning	<u>4-3</u>
Configuring the system	<u>4-4</u>

Configuring the shelf	<u>4-7</u>
Configuring a slot	<u>4-9</u>
Creating a new circuit pack	<u>4-11</u>
Reassigning a circuit pack	<u>4-14</u>
Configuring an optical SDH/SONET port	<u>4-16</u>
Setting the parameters of optical ports	<u>4-19</u>
Configuring a tributary	<u>4-26</u>
Provisionable parameters of tributaries	<u>4-28</u>
Removing equipment from the system	<u>4-29</u>
Retrieving equipment info for the system	<u>4-31</u>
Retrieving equipment info for the shelf	<u>4-33</u>
Retrieving equipment info for slots	<u>4-35</u>
Viewing data of a slot	<u>4-36</u>
Retrieving equipment info for circuit packs	<u>4-37</u>
Viewing data of a circuit pack	<u>4-38</u>
Retrieving equipment info for optical SDH/SONET ports	<u>4-40</u>
Viewing data of a optical SDH/SONET port	<u>4-41</u>
Retrieving equipment info for tributary	<u>4-43</u>
Viewing data of a tributary	<u>4-44</u>
Retrieving equipment info for the backplane	<u>4-46</u>
Viewing data of the backplane	<u>4-47</u>
Viewing an equipment protection group	<u>4-48</u>
Parameters for a 1+1 equipment protection	<u>4-49</u>
Switching a 1+1 equipment protection	<u>4-50</u>

5 Alarm management

Overview	5-1
Retrieving the <i>WaveStar</i> [®] CIT NE Alarm List	5-3
The <i>WaveStar</i> [®] CIT NE Alarm List	5-5
Retrieving the <i>WaveStar</i> [®] CIT NE Alarm Log	5-9
Identifying SDH tributaries in alarm messages	5-10
Performing an LED test	5-14
Retrieving ASAP information	5-15
Creating a new ASAP	5-18
Creating non-reporting ASAPs	5-21
Modifying an existing ASAP	5-23
Setting ASAPs for a shelf	5-26
Setting the port monitoring mode	5-29
Configuring fault management parameters for an SDH port	5-31
Configuring fault management parameters for a SONET port	5-36
Enabling or disabling autonomous alarm forwarding	5-41

6 Timing provisioning

Overview	6-1
Viewing the timing configuration	6-3
Parameters of the “Synchronization Characteristics” window	6-5
The External Timing Input Port tabs	6-6
The External Timing Output Port tabs	6-7
The Timing Reference tabs	6-12

The System Timing Parameters tab	6-15
Configuring the external timing output ports SDH mode	6-19
Configuring the external timing output ports SONET mode	6-23
Configuring the external timing input ports SDH mode	6-27
Configuring the external timing input ports SONET mode	6-29
Configuring the timing references	6-31
Configuring the system timing	6-34
Forced Switching of the timing generator to the holdover mode	6-37
Switching to another timing reference	6-39

7 Traffic provisioning

Overview	7-1
Viewing existing cross-connections	7-3
Parameters of the window “View Cross Connections”	7-5
Retrieve Cross-connection Lists	7-8
Supporting information on the “Cross Connection List”	7-10
Substructuring of input and output signals	7-12
Creating a new cross-connection	7-16
Modifying a cross-connection	7-21
Rolling a cross-connection	7-23
Bridging a cross-connection	7-26
Deleting a cross-connection	7-29
Viewing an existing protection group	7-32
Parameters of the window “View Protection” for a 1+1 MSP or APS	7-34
Parameters of the window “View Protection” for a 2-Fiber MS-SPRing or 2-fiber BLSR	7-37

Parameters of the window “View Protection” for SNCP and UPSR	7-40
Creating a cross-connection in a 2-fiber MS-SPRing network environment	7-42
Creating a new 1+1 MSP or 1+1 APS (NE level)	7-46
Creating a new 2-fiber MS-SPRing (NE level)	7-49
Creating an SNCP or UPSR (NE level)	7-52
Deleting a protection group	7-56

8 Traffic maintenance

Overview	8-1
Switching an MSP or APS	8-2
Switching a 2-fiber MS-SPRing or 2-fiber BLSR	8-4
Switching a UPSR or SNCP	8-6
Clearing a protection switch request	8-8
Retrieve protection switch reports	8-10
Supporting information on the “BLSR Protection Switch List”	8-11
Supporting information on the “NE Protection Switch Activity Log”	8-12

9 Performance monitoring

Overview	9-1
Enabling or disabling performance monitoring data collection	9-2
Retrieving performance monitoring settings for individual ports or tributaries	9-6
Retrieving performance monitoring reports	9-9

10 Software upgrade

Overview	10-1

Performing an initial software download using the CIT	10-2
Performing a software download for upgrade purposes using the <i>WaveStar</i> ® CIT	10-7
Activating an NE software generic	10-12
Retrieving NE software generic information	10-14
Supporting information for “Retrieving NE software generic information”	10-15
11 Database backup	
Overview	11-1
Limiting the number of saved backups	11-2
Manually backup database to the <i>WaveStar</i> ® CIT	11-3
Retrieving NE database information	11-5
Supporting information for “Retrieving NE database information”	11-6
12 Periodic activities	
Overview	12-1
Replacing the air filter	12-2
13 Security and administration concepts	
Overview	13-1
Security management	13-2
User administration	13-3
History logs	13-12
14 Management communication setup concepts	
Overview	14-1
Basic DCN principles	14-2

DCN configurations	<u>14-6</u>
DCN configuration guidelines	<u>14-11</u>
Partition repair guidelines	<u>14-12</u>
DCN protocols and services	<u>14-16</u>
NSAP address format	<u>14-19</u>
Data communication channels	<u>14-24</u>
LAN access	<u>14-31</u>
Name-to-address translation	<u>14-32</u>
NE name administration	<u>14-37</u>
System provisioning	<u>14-38</u>

15 Equipment provisioning concepts

Overview	<u>15-1</u>
Equipment provisioning and autoprovisioning	<u>15-2</u>
<i>WaveStar</i> [®] CIT methods to perform provisioning	<u>15-3</u>
Provisioning of new components	<u>15-5</u>
Shelf configuration	<u>15-6</u>
Overview of access identifiers	<u>15-8</u>
Shelf provisioning	<u>15-13</u>
Slot/circuit pack provisioning	<u>15-14</u>
Port and tributary provisioning	<u>15-15</u>
Gigabit Ethernet (GE1/SX4) Interface	<u>15-16</u>
Equipment protection	<u>15-18</u>

16 Alarm management concepts

Overview	<u>16-1</u>

***LambdaUnite*[™] MSS fault management**

Overview [16-2](#)

Basic fault management concepts [16-3](#)

LambdaUnite[™] MSS fault management principle [16-6](#)

***LambdaUnite*[™] CIT alarm presentation formats**

Overview [16-9](#)

Alarm severities [16-10](#)

Alarm format preferences [16-12](#)

Signalling of alarms

Overview [16-17](#)

WaveStar[®] CIT visual alarm indicators [16-19](#)

NE local indications [16-21](#)

Impact of state changes on the signalling of alarms [16-22](#)

Alarm provisioning

Overview [16-24](#)

Alarm severity assignment profiles [16-25](#)

Port monitoring mode [16-34](#)

Forward error correction [16-35](#)

Operations interfaces

Overview [16-38](#)

The *LambdaUnite*[™] MSS user panel [16-39](#)

ACO interaction with an alarm test [16-42](#)

Circuit pack status indicators [16-44](#)

Office alarm interfaces [16-48](#)

17 Timing provisioning concepts

Overview	<u>17-1</u>
Timing generator	<u>17-2</u>
Timing configuration	<u>17-3</u>
Timing quality	<u>17-4</u>
Timing protection	<u>17-8</u>

18 Traffic provisioning concepts

Overview	<u>18-1</u>
Cross-connection management	<u>18-2</u>
Cross-connection wizard	<u>18-6</u>
Protection mechanisms	<u>18-12</u>
Path Protection	<u>18-13</u>
Line Protection	<u>18-18</u>
Ring Protection	<u>18-20</u>
Protection configurations	<u>18-24</u>

19 Performance monitoring concepts

Overview	<u>19-1</u>
Introduction	<u>19-2</u>
The performance monitoring process	<u>19-5</u>
Performance measurements	<u>19-6</u>
Performance monitoring reports	<u>19-12</u>
Impact of configuration changes on performance monitoring	<u>19-18</u>

20 Software upgrade concepts

Overview	<u>20-1</u>
NE memory concept	<u>20-2</u>
Software download	<u>20-3</u>

21 Database backup concepts

Overview	<u>21-1</u>
Configuration backup and restoration	<u>21-2</u>

22 *WaveStar*[®] CIT Tutorial

Overview	<u>22-1</u>
Installation procedures	
Overview	<u>22-4</u>
Installing the <i>WaveStar</i> [®] CIT	<u>22-5</u>
Connecting the <i>WaveStar</i> [®] CIT to the NE	<u>22-8</u>
<i>WaveStar</i> [®] CIT login/logout procedure	<u>22-11</u>
General <i>WaveStar</i> [®] CIT concept	<u>22-13</u>
<i>WaveStar</i>[®] CIT main window	
Overview	<u>22-14</u>
Elements of the <i>WaveStar</i> [®] CIT user interface	<u>22-15</u>
Tool bar of the <i>WaveStar</i> [®] CIT	<u>22-17</u>
Standard window components	<u>22-19</u>
Selection windows	<u>22-24</u>
General window handling	<u>22-27</u>
General pushbuttons	<u>22-30</u>

Basic operations [22-32](#)

Network element selection and login [22-33](#)

Overview of the menu structure [22-37](#)

Logout from NE(s) [22-39](#)

System view

Overview [22-41](#)

Shelf view [22-42](#)

The ring map [22-52](#)

Overview of the shelf-view menu structure [22-54](#)

Reports [22-61](#)

View rolling events [22-62](#)

Cut Through view

Overview [22-63](#)

Entering the Cut Through view [22-64](#)

Interactive – Execute TL1 single commands [22-67](#)

Interactive – Manage a listbox file [22-69](#)

Working with script files [22-70](#)

Working with logs [22-72](#)

GL Glossary [GL-1](#)

IN Index [IN-1](#)



About this information product

.....

Purpose This User Operations Guide provides operations, administration and maintenance information about the *LambdaUnite*[™] MSS.

Reason for reissue

This is the initial version of this guide for *LambdaUnite* MSS Release 1.0.

Safety labels The present manual contains basic safety instructions which have to be strictly observed when handling the equipment and systems described.

The most important safety instructions are collected in the “Safety” chapter in Fascicle 1 of this manual.

Strictly observe the warnings and safety instructions described in Fascicle 1 (“Safety”) before carrying out work of any kind on the equipment and systems described.

All safety instructions 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.

Example:



Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes. Ensure that the line circuit-breaker on the fuse panel is in the "OFF" position before removing or inserting the power supply plug.

Classification of hazards

There are three classes of hazards. They are designated using the head words "Danger", "Warning" and "Caution". Their meaning is as follows:

- ***Danger***
is used to mark safety warnings which, if not followed, will certainly or with a very high degree of probability result in death or extremely serious injury.
- ***Warning***
is used to mark safety warnings which, if not followed, can lead to serious injury or permanent damage to the health of an individual or to property.
- ***Caution***
is used to mark safety warnings which, if not followed, can lead to injury or property damage - including financial losses due to extensive operational impairment.

Warning symbols

The examples below show the warning symbols used.



Example of a general warning about a danger.

**DANGER**

Example of a warning about laser radiation.

**DANGER**

Warning about devices sensitive to electrostatic discharge (ESD)

The safety instructions for the classes “Danger”, “Warning” and “Caution” always have a warning symbol, the “Important” and “Notice” safety instructions can, but do not always have a warning symbol.

Conventions used

These conventions are used in this document:

Numbering

The chapters of this document are numbered consecutively. The page numbering restarts at “1” in each chapter. To facilitate identifying pages in different chapters, the page numbers are prefixed with the chapter number. For example, page 2-3 is the third page in chapter 2.

Cross-references

Cross-reference conventions are identical with those used for numbering, i.e. the first number in a reference to a particular page refers to the corresponding chapter.

Keyword blocks

This document contains so-called keyword blocks to facilitate the location of specific text passages. The keyword blocks are placed to the left of the main text and indicate the contents of a paragraph or group of paragraphs.

Typographical conventions

Special typographical conventions apply to elements of the graphical user interface (GUI), file names and system path information, keyboard entries, alarm messages etc.

- Elements of the graphical user interface (GUI)

These are examples of text that appears on a graphical user interface (GUI), such as menu options, window titles or push-buttons:

- **Provision...**, **Delete**, **Apply**, **Close**, **OK** (push-button)
- **Provision Timing/Sync** (window title)
- **View Equipment Details...** (menu option)
- **Administration** → **Security** → **User Provisioning...** (path for invoking a window)
- File names and system path information
These are examples of file names and system path information:
 - *setup.exe*
 - *C:\Program Files\Lucent Technologies*
- Keyboard entries
These are examples of keyboard entries:
 - **F1**, **Esc X**, **Alt-F**, **Ctrl-D**, **Ctrl-Alt-Del** (simple keyboard entries)
A hyphen between two keys means that both keys have to be pressed simultaneously. Otherwise, a single key has to be pressed, or several keys have to be pressed in sequence.
 - `copy abc xyz` (command)
A complete command has to be entered.
- Alarms and error messages
These are examples of alarms and error messages:
 - Loss of Signal
 - Circuit Pack Failure
 - HP-UNEQ, MS-AIS, LOS, LOF
 - Not enough disk space available

Abbreviations

Abbreviations used in this document can be found in the “Glossary” unless it can be assumed that the reader is familiar with the abbreviation.

Related documentation

This section briefly describes the documents that are included in the *LambdaUnite* MSS documentation set.

- Installation Guide

The *LambdaUnite* MSS Installation Guide is a step-by-step guide to system installation and setup. It also includes information needed for pre-installation site planning and post-installation acceptance testing.

- Applications and Planning Guide

The *LambdaUnite* MSS Applications and Planning Guide (APG) is for use by network planners, analysts and managers. It is also for use by the Lucent Account Team. It presents a detailed overview of the system, describes its applications, gives planning requirements, engineering rules, ordering information, and technical specifications.

- User Operations Guide

The *LambdaUnite* MSS User Operations Guide provides step-by-step information for use in daily system operations. The manual demonstrates how to perform system provisioning, operations, and administrative tasks by use of *WaveStar*® CIT.

- Alarm Messages and Trouble Clearing Guide

The *LambdaUnite* MSS Alarm Messages and Trouble Clearing Guide gives detailed information on each possible alarm message. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.

- Operations System Engineering Guide

The *LambdaUnite* MSS Operations System Engineering Guide serves as a reference for all TL1 commands which can be used to operate the network element. The manual also gives an introduction to the concept of the TL1 commands and instructs how to use them.

- *WaveStar* SNMS Provisioning Guide (Application *LambdaUnite* MSS)

The *WaveStar* SNMS Provisioning Guide (Application *LambdaUnite* MSS) gives instructions on how to perform system provisioning, operations, and administrative tasks by use of *WaveStar* SNMS.

The following table lists the documents included in the *LambdaUnite* MSS documentation set.

Document Number	Title
109088559 (365-374-020)	<i>LambdaUnite</i> MSS Applications and Planning Guide
CC109088567 (365-374-021)	<i>LambdaUnite</i> MSS User Operations Guide
109088617 (365-374-022)	<i>LambdaUnite</i> MSS Alarm Messages and Trouble Clearing Guide
109088575 (365-374-023)	<i>LambdaUnite</i> MSS Installation Guide
109088583 (365-374-024)	<i>LambdaUnite</i> MSS Operations System Engineering Guide (TL1 Reference Manual)
109088609 (365-374-025)	<i>WaveStar</i> SNMS Provisioning Guide (Application <i>LambdaUnite</i> MSS)
109088591	CD-ROM Documentation <i>LambdaUnite</i> MSS (all manuals on one CD-ROM)

Documented feature set This manual describes *LambdaUnite* MSS release 1.0. For technical reasons some features have been documented that will not be available until later software versions. For precise information about the availability of features, please consult the Software Release Description. This provides details of the status at the time of software delivery.

How to comment Because customer satisfaction is extremely important to Lucent Technologies, every attempt is made to encourage feedback from customers about our information products.

Customer Comment Form

A customer comment form is located immediately after the title page of this document. Please fill out the form and fax it to the number provided on the form.

How to order If the customer comment form is missing, send or fax comments about this document to

Lucent Technologies Network Systems GmbH

Lucent Learning

Thurn- und-Taxis-Str. 10
90327 Nürnberg, Germany
Fax: +49 911 526 3545



1 Safety

Overview

Purpose The aim of this chapter on safety is to provide users of *LambdaUnite*[™] MSS systems with the relevant information and safety guidelines to safeguard against personal injury. Furthermore, this chapter may be useful to prevent material damage to the equipment.

The present chapter on safety **must** be read by the responsible technical personnel before carrying out relevant work on the system. The valid version of this document must always be kept close to the equipment.

Potential sources of danger The *LambdaUnite* MSS equipment 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 equipment 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 the following:

- live parts,
- laser light,
- hot surfaces, or
- sharp edges

Contents

General notes on safety	<u>1-3</u>
Structure of safety instructions	<u>1-4</u>
Basic safety aspects	<u>1-6</u>
Specific safety areas	<u>1-10</u>
Laser safety	<u>1-11</u>
Optical circuit pack specifications	<u>1-14</u>
Laser product classification	<u>1-15</u>
Electrostatic discharge	<u>1-18</u>
Safety requirements in specific deployment phases	<u>1-20</u>



General notes on safety

Overview

Purpose This section provides general information on the structure of safety instructions and summarizes general safety requirements.

Contents		
	Structure of safety instructions	1-4
	Basic safety aspects	1-6



Structure of safety instructions

General structure All safety instructions include a **warning symbol** and a **signal word** that classify 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 minimise the danger.

Example:



DANGER

Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes.

Ensure that the line circuit breaker on the Power Interface (PI) is in the “OFF” position before removing or inserting the power supply plug.

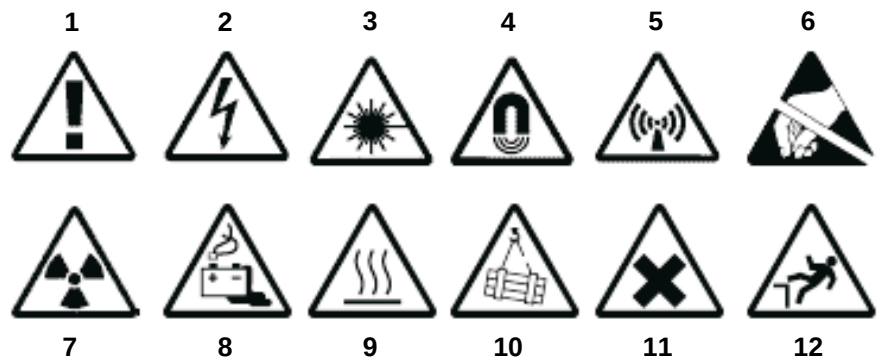
Danger classification There are three classes of safety instructions: “DANGER”, “WARNING” and “CAUTION”. Which class is relevant depends on the consequences of ignoring the safety instruction:

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.

Warning symbols These warning symbols are defined for safety instructions:



Legend:

1	General warning of danger
2	Electric shock
3	Hazard of laser radiation
4	Magnetic hazard
5	Electromagnetic radiation
6	Components sensitive to electrostatic discharge (ESD)
7	Radioactivity
8	Hazard caused by batteries
9	Hot surface
10	Heavy load
11	Unhealthy, irritating substance
12	Hazard of falling



Basic safety aspects

General safety requirements

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

- Transport, storage and operation of the system must be under the ***permissible conditions only***.
See accompanying documentation and information on the system.
- 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 system, the personnel requires ***special training***.
- The system must be operated by ***expert and authorised users only***.
The user must operate the system only after having ***read and understood*** this 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.
- The 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 system must be operated only with the connections and under the environmental conditions as described in the documentation.
- 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 authorised 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 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.

- Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived.
- Non-system software is used at one's **own risk**. The use/installation of non-system software can adversely affect the normal functioning of the system.
- Only use **tested and virus-free** data carriers (floppy disks, streamer tapes, ...).

Summary of important safety instructions

Especially observe the following safety instructions, they are of particular importance for *LambdaUnite™* MSS systems::

- This equipment is to be installed only in **Restricted Access Areas** in business and customer premises.
Applications in accordance with Articles 110-16, 110-17 and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other installations exempt from the enforcement of the National Electrical Code may be engineered according to the accepted practices of the local telecommunications utility.
- This product should only be operated from the type of power source indicated on the marking label.
- This equipment must be provided with a readily accessible disconnect device as part of the building installation.
- Disconnect up to four (4) power supply connections when removing power from the system.
- Installation must include an independent frame ground drop to the building ground. Refer to the *LambdaUnite MSS Installation Guide*.
- For information on proper mounting instructions, consult the *LambdaUnite MSS Installation Guide*.
- Install only equipment identified in the *LambdaUnite MSS Installation Guide* provided with this product. Use of other equipment may result in improper connection of circuitry leading to fire or injury to persons.

- To reduce the risk of electrical shock, do not disassemble this product. Installation and service should be performed by trained personnel only. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electrical shock when the unit is subsequently used.
- Slots and openings in this product are provided for ventilation. To protect the product from overheating, these openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.
- Never push objects of any kind into this product through 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 liquids of any kind on the product.
- CAUTION: This equipment is designed to permit the connection of the grounded conductor of the DC supply circuit to the grounding conductor at the equipment.
 1. This equipment shall be connected directly to the DC supply system grounding electrode conductor or to a bonding jumper from a grounding terminal bar or bus to which the DC supply system grounding electrode conductor is connected.
 2. This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system shall not be grounded elsewhere.
 3. The DC supply source is to be located within the same premises as this equipment.
 4. There shall be no switching or disconnection devices in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.



CAUTION

LambdaUnite MSS systems contain optical circuit packs that can emit laser radiation assessed as IEC Hazard Level 3A.

Therefore, LambdaUnite MSS systems may only be installed in restricted access locations! Restricted access locations are controlled environments where there is no ready access to the general public, but only to authorized persons who have received adequate training in laser safety.



Specific safety areas

Overview

Purpose The aspects of “laser safety” and “handling of components sensitive to electrostatic discharge (ESD)” are of vital importance for the *LambdaUnite*[™] MSS equipment. Therefore, the key safety instructions for these subjects are summarised in the following.

Contents

Laser safety	<u>1-11</u>
Optical circuit pack specifications	<u>1-14</u>
Laser product classification	<u>1-15</u>
Electrostatic discharge	<u>1-18</u>

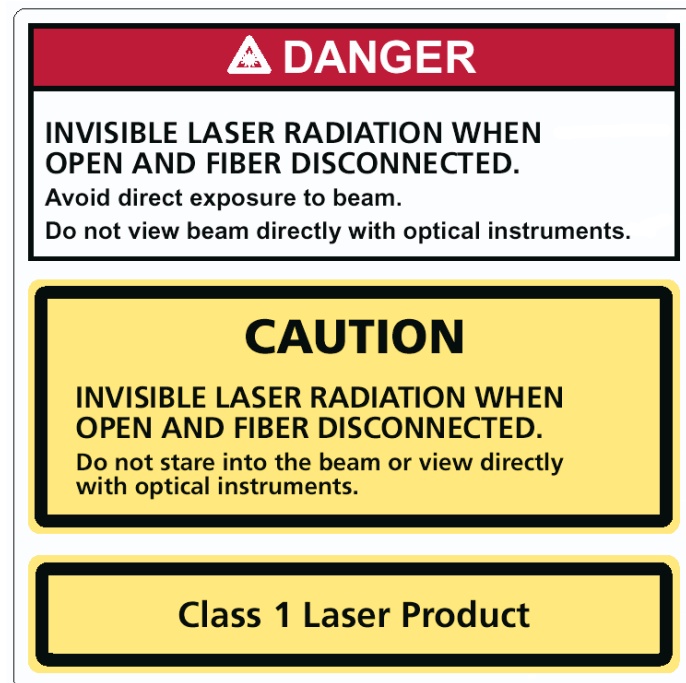


Laser safety

System design The *LambdaUnite*™ MSS system complies with the Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH) regulations FDA/CDRH 21 CFR 1040.10 and 1040.11 as a Class I and with IEC 60825-1 as a Class 1 Optical Fiber Telecommunication laser product.

The system has been designed to ensure that the operating personnel is not endangered by laser radiation during normal system operation. The safety measures specified in the FDA/CDRH regulations and the international standards IEC 60825 and DIN/EN 60825 respectively are met. Please also refer to "Laser product classification" (1-15).

These laser warning labels (not to scale) are affixed on the *LambdaUnite* MSS equipment. They refer to the system as a whole in normal operation.





Potential sources of danger

Beware of the following potential sources of danger which will remain despite all safety measures taken:

- Laser radiation can cause damage to the skin and eyes.
- Laser radiation from optical transmission systems is in a wavelength range that is invisible to the human eye.

Laser classes

The maximum output power of laser radiation depends on the type of laser diode used. The international standards IEC 60825 and DIN/EN 60825 respectively as well as the FDA/CDRH regulations define the maximum output power of laser radiation for each laser class in accordance with the wavelength.

The classification scheme is based on the ability of the laser emission or the reflected laser emission to cause injury to the eye or skin during normal operating conditions.

Please also refer to “Laser product classification” (1-15).

Laser safety instructions

Observe the following instructions to avoid exposing yourself and others to risk:

- Read the relevant descriptions in the manuals before taking equipment into operation or carrying out any installation and maintenance work on the optical port units, and follow the instructions. Ignoring the instructions may result in hazardous laser radiation exposure.
- Do not view directly into the laser beam with optical instruments such as a fiber microscope, because viewing of laser emission in excess of Class 1 limits significantly increases the risk of eye damage.
- Never look into the end of an exposed fiber or an open connector as long as the optical source is still switched on.

- Ensure that the optical source is switched off before disconnecting optical fiber connectors.
- In the event of doubt, check that the optical source is switched off by measuring with an optical power meter.



CAUTION

Use of controls, adjustments and procedures other than those specified herein may result in hazardous laser radiation exposure.



Optical circuit pack specifications

Specifications The following table contains the specifications of the *LambdaUnite*[™] MSS optical circuit packs.

Circuit pack	Wavelength [nm]	Fiber type ¹ (core/cladding diameter [μm])	Maximum output power [mW / dBm]	Laser class ² (IEC / FDA)
2.5-Gbit/s optical circuit packs				
OP2G5/1.3IOR4 (KFA12)	1310	SM (9/125)	0.5 / -3	1 / I
10-Gbit/s optical circuit packs				
OP10/1.3IOR1 (KFA7)	1310	SM (9/125)	0.8 / -9.7	1 / I
OP10/1.5IR1 (KFA14)	1550	SM (9/125)	1.6 / +2	1 / I
OP10/1.5LR1 (KFA6)	1550	SM (9/125)	2 / +3	1 / I
OP10/01...80/800G (KFA9, KFA81...159)	1530.72 ... 1562.23	SM (9/125)	1.6 / +2	1 / I
OP10/01...16/PWDM (KFA11, KFA61...75)	1530.33 ... 1560.61	SM (9/125)	2.5 / +4	1 / I
Gigabit-Ethernet circuit pack				
GE1/SX/4 (KFA13)	850	MM (50/125)	0.4 / -4	1 / I

Notes:

1. SM: Single-mode fiber, MM: multi-mode fiber.
2. It is the class of the circuit pack, not that of the telecommunications system as a whole, that is specified.

Connector types All optical circuit packs are equipped with LC-type connectors.



Laser product classification

Standards compliance The *LambdaUnite*[™] MSS product complies with the applicable IEC standards and the Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH) regulations.

FDA/CDRH regulations Laser products are classified in accordance with the FDA/CDRH - 21 CFR 1010 and 1040. The classification scheme is based on the ability of the laser emission to cause injury to the eye or skin during normal operating conditions.

In the United States, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to "FDA/CDRH laser classification" (1-16)):

- Class I,
- Class IIIb or
- Class IV.

Laser classification is dependent upon operating wavelength, output power and fiber mode field diameter (core diameter).

IEC requirements The International Electro-Technical Commission (IEC) establishes standards for the electrical and electronic industries. IEC 60825 has been established for the worldwide safety of laser products.

According to the IEC classification, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to "IEC laser classification" (1-16)):

- Class 1,
- Class 3A,
- Class 3B or
- Class 4.

There are some major differences between the FDA/CDRH regulations and the IEC requirements:

1. The Accessible Emission Limits (AEL) are different.
2. Class 3A applies to all wavelengths.

3. Class 3B requires strict engineering controls.
4. Classification is under single fault conditions.

FDA/CDRH laser classification

The following table provides an overview of laser classes for wavelengths of 1310 nm and 1550 nm in accordance with the FDA/CDRH regulations.

Laser class	Wavelength	Max. output power of laser radiation	
I	1310 nm	1.53 mW	+1.85 dBm
	1550 nm	8.52 mW	+9.3 dBm
IIIb	1310 nm	500 mW	+27 dBm
	1550 nm	500 mW	+27 dBm
IV	1310 nm	> 500 mW	> +27 dBm
	1550 nm	> 500 mW	> +27 dBm

Explanatory note: In the United States, lasers and laser systems are assigned to one of the following classes: Roman numerals I, IIa, II, IIIa, IIIb, and IV. Classes I, IIIb and IV apply to lasers of all wavelengths. Classes IIa, II and IIIa apply only to those lasers operating within the visible wavelength range (400-700 nm). Lucent Technologies laser products typically operate in the infrared wavelength range (greater than 700 nm) and, therefore, are primarily in the class I or class IIIb classifications.

IEC laser classification

The following table provides an overview of laser classes for wavelengths of 1310 nm and 1550 nm in accordance with the IEC 60825 standard.

Laser class	Wavelength	Max. output power of laser radiation	
1	1310 nm	8.85 mW	+9.5 dBm
	1550 nm	10 mW	+10 dBm
3A	1310 nm	24 mW	+13.8 dBm
	1550 nm	50 mW	+17 dBm
3B	1310 nm	500 mW	+27 dBm
	1550 nm	500 mW	+27 dBm

Laser class	Wavelength	Max. output power of laser radiation	
4	1310 nm	> 500 mW	> +27 dBm
	1550 nm	> 500 mW	> +27 dBm

Hazard level assignment

“Hazard level” refers to the potential hazard from laser emission at any location in an end-to-end optical fiber communication system that may be accessible during service or in the event of a failure. The assignment of hazard level uses the AELs for the classes.

Hazard levels for optical transmission equipment are assigned in either of the following two ways:

- the actual output power from the connector or fiber cut.
- if automatic power reduction is used, the output power at the connector or fiber cut at one second after automatic power reduction takes place, provided that maximum output and restart conditions are met.

Classification of optical telecommunication equipment

Optical telecommunication equipment is generally classified as IEC Class 1 or FDA/CDRH Class I, because under normal operating conditions the transmitter ports terminate on optical fiber connectors. These are covered by a front panel to ensure protection against emissions from any energized, unterminated transmitter.

The circuit packs themselves, however, may be IEC Class 1 or 3A or FDA/CDRH Class I or IIb.

□

Electrostatic discharge

Introduction Electrostatic discharge (ESD), caused by touching with the hand for example, can destroy semiconductor components. The correct operation of the complete system is then no longer assured.

Industry experience has shown that **all** semiconductor components can be damaged by static electricity that builds up on work surfaces and personnel. The electrostatic discharge can also affect the components indirectly via contacts or conductor tracks. The electrostatic charges are produced by various charging effects of movement and contact with other objects. Dry air allows greater static charges to accumulate. Higher potentials are measured in areas with low relative humidity, but potentials high enough to cause damage can occur anywhere.

The barred-hand symbol Circuit packs containing components that are especially sensitive to electrostatic discharge are identified by warning labels bearing the barred-hand symbol.



ESD instructions Observe the following ESD instructions to avoid damage to electrostatic-sensitive components:

- Wear working garment made of 100% cotton to avoid electrostatic charging.
- Touch the circuit packs at the edges or the insertion and removal facilities only.
- Ensure that the rack is grounded.
- Wear conductively connected wrist straps and connect them to the rack ESP bonding point.
- Work in an area which is protected against electrostatic discharge. Use conducting floor and bench mats which are conductively connected to the rack ESP bonding point.
- Conductively connect all test equipment and trolleys to the rack ESP bonding point.

- Store and ship circuit packs and components in their shipping packing. Circuit packs and components must be packed and unpacked only at workplaces suitably protected against build-up of charge.
- Whenever possible, maintain the relative humidity of air above 20%.



Safety requirements in specific deployment phases

Overview

Purpose To enable rapid orientation, safety instructions are given on the following pages, which are assigned to various stages in the life cycle of the *LambdaUnite*[™] MSS equipment (“deployment phases”).

Deployment phases The instructions are arranged according to the following deployment phases:

- “Transportation” (1-21)
- “Storage” (1-24)
- “Installation” (1-26)
- “Taking into operation” (1-29)
- “Operation and maintenance” (1-31)
- “Taking out of operation” (1-36)



Transportation

Weight



WARNING

Risk of injury due to unsecured shelf.

A fully-equipped shelf weighs more than 30 kg and can cause considerable injuries if it is knocked over or dropped. This can also cause serious damage to the shelf.

Use a sturdy vehicle for transportation and secure the shelf against dropping. At least two persons are required for lifting the shelf.

Packaging



CAUTION

Adverse effect on operation due to incorrect packaging.

Dampness and soiling can cause corrosion or tracking paths. This can cause malfunctioning of the system components. Shocks can cause damage.

Protect the system components against dampness, soiling and shocks. Use the original packaging if possible.

Climatic conditions



CAUTION

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

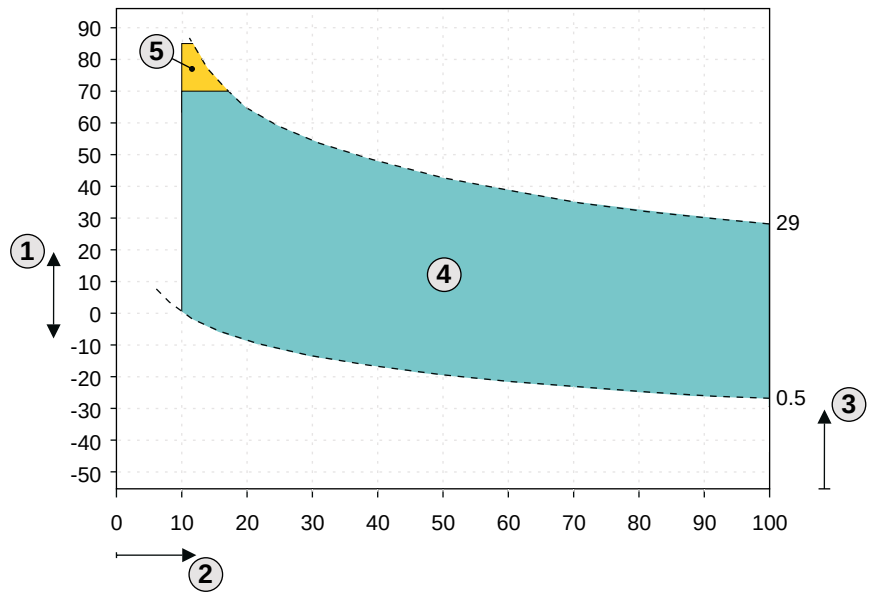
Ensure that the climatic limits for transportation and storage of LambdaUnite™ MSS equipment are complied with during transportation; please refer to “Climatic limits for transportation and storage” (1-22).

Climatic limits for transportation and storage

These are the climatic limits for transportation and storage of LambdaUnite MSS systems:

Temperature range	-40 °C to +70 °C (exceptional: +85 °C)
Humidity range	relative humidity: 10% to 100% absolute humidity: 0.5 g/m ³ to 29 g/m ³

The following climatogram visualizes these climatic limits:



Legend:

- 1 Air temperature [°C]
- 2 Relative humidity [%]
- 3 Absolute humidity [g/m³]. The dashed curves specify a constant absolute humidity of 0.5 g/m³ or 29 g/m³, respectively.
- 4 Permissible range for transportation and storage of *LambdaUnite* MSS systems.
- 5 Exceptional conditions, permissible for a short duration only.



Storage

Weight



WARNING

Risk of injury due to unsecured shelf.

A fully-equipped shelf weighs more than 30 kg and can cause considerable injuries if it is knocked over or dropped. This can also cause serious damage to the shelf.

Use only a stable base for storage and secure the shelf against dropping. At least two persons are required for lifting the shelf.

Electrostatic discharge (ESD)



CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Circuit packs must therefore always be kept in antistatic covers. Use the original packaging if possible. Always observe the ESD instructions (cf. “Electrostatic discharge” (1-18)).

Packaging



CAUTION

Adverse effect on operation due to incorrect packaging.

Dampness and soiling can cause corrosion or tracking paths. This can cause malfunctioning of the system components. Shocks can cause damage.

Protect the system components against dampness, soiling and shocks. Use the original packaging if possible.

Climatic conditions



CAUTION

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

Ensure that the climatic limits for transportation and storage of LambdaUnite™ MSS equipment are complied with during storage; please refer to “Climatic limits for transportation and storage” (1-22).



Installation

Weight



WARNING

Risk of injury due to unsecured shelf.

A fully-equipped shelf weighs more than 30 kg and can cause considerable injuries if it is knocked over or dropped. This can also cause serious damage to the shelf.

At least two persons are required for lifting the shelf.

Laser warning labels



WARNING

Ineffectiveness of laser warning labels if removed or concealed.

Warning labels on the system and especially on the optical components warn of the dangers of invisible laser radiation. Removed, concealed or illegible labels can lead to incorrect action and thus cause serious injuries to the eyes of operating staff.

Ensure that the laser warning labels are not removed or concealed and always clearly legible.

Electrostatic discharge (ESD)



CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. “Electrostatic discharge” (1-18)).

Overheating



CAUTION

Risk of fire due to overheating.

Inadequate heat dissipation can cause heat accumulation or even a fire in the network element.

You must therefore ensure that

- *the fan unit is installed,*
- *the individual fans are not obstructed,*
- *the minimum separation is maintained between two shelves in a rack (follow the installation instructions given in the LambdaUnite™ MSS Installation Guide).*

Detector diodes



CAUTION

Destruction of the detector diodes caused by too high an input power.

Connecting the output and input of optical circuit packs with a transmit power in excess of -3 dBm over short distances will cause the destruction of the detector diodes, as the input power is then too high.

Use an optical attenuator pad of approx. 10 to 20 dB when establishing connections over short distances for test purposes.



Taking into operation

Invisible laser radiation



DANGER

Injury to eyes caused by invisible laser radiation.

LambdaUnite™ MSS systems operate with invisible laser radiation. Laser radiation can cause considerable injuries to the eyes.

Never look into the end of an exposed fiber or into an open optical connector as long as the optical source is switched on. Always observe the laser warning instructions (cf. “Laser safety” (1-11)).

Arcing



DANGER

Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes.

Ensure that the line circuit breaker on the Power Interface (PI) is in the “OFF” position before removing or inserting the power supply plug.

Supply voltage



CAUTION

Destruction of components due to a supply voltage of incorrect polarity or too high.

LambdaUnite MSS equipment operates at a nominal voltage of -48 V or -60 V. The permissible tolerance range is -40.5 V to -60 V.

Ensure that the supply voltage has the correct range and polarity before connecting the voltage.

Fusing



CAUTION

Risk of fire in the event of a short-circuit.

A short-circuit can cause a fire in the network element.

Protect all supply lines with line circuit breakers matched to the load of the shelf equipment. Note the relevant guide values in the LambdaUnite MSS Installation Guide.

Condensation



CAUTION

Condensation causes malfunctioning

Condensation can occur in the network element during transport, especially on moving from outside to closed rooms; this can cause malfunctioning of the circuit packs.

Ensure that circuit packs and shelves have reached room temperature and are dry before taking them into operation.



Operation and maintenance

Invisible laser radiation



DANGER

Injury to eyes caused by invisible laser radiation.

LambdaUnite™ MSS systems operate with invisible laser radiation. Laser radiation can cause considerable injuries to the eyes.

Never look into the end of an exposed fiber or into an open optical connector as long as the optical source is switched on. Always observe the laser warning instructions (cf. “Laser safety” (1-11)).

Arcing



DANGER

Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes.

Ensure that the line circuit breaker on the Power Interface (PI) is in the “OFF” position before removing or inserting the power supply plug.

Laser warning labels



WARNING

Ineffectiveness of laser warning labels if removed or concealed.

Warning labels on the system and especially on the optical components warn of the dangers of invisible laser radiation. Removed, concealed or illegible labels can lead to incorrect action and thus cause serious injuries to the eyes of operating staff.

Ensure that the laser warning labels are not removed or concealed and always clearly legible.

Electrostatic discharge (ESD)



CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-18)).

Overheating



CAUTION

Risk of fire due to overheating.

Inadequate heat dissipation can cause heat accumulation or even a fire in the network element.

You must therefore ensure that

- *the fan unit is installed,*
- *the individual fans are not obstructed,*
- *the minimum separation is maintained between two shelves in a rack (follow the installation instructions given in the LambdaUnite MSS Installation Guide).*

Detector diodes



CAUTION

Destruction of the detector diodes caused by too high an input power.

Connecting the output and input of optical circuit packs with a transmit power in excess of -3 dBm over short distances will cause the destruction of the detector diodes, as the input power is then too high.

Use an optical attenuator pad of approx. 10 to 20 dB when establishing connections over short distances for test purposes.

Short-circuit



CAUTION

Destruction of circuit packs in the event of a short-circuit.

A short-circuit in the network element can cause destruction of electronic components and thus malfunctioning of the complete system.

You must therefore not handle objects such as a screwdriver in the circuit pack area of the shelf.

Test voltage



CAUTION

Destruction of components due to test voltage of incorrect polarity or too high.

The use of test voltages above 6 V DC for measurements on circuit packs can cause destruction of components and thus malfunctioning of the complete system.

Ensure that the test voltage does not exceed 6 V DC and that the test equipment is connected with the correct polarity.

Climatic conditions



CAUTION

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

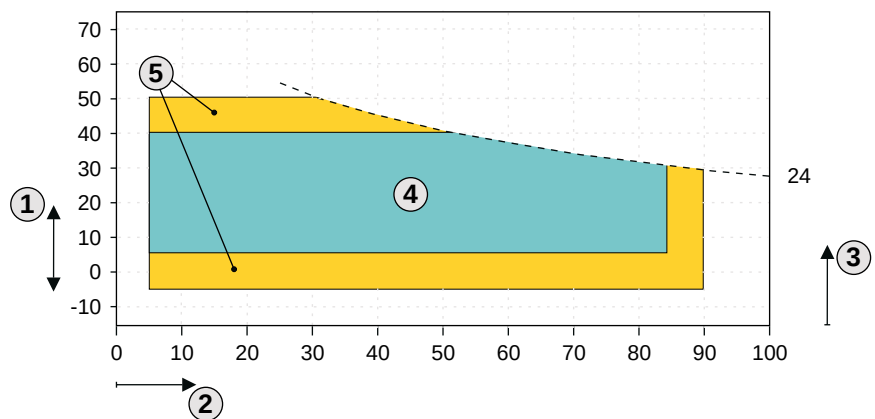
Ensure that the “Climatic limits for the operation of LambdaUnite MSS equipment” (1-35) are complied with during operation.

**Climatic limits for the
operation of *LambdaUnite*
MSS equipment**

These are the climatic limits for the operation of *LambdaUnite* MSS systems:

Temperature range	+5 °C to +40 °C (exceptional: +50 °C)
Humidity range	relative humidity: 5% to 85% (exceptional: 90%), absolute humidity: 0 to 24 g water per kg dry air

The following climatogram visualizes these climatic limits:



Legend:

- 1 Air temperature [°C]
- 2 Relative humidity [%]
- 3 Absolute humidity [g water/kg dry air]. The dashed curve specifies a constant absolute humidity of 24 g water per kg dry air.
- 4 Permissible range for the operation of *LambdaUnite* MSS systems.
- 5 Exceptional conditions, permissible for a short duration only.



Taking out of operation

Invisible laser radiation



DANGER

Injury to eyes caused by invisible laser radiation.

LambdaUnite™ MSS systems operate with invisible laser radiation. Laser radiation can cause considerable injuries to the eyes.

Never look into the end of an exposed fiber or into an open optical connector as long as the optical source is switched on. Always observe the laser warning instructions (cf. “Laser safety” (1-11)).

Arcing



DANGER

Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes.

Ensure that the line circuit breaker on the Power Interface (PI) is in the “OFF” position before removing or inserting the power supply plug.

Weight



WARNING

Risk of injury due to unsecured shelf.

A fully-equipped shelf weighs more than 30 kg and can cause considerable injuries if it is knocked over or dropped. This can also cause serious damage to the shelf.

At least two persons are required for lifting the shelf.

Electrostatic discharge (ESD)



CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. “Electrostatic discharge” (1-18)).

Disposal

The equipment in the *LambdaUnite* MSS system series must be disposed of at the end of its lifetime. Please contact us in this case and we will arrange for proper and environment-friendly disposal of your equipment (most parts of the system can be recycled).





2 Security administration

Overview

Purpose This chapter describes the security administration tasks.

Contents

Administering user logins	<u>2-3</u>
Creating a user login	<u>2-5</u>
Modifying a user login	<u>2-8</u>
Deleting a user login	<u>2-10</u>
Disabling user logins	<u>2-11</u>
Enabling user logins	<u>2-13</u>
Logging out NE users	<u>2-15</u>
Supporting information for “Administering user logins”	<u>2-17</u>
Changing super user ids	<u>2-19</u>
Changing user passwords	<u>2-22</u>
Modifying user security parameters	<u>2-27</u>
Modifying a user’s own notification list	<u>2-28</u>
Modifying user security parameters by admin	<u>2-30</u>

Supporting information for “Modifying user security parameters by admin”	<u>2-32</u>
Provision global security parameters	<u>2-33</u>
Retrieving security information	<u>2-35</u>
Displaying a list of all users logged into an NE	<u>2-36</u>
Displaying login information for an NE	<u>2-38</u>
Retrieve security log	<u>2-40</u>
Retrieve system wide security parameters	<u>2-41</u>
Retrieve security info of own user	<u>2-43</u>
Retrieve security info of all or other user	<u>2-45</u>



Administering user logins

Overview

Purpose User administration basically consists of:

- “Creating a user login” (2-5),
- “Modifying a user login” (2-8),
- “Deleting a user login” (2-10),
- “Disabling user logins” (2-11),
- “Enabling user logins” (2-13).
- “Logging out NE users” (2-15)

It is suggested to use “User administration” (13-3) as an entry point for user administration activities.

Furthermore, it is recommended to have a list prepared of all the users that probably will need to have access to the *WaveStar*® CIT and the NEs, especially if several user logins are to be created or modified for different NEs. The list should contain the designated user IDs, associated passwords, access privileges and other related security parameters, and should be as complete as possible.

Related information For related information, please refer to:

- “User administration” (13-3).
- “Retrieving security information” (2-35)
- Chapter 22, “*WaveStar* CIT Tutorial”

Contents

Creating a user login	2-5
Modifying a user login	2-8
Deleting a user login	2-10
Disabling user logins	2-11
Enabling user logins	2-13
Logging out NE users	2-15

Supporting information for “Administering user logins”

[2-17](#)



Creating a user login

Before you begin The starting point for the following procedure is according to “User administration” (13-3). The procedure itself is limited to the necessary steps to create a new user login using “The NE User Provisioning window” (2-18).

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Important! Please note that any user administration changes will not take effect until the next login session.

Procedure Complete the following steps to create a new user login.

- 1 In the NE **User Provisioning** window, select **New User**, place the cursor in the associated text box and type in the user ID.

Reference:

Please refer to “Valid user login” (13-5) .

- 2 Select the **User Class**, either **MEMADMIN** or **Other**, for the new user by selecting respective radio button.

Reference:

Please refer to “User class” (13-8) .

- 3 Place the cursor in the **Enter Password** text box and type in the password assigned to the new user.

The password may be preliminary. Each user is permitted to change her/his own password.

Reference:

Please refer to “Valid password” (13-5) .

-
- 4 Confirm the password by typing it in again in the **Confirm Password** text box.
-

- 5 Assign a user type to the new user by using the **User Type** drop-down list box (per default the **User Type** is set to **Other**):

IF ...	THEN ...
you choose a predefined user type	the corresponding user privilege codes will be assigned automatically for the five functional categories.
you choose “Other”	you will have to assign the user privilege codes manually by using the corresponding drop-down list boxes. If you choose to do nothing with the user privilege code values, then they are set to a value of S1, P0; T0; PM0; M0 .

- 6 Specify the notifications a user may receive by using the **Notification List** drop down list box.
-

- 7 Select if the **Password Aging Interval** function should be enabled or disabled (per default the **Password Aging Interval** is enabled and set to **90 Days**).

IF ...	THEN ...
you want to enable the Password Aging Interval	select the right check box. You can set the Password Aging Interval by using the up/down arrows of the Days spin box or typing it in directly. Reference: Please refer to “Password aging” (13-9).
you want to disable the Password Aging Interval	select Disable .

-
- 8 Select if the **Inactivity Timeout** function should be enabled or disabled (per default the **Inactivity Timeout** is enabled and set to **30 Minutes**).

IF ...	THEN ...
you want to enable Inactivity Timeout	select the right check box. You can set value for Inactivity Timeout by using the up/down arrows of the Minutes spin box or typing it in directly. Reference: Please refer to “Inactivity time-out period” (13-8).
you want to disable Inactivity Timeout	select Disable .

.....

- 9 Make sure that the settings in the NE **User Provisioning** window are correct.
-

- 10 Click **Add** to add the new user login.
-

- 11 Confirm your changes in the confirmation window by clicking **Yes**.

Result:

Another window opens with the question: “**Are you sure you want to add a new user**”

You may now:

1. Click **Yes** to save the new user login and related security parameters also to the *WaveStar* CIT security database, or
2. Click **No** to close the confirmation window without adopting the *WaveStar* CIT security database.

END OF STEPS

.....



Modifying a user login

Before you begin The starting point for the following procedure is according to “User administration” (13-3). The procedure itself is limited to the necessary steps to modify an existing user login using “The NE User Provisioning window” (2-18).

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Important! Any user administration changes will not take effect until the next login session.

Procedure Complete the following steps to modify an existing user login.

- 1 In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.
-

- 2 Modify the related security parameters according to your needs by changing only the parameters to be modified.

Example:

If you only want to assign another **Password Aging Interval** then it is not necessary to enter the user’s password.

- 3 Make sure that the settings in the NE **User Provisioning** window are correct.
-

- 4 Click **Modify** to change the user login.
-

- 5 Confirm your changes in the confirmation window by clicking **Yes**.

Result:

Another window opens with the question: “***Are you sure you want to modify this user?***”

You may now:

1. Click **Yes** to save the user related security parameters also to the *WaveStar* CIT security database, or
2. Click **No** to close the confirmation window without adopting the *WaveStar* CIT security database.

END OF STEPS



Deleting a user login

Before you begin The starting point for the following procedure is according to “User administration” (13-3). The procedure itself is limited to the necessary steps to delete an existing user login using the NE **User Provisioning** window.

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Important! Any user administration changes will not take effect until the next login session.

Instructions Complete the following steps to modify an existing user login.

- 1 In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.
-

- 2 Click **Delete** to delete the user login and confirm the deletion in the confirmation window by clicking **Yes**.

Notice that the deleted user login will still be visible in the **Existing User** drop down list box because user administration changes do not take effect until the next login session.

Also notice that if the user has an active session with the NE at the time he is deleted, that session will not be terminated.

END OF STEPS



Disabling user logins

Before you begin Prior to performing this task, you must be logged into the *WaveStar*[®] CIT and the respective network element.

Required privilege code

You must be a security administrator with a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions **Important!** Any user administration changes will not take effect until the next login session.

Complete the following steps to disable existing user logins.

- 1 From **the System View** or **Shelf View** main menu select **Administration → Security → Disable User Login ...**

Result:

The *WaveStar* CIT **Disable User Login** window is displayed. It shows a list of all provisioned users (except the superusers) and their login status.

- 2 You can disable a single or all users logins.

IF ...

you want to disable all user logins,

you want to disable a single user login,

THEN

select the radio button **Disable all the user logins**.

select a user login and select the radio button **Disable only the selected user login**.

Important! Be sure that you have not selected a superusers, because for that case it wouldn't be possible to login to the system at all, and the system would have to be re-loaded again.

- 3 Click **OK**.
-

Result:

A confirmation screen pops up asking you to confirm your selection.

- 4 Click Yes.

Result:

The **Disable User Login** window is dismissed.

END OF STEPS



Enabling user logins

Before you begin Prior to performing this task, you must be logged into the *WaveStar*[®] CIT and the respective network element.

Required privilege code

You must be a security administrator with a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions **Important!** Any user administration changes will not take effect until the next login session.

Complete the following steps to enable existing user logins.

- 1 From **the System View** or **Shelf View** main menu select **Administration → Security → Enable User Login ...**

Result:

The *WaveStar* CIT **Enable User Login** window is displayed. It shows a list of all currently disabled users and their login status.

- 2 You can enable a single or all users logins.

IF ...

you want to enable all user logins,

you want to enable a single user login,

THEN ...

select the radio button **Enable all the user logins**.

select a user login and select the radio button **Enable only the selected user login**.

- 3 Click **OK**.

Result:

A confirmation screen pops up asking you to confirm your selection.

-
- 4 Click Yes.

Result:

The **Enable User Login** window is dismissed.

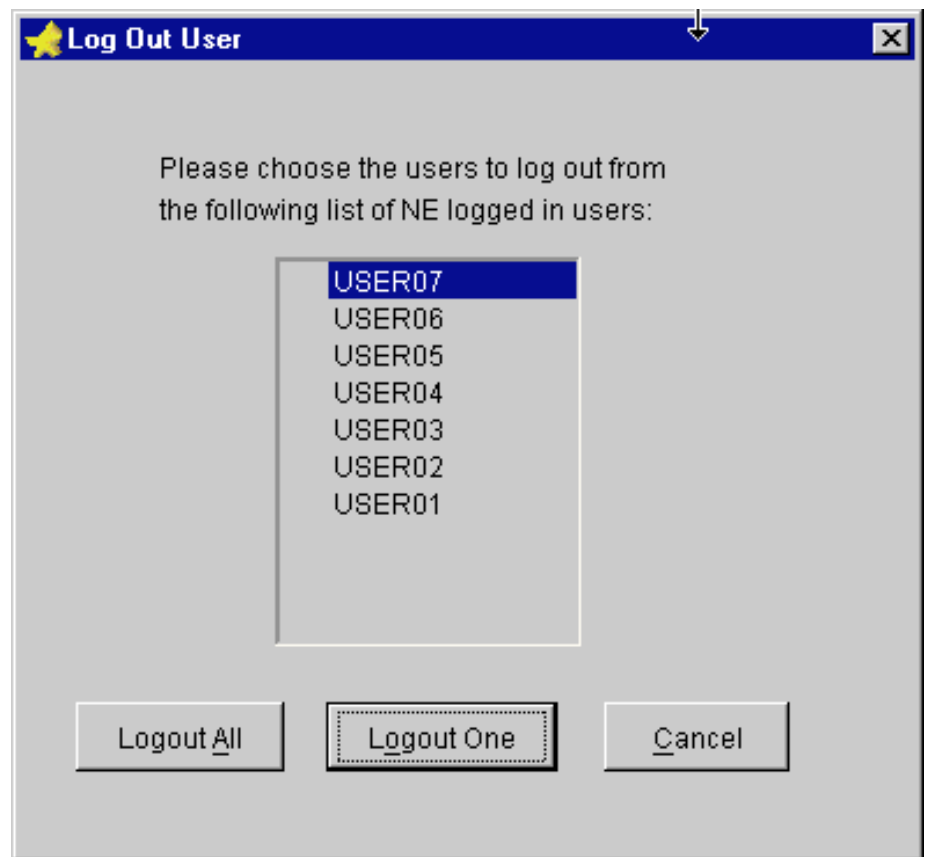
END OF STEPS



Logging out NE users

When to use Use this procedure to terminate another user's login association with an NE.

The *Log Out User* window The WaveStar® CIT **Log Out User** window can be invoked from the WaveStar CIT **System View** or **Shelf View** main menu via **Administration** → **Security** → **Logout NE User**



Related information For related information, please refer to:

- Chapter 22, “WaveStar CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the WaveStar CIT and the respective network element.

Required privilege code

You must be a security administrator with a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to log out users from the NE.
.....

- 1 From **the System View** or **Shelf View** main menu select **Administration → Security → Logout NE User ...**

Result:

The WaveStar CIT **Log Out User** window is displayed. It shows a list of all users currently logged into the NE.

The CIT does not display your own UID, because this screen cannot be used to log out yourself.
.....

- 2 You can log out a single or all users from the NE.

IF ...	THEN
you want to logout all users,	click Logout All .
you want to logout a single user,	select a user and click Logout One .

Result:

A confirmation screen pops up asking you to confirm your selection.
.....

- 3 Click Yes.

Result:

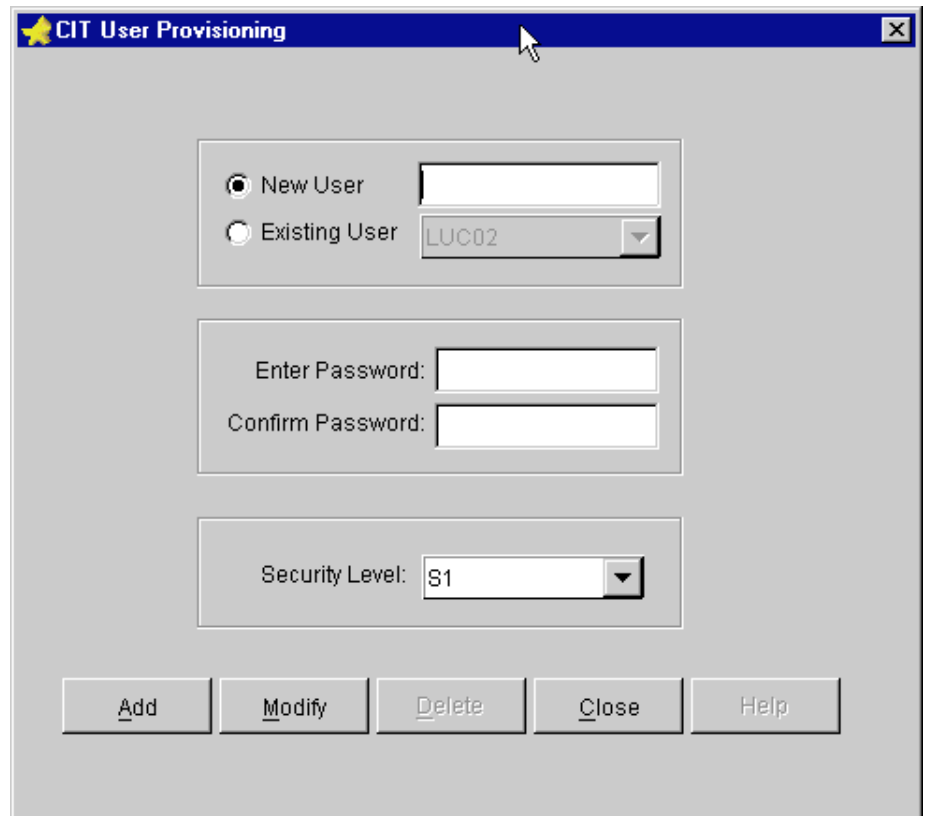
The **Log Out User** form is dismissed.

END OF STEPS
..... ☐

Supporting information for “Administering user logins”

The *WaveStar*® CIT User Provisioning window

The *WaveStar* CIT **User Provisioning** window can be invoked from the *WaveStar* CIT main window via **Administration** → **Security** → **User Provisioning**....



Use this window to create, modify or delete a user login for a user which has or shall have a user ID, password and access privileges for the *WaveStar* CIT.

**The NE User Provisioning
window**

The NE **User Provisioning** window can be invoked from the **System View** or **Shelf View** main menu via **Administration** → **Security** → **User Provisioning...** .

The screenshot shows the 'User Provisioning' window with the following fields and controls:

- New User:** ☐ (selected)
- Existing User:** ☐ LUC01 (dropdown)
- User Class:** ☐ MEMADMIN, ☒ Other
- Enter Password:**
- Confirm Password:**
- Password Aging Interval:** ☐ Disable, ☒ 90 Days (spinner)
- Inactivity Timeout:** ☐ Disable, ☒ 30 Minutes (spinner)
- User Type:** Other (dropdown)
- Provisioning:** No Authorization (dropdown)
- Security:** S1 (dropdown)
- Maintenance:** No Authorization (dropdown)
- Performance Management:** No Authorization (dropdown)
- Test:** No Authorization (dropdown)
- Notification List:** OWN (dropdown)
- Buttons:** Add, Modify, Delete, Cancel, Help

Use this window to create, modify or delete a user login for a user which has or shall have a user ID, password, password aging, inactivity timeout and access privileges for the network element you are currently connected to.

Changing super user ids

Overview

Purpose Use the following procedures to change super user ids on the *WaveStar*[®] CIT.

Related information For related information, please refer to:

- Chapter 13, “Security and administration concepts”.
- Chapter 22, “*WaveStar* CIT Tutorial”



Changing super user ids on the WaveStar® CIT

When to use Use this procedure to change super user ids on the WaveStar CIT.

Before you begin Prior to performing this task, you must be logged into the WaveStar CIT. Only a superuser is permitted to change a super user id.

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to change your password.

- 1 From the WaveStar CIT main menu, select **Administration** → **Security** → **Change Superuser Login ID...**

Result:

The **Change Super User ID** form is displayed:

- 2 Select the super user Login ID you want to change. Click on the respective radio button.
-

- 3 Key in the new Login ID.

Note

Login IDs are case sensitive and must start with a letter.

- 4 Click **OK**.

Result:

A confirmation screen pops up asking you to confirm your changes.

- 5 Click **Yes**.

Result:

The super user Login ID is updated and the **Change Super User ID** form is dismissed.

The changed super user Login ID will take effect the next time you log into the *WaveStar* CIT.

END OF STEPS



Changing user passwords

Overview

Purpose Use this procedure to change your own password either on the *WaveStar*® CIT or on the NE (for the user ID currently logged in with).

Related information For related information, please refer to:

- Chapter 13, “Security and administration concepts”.
- “User administration” (13-3).
- Chapter 22, “*WaveStar* CIT Tutorial”



Changing the user password on the WaveStar[®] CIT

When to use Use this procedure to change your own password (for the user ID currently logged in with) on the WaveStar CIT.

Related information To administer passwords and other login information for other users, please refer to “Administering user logins” (2-3).

Before you begin Each user is permitted to change her/his own password.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to change your password.

- 1 From the WaveStar CIT main window, select **Administration** → **Change Password...**

Result:

The **Change Password** form is displayed:

- 2 Place the cursor into the **Old Password** field and key in the password you are currently using.
-

- 3 Place the cursor into the **New Password** field and key in the new password.

Note

Passwords are case sensitive and must start with a letter.

- 4 Place the cursor into the **Confirm Password** field and key in the new password a second time.
-

- 5 Click **OK**.

Result:

The password is updated and the **Change Password** form is dismissed.

The changed password will take effect the next time you log into the *WaveStar* CIT.

END OF STEPS



Changing the user password on the NE

When to use Use this procedure to change your own password on the NE (for the user ID currently logged in with).

Before you begin Prior to performing this task, you must be logged into the *WaveStar*[®] CIT and the respective network element.

Required privilege code

You must have a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to change your password.

- 1 From **the System View** or **Shelf View** main menu, select **Administration** → **Change Password...**

Result:

The **Change Password** form is displayed:

- 2 Place the cursor into the **Old Password** field and key in the password you are currently using.
-

- 3 Place the cursor into the **New Password** field and key in the new password.

Note

Passwords are case sensitive and must start with a letter.

The new password cannot be a password used for this login in the past.

- 4 Place the cursor into the **Confirm Password** field and key in the new password a second time.
-

- 5 Click **OK**.
-

Result:

The password is updated and the **Change Password** form is dismissed.

The changed password will take effect the next time you log into the *WaveStar* CIT.

END OF STEPS



Modifying user security parameters

Overview

Purpose	This section describes how to modify and provision user security parameters.		
Contents			
	Modifying a user’s own notification list		2-28
	Modifying user security parameters by admin		2-30
	Supporting information for “Modifying user security parameters by admin”		2-32
	Provision global security parameters		2-33



Modifying a user's own notification list

When to use If you want to change your registration notification list, but cannot access the NE **User Provisioning** window (unless you are a SuperUser), you can perform this procedure to accomplish this task.

Related information For related information, please refer to:

- “Notification list” (13-8).
- “Administering user logins” (2-3)
- Chapter 22, “ WaveStar® CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must be at least a general user with a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

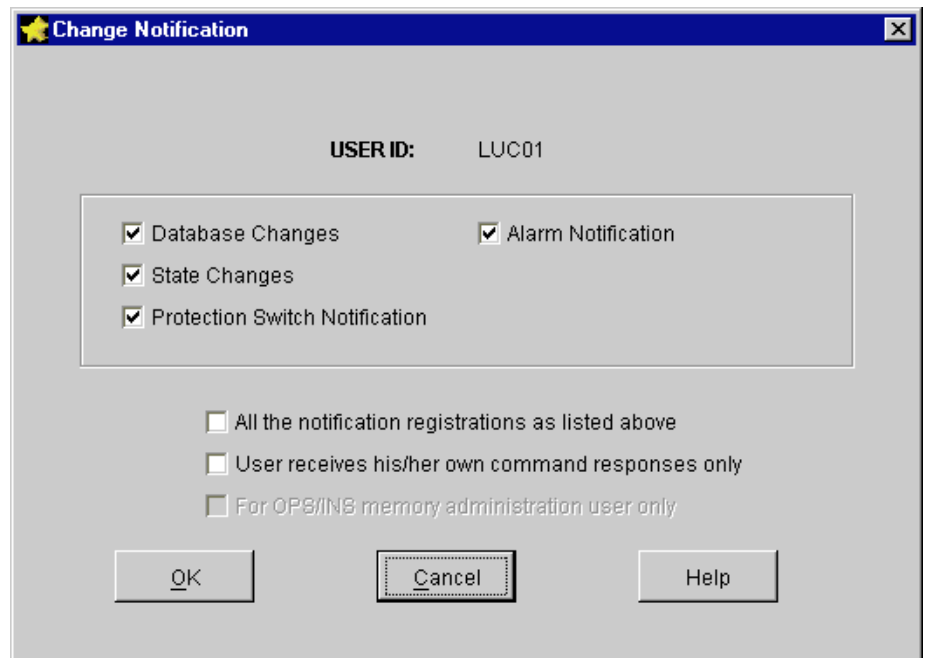
- WaveStar CIT

Instructions Complete the following steps to modify the User notifications.

- 1 From **the System View** or **Shelf View** main menu select **Administration → Change Notifications ...**

Result:

The **Change Notification** form is displayed:



The screenshot shows a dialog box titled "Change Notification" with a yellow star icon in the top-left corner. The dialog has a blue title bar and a gray body. At the top, it displays "USER ID: LUC01". Below this is a group box containing five checked checkboxes: "Database Changes", "State Changes", "Protection Switch Notification", "Alarm Notification", and "All the notification registrations as listed above". Below the group box are three unchecked checkboxes: "User receives his/her own command responses only" and "For OPS/INS memory administration user only". At the bottom are three buttons: "OK", "Cancel", and "Help".

-
- 2 Define the notification types you want to receive.
-

- 3 Click **OK**.

Result:

The notification list is updated and the **Change Notification** form is dismissed.

The modification will take effect only with the next login.

END OF STEPS



Modifying user security parameters by admin

When to use Use this procedure to modify user security parameters.

Related information For related information, please refer to:

- “User administration” (13-3)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Important! Any user administration changes will take effect not before the next login session.

Procedure Complete the following steps to modify the security parameters for an existing user login.

- 1 From the **System View** or **Shelf View** main menu select **Administration** → **Security** → **User Provisioning...**

Result:

The NE **User Provisioning** window is displayed:

- 2 In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.
-

- 3 Modify the related security parameters according to your needs by changing only the parameters to be modified.

Example:

If you only want to assign another priority level then it is not necessary to enter the user's password.

Reference:

For a detailed description of the parameters and their usage refer to “User administration” (13-3).

-
- 4 Make sure that the settings in the NE **User Provisioning** window are correct.
 - 5 Click **Modify** to change the user login.
 - 6 Confirm your changes in the confirmation window by clicking **Yes**.

Result:

Another window opens with the question: ***“Do you want to save the security changes in the CIT security database?”***

You may now:

1. Click **Yes** to save the user related security parameters also to the *WaveStar* CIT security database, or
2. Click **No** to close that window without adopting the *WaveStar* CIT security database.

END OF STEPS



Supporting information for “Modifying user security parameters by admin”

The network element *User Provisioning* window

Use this window to create, modify or delete a user login for a user which has or shall have a user ID, password, password aging, inactivity timeout and access privileges for the network element you are currently connected to.

User Provisioning

☒ **New User:**
☐ **Existing User:**

User Class:
☐ MEMADMIN
☒ Other

Enter Password:
Confirm Password:

Password Aging Interval
☐ Disable ☒ 90 Days

Inactivity Timeout
☐ Disable ☒ 30 Minutes

User Type: Other
Provisioning: No Authorization
Security: S1

Maintenance: No Authorization
Performance Management: No Authorization
Test: No Authorization

Notification List: OWN

Add Modify Delete Cancel Help

7

Provision global security parameters

When to use Use this procedure to provision global security parameters for an NE.

Related information For related information, please refer to:

- “User id lockout threshold” (13-9).
- “User id lockout period” (13-9).
- “User id lockout aging period” (13-10).
- “User id aging period” (13-10).
- Chapter 22, “ *WaveStar*[®] CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must be a security administrator with a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to modify the User ID Lockout parameters.

- 1 From the **System View** or **Shelf View** main menu select **Administration** → **Security** → **Security Provisioning....**

Result:

The **Provision NE Security** form is displayed:

The screenshot shows a Windows-style dialog box titled "Provision NE Security". It contains four main configuration areas:

- User ID Lockout Threshold:** A spin box with the value "2".
- User ID Lockout Interval:** Two radio buttons. The first is labeled "Disable" and is unselected. The second is labeled "40 Minutes" and is selected.
- User ID Aging Period:** Two radio buttons. The first is labeled "Disable" and is selected. The second is labeled "10 Days" and is unselected.
- User ID Lockout Aging Period:** A spin box with the value "99" and the unit "Minutes".

At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Help".

-
- 2 Define the parameters by using the up/down arrows of the spin boxes or typing it in directly.
-

- 3 Click **OK**.

Result:

A confirmation screen pops up asking you to confirm your changes.

- 4 Click **Yes**.

Result:

The parameters are updated and the **Provision NE Security** form is dismissed.

The modification will take effect only with the next login.

END OF STEPS



Retrieving security information

Overview

Purpose Use the following procedures to retrieve security information.

Contents

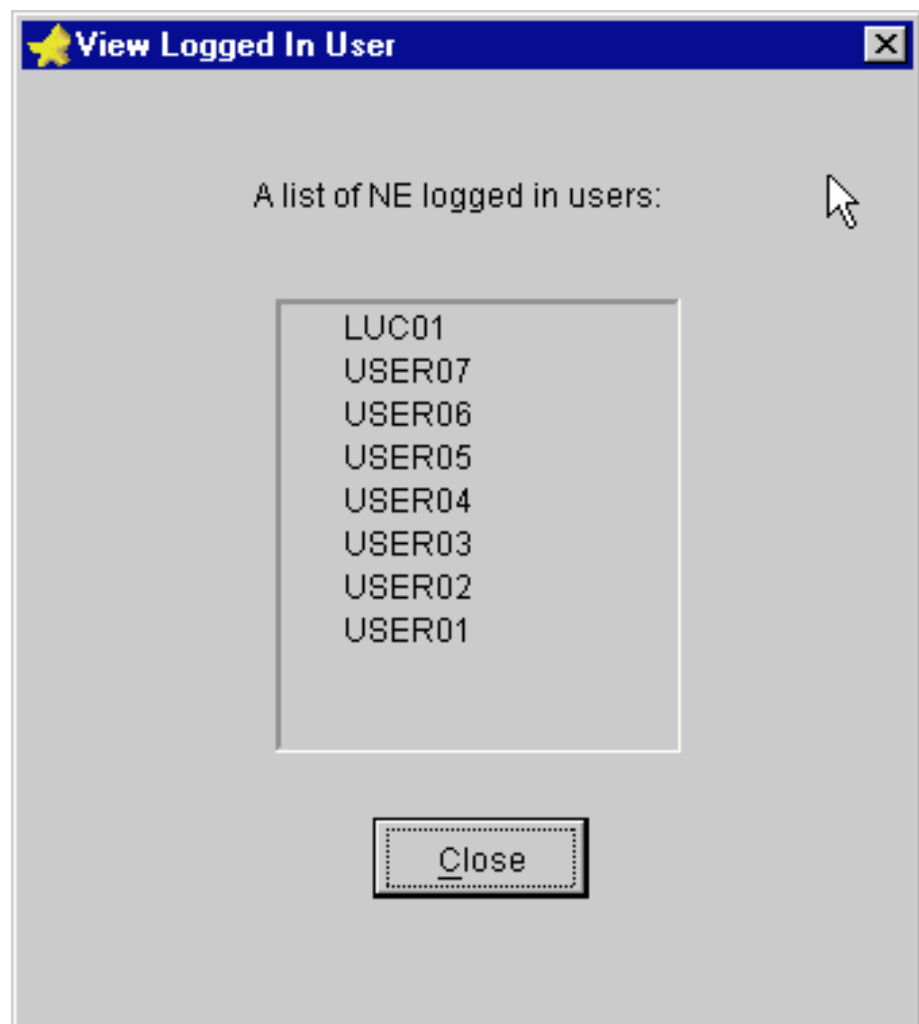
Displaying a list of all users logged into an NE	<u>2-36</u>
Displaying login information for an NE	<u>2-38</u>
Retrieve security log	<u>2-40</u>
Retrieve system wide security parameters	<u>2-41</u>
Retrieve security info of own user	<u>2-43</u>
Retrieve security info of all or other user	<u>2-45</u>



Displaying a list of all users logged into an NE

When to use Use this procedure to display a list of all users logged into an NE.

The *View Logged In User* window The *WaveStar*® CIT **View Logged In User** window can be invoked from the *WaveStar* CIT **System View** or **Shelf View** main menu via **Administration** → **Security** → **View Logged-In Users**



Related information For related information, please refer to:

- Chapter 22, “*WaveStar* CIT Tutorial”
- Chapter 13, “Security and administration concepts”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to get information on the users logged in to the NE.

.....

- 1 From **the System View** or **Shelf View** main menu select **Administration → Security → View Logged In Users**.

Result:

The *WaveStar* CIT **View Logged In Users** window is displayed. It shows information on all users currently logged into the NE.

Reference:

Refer to Chapter 13, “Security and administration concepts”.

END OF STEPS

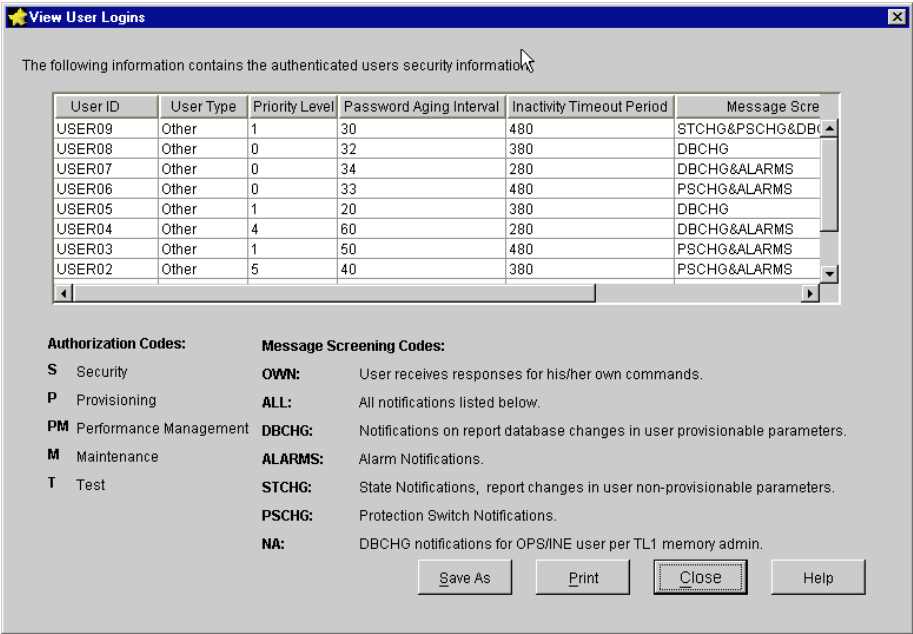
.....



Displaying login information for an NE

When to use Use this procedure to get information on all logins into an NE.

The *View User Logins* window The *WaveStar*® CIT **View User Logins** window can be invoked from the *WaveStar* CIT **System View** or **Shelf View** main menu via **Administration → Security → View User Logins ...**



Related information For related information, please refer to:

- Chapter 22, “WaveStar CIT Tutorial”
- Chapter 13, “Security and administration concepts”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have a user privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to get information on the logins into the NE.

.....

- 1 From **the System View** or **Shelf View** main menu select **Administration → Security → View User Logins ...**

Result:

The *WaveStar* CIT “View User Logins” window is displayed. It shows a list of all user logins for the NE.

END OF STEPS

.....



Retrieve security log

When to use Use this procedure to retrieve the security log.

Related information For related information, please refer to:

- Chapter 22, “ WaveStar® CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the WaveStar CIT and the respective network element.

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to retrieve the security log file.

- 1 From **the System View** or **Shelf View** main menu select **Reports** → **NE Security Log**

Result:

The **Select Start Date/Time for NE Security Log** window is displayed.

- 2 Define the start date/ time for the starting point of the report.

Important! If both startdate and starttime are omitted, the entire log is retrieved. Both, start date and start time, must be specified, or both must be omitted.

- 3 Click **OK**.

Result:

The WaveStar CIT **NE Security Log** window is displayed.

Reference:

Refer to Chapter 13, “Security and administration concepts”.

END OF STEPS



Retrieve system wide security parameters

When to use Use this procedure to retrieve system wide security parameters for your NE user.

Related information For related information, please refer to:

- “User id lockout threshold” (13-9).
- “User id lockout period” (13-9).
- “User id lockout aging period” (13-10).
- “User id aging period” (13-10).
- Chapter 22, “ *WaveStar*[®] CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to get information on system wide security parameters.

- 1 From the **System View** or **Shelf View** main menu select **Administration** → **Security** → **Security Provisioning....**

Result:

The **Provision NE Security** form is displayed:

The screenshot shows a dialog box titled "Provision NE Security" with a yellow star icon in the title bar. The dialog contains four configuration sections arranged in a 2x2 grid:

- User ID Lockout Threshold:** A text box containing the value "2" with a small up/down arrow icon to its right.
- User ID Lockout Interval:** A section with two radio buttons. The first is labeled "Disable" and is unselected. The second is selected and is followed by a text box containing "40" and the word "Minutes".
- User ID Aging Period:** A section with two radio buttons. The first is labeled "Disable" and is selected. The second is unselected and is followed by a text box containing "10" and the word "Days".
- User ID Lockout Aging Period:** A text box containing the value "99" with a small up/down arrow icon to its right, followed by the word "Minutes".

At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Help".

END OF STEPS



Retrieve security info of own user

When to use Use this procedure to retrieve security information of your own user.

Related information For related information, please refer to:

- Chapter 22, “*WaveStar*® CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

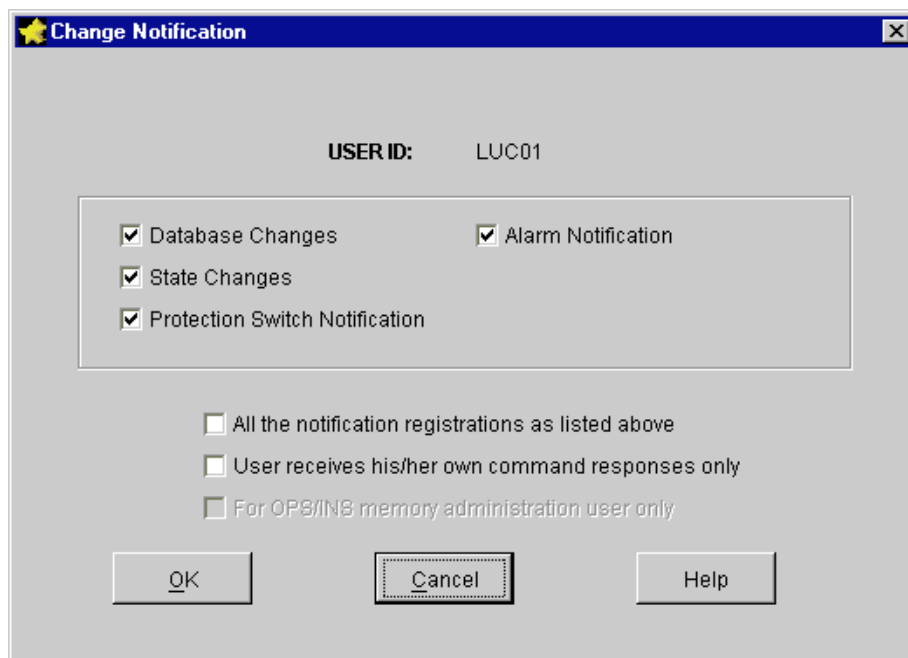
- *WaveStar* CIT

Instructions Complete the following steps to get security information on your own user.

- 1 From **the System View** or **Shelf View** main menu select **Administration → Change Notifications**

Result:

The **Change Notification** form is displayed:



The image shows a Windows-style dialog box titled "Change Notification" with a yellow star icon in the title bar. The dialog has a light gray background. At the top, it displays "USER ID: LUC01". Below this is a rectangular box containing four checked checkboxes: "Database Changes", "State Changes", "Protection Switch Notification", and "Alarm Notification". Below this box are three unchecked checkboxes: "All the notification registrations as listed above", "User receives his/her own command responses only", and "For OPS/INS memory administration user only". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Reference:

Refer to Chapter 13, "Security and administration concepts".

END OF STEPS



Retrieve security info of all or other user

When to use Use this procedure to retrieve security info of all or other users.

Related information For related information, please refer to:

- Chapter 22, “*WaveStar*® CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have a user privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to get information on the logins into the actual NE.

- 1 From the **System View** or **Shelf View** main menu select **Administration** → **Security** → **User Provisioning...**

Result:

The NE **User Provisioning** window is displayed.

- 2 In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.

Result:

In the NE **User Provisioning** window the information for the selected user are displayed.

Reference:

Refer to “User administration” (13-3).

END OF STEPS





3 Management communication setup

Overview

Purpose This chapter describes the procedures which have to be performed for the management communication setup.

Contents

Changing the NE name (TID)	3-3
Configuring the data communication network (high level)	3-6
Configuring the basic DCN parameters for the <i>WaveStar</i> [®] CIT	3-9
Supporting information for “Configuring the basic DCN parameters for the <i>WaveStar</i> CIT”	3-12
Configuring the LDB timers for the <i>WaveStar</i> CIT	3-15
Supporting information for “Configuring the LDB timers for the <i>WaveStar</i> CIT”	3-17
Administering the address list at the <i>WaveStar</i> CIT	3-18
Supporting information for “Administering the address list at the <i>WaveStar</i> CIT”	3-22
Configuring the basic DCN parameters for an NE	3-28
Supporting information for “Configuring the basic DCN parameters for an NE”	3-32

Configuring data communication channels	3-36
Supporting information for “Configuring data communication channels”	3-39
Configuring the TARP parameters for an NE	3-44
Supporting information for “Configuring the TARP parameters for an NE”	3-46
Assigning TARP manual adjacencies	3-47
Supporting information for “Assigning TARP manual adjacencies”	3-52
Setting system parameters	3-53
Supporting information for “Setting system parameters”	3-55
Setting date and time	3-56
Supporting information for “Setting date and time”	3-58

□

Changing the NE name (TID)

When to use Use this procedure to change an NE's name (also referred to as the target identifier, TID).

NE names NE names must be unique within a network to guarantee the reachability by management systems and the proper interworking of NEs.

Related information For related information, please refer to:

- “NE name administration” (14-37).
- Chapter 22, “ *WaveStar*® CIT Tutorial”

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the subject NE, and
- have proper access privileges to perform this task.

Required privilege codes

You must have at least privilege codes of S4 and M4 and P1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to change a network element's name.

- 1 From the **System View** main menu, select **Fault** → **Enter/Exit Maintenance Condition...** → **Enter Maintenance Condition ...**
 - 2 Confirm the resulting system message by clicking **YES**.
 - 3 Invoke the **Provision TID/NE Name** window from the **System View** main menu via **Administration** → **Set TID...**
-

-
- 4 Place the cursor in the **New TID/NE Name** text box and key in the new TID observing the following configuration rules:
- Each NE name must be unique within the network.
 - The following characters are allowed in an NE name:
 - Upper-case letters (“A” .. “Z”),
 - Lower-case letters (“a” .. “z”),
 - Special characters(“-”, “+”, “_”, “.”, “/”),
 - Digits (“0” .. “9”).
 - An NE name must not end and begin with an special character.
 - Each NE name must be maximally 20 characters in length.
 - The NE name may contain segments separated by hyphens (“-”) or slashes (“/”), but each segment must begin with a letter.

Please note that NE names are case-insensitive.

- 5 Make sure that the new TID is correct.

IF ...	THEN ...
the new TID is correct,	continue with Step 6.
the new TID is not correct,	correct the entry in the New TID/NE Name text box and continue with Step 6.

- 6 Place the cursor in the **Confirm TID/NE Name** text box and key in the new TID again.

Important! Take a note of the TID you are going to assign to the NE!

- 7 Click **OK** to assign the new TID and to dismiss the window.
-

- 8 From the **System View** main menu, select **Fault → Enter/Exit Maintenance Condition... → Exit Maintenance Condition...**
-

- 9 Confirm the resulting system message by clicking **OK**.
-

Result:

The *LambdaUnite*[™] MSS NE will now perform a system reset. As a consequence, the management association between the *WaveStar* CIT and the NE will be lost.

After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar* CIT to the NE, now using the new TID.

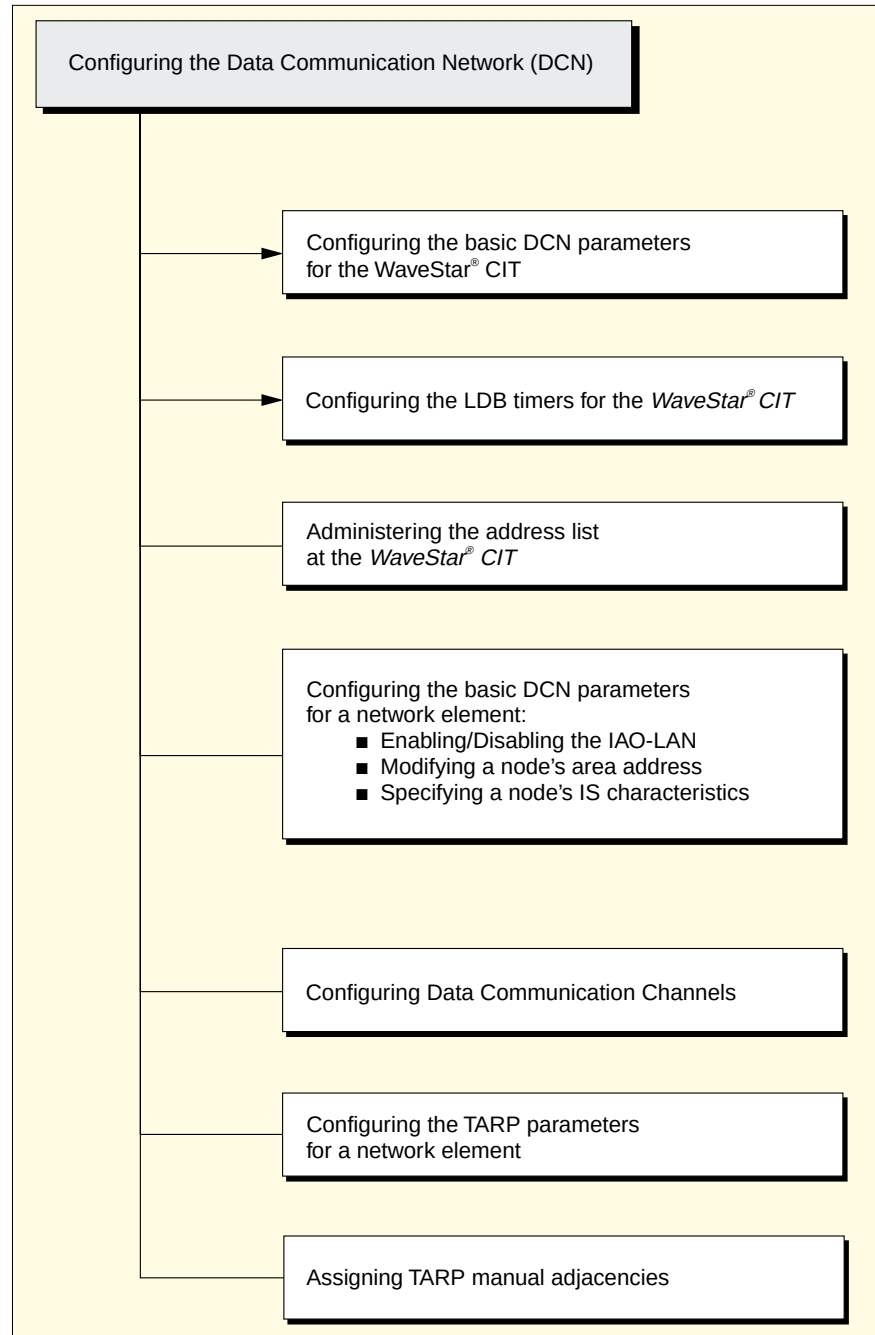
END OF STEPS



Configuring the data communication network (high level)

When to use	This task description serves as an overview of the individual procedures that must be carried out to configure the Data Communication Network (DCN) for <i>LambdaUnite</i> ™ MSS network elements and the <i>WaveStar</i> ® CIT.
Related information	For related information, please refer to: • Chapter 14, “Management communication setup concepts” • Chapter 22, “<i>WaveStar</i> CIT Tutorial”
Before you begin	Please refer to the individual procedures for information about the required privileges. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Configuring the DCN	Important! The sequence of carrying out these procedures is optional, and each of the procedures may also be carried out separately.

Configuring the Data Communication Network (DCN) for *LambdaUnite* MSS network elements and the *WaveStar* CIT consists of the procedures listed below.



References

For brief descriptions of the individual procedures refer to:

- “Configuring the basic DCN parameters for the *WaveStar* CIT” (3-9)
- “Configuring the LDB timers for the *WaveStar* CIT” (3-15)
- “Administering the address list at the *WaveStar* CIT” (3-18)
- “Configuring the basic DCN parameters for an NE” (3-28)
- “Configuring data communication channels” (3-36)
- “Configuring the TARP parameters for an NE” (3-44)
- “Assigning TARP manual adjacencies” (3-47)

□

Configuring the basic DCN parameters for the *WaveStar*® CIT

When to use Use this procedure to configure the network layer parameters relevant to the *WaveStar* CIT.

This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Related information For related information, please refer to:

- Chapter 14, “Management communication setup concepts”
- Chapter 22, “*WaveStar* CIT Tutorial”

Before you begin Prior to performing this task, you must:

- have a valid user login and password for the *WaveStar* CIT,
- be logged into the subject *WaveStar* CIT, and
- have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the network layer parameters relevant to the *WaveStar* CIT.

- 1** From the *WaveStar* CIT main menu select **Administration** → **Data Communications...**

Result:

The **CIT Data Communication** window opens.

- 2** Select the **Network Layer** tab.
-

- 3** Check the actual setting of the area address in the **Primary Area Address** segment.

If you like to change the area address:

1. Disable the Auto-Learn NSAP function, and
2. Select **Modify...** in the **Primary Area Address** segment.

Result:

The **Modify Primary Area Address** window opens.

-
- 4 In the **Modify Primary Area Address** window, you can now override the area address as a whole.

Click **OK** to confirm your changes.

Result:

The **Modify Primary Area Address** window is closed.

-
- 5 If desired, change the maximum value of the routing metric in the **Max Link Metric** spin box.

-
- 6 If desired, change the value of ESCT in the **End System Config. Timer** spin box.

-
- 7 You may now proceed working in the **CIT Data Communication** window to configure the TARP loop detection buffer (LDB) timers for the WaveStar CIT, or you may save your changes and close the window.

IF ...	THEN ...
you want to proceed configuring the TARP loop detection buffer (LDB) timers,	click Apply and confirm your changes in the confirmation window, and refer to “Configuring the LDB timers for the WaveStar CIT” (3-15). END OF STEPS
you want to save your changes and close the window,	click OK and continue with Step 8.

-
- 8** Close and restart the *WaveStar* CIT application for your changes to take effect.

END OF STEPS



Supporting information for “Configuring the basic DCN parameters for the *WaveStar*® CIT”

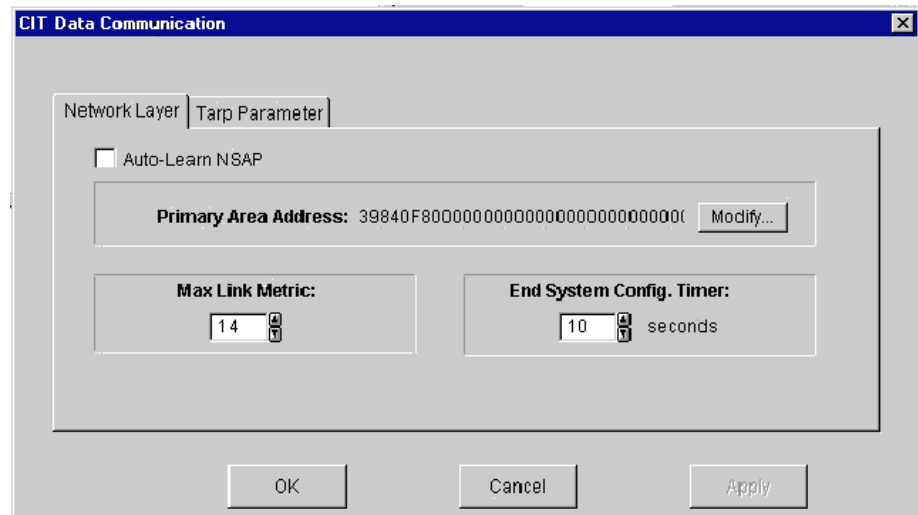
“Auto-Learn NSAP” function

When the *WaveStar* CIT application is started it initially has no NSAP address. If the Auto-Learn NSAP function is enabled, it is possible to request the area address of the connected network elements automatically. However, a precondition is that the *WaveStar* CIT is physically connected to an NE. The *WaveStar* CIT adopts the retrieved area address because the *WaveStar* CIT and the NEs on the LAN must have the same area address. The system identifier of the *WaveStar* CIT’s NSAP address depends on the PC hardware.

If the Auto-Learn NSAP function is disabled, you have to enter the *WaveStar* CIT’s NSAP address manually, either directly in the **Primary Area Address** field or by using the **Modify Primary Area Address** window. Notice that manually modifying the NSAP address is not possible as long as the Auto-Learn NSAP function is enabled.

The *Network Layer* tab

The following structure diagram displays the **Network Layer** tab of the **CIT Data Communication** window.



The **Network Layer** tab of the **CIT Data Communication** window enables you to

- view and modify the *WaveStar* CIT’s area address (**Primary Area Address**).
- set the maximum value of the routing metric (**Max Link Metric**).
- set the *WaveStar* CIT’s ESCT (**End System Config. Timer**).

Elements of the *Network Layer* tab

The elements of the **Network Layer** tab and their meaning are listed in the following table.

Window element	Meaning	Value range
Auto-Learn NSAP	This function enables the <i>WaveStar</i> CIT to automatically “learn” its area address by requesting the area address of the connected network elements. Please refer to the explanation below.	enabled (default)
Primary Area Address	The complete area address in hexadecimal representation.	

Window element	Meaning	Value range
Modify...	Click this button to invoke a configuration window for the Primary Area Address . This button will be greyed-out as long as the Auto-Learn NSAP function is enabled.	
Max Link Metric	The maximum value of the routing metric	1 to 63 Default: 14
End System Config. Timer	The WaveStar CIT’s end systems periodically generate ES Hellos (ESHs). The interval between two ESHs is determined by the End System Configuration Timer (ESCT).	1 to 1000 seconds Default: 10 seconds



Configuring the LDB timers for the *WaveStar*® CIT

When to use Use this procedure to configure the TARP loop detection buffer (LDB) entry timer and flush timer for the *WaveStar* CIT.

This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Related information For related information, please refer to:

- “Name-to-address translation” (14-32), “TARP” (14-33)
- Chapter 22, “*WaveStar* CIT Tutorial”

Before you begin Prior to performing this task, you must:

- have a valid user login and password for the *WaveStar* CIT,
- be logged into the subject *WaveStar* CIT, and
- have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1** From the *WaveStar* CIT main menu select **Administration** → **Data Communications...**

Result:

The **CIT Data Communication** window opens.

- 2** Select the **TARP Parameters** tab.

The **TARP Parameters** tab is editable only on osinode1, on other nodes it is always disabled.

- 3** If desired, enable the TARPT functionalities according to your needs.

-
- 4** Close and restart the *WaveStar* CIT application for your changes to take effect.

END OF STEPS



Supporting information for “Configuring the LDB timers for the WaveStar[®] CIT”

WaveStar CIT TARP functionality

The *WaveStar* CIT supports the TARP propagation, the TARP originator and the TARP responder functionality which all can be disabled or enabled.

The TARP Parameters tab

The **TARP Parameters** tab of the **CIT Data Communication** window allow you to enable or disable the following TARP functionalities by selecting the resüpective radio button:

- TARP propagation function
- TARP responder function.



Administering the address list at the *WaveStar*® CIT

When to use Use this procedure to generate and maintain a local CIT file containing the TIDs and NSAPs addresses for NEs that might be connected to the CIT via OSI.

For systems that have no access to an SDS database and which do not support TARP for Name/Address resolution, it is necessary to provide a mechanism to manually enter a list of TID/NSAP pairs.

This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Related information For related information, please refer to:

- Chapter 14, “Management communication setup concepts”
- Chapter 22, “*WaveStar* CIT Tutorial”

Before you begin Due to the fact that the static routing tables of *all WaveStar* CITs managing the NEs must reflect the current network situation and must be synchronised, it might be useful to generate and maintain a routing information text file which can be imported into all *WaveStar* CITs concerned.

Prior to performing this task, you must:

- have a valid user login and password for the *WaveStar* CIT,
- be logged into the subject *WaveStar* CIT, and
- have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to administer the static routing table (**Address List**) at the *WaveStar* CIT.

- 1 From the *WaveStar* CIT main menu select **Administration** → **Address List...**

Result:

The **Address Provisioning** window opens.

- 2 Depending on the action you want to perform:

IF ...	THEN ...
<i>you want to add new entries</i> to the list,	continue with Step 3.
<i>you want to remove entries</i> from the list,	continue with Step 7.
<i>you want to modify entries</i> in the list,	continue with Step 10.
<i>you want to import</i> a list from a text file,	continue with Step 15.
<i>you want to export</i> the Address List into a text file,	continue with Step 18.

- 3 Click **Add**.

Result:

The **Protocol Provisioning** window opens.

- 4 Enter the information of for the NE to be added, and verify that your entries are correct (refer to “Elements of the Address Provisioning window” (3-23)).

- 5 Click **OK** to save the new entry in the **Address List**.

- 6 Repeat Step 3 to Step 5 to add another NE address information.
Otherwise, click **OK** to save the **Address List** and to dismiss the window.

END OF STEPS

- 7 In the displayed list, select the entry to be removed.

-
- 8 Click **Delete** to remove the selected entry from the list.
-

- 9 Repeat Step 7 and Step 8 to remove another entry from the list.
Otherwise, click **OK** to save the **Address List** and to dismiss the window.

END OF STEPS

- 10 In the displayed list, select the entry to be modified.
-

- 11 Click **Modify**.

Result:

The **Protocol Provisioning** window opens.

- 12 Modify the information for the selected entry, and verify that your entries are correct (refer to “Elements of the Address Provisioning window” (3-23)).
-

- 13 Click **OK** to save the modified information and to dismiss the window.
-

- 14 Repeat Step 10 to Step 13 to modify another TID/NSAP address pair.
Otherwise, click **Close** to save the **Address List** and to dismiss the window.

END OF STEPS

- 15 Click **Import...**

Result:

A file selection dialog window opens.

- 16 Select the file to be imported from the file selection dialog window and click **Open**.
-

Result:

The **Address List** is replaced by the imported list.

Please note that if the import file has not the expected structure (cf. "Import file format" (3-26)), then importing of the file will be rejected with a corresponding error message.

-
- 17** Click **OK** to save the **Address List** and to dismiss the window.
-

- 18** Click **Export...**

Result:

A file selection dialog window opens.

-
- 19** Select the path where the file has to be stored and enter a filename and click **OK**.

Result:

The **Address List** is stored at the specified location and by the specified filename.

-
- 20** Click **OK** to save the **Address List** and to dismiss the window.

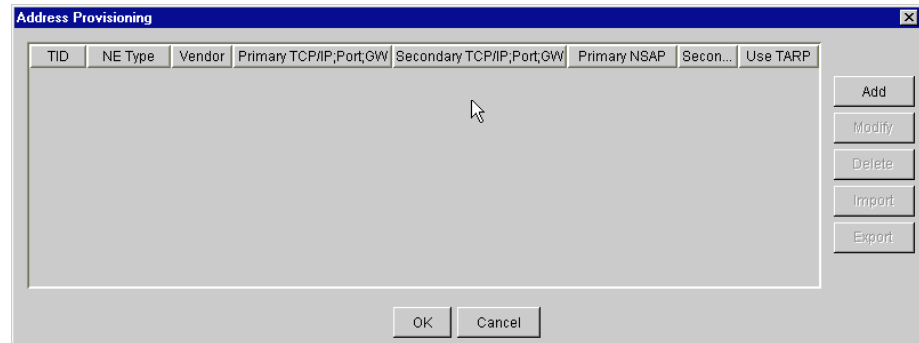
END OF STEPS



Supporting information for “Administering the address list at the WaveStar® CIT”

The *Address Provisioning* window

The **Address Provisioning** window can be invoked from the WaveStar CIT main menu via **Administration** → **Address List...**



The *Protocol Provisioning* window

The **Protocol Provisioning** window can be invoked from the **Address Provisioning** window.

Elements of the *Address Provisioning* window

The elements of the **Address Provisioning** window and their meaning are listed in the following table.

Window element	Meaning
NE Name List	This displays a list of the existing TIDs in the CITs file and enables you to select or enter or modify a TID. Upon selection of an existing TID, the screen is filled with the current Address provisioning for that TID. If no TID is selected, the address fields are empty, ready to be filled in with the information for a new list entry.

Window element	Meaning
NE Type	This field displays the NE type for the selected/entered NE name. You can also enter or modify the NE name. You can select from a list of supported NE types or Other. Observe the configuration rules given on page “NE name configuration rules” (3-24).
NSAP Address	The text boxes in this group box represent the individual fields of an NE’s NSAP address. Please refer to “NSAP address format” (14-19). These text boxes can be used to enter an NSAP address corresponding to the TID in the NE Name group box. The NSAP text box at the bottom of the group box is a read-only box and indicates the complete NSAP address.
Vendor	This field displays and enables the user to enter or modify the system vendor, e.g. Lucent.
Use for OSI Connection	Values Primary or Secondary (or checkbox). Default: Primary. Secondary is not applicable if no Secondary NSAP is defined. The selected address is used for OSI connections to this NE.
OSI	
Primary OSI NSAP (TARP Override)	This field displays a primary NSAP address as a 40 character NSAP entry or 20 octets. In this field the displayed NSAP address can be modified. You can enter this field either as a single string of 40 characters or in individual fields.
Secondary OSI NSAP (TARP Override)	This field displays a secondary NSAP address as a 40 character NSAP entry or 20 octets. In this field the displayed NSAP address can be modified. You can either write your entry into this field as a single string of 40 characters or into individual fields.
NE name configuration rules	The following NE name configuration rules must be observed: • The following characters are allowed in an NE name: - Upper-case letters (‘A’ .. ‘Z’), - Lower-case letters (‘a’ .. ‘z’), - Digits (‘0’ .. ‘9’), - Hyphen (“-”). • Each NE name must be unique within the network.

- Each NE name must be maximally 20 characters in length.
- The NE name may contain segments separated by hyphens (“-”), but each segment must begin with a letter.

Please note that NE names are case-insensitive.

Pushbuttons The **Address Provisioning** window provides the following pushbuttons:

Close	Use this button to dismiss the window.
Add	Use this button to add a new new NE Name with its accompanying data. This option is dimmed if the you select an existing entry in the list.
Delete	Use this button to remove an existing NE Name with its accompanying data. This option is dimmed until you select an existing entry in the list.
Modify	Use this button to modify an existing NE Name and its accompanying data. This option is dimmed until you select an existing entry in the list.
Apply	Use this button to apply changes to the static routing table.
Import...	Use this button to import a standard text file (cf. “Import file format” (3-26)) containing a list of NE Names with their accompanying data. The imported list will replace the existing static routing table of the WaveStar CIT. Clicking on this field invokes a Microsoft Windows standard browser window from which you can select a file, which is then be used to replace the existing Address List on the CIT. It is your responsibility to build this file in the proper manner.

Export... Enables you to select a file to be generated with the fields supported above. Clicking on this field invokes a Microsoft Windows Standard Browser window from which you can select a file. Selection will cause the Address List to be entered into that file name in the format below.

Import file format The file to be imported must have the following structure:

- The import file may be a standard text file.
- Each line shall represent a single NE.
Fields on each line shall be semicolon separated and as follows:
 - The first field represents the TID. The TID format must be in accordance with the TID configuration rules (cf. “Elements of the Address Provisioning window” (3-23)).
 - NE Type..
 - Vendor, e.g. Lucent
 - A primary IP address,
 - For a primary TCP/IP Gateway NE only, an integer field is required which is the port number, ranging from 0 to 65535, inclusive. If this field is missing or an invalid integer, the primary TCP/IP Gateway is set to Disable, even if this overrides the value in the primary TCP/IP Gateway Enable field (since the port number is needed to enable the Gateway).
 - For a TCP/IP Gateway NE only, an integer field to enable or disable the primary TCP/IP Gateway. 0 implies Disable, 1 implies Enable. If fields 6 and 7 are not filled in, i.e. ‘-’, then primary TCP/IP Gateway is Disable.
 - A secondary IP address
 - For a secondary TCP/IP Gateway NE only, an integer field is required which is the port number, ranging from 0 to 65535, inclusive. If this field is missing or an invalid integer, the secondary TCP/IP Gateway is set to Disable, even if this overrides the value in the secondary TCP/IP Gateway Enable field (since the port number is needed to enable the Gateway).

- For a TCP/IP Gateway NE only, an integer field to enable or disable the secondary TCP/IP Gateway. 0 implies Disable, 1 implies Enable. If fields 8 and 9 are not filled in, i.e. '-', then secondary TCP/IP Gateway is Disable.
- A Primary NSAP (in accordance with the ISO-DCC NSAP address format). Please refer to “NSAP address format” (14-19).
- A Secondary NSAP (in accordance with the ISO-DCC NSAP address format). Please refer to “NSAP address format” (14-19).
- Comments can be added to the file as needed. Comments are designated by the pound '#' character.
- All fields must be present. A dash '-' is used if values do not apply.

Important! If any given import file has not the expected structure, then importing of the file will be rejected with a corresponding error message.



Configuring the basic DCN parameters for an NE

When to use Use this procedure to configure the basic DCN parameters for a network element. Configuring the basic DCN parameters includes:

- Enabling/Disabling the Intraoffice LAN (IAO-LAN),
- Modifying a node's area address (the area address is the configurable part of the NSAP address),
- Specifying the node's intermediate system (IS) characteristics,
- Modifying Transport Layer parameters.

This procedure is part of the DCN configuration; please refer to "Configuring the data communication network (high level)" (3-6).

Related information For related information, please refer to:

- "NSAP address format" (14-19)
- "Supporting information for "Configuring the basic DCN parameters for an NE"" (3-32)
- Chapter 14, "Management communication setup concepts"
- Chapter 22, "WaveStar® CIT Tutorial"

Before you begin Prior to performing this task, you must:

1. log into the WaveStar CIT, and
2. connect to the NE.

Required privilege code

You must have at least a privilege code of:

- S4

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps to configure the basic DCN parameters for an NE.

- 1 At the *WaveStar* CIT, select **Administration** → **Data Communications...** from the **System View** or **Shelf View** main menu.

Result:

The equipment selection window opens.

- 2 By means of the equipment selection window, select an IAO LAN interface, or the system (osinode) for which you want to configure the basic DCN parameters. Each of these object types have their own provisioning screen.

Result:

The **Data Communications** window opens. If you have selected an IAO LAN AID, only the **LAN Management** tab is applicable.

- 3 If you like to view (and possibly change) the LAN status, then select the **LAN Management** tab.

Otherwise continue with Step 8.

- 4 You may now enable or disable the LAN access for the selected LAN port.

Restriction:

Please note that LAN1 cannot be disabled.

- 5 You may now enable or disable the **LAN TARP Storm Suppression** for the selected LAN port.

If disabled the feature **LAN TARP Storm Suppression** can only be enabled if TARP propagation is enabled.

-
- 6
- If desired, change the value for the LAN Router Priority by means of the **LAN Designated Router Priority** spin box. The possible values range from 1 to 127.
-
- 7
- If you have made any changes in the **LAN Management** tab click **Apply** and confirm your changes in the confirmation window.
-
- 8
- Select the **Network Layer** tab.
-
- 9
- Check the actual setting of the area address in the **Network Service Access Point** segment.
-

IF ...	THEN ...
you like to change the node's area address,	select Modify... and continue with Step 10.
you want to leave the node's area address unchanged,	continue with Step 11.

.....

- 10
- In the **NSAP/Area Address Provision** window, you can now change each area address field individually in the **AFI**, **IDI** etc. text boxes.
- Click **OK** to confirm your changes.

Result:

The **NSAP/Area Address Provision** window is closed.

Please note that subsequently the DCC controller is restarted.

Wait until the restart has finished.

.....

- 11
- Specify the node's IS routing capability by means of the **Routing Capability** check boxes in the **Intermediate System** group box depending on whether the node shall act as a **Level 1**, a **Level 1&2** or a **Level 1&2 w/Partition repair** router.
-
- 12
- If you have made any changes in the **Network Layer** tab click **Apply** and confirm your changes in the confirmation window.
-

-
- 13** You may now select another tab of the **Data Communications** window to configure TARP parameters or manual adjacencies for example, or you may save your changes and close the window.

IF ...

you want to save your
changes and select another
tab of the **Data**

Communications window,

you want to save your
changes and close the **Data**
Communications window,

THEN ...

click **Apply**
and confirm your changes in the
confirmation window, and refer to the
corresponding task description.

click **Apply** and then **Close**
and confirm your changes in the
confirmation window.
Please note that subsequently the DCC
controller is restarted. Wait until the
restart has finished.

END OF STEPS

.....



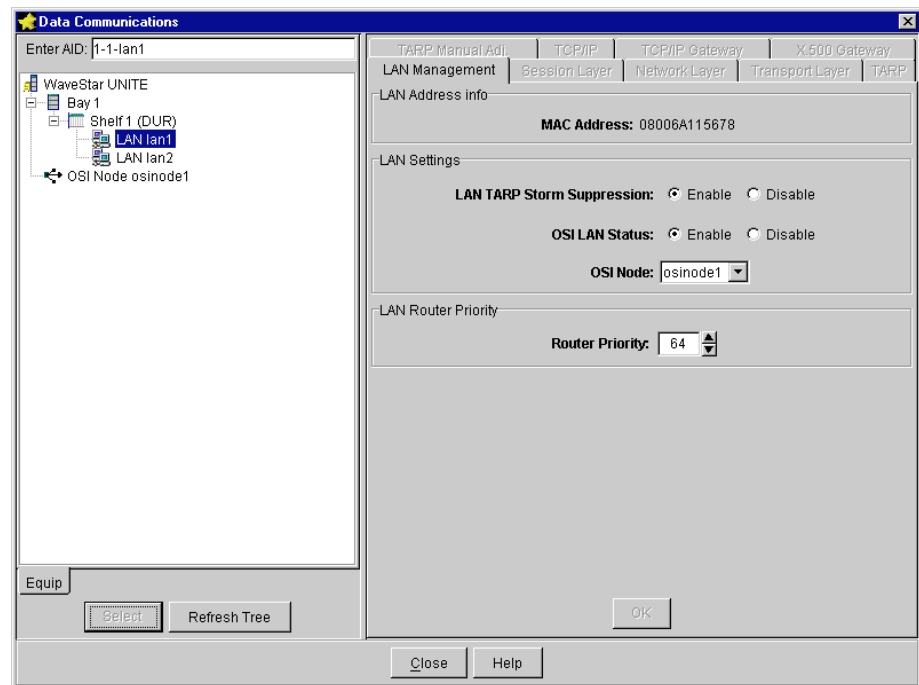
Supporting information for “Configuring the basic DCN parameters for an NE”

Network elements and nodes

A distinction has to be made between network elements and nodes. Network elements can be identified by their target identifier (TID), i.e. their NE name (“NE name” and “TID” are used synonymously throughout this User Operations Guide), whereas a node is identified by its Network Service Access Point (NSAP) address. Each NSAP address within a network constitutes a node which can individually be addressed.

The LAN Management tab

The **LAN Management** tab of the **Data Communications** window makes it possible to manage the OSI LAN for a selected LAN port. The LAN access is enabled in the basic configuration. The **LAN Management** tab also offers the opportunity to modify the LAN Router Priority.



Elements of the LAN Management tab

The elements of the **LAN Layer** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range
AID	This field displays the AID of the selected IAO LAN port. This field is read only.	
MAC Address	MAC address of the selected IAO LAN port. This field is read only.	
LAN Status	This field can be used to enable or disable the LAN for the selected LAN Port.	Enable or Disable.(Default: LAN1 is always Enabled, e.g. cannot be disabled)
OSI Node	This field displays the assignment of the LANs to an OSI-node in a NE.	For LAN1: osinode1
LAN Router Priority	Indicates the priority of the router connected to the LAN. A higher number has priority over a lower one. From all routers connected to the LAN, the router with the highest priority is selected as the Designated router. The designated Router takes care of routing of packets in the Q-LAN.	1- 127
LAN TARP Storm Suppression	This field allows you to enable or disable External LAN TARP Storm Suppression.	Enable or Disable

The *Network Layer* tab

The **Network Layer** tab of the **Data Communications** window provides information on the actual network layer configuration and

The screenshot shows the WaveStar UNITE software window. On the left, a tree view displays the network hierarchy: WaveStar UNITE > Bay 1 > Shelf 1 (DUR) > LAN lan1 > OSI Node osinode1. The 'OSI Node osinode1' is selected and highlighted. Below the tree are 'Equip', 'Select', and 'Refresh Tree' buttons. The main area on the right has tabs for 'TARP Manual Adj.', 'TCP/IP', 'TCP/IP Gateway', and 'X-500 Gateway'. The 'TCP/IP' tab is active, showing sub-tabs for 'LAN Management', 'Session Layer', 'Network Layer', 'Transport Layer', and 'TARP'. Under 'Network Service Access Point', there's a field for 'NSAP: 39840F8010010000000000000000006A1123451D' and a 'Modify' button. Under 'Intermediate System', there's a 'Routing capability:' label and a dropdown menu set to 'Level 1&2 w/Partition Repair'. At the bottom right is an 'OK' button. The very bottom of the window has 'Close' and 'Help' buttons.

The elements of the **Network Layer** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range
AID	AID of the selected osinode.	read-only;
NSAP	This field displays the current NSAP dependent on the actual setting of the configurable NSAP address fields.	read-only; please refer to “NSAP address fields” (14-20)

Window element	Meaning	Value range
Intermediate System Routing Capability	The node’s IS routing capability.	The following values can be selected: • Level 1 (default) • Level 1&2 • Level 1&2 with Partition Repair



Configuring data communication channels

When to use Use this procedure to create new or modify existing DCC terminations.

This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Related information For related information, please refer to:

- Chapter 14, “Management communication setup concepts”
- Chapter 22, “ *WaveStar*® CIT Tutorial”
- “Supporting information for “Configuring data communication channels”” (3-39)

Before you begin Prior to performing this task, you must have an overview of the current network topology.

Furthermore, you must:

1. log into the *WaveStar* CIT, and
2. connect to the NE.

Required privilege codes

You must have at least a privilege code of:

- S1
to view the currently enabled DCC terminations,
- S4
to create new or modify existing DCC terminations.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to create a new DCC termination or to modify an existing DCC termination.

- 1 At the *WaveStar* CIT, open the **View DCC Terminations** window and verify that at least one DCC channel is indicated available by

checking the **Remaining Channels** field (cf. “The View DCC Terminations window” (3-39)).

-
- 2**
- | IF ... | THEN ... |
|--|---|
| there is at least one DCC channel available, | continue with Step 3. |
| there are no DCC channels available, | disable dispensable DCC channels, and continue with Step 3. |
-
- 3** Invoke the **Configure DCC Terminations** window from the **System View** main menu via **Configuration → DCC Terminations...**; see “The Configure DCC Terminations window” (3-41).
-
- 4** Select the system or an individual optical port unit for which you want to configure the DCC terminations by means of the equipment selection part of the window.
-
- 5** In the parameter part, select the action you want to perform
-
- 6**
- | If you want to... | then ... |
|---|---|
| create a new DCC termination, | select New Termination and continue with Step 7. |
| modify an existing DCC termination, | select Current Terminations and continue with Step 8. |
| disable a currently enabled DCC termination, | select Current Terminations and continue with Step 11. |
-
- 7** In the **Select a port for New Termination** group box, select the working optical interface port, and continue with Step 9.
-
- 8** In the **Select a port for Current Termination** group box, select the working optical interface port, and continue with Step 9.
-

-
- 9** In the **DCC Channel Parameters** group box, choose the LAPD mode (either **UITS** (default) or **AITs**) in the **LAPD Mode:** drop down list box.
-

- 10** Enable the DCC termination by selecting the **Enabled** option in the **DCC Channel Parameters** group box.

END OF STEPS

.....

- 11** In the **Select a port for Current Termination** group box, select the working optical interface port for which you want to disable the DCC communication.
-

- 12** Disable the DCC termination by selecting the **Disable Termination** option in the **DCC Channel Parameters** group box.

Important! Disabling a previously enabled DCC at an NE needs to be coordinated with disabling the same DCC at the opposite end of the DCC link (remote NE) to avoid persistent alarms from the remote NE.

END OF STEPS

.....



Supporting information for “Configuring data communication channels”

Preconditions for enabling a DCC

You are permitted to enable a DCC if all of the following preconditions are fulfilled:

- A XC320 must be plugged in (To get a DCC channel work a XC320 must be physically available and work).
- The corresponding optical interface port is provisioned (configured) or at least pre-provisioned.
- The DCC is not yet enabled.
- There are RS/MS-DCC channels available. Please refer to “Max. number of active DCC links” (3-39) below.

Max. number of active DCC links

The maximum number of simultaneously supported RS/MS-DCC channels per DCC controller is 64. Each DCC controller thus can support up to 64 active DCC links. Upon circuit pack insertion, DCCs are left in the disabled state.

Preconditions for disabling a DCC

You should disable a DCC only if **all** of the following preconditions are fulfilled:

- The DCC is currently enabled.
- The DCC is currently not needed for MS-SPRing management.
- The DCC is not the only management connection to remote NEs.

Relevant windows

The following *WaveStar*[®] CIT windows are relevant to perform this task:

- **View DCC Terminations**
- **Configure DCC Terminations**

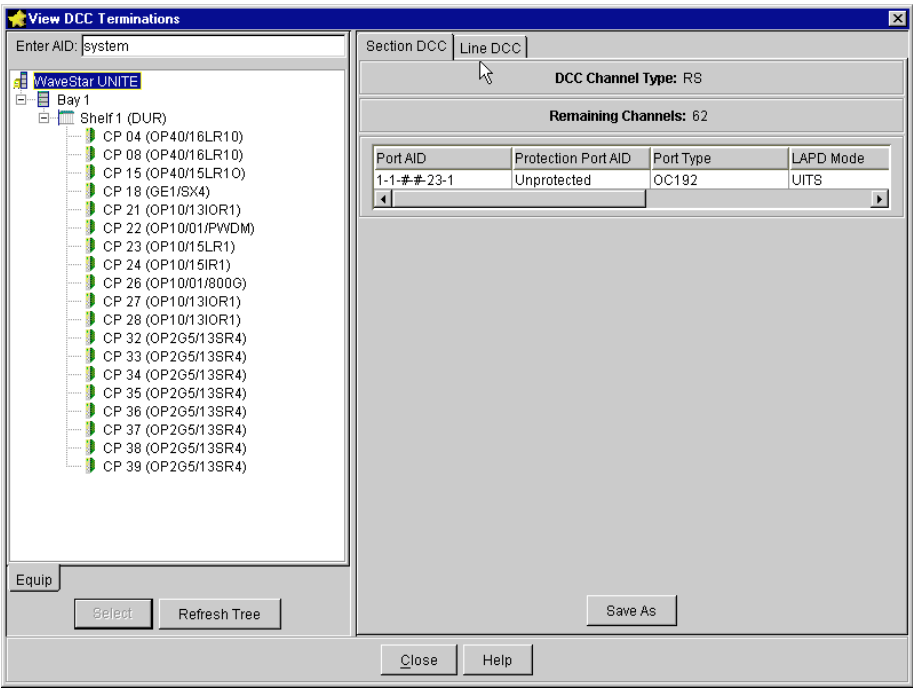
The *View DCC Terminations* window

The **View DCC Terminations** window provides information on the current DCC configuration.

There are two possible ways to invoke this window:

- By selecting the **DCC Terminations** option from the pop-up menu that opens when you right-click on an optical port unit of the **System View** window.
- By selecting **View → DCC Terminations...** in the **System View** main menu.

Please note that you must either select the system or an optical port AID from the **Equipment Selection** window, before the **View DCC Terminations** window opens.



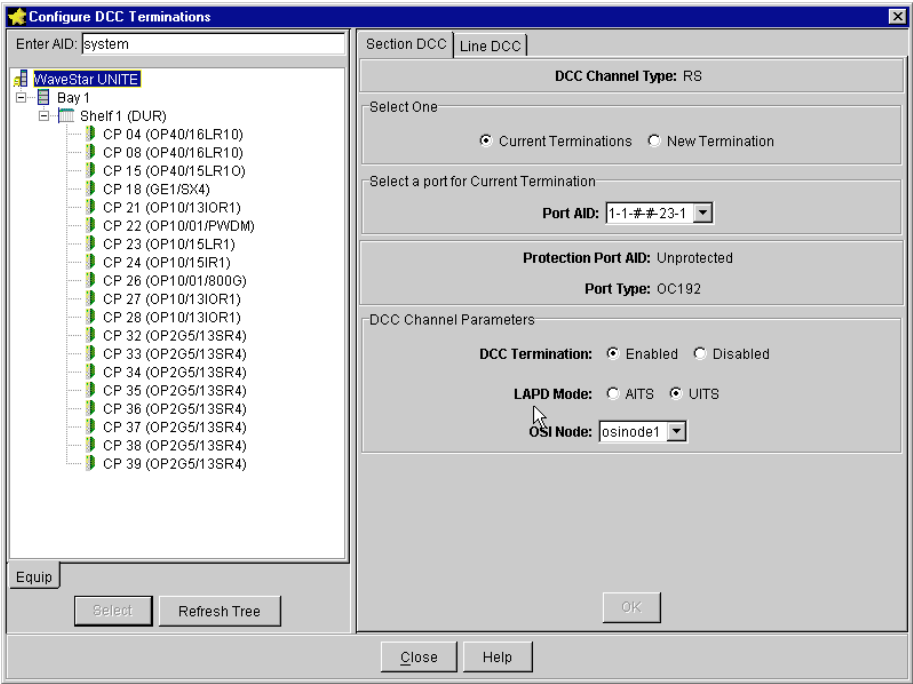
Elements of the View DCC Terminations window

The window elements of the **View DCC Terminations** window and their meaning are listed in the following table (please also refer to “Data communication channels” (14-24)). These window elements are displayed for each LAPD channel.

The following table lists the window elements of the **View DCC Terminations** window and explains their meaning.

Parameter	Meaning
DCC Channel Type	If the default interface standard is set to SDH, this field’s values can be RS or MS . Otherwise when the Default Interface Standard is set to SONET, this field’s values can be Section or Line .
Remaining Channels	Indicates the remaining number of DCC Channels which have not been terminated.
Scrollable table with details on each terminated port:	
(Working) Port AID	The AID of the “working” optical interface port. All optical interface ports with DCC enabled are considered to be “working” ports.
Port Type	The type of the associated optical interface port. This can be either - for the SONET optical interfaces: OC-768, OC-192, OC-48. - for the SDH optical interfaces: STM-256o, STM-64o, STM-16o.
Channel Enable	This can be either Enabled Disabled
LAPD Mode	The assigned LAPD mode. This can be either UITS (default) (unacknowledged service) or AIMS (acknowledged service).
The Configure DCC Terminations window	In the Configure DCC Terminations window, you can set all the parameters required for the operation of data communication channels.

The **Configure DCC Terminations** window can be invoked from the **System View** main menu via **Configuration → DCC Terminations...**



Elements of the *Configure DCC Terminations* window

The parameter part on the right-hand side of the **Configure DCC Terminations** window contains two tabs, one for the **Section DCC** (RS DCC) and one for the **Line DCC** (MS DCC).

The window elements of the parameter part of the **Configure DCC Terminations** window are listed in the following table (please also refer to “Data communication channels” (14-24)). If applicable, the permitted value range as well as the default setting of the parameters are also given.

Window element	Value range	Default Setting
OSI Node	osinode 1	osinode 1; read-only

Window element	Value range	Default Setting
DCC Channel Type	If the default interface standard is set to SDH, this field’s values can be RS or MS . Otherwise when the Default Interface Standard is set to SONET, this field’s values can be Section or Line .	Section/RS
Selection group box (Select One)	Current Terminations or New Termination	Current Terminations
(Working) Port AID	dependent on the previous selection.	only selectable optical interface ports are listed
Port Type	The type of the associated optical interface port. This can be either - for the SONET optical interfaces: OC-768, OC-192, OC-48. - for the SDH optical interfaces: STM-256o, STM-64o, STM-16o.	no default setting; read-only
DCC Channel Parameters		
Disable Termination	This checkbox allows the user to disable the DCC termination for the port being displayed. If the port is part of a BLSR/MSP protection group, this field is dimmed. This is the mechanism for removing a port from the pool of DCC terminations.	
LAPD Mode	This parameter indicates the type of LAPD service: • AITS • UITS	



Configuring the TARP parameters for an NE

When to use This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Use this procedure to

- enable or disable the TARP propagation functionality,, or to
- enable or disable the TARP responder functionality.

for a selected node.

Related information For related information, please refer to:

- Chapter 14, “Management communication setup concepts”
- Chapter 22, “ *WaveStar*[®] CIT Tutorial”

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT and the respective network element.

Required privilege code

You must have at least a privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the TARP parameters for an NE:

- 1 At the *WaveStar* CIT, select **Administration** → **Data Communications...** from the **System View** or **Shelf View** main menu.

Result:

The equipment selection window opens.

- 2 By means of the equipment selection window, select osinode1.

Result:

The **Data Communications** window opens.

-
- 3 Select the **TARP** tab of the **Data Communications** window.

 - 4 Enable or disable the TARP propagation functionality according to your needs by selecting the corresponding check box in the **TARP Propagation** group box. The TARP propagation functionality is enabled by default.

 - 5 Enable or disable the TARP Responder functionality according to your needs by selecting the corresponding check box in the **TARP Responder** group box. The TARP responder functionality is enabled by default.
- Important!** Editable only on osinode1, on other nodes always Disabled.
-
- 6 You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

If you want to ...

save your changes and select another tab of the **Data Communications** window,

save your changes and close the **Data Communications** window,

then ...

click **Apply** and confirm your changes in the confirmation window, and refer to the corresponding task description.
END OF STEPS

click **OK** and confirm your changes in the confirmation window.
END OF STEPS

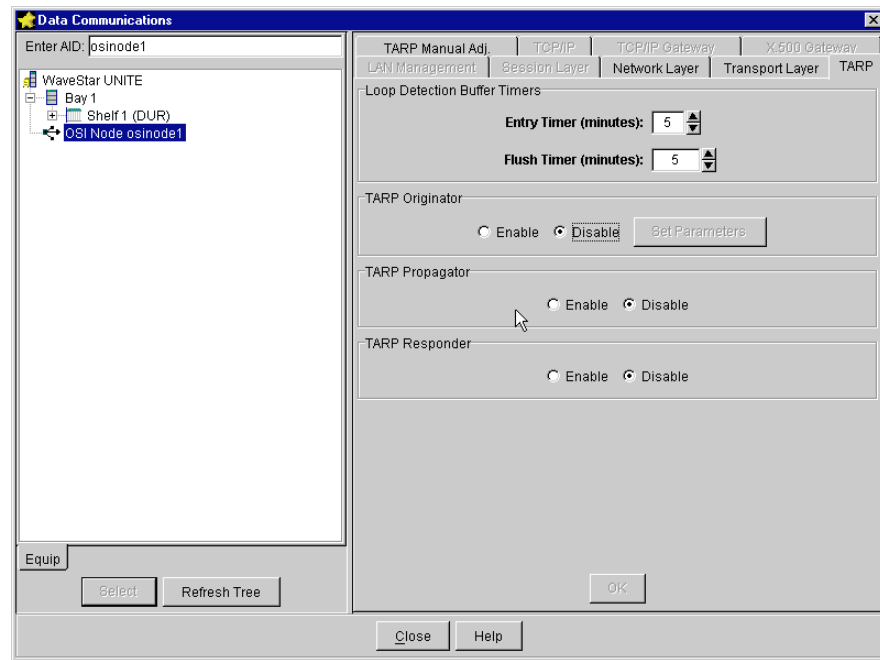
END OF STEPS



Supporting information for” Configuring the TARP parameters for an NE”

The **Data Communications** window

The **TARP** tab of the **Data Communications** window is relevant to perform this task.



The **TARP** tab of the **Data Communications** window makes it possible to

- enable or disable the TARP propagation functionality, and to
- enable or disable the TARP responder functionality.

for a selected node.

□

Assigning TARP manual adjacencies

When to use This procedure is part of the DCN configuration; please refer to “Configuring the data communication network (high level)” (3-6).

Use this procedure to manually assign adjacent nodes that support TARP (“TARP manual adjacencies”) by entering their Network Entity Title (NET).

Two TARP manual adjacencies can be created for one DCC.

The area address together with the system identifier (SYSTEM field) of the NSAP address is also called the Network Entity Title (NET; cf. “ISO-DCC NSAP address format” (14-20)).

Related information For related information, please refer to:

- Chapter 14, “Management communication setup concepts”
- Chapter 22, “*WaveStar*® CIT Tutorial”

Before you begin Prior to performing this task, you must:

1. log into the *WaveStar* CIT, and
2. connect to the NE.

Take notes of the NSAP addresses of the TARP manual adjacencies you are going to assign.

Required privilege code

You must have at least a privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to assign TARP manual adjacencies:

- 1 At the *WaveStar* CIT, select **Administration** → **Data Communications...** from the **System View** or **Shelf View** main menu.

Result:

The equipment selection window opens.

-
- 2 By means of the equipment selection window, select osinode 1.

Result:

The **Data Communications** window opens.

.....

- 3 Select the **TARP Manual Adj.** tab of the **Data Communications** window.
-

- 4 Depending on whether you want to assign a new, modify or delete an existing TARP manual adjacency:

If you want to ...	then ...
add a manual adjacency, there must be an empty TARP Manual Adjacency (between the field MAJ1: or MAJ2: and the corresponding Modify button no Network Entity Title (NET) has to be displayed).	continue with Step 5.
modify an existing manual adjacency,	continue with Step 9.
delete an existing manual adjacency,	continue with Step 13.

.....

- 5 Click **Modify** beside the empty **TARP Manual Adjacency**.

Result:

The **NSAP/Area Address Provision** window opens.

-
- 6 Enter the individual fields of the TARP manual adjacency's NET into the corresponding text boxes in the **NSAP/Area Address Provision** window.
-

- 7 Make sure that the NET is correct.

IF ...

the NET is correct,

the NET is not correct,

THEN ...

continue with Step 8.

correct the corresponding entries
and continue with Step 8.

- 8 Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

- 9 Click **Modify...** beside the text box of the MAJx you want to modify.

Result:

The **NSAP/Area Address Provision** window opens.

In principle the window is the same as the window used in Step 5.

-
- 10** Enter the individual fields of the TARP manual adjacency's NET into the corresponding text boxes in the **NSAP/Area Address Provision** window.
-

- 11** Make sure that the NET is correct.

IF ...	THEN ...
the NET is correct,	continue with Step 12.
the NET is not correct,	correct the corresponding entries and continue with Step 12.

.....

- 12** Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

.....

- 13** Click **Modify** beside the **TARP Manual Adjacency** you want to delete.

Result:

The **NSAP/Area Address Provision** window opens.

In principle the window is the same as the window used in Step 5.

.....

- 14** Remove all the entries in the individual fields of the TARP manual adjacency's NET in the **NSAP/Area Address Provision** window.
-

- 15** Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

.....

- 16** You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save
-

your changes and close the window.

IF ...	THEN ...
you want to save your changes and select another tab of the Data Communications window,	click Apply and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS
you want to save your changes and close the Data Communications window,	click Apply and then Close and confirm your changes in the confirmation window. END OF STEPS
END OF STEPS	

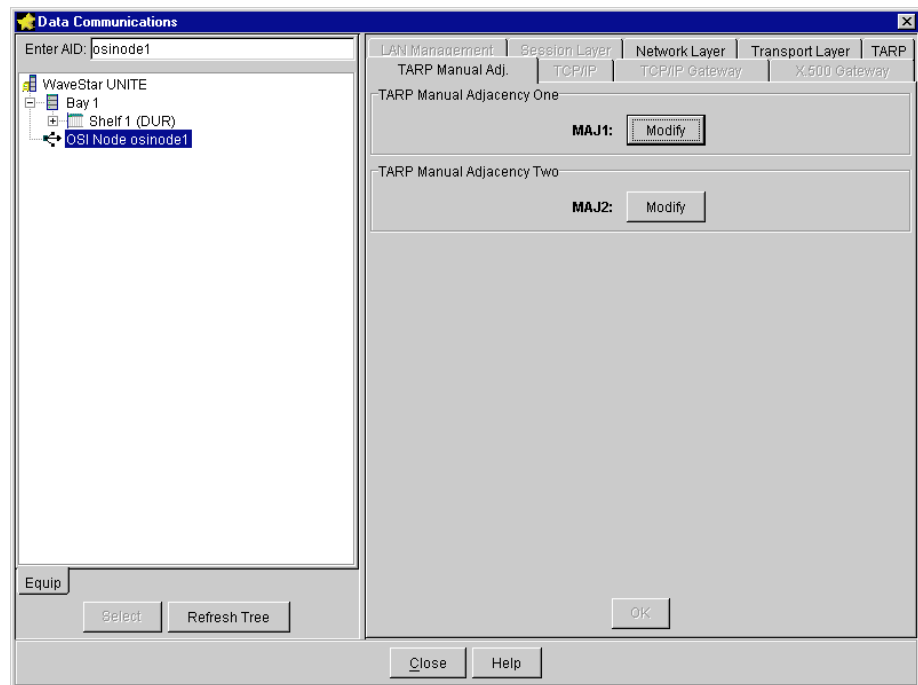


Supporting information for “Assigning TARP manual adjacencies”

The *Data Communications* window

The **TARP MAJ** tab of the **Data Communications** window is relevant to perform this task.

The **TARP Manual Adj.** tab of the **Data Communications** window makes it possible to enter new or modify existing TARP manual adjacencies.



□

Setting system parameters

When to use Use this procedure to set system parameters.

Related information For related information, see:

- “Overview of access identifiers” (15-8)
- “Alarm severities” (16-10)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code(s)

You must have at least a privilege code of P3, Provisioning, or M3, Maintenance, to set the system parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to set the system parameters:

- 1 From the **System View** main menu, select **Fault** → **Enter/Exit Maintenance Condition...** → **Enter Maintenance Condition ...**
 - 2 Confirm the resulting system message by clicking **YES**.
 - 3 From the *WaveStar* CIT System View or Shelf View main menu, select **Configuration** → **Provision**.
-

Result:

The window **Provision Parameters for Protection Groups or Equipment** opens. The **Equipment** selection tab appears on the left side of the window.

- 4 Select the system in the **Equipment** selection tab and click on **Provision**.

Result:

The selection window for the system parameters appears on the right side of the window.

-
- 5 Set the **Optical Interface Standard** to be used for the actual NE by selecting the according radio button (**SONET** or **SDH**).
 - 6 Set the **Tributary Mode Default** to be used for the actual NE by selecting the according radio button (**Adaptive-Rate** or **Fixed-Rate**).
 - 7 Set the **System Synch Characteristics** to be used for the actual NE by selecting the according radio button (**SONET** or **SDH**).
 - 8 Click the **Apply** pushbutton.
 - 9 From the **System View** main menu, select **Fault** → **Enter/Exit Maintenance Condition...** → **Exit Maintenance Condition...**
 - 10 Confirm the resulting system message by clicking **OK**.
-

Result:

The *LambdaUnite*[™] MSS NE will now perform a system reset. As a consequence, the management association between the *WaveStar* CIT and the NE will be lost.

After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar* CIT to the NE.

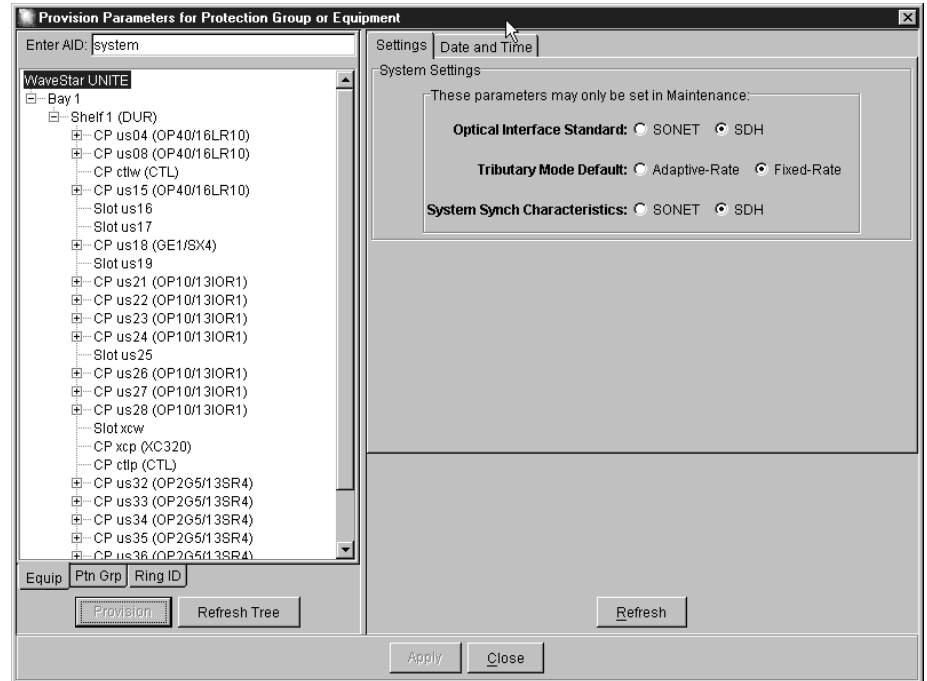
END OF STEPS



Supporting information for “Setting system parameters”

Relevant WaveStar® CIT window

The following window is used to set system parameters:



□

Setting date and time

When to use	Use this procedure to set time and date of the system. The network element clock must be set again after each power on or reboot.
Related information	For related information, see: • “Overview of access identifiers” (15-8) • “Alarm severities” (16-10)
Before you begin	Prior to performing this task, you must be logged into the <i>WaveStar</i>® CIT and the respective network element. Required privilege code(s) You must have at least a privilege code of P3, Provisioning, or M3, Maintenance, to set the system parameters. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Complete the following steps to set the date and time of the system: 1 From the <i>WaveStar</i> CIT System View or Shelf View main menu, select Configuration → Provision. Result: The window Provision Parameters for Protection Groups or Equipment opens. The Equipment selection tab appears on the left side of the window. 2 Select the system in the Equipment selection tab and click on Provision. Result: The selection window for time and date appears on the right side of the window.

-
- 3** Select the day (by clicking on the respective date), month (via the drop-down list box) and year (via the spin-box) in the group box **Date**.
-

- 4** Set the time in the group box **Time**.
-

- 5** Click the **Apply** pushbutton.

Important! The settings made in this window come into effect and will be shown after re-opening the window.

END OF STEPS



Supporting information for “Setting date and time”

Relevant WaveStar® CIT window

The following window is used to set the date and time of the system:

Enter AID: system

WaveStar UNITE

Bay 1

Shelf 1 (DUR)

CP 04 (OP40/16LR10)

CP 08 (OP40/16LR10)

CP ctlw (CTL)

CP 15 (OP40/16LR10)

Slot 16

Slot 17

CP 18 (GE1/SX4)

Slot 19

CP 21 (OP10/13IOR1)

CP 22 (OP10/13IOR1)

CP 23 (OP10/13IOR1)

CP 24 (OP10/13IOR1)

Slot 25

CP 26 (OP10/13IOR1)

CP 27 (OP10/13IOR1)

CP 28 (OP10/13IOR1)

Slot xcw

CP xcp (XC320)

CP ctlp (CTL)

CP 32 (OP2G5/13SR4)

CP 33 (OP2G5/13SR4)

CP 34 (OP2G5/13SR4)

CP 35 (OP2G5/13SR4)

CP 36 (OP2G5/13SR4)

Equip Ptn Grp Ring ID Path Ptn

Provision Refresh Tree

Settings Date and Time

System AID: system

Date

Year: 2001 Month: July

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Time

Hour: 1 Minute: 13

☐ am ☒ pm

Refresh

Apply Close



4 Equipment provisioning

Overview

Purpose	This chapter describes the procedures which have to be carried out for the provisioning of the hardware components of the <i>LambdaUnite</i> [™] MSS.
Provisioning hierarchy	Some provisioning parameters relate to other provisioning parameters and must be completed in a hierarchical fashion.
Provisioning of an NE with an empty database	If an initial load to the non-volatile memory (NVM) of a newly established network element has been performed, it has an empty database, meaning that it has no configuration data. Before the NE can be managed at least the Target Identifier (TID) has to be set. The steps of this basic provisioning are described in the chapter Chapter 3, “Management communication setup”:
Configuration data	After the basic steps have been carried out, the definition of the configuration data can be carried out. This finally leads to the normal operation of an NE within a network according to the given needs. Additionally to the setting of the configuration data for normal operation, this chapter includes procedures related to the hardware such a removing equipment from the system and the switching of equipment protections.

Download of existing data Besides the step-by-step configuration, it is possible to download existing configuration data from a data carrier to the NE.

Contents

Initial equipment provisioning	<u>4-3</u>
Configuring the system	<u>4-4</u>
Configuring the shelf	<u>4-7</u>
Configuring a slot	<u>4-9</u>
Creating a new circuit pack	<u>4-11</u>
Reassigning a circuit pack	<u>4-14</u>
Configuring an optical SDH/SONET port	<u>4-16</u>
Setting the parameters of optical ports	<u>4-19</u>
Configuring a tributary	<u>4-26</u>
Provisionable parameters of tributaries	<u>4-28</u>
Removing equipment from the system	<u>4-29</u>
Retrieving equipment info for the system	<u>4-31</u>
Retrieving equipment info for the shelf	<u>4-33</u>
Retrieving equipment info for slots	<u>4-35</u>
Viewing data of a slot	<u>4-36</u>
Retrieving equipment info for circuit packs	<u>4-37</u>
Viewing data of a circuit pack	<u>4-38</u>
Retrieving equipment info for optical SDH/SONET ports	<u>4-40</u>
Viewing data of a optical SDH/SONET port	<u>4-41</u>
Retrieving equipment info for tributary	<u>4-43</u>
Viewing data of a tributary	<u>4-44</u>
Retrieving equipment info for the backplane	<u>4-46</u>
Viewing data of the backplane	<u>4-47</u>
Viewing an equipment protection group	<u>4-48</u>
Parameters for a 1+1 equipment protection	<u>4-49</u>
Switching a 1+1 equipment protection	<u>4-50</u>



Initial equipment provisioning

When to use This procedure shows the provisioning steps which have to be carried out for the setting of the configuration data of the hardware components belonging to a network element with an empty database.

Before you begin Prior to performing the following tasks, you must be logged into the *WaveStar*® CIT and a network element (directly or remotely).

Required privilege code

The required privilege codes are described in the respective steps.

Required equipment

The following equipment is required to perform the tasks below:

- *WaveStar* CIT

Instructions

- 1 Log into the *WaveStar* CIT and the respective NE (cf. “*WaveStar* CIT login/logout procedure” (22-11) and “Logging into an NE” (22-34))

- 2 All mandatory circuit packs and all other circuit packs which are already plugged-in are autoprovisioned.

- 3 System provisioning (cf. “Configuring the system” (4-4))

- 4 Port provisioning (cf. Chapter 6, “Timing provisioning”, “Configuring an optical SDH/SONET port” (4-16))

- 5 Tributary provisioning (cf. “Configuring a tributary” (4-26))

END OF STEPS



Configuring the system

When to use Use this procedure to set or modify various parameters associated with the entire system.

Related information For related information, see:

- “Provisioning of new components” (15-5)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of M1+S4+ P3+PM3, to configure system parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the shelf parameters:

- 1 In the **System View** of the *WaveStar* CIT select **Provision System** after right-clicking outside of the shelf.

Result:

The **Provision Sytem** window appears.

- 2 Set the the parameters according to your needs. Please refer to “Setting the System provisionable parameters” (4-5) for hints on the selection of the parameters values.

END OF STEPS

Alternative instructions Another possibility to configure the shelf parameters is:

- 1 In the **Shelf View** of the CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window.

Result:

The **Equipment** selection tab appears on the left side of the window.

- 2 Select the system in the **Equipment** selection tab and click on the pushbutton **Provision**.

Result:

The system provisioning window appears on the right side of the window.

- 3 Set the the parameters according to your needs. Please refer to “Setting the System provisionable parameters” (4-5) for hints on the selection of the parameters values.

END OF STEPS

Setting the System provisionable parameters

IF	THEN
you want to change the Interface Standard Default to SONET,	set the Optical Interface Standard to SONET .
you want to change the Interface Standard Default to SDH,	set the Optical Interface Standard to SDH . This is the default value.
you want a fixed tributary rate list,	set the Tributary Mode Default to Fixed-Rate .
you want the tributary signal rate list to adapt,	set the Tributary Mode Default to Adaptive-Rate .
you want that the System Synchronization is in SDH Characteristics,	set the System Synch Characteristics to SDH . This is the default value.

IF	THEN
you want that the System Synchronization is in SONET Characteristics,	set the System Synch Characteristics to SONET .



Configuring the shelf

When to use Use this procedure to set or modify shelf parameters. This can be done during the setup of a new network element or during operation.

Related information For related information, see:

- “Shelf provisioning” (15-13)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P3+ M1, Provisioning, to configure shelf parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the shelf parameters:

- 1 In the **System View** of the *WaveStar* CIT select **Provision Shelf** after right-clicking on the shelf.

Result:

The Provision shelf window appears.

- 2 Select the **Alarm Severity Assignment Profile (ASAP)**. In this case you select the Equipment ASAP (cf. “Alarm severity assignment profiles” (16-25)).

END OF STEPS

Alternative instructions Another possibility to configure the shelf parameters is:

- 1 In the **System View** of the CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window .

Result:

The **Equipment** selection tab appears on the left side of the window.

- 2 Select the shelf in the **Equipment** selection tab and click on the pushbutton **Provision**.

Result:

The shelf provisioning window appears on the right side of the window.

- 3 Select the **Alarm Severity Assignment Profile (ASAP)**. In this case you select the Equipment ASAP (cf. “Alarm severity assignment profiles” (16-25)).

END OF STEPS



Configuring a slot

When to use Use this procedure to set or modify slot parameters before the slot is equipped. This can be done during the setup of a new network element or during operation.

Related information For related information, see:

- “Slot/circuit pack provisioning” (15-14)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P3+M1, to configure slot parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the slot parameters:

- 1 In the **System View** of the *WaveStar* CIT select **Provision Slot** after right-clicking on the requested slot.

Result:

The slot provisioning window appears. This is possible only for empty slots. The slot AID is displayed.

- 2 Select the **Alarm Severity Assignment Profile (ASAP)**. In this case you select the Equipment ASAP (cf. “Alarm severity assignment profiles” (16-25)).
-

- 3 Define in the drop-down list box **Apply To:**, whether the setting shall be applied to the selected slot only, or to all slots in the shelf.

END OF STEPS

Alternative instructions Another possibility to configure the slot parameters is:

- 1 In the **System View** of the CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window .

Result:

The **Equipment** selection tab appears on the left side of the window.

- 2 Select the shelf in the **Equipment** selection tab and click on **+**.

Result:

The equipped and the empty slots of the shelf are displayed.

- 3 Select the desired slot (equipped or unequipped) and click on the pushbutton **Provision**.

Result:

If you have selected an equipped slot two tabs become visible on the right side of the window. Select the tab **Slot**.

- 4 Select the **Alarm Severity Assignment Profile** (ASAP). In this case you select the Equipment ASAP (cf. “Alarm severity assignment profiles” (16-25)).

- 5 Define in the drop-down list box **Apply To:**, whether the setting shall be applied to the selected slot only, or to all slots in the shelf.

END OF STEPS



Creating a new circuit pack

When to use Use this procedure to define a new circuit pack for a certain slot in a network element (pre-provisioning).

Related information For related information, see:

- “Provisioning of new components” (15-5)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P3+M1, Provisioning, to create a new circuit pack.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to create a new circuit pack:

- 1 In the **System View** of the *WaveStar* CIT select **Create New Circuit Pack** after right-clicking on the requested slot.

Result:

The window **Establish Circuit Pack** opens.

- 2 Select the circuit pack type in the drop-down list box **Select CP Type**.
-

- 3 Select the **Alarm Severity Assignment Profile** in the respective drop-down list boxes.

By clicking on the pushbutton **View Details** you can call up a table with details on the ASAPs. Please refer to “Alarm severity assignment profiles” (16-25).

-
- Click on **OK** to apply your settings. The window closes. If you wish to discard your changes, click on **Close**.

Result:

The window closes. and the selected circuit pack type is displayed in the **System View**.

END OF STEPS

Alternative instructions Another possibility to create a new circuit pack is:

- In the **System View** of the *WaveStar* CIT, select **Configuration** → **Create New** → **Circuit Pack....**

Result:

The **Create New Circuit Pack** window opens.

- Select the shelf in the **Equipment** selection tab on the left side of the window and click on **+**.
-

- Select the slot for which you wish to create the circuit pack.
-

- Click on the pushbutton **Select Slot**.

Result:

The selection fields for the new circuit pack become visible on the right side of the window.

- Select the circuit pack type in the drop-down list box **Select CP Type**.
-

- Select the **Alarm Severity Assignment Profile** in the respective drop-down list boxes.

By clicking on the pushbutton **View Details** you can call up a table with details on the ASAPs. Please refer to “Alarm severity assignment profiles” (16-25).

-
- 7** Click on **Apply**. The window closes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Reassigning a circuit pack

When to use Use this procedure to change the assignment of a slot, i.e. another type of circuit pack than currently provisioned. This can only be done for slots where different types of circuit packs are allowed (e.g. all universal slots).

Related information For related information, see:

- “Slot/circuit pack provisioning” (15-14)
- “Deleting a cross-connection” (7-29)
- “Deleting a protection group” (7-56)

Before you begin A typical application of this procedure is the exchange of OC192/STM-64 circuit pack types with different wavelengths. These circuit packs can be reassigned while configured cross-connections and protection groups can be preserved.

Please note that reassignment of required (core) circuit packs is not possible.

Please observe the following rules for the exchange of circuit packs:

1. The old circuit pack has to be an optical circuit pack.
2. The new circuit pack must also be an optical circuit pack.
3. The old circuit pack has already be removed and the slot is empty or the new circuit pack has already been inserted.
4. The new circuit pack has to support the same number of ports as the old one.
5. The new circuit pack has to support the same transmission capacity as the old one.
6. The new circuit pack has to support the current port configuration concerning Forward Error Correction (FEC).

Required privilege code

You must have at least a privilege code of P3+M1, to reassign a circuit pack.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions



CAUTION

Deletion of provisioned equipment will remove all parameter settings. Removing or modifying a working circuit pack will interrupt service! In order to prevent service interruptions, you should verify that the respective circuit pack is out of service.

Complete the following steps to configure circuit pack parameters:

- 1 Physically remove the current circuit pack and insert the new circuit pack or leave the slot empty.

- 2 Call up the **System View** of the WaveStar CIT.

Result:

The circuit pack is displayed with several diagonal grey lines to show that the slot is still assigned to this circuit pack.

- 3 Select the desired circuit pack in the **System View**, click the right mouse button and select the option **Exchange Circuit Pack...** in the pop-up menu. You can also select **Exchange Circuit Pack...** via the menu **Configuration**.

Result:

The window **Exchange Circuit Pack** opens. A list with all exchangeable circuit packs is displayed.

- 4 Select the desired circuit pack type.

- 5 If not yet done, physically insert the new circuit pack.

Result:

The slot will be autoprovisioned for the new circuit pack.

END OF STEPS



Configuring an optical SDH/SONET port

When to use Use this procedure to configure one or more optical port(s) of the same type for the operation of a *LambdaUnite*TM MSS system.

Related information For related information, see:

- “Port and tributary provisioning” (15-15)
- “Reassigning a circuit pack” (4-14)

Before you begin Prior to performing this task, you must insert the optical port unit you want to configure into the correct slot of the shelf. Furthermore, the circuit pack provisioning must be completed before a certain port can be configured (cf. “Slot/circuit pack provisioning” (15-14) and “Reassigning a circuit pack” (4-14)).

You must be logged into the *WaveStar*[®] CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P3+M1 to configure an optical port.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps in order to configure the parameters of one or more optical port(s):

- 1 In the **System View** of the *WaveStar* CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups of Equipment** window.

Result:

On the left side of the window, the equipment selection tab becomes visible. The shelf is listed.

- 2 Double click on the shelf or click on the + in front of the shelf name.

Result:

The list of circuit packs and slots which are available becomes visible.

-
- 3 Select the desired optical port unit. Double click on the port unit or click on the **+** in front of the unit name.

-
- 4 Select the desired port (type). Click on the **Provision** pushbutton.

Result:

On the right side of the window the provisionable parameters are displayed.

-
- 5 Set the parameters according to your needs. Please refer to “Setting the parameters of optical ports” (4-19) for hints on the selection of the parameter values.

-
- 6 For substructuring the input signal click on the button **Use Form** next to the text box **Input Signal Rate List**.

Result:

The window **Signal Rate Entry Form for Input Signal Rate List** opens.

The substructuring is a prerequisite for the cross-connection switching. Configure the substructure according to the cross-connection plan for the respective network element.

First select a signal rate, then select all tributaries which are necessary to fill the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**.

Substructuring should be made by clustering

- VC-3, VC-4, VC4-4C, VC4-16C, VC4-64C for STM-16 and STM-64 (in SDH Standard)
- STS-1C, STS-3C, STS-12C, STS-48C, STS-192C for OC-48 and OC-192 (in SONET Standard)

tributaries, i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Input Signal Rate List**.

Please refer to “Setting the parameters of optical ports” (4-19) for the meaning of the display.

- 7 For substructuring the output signal click on the button **Use Form** next to the text box **Unequipped Output Signal**.

Result:

The window **Signal Rate Entry Form for Unequipped Output Signal** opens.

First select a signal rate, then select all tributaries which are necessary for the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**. Substructuring should be made by clustering VC-3, VC-4, VC4-4C, VC4-16C, VC4-64C channels in SDH Standard or by clustering STS-1C, STS-3C, STS-12C, STS-48C, STS-192C channels in SONET Standard , i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Unequipped Output Signal**. Please refer to “Setting the parameters of optical ports” (4-19) for the meaning of the display.

- 8 Select the Alarm Severity Profile in the respective drop-down list box. You can choose between the default and a specific ASAP.
-

- 9 Select the destination port(s) in the **Apply To:** drop-down listbox. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack or to all ports on this type in the shelf. By using the latter options, you can decrease your provisioning time significantly.
-

- 10 Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Setting the parameters of optical ports

Purpose Use this procedure to configure the optical ports according to the needs of the network environment. Especially the correct transmission rate, the alarm behavior, the transmission of timing information and the laser state are concerned. The following settings can all be carried out in the **Provision Parameters for Protection Groups or Equipment** window.

Setting the *Standard* parameters

IF	THEN
you want, that the Provisioning values for Service shall be accepted,	set the Service Condition to In Service .
you want, that the Provisioning values for Service shall not be accepted,	set the Service Condition to Out of Service .
you want to change the Interface Standard to SONET,	set the Interface Standard to SONET .
you want to change the Interface Standard to SDH,	set the Interface Standard to SDH .

Setting the *Transmission* parameters

IF	THEN
you want a fixed tributary rate list,	set the Tributary Mode to Fixed-Rate .
you want the tributary signal rate list to adapt,	set the Tributary Mode to Adaptive-Rate (only for SONET).
you want the port to cause alarms during normal operation, but not if there is no valid signal present at the port, e.g. during preprovisioning,	set in the drop-down list box Port Mode the value to Auto . This is the default value.

IF	THEN
there is a valid signal present at the port and you want the port to cause alarms,	set in the drop-down list box Port Mode the value to Monitored .
you do not want the port to cause alarms,	set in the drop-down list box Port Mode the value to Not Monitored .

Substructuring

IF

it is necessary to create a substructure for the input or output signal,

THEN

click on the button Use Form and define the substructure according to the required cross-connections.

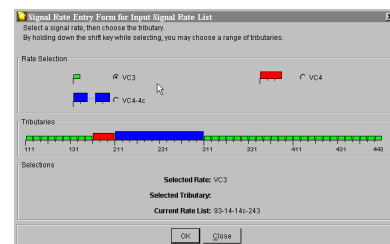
First select a signal rate, then select all tributaries which are necessary to fill the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**. Substructuring should be made by clustering (VC3, VC4, VC4-4C, VC4-16C, VC4-64C in SDH Standard and STS1, STS3c, STS12C, STS48C, STS192C in SONET Standard) tributaries, i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Input Signal Rate List** or **Unequipped Output Signal** respectively in the following form **<NX-NX-NX-...>**. X= **3, 4, 4C, 16C, 64C** in SDH Standard. In SONET Standard X= **1, 3, 12, 48, 192**. X is the transmission rate. N is the number of subsequent X.

Example:

64–303 for an STM-16 port designates a substructure of 6 VC-4 (timeslots 111 to 221) and 30 VC-3 (timeslots 231 to 443).

Nonexample:

The following figure shows the **Signal Rate Entry Form for Input Signal Rate List** window. It shows the substructure of an STM-16 signal with 33 VC-3, 1 VC-4 and 1 VC-4-4C.



Setting the *Fault Management* parameters

IF	THEN
you wish the measurement of bit error rate by POISSON (temporay equal allocation of bit errors with a measured bit error rate of 10E-3 ... 10E-9),	set Signal Degrade/ Fail Mode to POISSON .
you wish the Signal Degrade/Signal Fail Mode BURST (bit errors exceed threshold during some seconds),	set Signal Degrade/ Fail Mode to BURST .
you wish to activate the Forward Error Correction in an intrusive service affecting way,	set the parameter FEC Encoding / Decoding to Enabled or Disabled , respectively. Only applies to OC192 and some STM-64 and higher rate ports and shall otherwise be dimmed or removed. For further information on the FEC types, please refer to “Forward error correction” (16-35).
the Forward Error Correction is enabled via FEC Correction Enable and you wish to start or stop the FEC bit error correction at any time,	set the parameter FEC Correction to Enabled or Disabled , respectively. Only applies to OC192/STM-64 and higher rate ports and shall otherwise be dimmed or removed.
you wish that the redundant information is stored and transported in previously unused overhead bytes, so that the framing structure as well as the bit rate remain unchanged,	set the parameter FEC Type to In-Band . Only applies to OC192/STM-64 and higher rate ports and shall otherwise be dimmed or removed.

IF	THEN
you wish that the redundant information is appended to the original signal resulting in an optical signal with a modified framing structure and extended bit rate.	set the parameter FEC Type to Out-Band .
you wish to change the measurement periode for determining bursty errors,	select the required values in the drop-down list box HP Degraded Interval . The values 2 to 10 (seconds) are possible. If the value of Signal Degrade/ Signal Fail Mode is POISSON then HP Degraded Interval shall be dimmed or removed.
you wish to change the threshold value for bursty errors,	select the required values in the drop-down list box HP Degraded Threshold . The values 0 to 50 (as a percentage) at increments of 5 are possible. If the value of Signal Degrade/ Signal Fail Mode is POISSON then HP Degraded Threshold shall be dimmed or removed.
you wish to change the threshold for the Bit Error Rate (signal degrade),	select the required value in the drop-down list box Optical Line BER Tresh . The values 10E-5, 10E-6 (default value), 10E-7, 10E-8, 10E-9 are possible.
you wish to change the treshold for the Excessive Bit Error Rate (signal failure),	select the required value in the drop-down list box Optical Line EBER Tresh . The values 10E-5, 10E-4 and 10E-3 (default value) are possible.
you wish to change between the default and a specific ASAP,	select the required ASAP name in the drop-down list box Alarm Severity Profile .

Timing settings

IF	THEN
you wish to prevent the optical line from being used for synchronization, e.g. because a timing loop might occur,	set the parameter Force DUS (SONET) Force DNU (SDH) to Enabled .
you wish the optical line to be used for synchronization,	set the parameter Force DUS (SONET) Force DNU (SDH) to Disabled (default), in this case the current timing marker information for that line is transmitted.

Optical Channel settings

IF	THEN
you wish to enable the optical channel for an OC-192 or STM-64 port,	set the parameter Optical Channel to Enabled .
you wish to disable the optical channel for an OC-192 or STM-64 port,	set the parameter Optical Channel to Disabled .

Interworking settings

IF	THEN
you wish to insert the hex value CC into the Z0 byte for an OC48 port,	set the parameter Z0 Insertion value to CChex . In SDH Standard these bytes are defined as spare bytes and the parameter is not shown.
you wish to insert the STS-Id into the Z0 byte for an OC48 port,	set the parameter Z0 Insertion value to STS-Id .
you wish to select the Single MS Remote Error Indication Mode for an STM-64/OC192 port,	set the parameter MS REI Mode to Single (M1 byte) .

IF

you wish to select the Extended MS Remote Error Indication Mode for an STM-64/OC192 port,

THEN

set the parameter **MS REI Mode** to **Extended (M0/M1 byte)**. At the source direction the Remote Error Information as received from the associated termination sink function is written into M0/M1.



Configuring a tributary

When to use Use this procedure to configure tributaries belonging to optical signals.

Related information For related information, see:

- “Reassigning a circuit pack” (4-14)
- “Configuring an optical SDH/SONET port” (4-16)

Before you begin Prior to performing this task, you must insert the port unit you want to configure into the correct slot of a shelf. Furthermore, the circuit pack provisioning and the port provisioning must be completed before a certain tributary can be configured (cf. “Reassigning a circuit pack” (4-14) and “Configuring an optical SDH/SONET port” (4-16)).

Required privilege code

You must have at least a privilege code of P3+M1, to configure tributaries.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps in order to configure the parameters of a tributary:

- 1 In the **System View** of the WaveStar CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window.

Result:

On the left side of the window, the **Equipment** selection tab is displayed. The shelf belonging to the system is listed.

- 2 Double-click on the shelf or click on the + in front of the shelf name.

Result:

The list of circuit packs and slots which are available becomes visible below the shelf name.

- 3 Select the desired port unit. Double click on the port unit or click on the + in front of the unit name.

Result:

The list of ports which are available becomes visible below the port unit name.

- 4 Select the desired port. Double click on the port or click on the + in front of the port.

Result:

The list of tributaries which are available becomes visible below the port.

- 5 Select the desired tributary (type).

Result:

On the right side of the window, the provisionable parameters are displayed.

- 6 Set the parameters according to your needs. Please refer to “Provisionable parameters of tributaries” (4-28) for the description of the parameters.
-

- 7 Select the destination tributary(s) in the **Apply To:** drop-down list-box. Here, you can specify whether the settings should apply only to the above selected tributary or to all tributaries of the respective port or to all tributaries on the respective circuit pack. By using the latter options, you can decrease your provisioning time significantly.
-

- 8 Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Provisionable parameters of tributaries

Important settings Configure the tributary according to the needs of the network environment. Especially the alarm behaviour is concerned.

The following table shows for VCor STS tributaries which parameters are provisionable, and explains them:

Parameter	Values	Meaning
Fault Management		
Tributary Monitoring Mode	Monitored (MON)	An alarm is caused, if necessary.
	Not Monitored (NMON)(default)	No alarms are caused.
Tributary Alarm Severity Assignment Profile	<ASAP name> (24 characters max.), Default	Selection between the default and a specific ASAP
HP DEG Interval	2 to 10 (seconds), initial value: 7	This parameter defines the measurement periode for determining bursty errors. If the value of Signal Degrade/Fail Mode is Poisson then HP Degraded Intervall dimmed or removed.
HP Degraded Threshold	0 ... 50 in steps of 5	This parameter defines the treshold value for bursty errors. If the value of Signal Degrade/Fail Mode is Poisson then HP Degraded Threshold dimmed or removed.
HP DEXC Threshold	10E-3 (initial value), 10E-4 , 10E-5 ,	This parameter defines the threshold for the Excessive Bit Error Ratio (EBER or EXC). If the threshold is exceeded HP-EXC is signalled. If the value of Signal Degrade/Fail Mode is Burst then HP DEXC Threshold dimmed or removed.
HP DEG Threshold	10E-5 , 10E-6 (initial value), 10E-7 , 10E-8 , 10E-9	This parameter defines the threshold for the tolerable signal degradation (BER). If the threshold is exceeded HP-DEG is signalled. If the value of Signal Degrade/Fail Mode is Burst then HP DEG Threshold dimmed or removed.
Signal Degrade/Fail Mode	POISSON	Temporary equal allocation of bit errors with a measured bit error rate of 10E-3 ... 10E-9
	BURST	Bit errors exceed threshold during some seconds

□

Removing equipment from the system

When to use Use this procedure to de-provision (delete) equipment which has been provisioned for the system. This can be necessary, for example, in the event of a reconfiguration.

Before you begin Prior to performing this task, you must:

- Delete cross-connections in which the equipment you want to remove is involved (cf. “Deleting a cross-connection” (7-29))
- Delete protection groups in which the equipment you want to delete is involved (cf. “Deleting a protection group” (7-56))
- Physically remove the equipment.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to remove equipment from the system.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions



CAUTION

Deletion of provisioned equipment will remove all parameter settings. Removing or modifying a working circuit pack will interrupt the service! In order to prevent service interruptions, you should verify that the respective circuit pack is out of service.

Complete the following steps to remove equipment from the system:

- 1 In the **System View** of the WaveStar CIT, via **Configuration** → **Delete...** call up the **Delete** window.

Result:

The **Delete** window appears.

-
- 2** Select the component you want to delete in the tab **Equipment**. You can delete the following types of component:

- Circuit Packs

Bay 1 and shelf 1-1 cannot be removed.

- 3** Click on **Select** to apply your changes. A confirmation window opens containing the warning that all provisioned parameters will be lost. Click on **Yes** to confirm your changes. Click on **No** to discard your changes.

END OF STEPS



Retrieving equipment info for the system

When to use Use the procedure to retrieve information on the entire system.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+S1+P1+PM1 to retrieve parameters of the system.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
-

- 2 Select *WaveStar* UNITE from the equipment selection tab or enter system in the AID-field.

For the meaning of values in Equipment Detail window please refer to “Setting the System provisionable parameters” (4-5)

END OF STEPS

Alternative instructions Another possibility to retrieve data of the entire system is:

- 1 In the **System View** of the *WaveStar* CIT select **View System Details** after right-clicking outside of the shelf.

END OF STEPS



Retrieving equipment info for the shelf

When to use Use the procedure to retrieve shelf parameters.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+P1 to retrieve data of the shelf.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
-

- 2 Select the shelf from the equipment selection tab or enter the corresponding AID.

For the meaning of values in Equipment Detail window please refer to “Configuring the shelf” (4-7)

END OF STEPS

Alternative instructions Another possibility to retrieve shelf data is:

- 1 In the **System View** of the *WaveStar* CIT select **View Shelf Details** after right-clicking on the shelf.

END OF STEPS



Retrieving equipment info for slots

When to use Use the procedure to retrieve slot parameters.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+P1 to retrieve parameters of the slot.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
- 2 Select desired slot from the equipment selection tab or enter the corresponding AID.

END OF STEPS

Alternative instructions Another possibility to retrieve slot data is:

- 1 In the **System View** of the *WaveStar* CIT select **View Slot Details** after right-clicking on the desired slot.

END OF STEPS



Viewing data of a slot

Status Data The following table shows the status data, which are shown in the View Equipment Details window for a desired slot.

Information field	Possible Values	Meaning
Slot AID	cf. “Over-view of access identifiers” (15-8)	The AID defined for the selected slot.
Acceptable Pack Types	OP2G5, OP10, GbE	List of circuit pack types which may validly be inserted into the slot.
Equipment ASAP Profile	24 charac- ters max.	Display the name of the provisioned ASAP.
Holder Status	Empty, Valid, Unexpected, Unknown	Holder status of the slot.

The Pack Data will display a “-” if the slot holder status is not VALID or UNEXPECTED, or if the parameter cannot be retrieved due to another reason.

For values in the Pack Data section please refer to “Viewing data of a circuit pack” (4-38).



Retrieving equipment info for circuit packs

When to use Use the procedure to retrieve information of the circuit packs.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+P1 to retrieve data of the circuit pack.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
- 2 Select the desired circuit pack from the equipment selection tab or enter the corresponding AID.

END OF STEPS

Alternative instructions Another possibility to retrieve circuit pack data is:

- 1 In the **System View** of the *WaveStar* CIT select **View Circuit Pack Details** after right-clicking on the desired circuit pack.

END OF STEPS



Viewing data of a circuit pack

Status Data The following table shows the status data, which are shown in the View Equipment Details window for a desired circuit pack.

Information field	Possible Values	Meaning
Pack Data		
Circuit Pack AID	cf. “Over-view of access identifiers” (15-8)	The AID defined for the selected circuit pack.
Apparatus Code	up to 9 characters	ASCII name assigned by the manufacturer to identify a particular circuit pack.
Series Number	for example 1.1.	Series number of the circuit pack.
CLEI Code	10 character alphanumeric code	CLEI code of the circuit pack.
Equipment Carrier Code	a 6 digit code	This is the Equipment Carrier Code.
Serial Number	this is an alphanumeric number	This is the circuit pack serial number.
Alarm Level	-	The level of the highest alarm, either equipment, communications, or quality of service, associated with the circuit pack shall be displayed.

Information field	Possible Values	Meaning
Equipment Alarm Profile	-	Display the name of the provisioned Alarm Profile.
Status		
Slot Alarm Level	-	The level of the highest alarm associated with the slot shall be displayed.
Holder Status	Empty, Valid, Unexpected, Illegal, Unknown	Holder status
Operational Status	Enabled, Disabled	This is the ability of the Circuit Pack to offer service.



Retrieving equipment info for optical SDH/SONET ports

When to use Use the procedure to retrieve information of the optical SDH/SONET ports.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+P1 to retrieve data of optical ports.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
-

- 2 Select an optical port from the equipment selection tab or enter the corresponding AID.

END OF STEPS

Alternative instructions Another possibility to retrieve optical port data is:

- 1 In the **System View** of the *WaveStar* CIT select **View Port Details** after right-clicking on the desired port.

END OF STEPS



Viewing data of a optical SDH/SONET port

Port Data For the meaning of the Port Data, Interworking, Optical Channel and Port Rate information refer to “Setting the parameters of optical ports” (4-19)

The following table shows the Timing and Setting status data, which are shown in the View Equipment Details window for a desired optical port.

Information field	Possible Values	Meaning
Force DNU (SDH) or Force DUS (SONET)	Enabled, Disabled	Shows the status of the funktion Force DNU or DUS.
Optical Wave-length	values in nanom-eter	Shows the optical Wavelength.
Optical Distance	INTRA-OFFICE, SHORT-HAUL, LONG-HAUL, VERY-LONG-HAUL, OLS-PASSIVE, OLS-400G, OLS-800G, XTREME	Indicate the type of application to which the optical transmitter on this port is suited.
Tributary Mode	Adaptive, Fixed	Shows the status of the Tributary Mode. In SDH “Fixed” is the only allowed tributary mode.

Information field	Possible Values	Meaning
FEC Encoding/Decoding	Enable, Disable	Shows the status of the FEC Encoding/Decoding switch. Only applies to STM-64/OC192 and higher rate ports.
FEC Correction	Enable, Disable	Shows the Status of the FEC Correction. Only applies to STM-64/OC192 and higher rate ports.
FEC Type	IN-BAND, OUT-BAND	Shows the Status of the FEC Type. Only applies to STM-64/OC192 and higher rate ports.
Laser Bias Current	Value given in mA Range : 0-65535 (Integer Value)	value of Laser Bias Current Applicable to rates STM-64/OC192
Optical Power Transmit	Value given in 0.1 dBm Range : -50.0 - +20.0	value of Optical Power Transmit Applicable to rates STM-64/OC192
Optical Power Receive	Value given in 0.1 dBm Range : -50.0 - +20.0	value of Optical Power Receive Applicable to rates STM-64/OC192



Retrieving equipment info for tributary

When to use Use the procedure to retrieve parameters of the tributary.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code M1+P1 to retrieve parameters of tributary.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
- 2 Select a tributary from the equipment selection tab or enter the corresponding AID.

END OF STEPS

Alternative instructions Another possibility to retrieve tributary data is:

- 1 In the **System View** of the *WaveStar* CIT select **Tributary Details** after right-clicking on a single port.
- 2 Select a tributary from the equipment selection tab or enter the corresponding AID.

END OF STEPS



Viewing data of a tributary

Trib Data The following table shows Trib data, which are shown in the View Equipment Details window for a desired tributary.

Information field	Possible Values	Meaning
<i>Trib Data</i>		
Tributary AID	cf. “Over-view of access identifiers” (15-8)	The AID defined for the selected tributary.
Port Type	OC48, OC192, STM16, STM64	This shall reflect the rate of the corresponding port.
Tributary Mode	Monitored, Not Monitored	Status of Tributary Monitoring Mode
Signal Degrade/Fail Mode	POISSON, BURST	Status of Signal Degrade/Signal Fail Mode
Loop-back Status	YES, NO	Crossconnect Loopback Status

Information field	Possible Values	Meaning
Loop-back Rate	STS-1, STS-3c, STS-12c, STS-48c, STS-192c, VC3, VC4, VC44c, VC416c, VC464c, Empty	Shows the crossconnect loopback rate. In case the loopback state is “No”, this field is greyed out and empty.

For the meaning of provisionable parameters in this window please refer to “Provisionable parameters of tributaries” (4-28)



Retrieving equipment info for the backplane

When to use Use the procedure to retrieve information of the backplane.

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code S1 or P1 for viewing backplane data.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

- 1 In the **System View** of the *WaveStar* CIT via **View** → **View Equipment Details**.
-
- 2 Select backplane from the equipment selection tab or enter the corresponding AID.

END OF STEPS



Viewing data of the backplane

Status Data The following table shows the data, which are shown in the View Equipment Details window for the backplane.

Information field	Possible Values	Meaning
Back-plane AID	cf. “Over-view of access identifiers” (15-8)	This shall be the backplane AID.
Apparatus Code	-	ASCII name assigned by the manufacturer.
Series Number	-	Series number of the backplane.
CLEI Code	-	This is the CLEI code
ECI Code	-	This shall be the Equipment Catalog Item.
Serial Number	-	This is the backplane serial number.
Alarm Level	-	The level of the highest alarm associated with the backplane shall be displayed.



Viewing an equipment protection group

When to use Use this procedure to query the status of an equipment protection group.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Protection configurations” (18-24)
- “Equipment protection” (15-18)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of M1+P1, to query an equipment protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the status of a protection group

- 1 In the **System View** of the *WaveStar* CIT, via the menu **View** → **Protection...** call up the **View Protection** window.

Result:

The **View Protection** window opens.

- 2 Select the components of the required protection group in the tab **Ptn Grp** on the left side of the window.

Reference:

The displayed parameters are described in “Parameters for a 1+1 equipment protection” (4-49).

END OF STEPS



Parameters for a 1+1 equipment protection

Status data The following table shows the status data which are shown in the **View Protection** window for a 1+1 equipment protection.

Information field	Possible value	Meaning
Protection Group AID	cf. "Overview of access identifiers" (15-8)	The AID defined for the selected protection group.
Protection Type	1+1 Equipment	
Circuit Pack Type(s)	XC320	The circuit pack type for which the equipment protection has been established.
Worker AID(s)	cf. "Overview of access identifiers" (15-8)	The circuit pack AID(s) of the worker.
Protection AID(s)	cf. "Overview of access identifiers" (15-8)	The circuit pack AID(s) of the protection.
Worker Alarm Status/Protection Alarm Status	Critical, Major, Minor, Cleared, Not Alarmed	The highest alarm status associated with worker/protection side. The alarm format is configurable via the Preference window (cf. Chapter 22, "WaveStar® CIT Tutorial").
Worker Fault Status/Protection Fault Status	Equipment Failed or None	The fault reason associated with worker/protection side.
Active Side	wkg, protn	The side (circuit pack) which is currently working
Switch Request State	No Request, Forced Switch, Manual Switch, Equipment Failed	Last switch request which caused a switch between the two circuit packs.



Switching a 1+1 equipment protection

When to use Use this procedure to switch from one circuit pack to the other in a 1+1 equipment protection.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Protection configurations” (18-24)
- “Viewing an equipment protection group” (4-48)

Before you begin Please note that a forced switch to a faulty circuit pack may cause a traffic interruption. Make sure that a forced switch is only carried out to a circuit pack that is working correctly.

Required privilege code

You must have at least a privilege code of M4+P1, Maintenance, to switch a 1+1 equipment protection.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to switch a 1+1 equipment protection:

- 1 Call up the **Protection Switch** window either in the System View via **Fault** → **Protection Switch**, or in the **System View** by right-clicking on the requested circuit pack, then selecting Protection Switch.

Result:

The **Protection Switch** window opens.

- 2 Select the respective equipment protection in the tab **Ptn Group** on the left side of the window.

Result:

Some data of the protection group are displayed.

3 Select the desired switch request in the field **Switch Type**. The following options are possible:

- **Forced To Worker**
- **Forced To Protection**
- **Manual To Worker**
- **Manual To Protection**
- **Clear**

4 Click on **Apply**.

END OF STEPS





5 Alarm management

Overview

Purpose The present chapter describes the procedures which have to be performed for the alarm management of the *LambdaUnite*[™] MSS network elements.

Contents

Retrieving the <i>WaveStar</i> [®] CIT NE Alarm List	5-3
The <i>WaveStar</i> CIT NE Alarm List	5-5
Retrieving the <i>WaveStar</i> CIT NE Alarm Log	5-9
Identifying SDH tributaries in alarm messages	5-10
Performing an LED test	5-14
Retrieving ASAP information	5-15
Creating a new ASAP	5-18
Creating non-reporting ASAPs	5-21
Modifying an existing ASAP	5-23
Setting ASAPs for a shelf	5-26
Setting the port monitoring mode	5-29
Configuring fault management parameters for an SDH port	5-31

Configuring fault management parameters for a SONET port	5-36
Enabling or disabling autonomous alarm forwarding	5-41



Retrieving the *WaveStar*[®] CIT NE Alarm List

Purpose Use this procedure to retrieve detailed information about the current alarm status of a *LambdaUnite*[™] MSS NE by using the *WaveStar* CIT .

Related information For related information concerning the *WaveStar* CIT **NE Alarm List**, please refer to

- “The *WaveStar* CIT NE Alarm List” (5-5)

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M1** to retrieve the *WaveStar* CIT **NE Alarm List**.

Required equipment

The following equipment is required to perform this procedure:

- *WaveStar* CIT

Instructions Proceed as follows to retrieve the *WaveStar* CIT **NE Alarm List**:

- 1 From the *WaveStar* CIT, invoke the **NE Alarm List** by either:
 - pressing the **Alarm List** button in the upper right area of the **System View** window, or
 - selecting **Fault** → **NE Alarm List** in the **System View** main menu, or
 - selecting **Reports** → **NE Alarm List** in the **System View** main menu.

Result:

The **NE Alarm List** window will be opened.

The **NE Alarm List** reflects the current alarm status at the time when it is invoked.

-
- 2 To make sure that the **NE Alarm List** reflects the current alarm status, click
 - the **Refresh** button in the **NE Alarm List** window or
 - again the **Alarm List** button

as soon as you observe changes in the alarm status display in the lower left corner of the **System View** window, or whenever you are unsure whether the alarm list is still synchronized to the current alarm status.

-
- 3 The following options are available:

If ...	then ...
you want to store the currently displayed alarm list as a standard text file (ASCII format)	click Save As and specify a filename and a destination.
you want to print out the currently displayed alarm list	click Print and specify a printer.
you want to dismiss the window	click Close button.
you want to update the alarm list	click Refresh or again the Alarm List button (cf. Step 2).
you want to get online help information	click Help button.
E N D O F S T E P S	



The WaveStar® CIT NE Alarm List

The “NE Alarm List” window

The WaveStar CIT provides a list of current alarms, the **NE Alarm List**, to retrieve detailed information about the current alarm status of a *LambdaUnite™* MSS network element (NE).

Alarm Level	AID	Date	Time	Affect on Service	Probable Cause	Signal Level Affected	Alarm Type	Description
MJ	extref0	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	extref1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MJ	line1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	line2	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
CR	line3	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	line4	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MJ	line5	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
CR	line6	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	1-1-##-tmng1-cp	01/01/00	12-03-50	NSA	REPLUNITMISS	EQPT	Equipment	TMG/STRAT3, Circuit Pac...
MN	1-1-##-switch1-cp	01/01/00	12-03-55	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit ...
MN	1-2-##-switch1-cp	01/01/00	12-11-11	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit ...
MN	1-1-t01-w-14-1	02/14/00	16-37-32	NSA	T-BERL	STM16	Communications	STM16 port, MSect Signal...

Structure of the “NE Alarm List”

The following table explains the structure of the WaveStar CIT **NE Alarm List**.

Column	Meaning
Alarm Level	This column indicates the alarm severity. Possible values are (depending on the Preferences setting, cf. “Alarm format preferences” (16-12)): - Critical/Major/Minor (CR/MJ/MN) or - Prompt/Deferred/Info (PR/DF/INF). PR/DF/INF is the default setting for <i>LambdaUnite</i> MSS systems.
AID	This column indicates the alarm issue point, i.e. the access identifier (AID) of the component for which an alarm is being reported (“exttmg1”, “1-1-##-ctlw-nvm” or “1-1-##-12-v4” for example). Please note that a special display format is being used for SDH tributary AIDs, please refer to “Identifying SDH tributaries in alarm messages” (5-10).

Column	Meaning
Date	These two columns indicate the date and time of occurrence, i.e. the date and time the alarm was reported by the NE.
Time	The date and time format depends on the country in which the WaveStar CIT is being used.
Affect on Service	This column indicates whether the corresponding alarm is service affecting or not. Possible values are: • service affecting (SA), • not service affecting (NSA), • not applicable (-).
Probable Cause	This column indicates the alarm short designation. A more detailed description of the alarm's probable cause can be found in the Description column.

Column	Meaning
Signal Level Affected	This column indicates the affected signal level for communication alarms or the type of alarm otherwise. Possible values are: • COM Common Alarms that apply to the system as a whole, processing errors for example. • ENV Environmental • EQPT Equipment • OC-48, OC-192, OC-768 Optical transport signals (SONET): OC-48 (2.5 Gbit/s), OC-192 (10 Gbit/s) or OC-768 (40 Gbit/s) • OUTT Output timing • STM-16, STM-64, STM-256 Optical transport signals (SDH): STM-16 (2.5 Gbit/s), STM-64 (10 Gbit/s) or STM-256 (40 Gbit/s) • STS-1, STS-3C, STS-12C, STS-48C, STS-192C Payload signals (SONET): STS-1, STS-3C, STS-12C, STS-48C or STS-192C • SYST System timing • VC-3, VC-4, VC-4-4C, VC-4-16C, VC-4-64C Payload signals (SDH): VC-3, VC-4, VC-4-4C, VC-4-16C or VC-4-64C • 1GE 1-Gbit/s Ethernet • VCG Virtual concatenation group tributary

Column	Meaning
Alarm Type	This column indicates the alarm category. Possible values are: • Communications, • Environmental, • Equipment, • Processing, • Quality of service.
Description	This column describes the alarm's probable cause in more detail.

- Pushbuttons** The **NE Alarm List** window provides the following pushbuttons:
1. **Save As**
Use this button to store the currently displayed alarm list as a standard text file which may then be used for editing and further processing.
 2. **Print**
Use this button to print out the currently displayed alarm list.
 3. **Close**
Use this button to dismiss the window.
 4. **Refresh**
Clicking the **Refresh** button causes the *WaveStar* CIT to retrieve the alarm information from the NE again to update the alarm list. Notice that there is a difference between the **Refresh** button and the **Update Alarms** button beside the **Alarm List** button. The **Update Alarms** button can only be used to manually refresh the alarm status display, not the alarm list.
 5. **Help**
Use this button to get online help information specific to the **NE Alarm List** window.



Retrieving the WaveStar[®] CIT NE Alarm Log

Purpose Use this procedure to retrieve alarm history information by using the WaveStar CIT.

The WaveStar CIT “NE Alarm Log” The WaveStar CIT **NE Alarm Log** window provides a detailed alarm history for each *LambdaUnite*[™] MSS NE. The most recent alarms, up to 1024 alarms ordered by their date and time of occurrence, are stored in the NE alarm log. The information contained is presented in an identical fashion as in the NE alarm list; please refer to “The WaveStar CIT NE Alarm List” (5-5).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M1** to retrieve the **NE Alarm Log**.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar CIT

Instructions Proceed as follows to retrieve the **NE Alarm Log**:

- 1 From the WaveStar CIT, invoke the **NE Alarm Log** by either:
 - selecting **Fault** → **NE Alarm Log...** in the **System View** main menu, or
 - selecting **Reports** → **NE Alarm Log...** in the **System View** main menu.

Result:

The **NE Alarm Log** window will be opened.

END OF STEPS



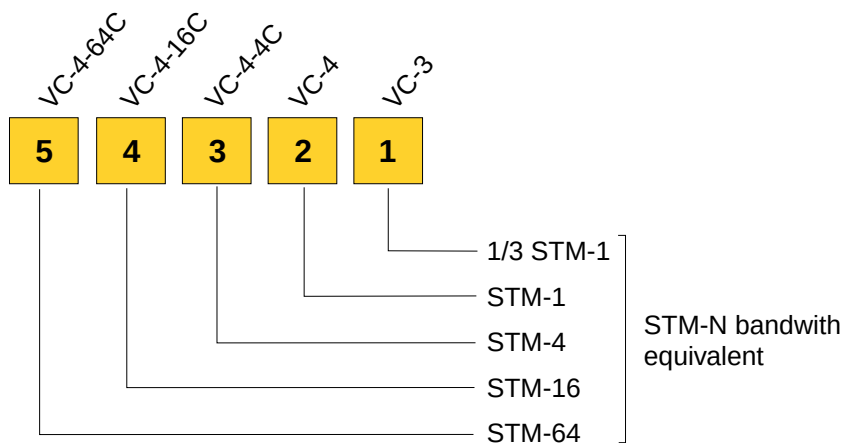
Identifying SDH tributaries in alarm messages

Purpose Use this procedure to uniquely identify SDH tributaries in case of tributary alarms reported in the *WaveStar*® CIT **NE Alarm List** or **NE Alarm Log**.

Representation of SDH tributaries in alarm messages

When tributary alarms are reported, the alarm messages in the *WaveStar* CIT **NE Alarm List** or **NE Alarm Log** contain the signal level affected, but not the port type. Therefore, a five-digit representation is used for SDH tributary AIDs to facilitate the correct identification of SDH tributaries. Please also refer to “SONET and SDH tributary numbering format” (16-14).

Each of the five digits represents a particular VC-N level:



The possible values of the individual digits are as follows:

Digit	Value	Meaning
1	0	no VC-3
	1, 2 or 3	the first, second or third VC-3 within an STM-1 frame.

Digit	Value	Meaning
2	0	no VC-4
	1, 2, 3 or 4	the first, second, third or fourth VC-4 within the corresponding STM-4 frame.
	*	An asterisk represents either a “1” or a fill character which can be ignored (if the second digit is not required, in the case of an STM-1 interface port for example).
3	0	no VC-4-4C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-4C within the corresponding STM-16 frame.
	*	An asterisk represents either a “1” or a fill character which can be ignored (if the third digit is not required, in the case of an STM-1 or STM-4 interface port for example).
4	0	no VC-4-16C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-16C within the corresponding STM-64 frame.
	*	An asterisk represents either a “1” or a fill character which can be ignored (if the fourth digit is not required, in the case of an STM-1, STM-4 or STM-16 interface port for example).
5	0	no VC-4-64C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-64C within the corresponding STM-256 frame.
	*	An asterisk represents either a “1” or a fill character which can be ignored (if the fifth digit is not required, in the case of an STM-1, STM-4, STM-16 or STM-64 interface port for example).

Required number of digits Depending on the STM level of an SDH port, a different number of digits is required to uniquely identify the tributaries contained.

STM-256 interface port	All five digits are required.

STM-64 interface port	Four digits are required.
STM-16 interface port or 1-Gbit/s Ethernet port	Three digits are required.
STM-4 interface port	Two digits are required.
STM-1 interface port	Only the last digit is required.

Examples These are examples of the *WaveStar* CIT numbering format of SDH tributaries in alarm messages:

- 1-1-#-#-4-3-***20 A 2.5-Gbit/s circuit pack is present in the respective slot (1-1-#-#-4). This is an STM-16 port, and thus three digits are required: The asterisk at position 3 represents a “1”, the asterisks at positions 4 and 5 can be ignored. Therefore, the AID indicates a VC-4 in the second STM-1 of the first STM-4 within the STM-16 frame.
- 1-1-#-#-9-1-***23 A 10-Gbit/s circuit pack is present in the respective slot (1-1-#-#-9). This is an STM-64 port, and thus four digits are required: The asterisk at position 3 represents a “1”, the asterisks at positions 4 and 5 can be ignored. Therefore, the AID indicates the third VC-3 in the second STM-1 of the first STM-4 in the first STM-16 within the STM-64 frame.

Instructions Proceed as follows to identify the correct tributary from the SDH tributary AID representation in the *WaveStar* CIT **NE Alarm List** or **NE Alarm Log**:

-
- 1 Determine the port type by means of the slot information in the AID and by using office records or the *WaveStar* CIT **System View** window for example.
-
- 2 Depending on the port unit type, determine the number of required digits in the tributary AID representation (cf. “Required number of digits” (5-11)).

All ***required*** digits with an asterisk represent “1”, all other digits with an asterisk can be ignored.

Please also refer to “SONET and SDH tributary numbering format” (16-14).

END OF STEPS



Performing an LED test

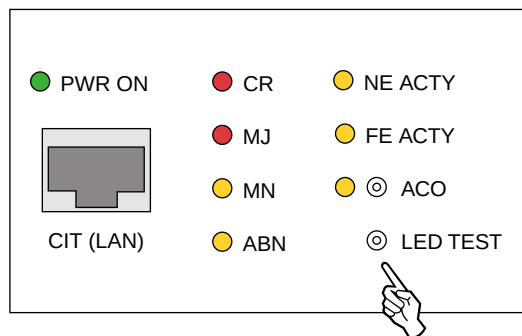
Purpose Use this procedure to test the correct functioning of the user panel and circuit pack LEDs.

Please note that the PWR ON LED on the user panel and the fan unit LEDs are not affected by the LED test.

Before you begin You or a service technician must be on-site at the NE to perform an LED test.

Instructions Proceed as follows to test the correct functioning of the user panel and circuit pack LEDs.

- 1 Press the “LED TEST” button on the user panel.



- 2 Verify the correct functioning of the user panel and circuit pack LEDs.

The sequence of LED indications should be as follows:

1. The LEDs on the user panel (except the PWR ON LED) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.
2. the LEDs on the circuit packs (except the fan unit LEDs) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

END OF STEPS



Retrieving ASAP information

Purpose Use this procedure to retrieve information about which alarm severity assignment profiles (ASAPs) are available, and about their current alarm severity assignments.

ASAP types These ASAP types are defined for *LambdaUnite*[™] MSS network elements:

- Automatic Protection Switch,
- BLSR/MS SPRing Protection Switch,
- DCN,
- Environmental,
- Equipment without SA/NSA,
- Equipment with SA/NSA,
- Ethernet,
- MSA/NIM,
- Path Protection SNCP_UPSR,
- Path terminating SDH,
- Port,
- System Timing.

Related information Please also refer to “Alarm severity assignment profiles” (16-25).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M1** to retrieve information about available ASAPs.

Required equipment

The following equipment is required to perform this procedure:

- *WaveStar*[®] CIT

Instructions Proceed as follows to retrieve information about available ASAPs and their current alarm severity assignments:

- 1 From the *WaveStar* CIT **System View**, invoke the **View Alarm Severity Profile** window by selecting either
- **View → View Alarms → View Alarm Severity Assignment Profile...** or

• **Fault → View Alarm Severity Assignment Profile**

from the **System View** main menu.

Result:

The **View Alarm Severity Profile** window will be opened.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available ASAP types. The available ASAPs for a specific ASAP type can be made visible by clicking on the “+” sign in front of the corresponding ASAP type.

- 2 You may now view the alarm severity assignments of a single, specific ASAP or of all ASAPs of a specific ASAP type:

If ...	then ...
you want to view the alarm severity assignments of a specific ASAP	expand the ASAP selection tree by clicking on the “+” sign in front of the ASAP type and select the desired ASAP.
you want to view the alarm severity assignments of all ASAPs of a specific ASAP type	select the ASAP type.

- 3 Click **View ASAP**.

Result:

The ASAP information will be displayed in the right-hand part of the **View Alarm Severity Profile** window.

A further possibility to retrieve information about a specific ASAP is clicking the **View Details...** button in the **Fault Management** part of

a provisioning window (for example, a circuit pack, slot or port provisioning window). In that case, only the ASAP information for the currently assigned ASAP will be displayed.

- 4 Click **Close** to close the **View Alarm Severity Profile** window.

END OF STEPS



Creating a new ASAP

Purpose Use this procedure to create a new alarm severity assignment profile (ASAP).

Related information

Please also refer to “Alarm severity assignment profiles” (16-25).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M3** to create a new ASAP.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions **Important!** Please be aware that an existing ASAP cannot be deleted. Therefore, and considering the fact that the maximum number of ASAPs is 64, you should make your decision which ASAPs to create very carefully, bearing in mind that individual alarm severity assignments can be modified for *all* existing ASAPs.

Proceed as follows to create a new ASAP:

- 1 From the WaveStar CIT **System View** main menu, select **Configuration → Alarms → Alarm Severity Assignment Profile...**

Result:

The **Provision Alarm Severity Profile** window will be opened.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available ASAP types. The available ASAPs for a specific ASAP type can be made visible by clicking on the “+” sign in front of the corresponding ASAP type.

-
- 2 Select **New ASAP** in the upper left-hand corner of the window, next to **Operations**.
-

- 3 Select the desired ASAP type from the selection tree.
-

- 4 Click **New ASAP** in the lower left-hand corner of the window.

Result:

The ASAP information will be displayed in the right-hand part of the **Provision Alarm Severity Profile** window.

- 5 Place the cursor into the **ASAP Name** text box and type in the name of the new ASAP observing the following rules:

1. The ASAP name is an alphanumeric string of up to 24 characters.
2. The following characters are permitted in an ASAP name:

- Upper case letters (A ... Z),
- Lower case letters (a ... z),
- Digits (0 ... 9),
- Special characters (separated by comma):
' , - , (,) , . , / , + , ! , * , [,] , ^ , { , } , | , < , > , ~ , % , # , _

3. These characters are **not** permitted:

- Comma,
- Special characters (separated by comma):
@ , : , = , " , ; , & , ?

Spaces in an ASAP name will be ignored.

The ASAP name is used to distinguish different ASAPs of the same type.

- 6 You may now change individual alarm severity assignments according to your needs, or you may leave the alarm severity assignments unchanged for the present to change them later.

Reference:

To change individual alarm severity assignments, please refer to "Modifying an existing ASAP" (5-23), starting with Step 6.

7 Click **Apply** to save the new ASAP.

8 Click **Close** to close the **Provision Alarm Severity Profile** window.

END OF STEPS



Creating non-reporting ASAPs

Purpose Use this procedure to create non-reporting alarm severity assignment profiles (ASAPs).

Related information

Please also refer to “Alarm severity assignment profiles” (16-25).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege code

You must have at least a privilege code of **M3** to provision alarm severity assignment profiles.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar[®] CIT

Instructions Proceed as follows to create a non-reporting ASAP:

- 1 From the WaveStar CIT **System View** main menu, select **Configuration → Alarms → Create NonReporting ASAPs ...**

Result:

The **Create NonReporting ASAP Profiles** window opens.

- 2 Move all those ASAP types for which you want to create a non-reporting ASAP from the **Available ASAP Types** list on the left to the **Selected ASAP Types** list on the right.

You can either move single ASAP types one by one, several ASAP types at once or all listed ASAP types at once:

1. To move a single ASAP type, select the desired ASAP type in the **Available ASAP Types** list and press the **Add** button. Alternatively, you can also double click on the desired ASAP type.
2. To move several ASAP types at once, hold down **Ctrl** (or **Strg**) on the keyboard, select the desired ASAP types in the **Available ASAP Types** list, and press the **Add** button.
3. To move all listed ASAP types at once, press the **Add All** button.

Those ASAP types for which a non-reporting ASAP has already been created will not be listed in the **Available ASAP Types** list.

-
- 3 When the **Selected ASAP Types** list contains all those ASAP types for which you want to create a non-reporting ASAP, click **OK** and confirm your selection by clicking **Yes** in the confirmation window.

Result:

For all ASAPs in the **Selected ASAP Types** list a new ASAP named “NonReporting” is created.

-
- 4 Click **Close** to dismiss the **Create NonReporting ASAP Profiles** window.

END OF STEPS



Modifying an existing ASAP

Purpose Use this procedure to rename an existing ASAP and/or modify alarm severity assignments.

All alarm severity assignments, including those in the “Default” ASAPs, can be modified individually. However, the alarm severity assignments of the “NonReporting” ASAPs should **not** be changed.

Related information

Please also refer to “Alarm severity assignment profiles” (16-25).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M1** to modify an existing ASAP.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions Proceed as follows to modify an existing ASAP:

- 1 From the WaveStar CIT **System View** main menu, select **Configuration → Alarms → Alarm Severity Assignment Profile...**

Result:

The **Provision Alarm Severity Profile** window will be opened.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available ASAP types. The available ASAPs for a specific ASAP type can be made visible by clicking on the “+” sign in front of the corresponding ASAP type.

- 2 Select **Provision ASAP** in the upper left-hand corner of the window, next to **Operations**.
-

-
- 3 Select the ASAP to be modified in the ASAP tree by clicking on the “+” sign next to the respective ASAP type and selecting the ASAP from the expanded list.
-

- 4 Click **Provision** in the lower left-hand corner of the window.

Result:

The ASAP information is displayed on the right-hand side of the **Provision Alarm Severity Profile** window.

- 5 As an option, you may rename any ASAP other than the “Default” ASAPs by placing the cursor into the **New Name** text box and typing in the new name.

Observe the following rules:

1. The “Default” ASAPs cannot be renamed.
2. The ASAP name is an alphanumeric string of up to 24 characters.
3. The following characters are permitted in an ASAP name:
 - Upper case letters (A ... Z),
 - Lower case letters (a ... z),
 - Digits (0 ... 9),
 - Special characters (separated by comma):
,-,(),.,/,+!,*,[,],^,{,},|,<,>~,%,#,_
4. These characters are **not** permitted:
 - Comma,
 - Special characters (separated by comma):
@,.,=,“,;, &, ?

Spaces in an ASAP name will be ignored.

Important! In the case of a service-dependent ASAP (distinction between SA and NSA alarm severity), the SA alarm severity cannot be less than the NSA alarm severity.

- 6 Proceed as follows to change an alarm severity assignment:
 1. Click on the respective alarm severity in the **Alarm Level**, **SA Alarm Level** or **NSA Alarm Level** column (depending on the selected ASAP type).

The first time you click on an alarm severity, a drop-down list pops up listing the selectable alarm severities. Afterwards, you have to click twice (with a short delay, not with a double-click) to expand that alarm severity selection list.
 2. Select the desired alarm severity from the drop-down list.

You can reset all alarm severities to their default values by clicking on the **Use Default Values** button.

.....
 - 7 Click **Apply** to apply your changes.
 - 8 Click **Close** to close the **Provision Alarm Severity Profile** window.
- END OF STEPS
-



Setting ASAPs for a shelf

Purpose Use this procedure to assign either non-reporting or default ASAPs to particular types of equipment (port, tributary or circuit pack) of a shelf.

Related information Please also refer to “Alarm severity assignment profiles” (16-25).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M1** to set ASAPs for a shelf.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions Proceed as follows to :

- 1 From the *WaveStar* CIT **System View**, select **Configuration** → **Alarms** → **Set ASAPs for a Shelf...**

Result:

The **Set ASAPs for a Shelf** window will be opened. Initially, the right-hand part of the window is empty.

- 2 In the left-hand part of the window, select **Shelf 1 (DUR)** and click **Select Shelf**.

Result:

The right-hand part of the window will be populated with a selection option for the ASAP name, descriptive text and three tabs for the port, tributary or circuit pack selection.

-
- 3 In the right-hand part of the window, select either **NonReporting** or **Default** in the **Select ASAP Name** group box depending on whether you want to assign a non-reporting or a default ASAP to particular types of equipment.

Please also pay attention to the descriptive text beneath the **Select ASAP Name** group box.

- 4 Select the type of equipment (port, tributary or circuit pack) for which you want to assign a non-reporting or a default ASAP by clicking on either of the following tabs:

- **Port Selection**
- **Trib Selection**
- **Circuit Pack Selection**

The **Available Port (Tributary, Circuit Pack) Types** list box on the left-hand side contains the available port, tributary or circuit pack types.

- 5 Move the port, tributary or circuit pack types for which you want to assign a non-reporting or a default ASAP from the **Available Port (Tributary, Circuit Pack) Types** list box to the **Selected Port (Tributary, Circuit Pack) Types** list box.

The following options exist to move entries from one list box to the other:

- Select an entry by clicking on it, then click **Add** (left → right) or **Remove** (right → left) respectively.
 - Select multiple entries in a list box by holding down **Ctrl** (or **Strg**) on the keyboard while clicking on the entries, then click **Add** (left → right) or **Remove** (right → left) respectively.
 - Double click on an entry.
 - To move *all entries* from one list box to the other, select an entry by clicking on it, then click **AddAll** (left → right) or **Clear** (right → left) respectively.
-

- 6 Verify your settings and correct if necessary. Then click **Apply**.
-

-
- 7 Click **Close** to close the **Set ASAPs for a Shelf** window.

END OF STEPS



Setting the port monitoring mode

Purpose Use this procedure to configure the port monitoring mode for a particular port.

Related information

Please also refer to “Port monitoring mode” (16-34).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **P3** to configure the port monitoring mode.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions Proceed as follows to configure the port monitoring mode for a particular port:

- 1 There are two possible ways to invoke a relevant WaveStar CIT window for configuring the port monitoring mode:
 1. From the **System View** main menu select **Configuration** → **Provision...** to invoke the **Provision Parameters for Protection Group or Equipment** window. Subsequently, specify a port by using the Windows-style Explorer or by entering the relevant AID.
 2. In the shelf display right-click on the alarm LED of a port. In the pop-up menu that opens, select the **Provision Port #** menu item (“#” represents the port number) to invoke the **Provision Port** window.

The **Port Mode** drop-down list box in the **Transmission** tab of the respective window indicates the actual setting of the port monitoring mode.

-
- 2 If you want to change the port monitoring mode setting, select either **Auto**, **Monitored** or **Not Monitored** from the **Port Mode** drop-down list box.

The meaning of the different port monitoring modes is as follows:

Auto	Port monitoring is disabled. However, as soon as a valid input signal is detected, the port monitoring mode is automatically switched to Monitored .
Monitored	The incoming port signal is monitored for defects.
Not Monitored	Port monitoring is disabled.

- 3 In the **Apply To** drop-down list box, you may now choose whether the settings you made shall apply:
- only to the selected port (**This Port Only**),
 - to all ports of the specified type on the selected circuit pack (**All Ports of this type, This Pack**), or
 - to all ports of the specified type within the selected shelf (**All Ports of this type, This Shelf**).

If you choose one of the latter two options you will next have the opportunity to apply either only the previously changed settings or all settings currently valid.

Please note that the **Apply To** drop-down list box is not available if there is only one port on the respective circuit pack.

- 4 Verify your settings and correct if necessary. Then click **Apply** in the **Provision Parameters for Protection Group or Equipment** window or **OK** in the **Provision Port** window to apply your changes.
-

- 5 Click **Close** to dismiss the window.

END OF STEPS



Configuring fault management parameters for an SDH port

- Purpose** Use this procedure to perform the following:
- Configure all relevant Forward Error Correction (FEC) parameters (only applicable to circuit packs which support both in-band and out-of-band FEC),
 - Configure parameters for bit error monitoring,
 - Select an alarm severity assignment profile (ASAP) and assign it to the respective port.

- Before you begin** Prior to performing this task, you must:
- have a valid user login and password,
 - be connected to the corresponding NE, and
 - have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **P3** to perform this procedure.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

- Instructions** Proceed as follows to configure fault management parameters for an SDH port:
-

- 1 There are two possible ways to invoke a relevant WaveStar CIT window for configuring the port monitoring mode:
 1. From the **System View** main menu select **Configuration** → **Provision...** to invoke the **Provision Parameters for Protection Group or Equipment** window. Subsequently, specify a port by using the Windows-style Explorer or by entering the relevant AID.
 2. In the shelf display right-click on the alarm LED of a port. In the pop-up menu that opens, select the **Provision Port #** menu item (“#” represents the port number) to invoke the **Provision Port** window.

- 2 Select the **Fault Management** tab.

Important! Modifying the FEC parameters during operation may be traffic affecting. Therefore, it is recommended to configure all FEC parameters prior to putting the corresponding circuit pack into operation and leave them unchanged during operation.

- 3 For SDH ports supporting FEC, you may now configure all relevant FEC parameters.

If ...	then ...
you want to configure FEC parameters	continue with Step 4.
you do not want to configure FEC parameters	continue with Step 7.

- 4 For those circuit packs that support both in-band and out-of-band FEC, define the type of FEC to be applied by means of the **FEC Type** checkboxes.

Possible values are:

- **In-band** (default setting)
- **Out-band**

- 5 Enable or disable FEC by selecting the **Enabled** or **Disabled** option for **FEC Encoding/Decoding**.

Enabling the FEC mode means that the required FEC information will be calculated and processed.

Important! Enabling of in-band FEC at the receiver while no BCH-encoded signal is transmitted leads to B1 bit errors to be detected erroneously. Therefore, make sure that in-band FEC is enabled only if a BCH-encoded signal is transmitted. High values of the RS-SES and RS-UAS performance monitoring parameters may be an indicator for a wrong FEC configuration.

-
- 6** Provided that FEC is enabled, you may start or stop the FEC bit error correction at any time by selecting the **Enabled** or **Disabled** option for **FEC Correction**.

The setting of the **FEC Correction** parameter has no influence as long as **FEC Encoding/Decoding** is disabled.

- 7** As an option, you may set the preferred mode to monitor the bit error performance during transmission. Possible values are:
- **Poisson** (default setting for SONET ports)
This mode of bit error monitoring means that a random (Poisson) distribution of bit errors is presumed.
 - **Burst** (default setting for SDH ports)
This mode of bit error monitoring means that a bursty distribution of bit errors is presumed.

To view or change the mode of bit error monitoring, select the **Transmission** tab and continue with Step 8. Otherwise, please continue with Step 14.

- 8** Set the mode of bit error monitoring to either **Poisson** or **Burst** by selecting the corresponding checkbox next to **Signal Degrade/Fail Mode**.
-

- 9** As an option, you may set the **HP Degraded Interval** to a value between 2 and 10 seconds. The default setting is 7 seconds.

Note: This parameter can only be set in **Burst** mode.

The **HP Degraded Interval** defines the threshold value for bursty errors.

- 10** As an option, you may set the **HP Degraded Threshold** to a value between 5% and 50% (in steps of 5%).

Note: This parameter can only be set in **Burst** mode.

The **HP Degraded Threshold** defines measurement interval for bursty errors.

11 Select the **Fault Management** tab.

12 As an option, you may set the **MS DEXC Threshold** to one of the following values:

- 10^{-3} (default value)
- 10^{-4}
- 10^{-5}

Note: This parameter can only be set in **Poisson** mode.

The configured threshold defines the bit error ratio in the Multiplex Section that must be exceeded before an Excessive Bit Error Ratio alarm is reported.

13 As an option, you may set the **MS Degrade Threshold** to one of the following values:

- 10^{-5}
- 10^{-6} (default value)
- 10^{-7}
- 10^{-8}
- 10^{-9}

Note: This parameter can only be set in **Poisson** mode.

The configured threshold defines the bit error ratio in the Multiplex Section that must be exceeded before a Degraded Signal alarm is reported.

14 From the available ASAPs in the **Alarm Severity Profile** drop-down list box, select one according to your needs.

15 In the **Apply To** drop-down list box, you may now choose whether the settings you made shall apply:

- only to the selected port (**This Port Only**),
- to all ports of the specified type on the selected circuit pack (**All Ports of this type, This Pack**), or
- to all ports of the specified type within the selected shelf (**All Ports of this type, This Shelf**).

If you choose one of the latter two options you will next have the opportunity to apply either only the previously changed settings or all settings currently valid.

Please note that the **Apply To** drop-down list box is not available if there is only one port on the respective circuit pack.

16 Verify your settings and correct if necessary. Then click **Apply** in the **Provision Parameters for Protection Group or Equipment** window or **OK** in the **Provision Port** window.

17 Click **Close** to dismiss the window.

END OF STEPS



Configuring fault management parameters for a SONET port

- Purpose** Use this procedure to perform the following:
- Configure all relevant Forward Error Correction (FEC) parameters (only applicable to circuit packs which support both in-band and out-of-band FEC),
 - Configure parameters for bit error monitoring,
 - Select an alarm severity assignment profile (ASAP) and assign it to the respective port.

- Before you begin** Prior to performing this task, you must:
- have a valid user login and password,
 - be connected to the corresponding NE, and
 - have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **P3** to perform this procedure.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

- Instructions** Proceed as follows to configure fault management parameters for a SONET port:
-

- 1 There are two possible ways to invoke a relevant WaveStar CIT window for configuring the port monitoring mode:
 1. From the **System View** main menu select **Configuration** → **Provision...** to invoke the **Provision Parameters for Protection Group or Equipment** window. Subsequently, specify a port by using the Windows-style Explorer or by entering the relevant AID.
 2. In the shelf display right-click on the alarm LED of a port. In the pop-up menu that opens, select the **Provision Port #** menu item (“#” represents the port number) to invoke the **Provision Port** window.

-
- 2 Select the **Fault Management** tab.
-

Important! Modifying the FEC parameters during operation may be traffic affecting. Therefore, it is recommended to configure all FEC parameters prior to putting the corresponding circuit pack into operation and leave them unchanged during operation.

- 3 For SONET ports supporting FEC, you may now configure all relevant FEC parameters.

If ...	then ...
you want to configure FEC parameters	continue with Step 4.
you do not want to configure FEC parameters	continue with Step 7.

- 4 For those circuit packs that support both in-band and out-of-band FEC, define the type of FEC to be applied by means of the **FEC Type** checkboxes.

Possible values are:

- **In-band** (default setting)
 - **Out-band**
-

- 5 Enable or disable FEC by selecting the **Enabled** or **Disabled** option for **FEC Encoding/Decoding**.

Enabling the FEC mode means that the required FEC information will be calculated and processed.

Important! Enabling of in-band FEC at the receiver while no BCH-encoded signal is transmitted leads to B1 bit errors to be detected erroneously. Therefore, make sure that in-band FEC is enabled only if a BCH-encoded signal is transmitted. High values of the SES-S and UAS-S performance monitoring parameters may be an indicator for a wrong FEC configuration.

-
- 6 Provided that FEC is enabled, you may start or stop the FEC bit error correction at any time by selecting the **Enabled** or **Disabled** option for **FEC Correction**.

The setting of the **FEC Correction** parameter has no influence as long as **FEC Encoding/Decoding** is disabled.

- 7 As an option, you may set the preferred mode to monitor the bit error performance during transmission. Possible values are:
- **Poisson** (default setting for SONET ports)
This mode of bit error monitoring means that a random (Poisson) distribution of bit errors is presumed.
 - **Burst** (default setting for SDH ports)
This mode of bit error monitoring means that a bursty distribution of bit errors is presumed.

To view or change the mode of bit error monitoring, continue with Step 8. Otherwise, please continue with Step 13.

- 8 Set the mode of bit error monitoring to either **Poisson** or **Burst** by selecting the corresponding checkbox next to **Signal Degrade/Fail Mode**.
-

- 9 As an option, you may set the **HP Degraded Interval** to a value between 2 and 10 seconds. The default setting is 7 seconds.

Note: This parameter can only be set in **Burst** mode.

The **HP Degraded Interval** defines the threshold value for bursty errors.

- 10 As an option, you may set the **HP Degraded Threshold** to a value between 5% and 50% (in steps of 5%).

Note: This parameter can only be set in **Burst** mode.

The **HP Degraded Threshold** defines measurement interval for bursty errors.

-
- 11** As an option, you may set the **Optical Line BER Threshold** to one of the following values:

- 10^{-5}
- 10^{-6} (default value)
- 10^{-7}
- 10^{-8}
- 10^{-9}

Note: This parameter can only be set in **Poisson** mode.

The configured threshold defines the bit error ratio in the Multiplex Section that must be exceeded before a Degraded Signal alarm is reported.

-
- 12** As an option, you may set the **Optical Line EBER Threshold** to one of the following values:

- 10^{-3} (default value)
- 10^{-4}
- 10^{-5}

Note: This parameter can only be set in **Poisson** mode.

The configured threshold defines the bit error ratio in the Multiplex Section that must be exceeded before an Excessive Bit Error Ratio alarm is reported.

-
- 13** From the available ASAPs in the **Alarm Severity Profile** drop-down list box, select one according to your needs.

-
- 14** In the **Apply To** drop-down list box, you may now choose whether the settings you made shall apply:

- only to the selected port (**This Port Only**),
- to all ports of the specified type on the selected circuit pack (**All Ports of this type, This Pack**), or
- to all ports of the specified type within the selected shelf (**All Ports of this type, This Shelf**).

If you choose one of the latter two options you will next have the opportunity to apply either only the previously changed settings or all settings currently valid.

Please note that the **Apply To** drop-down list box is not available if there is only one port on the respective circuit pack.

-
- 15** Verify your settings and correct if necessary. Then click **Apply** in the **Provision Parameters for Protection Group or Equipment** window or **OK** in the **Provision Port** window.
-

- 16** Click **Close** to dismiss the window.

END OF STEPS



Enabling or disabling autonomous alarm forwarding

Purpose Use this procedure to inhibit, temporarily, the forwarding of autonomously generated alarm notifications to management systems and to restart autonomous alarm forwarding again.

Related information Please also refer to “Autonomous alarm forwarding” (16-22).

Before you begin Prior to performing this task, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform this procedure.

Required privilege

You must have at least a privilege code of **M3** to enable or disable autonomous alarm forwarding.

Required equipment

The following equipment is required to perform this procedure:

- *WaveStar*® CIT

Instructions Proceed as follows to enable or disable autonomous alarm forwarding:

- 1 Autonomous alarm forwarding can be enabled/disabled either for the current management session or for all management sessions. Management sessions are TL1-based management associations between a network element and a management system, such as *WaveStar* CIT or *WaveStar* SNMS.

If ...	then ...
you want to enable or disable autonomous alarm forwarding for the current management session	select Fault → Inhibit/Allow Autonomous Message Reporting... → Current Session... from the <i>WaveStar</i> CIT System View main menu.
you want to enable or disable autonomous alarm forwarding for all management sessions	select Fault → Inhibit/Allow Autonomous Message Reporting... → All Sessions... from the <i>WaveStar</i> CIT System View main menu.

Result:

The **Provision Autonomous Reporting for Current Session** or **Provision Autonomous Reporting for All Sessions** respectively will be opened. The radio button (**allow** or **inhibit**) corresponding to the current setting is pre-selected. The **OK** button will become accessible if this selection is changed.

-
- 2** To disable autonomous alarm forwarding, select **inhibit**.
To enable autonomous alarm forwarding again, select **allow**.
-

- 3** Click **OK**.

Result:

Autonomous alarm forwarding will be enabled or disabled for the current management session or for all management sessions according to your selection. The “ABN” LED on the user panel will be lit when autonomous alarm forwarding is disabled.

-
- 4** Click **Close** to close the window.

END OF STEPS





6 Timing provisioning

Overview

Purpose This chapter describes the procedures which have to be performed for the configuration of the system timing of the *LambdaUnite*[™] MSS.

Contents

Viewing the timing configuration	6-3
Parameters of the “Synchronization Characteristics” window	6-5
The External Timing Input Port tabs	6-6
The External Timing Output Port tabs	6-7
The Timing Reference tabs	6-12
The System Timing Parameters tab	6-15
Configuring the external timing output ports SDH mode	6-19
Configuring the external timing output ports SONET mode	6-23
Configuring the external timing input ports SDH mode	6-27
Configuring the external timing input ports SONET mode	6-29
Configuring the timing references	6-31

Configuring the system timing	6-34
Forced Switching of the timing generator to the holdover mode	6-37
Switching to another timing reference	6-39

□

Viewing the timing configuration

When to use Use this procedure to view the configuration of the external timing input and output ports, the timing reference and the system timing.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”

Before you begin Prior to performing this task, verify that a *WaveStar*[®] CIT is connected and logged into the *LambdaUnite*[™] MSS system.

Required privilege code

You must have at least a privilege code of P1, Provisioning to query the data of the timing configuration.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the data of the timing configuration:

- 1 In the **System View** of the *WaveStar* CIT, select **View** → **Timing/Sync**

Result:

The **Synchronization Characteristics** window appears with the active **External Timing Input Port 1** tab. For port 2 click on the **External Timing Input Port 2** tab.

The corresponding parameters are described in “Configuring the external timing input ports SDH mode” (6-27) and “Configuring the external timing input ports SONET mode” (6-29).

- 2 Click on one of the **External Timing Output Port** tabs to query the data on the timing output port. The corresponding parameters are described in “Configuring the external timing output ports SONET mode” (6-23) and “Configuring the external timing output ports SDH mode” (6-19).

-
- 3 Click on one of the **External Timing Reference** tabs to query the data on the configured timing reference source. The corresponding parameters are described in “Configuring the timing references” (6-31).
.
 - 4 Click on one of the **Line Timing Reference** tabs to query the data on the configured timing reference source. The corresponding parameters are described in “Configuring the timing references” (6-31).
 - 5 Click on the **System Timing Parameters** tab to query the data on the internal SDH Equipment Clock (SEC). The corresponding parameters are described in “Configuring the system timing” (6-34).
 - 6 Click on **Close** to quit the window.

END OF STEPS



Parameters of the “Synchronization Characteristics” window

General The window **Synchronization Characteristics** contains 13 tabs:

- **External Timing Input Port 1**
- **External Timing Input Port 2**
- **External Timing Output Port 1**
- **External Timing Output Port 2**
- **External Timing Reference 1**
- **External Timing Reference 2**
- **Line Timing Reference 1**
- **Line Timing Reference 2**
- **Line Timing Reference 3**
- **Line Timing Reference 4**
- **Line Timing Reference 5**
- **Line Timing Reference 6**
- **System Timing Parameters**

The corresponding parameters are described as follows.

Push-button The window has one push-button. Via **Close** the window is closed.



The External Timing Input Port tabs

Overview The first tab displays the parameters of external timing input port 1. *LambdaUnite™* MSS provides two external timing input ports, including the following information fields for each.

Timing Input Format The information field **Timing Input Format** displays the format of the incoming timing signal. The displayed values can be:

SDH mode	SONET mode
2 MHz	SF (Super Frame)
2 Mbit - framed	ESF (Extended Super Frame)
2 Mbit - unframed	

SSM Support The SSM is supported for 2 Mbit/s - framed (**SDH** mode) and **ESF** (**SONET** mode) external timing input signals.

Possible values are:

- **supported** (default)
- **not supported**

S_a bit Location This parameter is only supported for framed 2 Mbit/s **SDH** signals.

Possible values are:

- S_{a4}
- S_{a5}
- S_{a6}
- S_{a7}
- S_{a8}
- **Disabled** (for unsupported signals)



The External Timing Output Port tabs

Overview *LambdaUnite*[™] MSS provides two external timing output ports. A 2 MHz, 2 Mbit/s or DS1 timing signal can be derived from the internal system clock and forwarded to the output ports. A timing signal can be derived from the system clock and is forwarded to both external timing outputs in parallel. It can be used as synchronization signal for an external network.

Regenerator Loop Delay Delay during which **DNU/DUS** is maintained after the Regenerator Loop conditions are no longer present.

This parameter can take the values:

- **0 ... 60 s**
Default value is **0s**.

Regenerator Loop (SDH mode)

This parameter indicates that a timing loop may be present from the timing output to one or both of the timing inputs through a Stand-Alone Synchronization Equipment (SASE) Office Clock. This might happen, if the NE forwards timing to the SASE and the same time receives a timing signal via one or both of the external timing input ports. If additionally the system clock is in the Locked Mode and derived from an external timing signal, **DNU** is forwarded to the timing outputs.

This parameter can take the values:

- **Disable (default)**
The Regenerator Loop functionality is disabled. Timing loops are not considered.
- **External Reference 1**
If the quality level of the incoming framed 2 Mbit/s timing signal at the exttmg0 input is equal to the quality level of the timing signal that is transmitted to the external timing output ports, **DNU** is inserted for the outgoing timing signal as the NE assumes that a timing loop is present.
- **External Reference 2**

If the quality level of the incoming framed 2 Mbit/s timing signal at the exttmg1 input is equal to the quality level of the timing signal that is transmitted to the external timing output ports, **DNU** is inserted for the outgoing timing signal as the NE assumes that a timing loop is present.

- **Both**

The **Regenerator Loop** functionality is applied to both external timing inputs.

Regenerator Loop (SONET mode)

This parameter indicates that a timing loop may be present from the timing output to one or both of the timing inputs through a Building Integrated Timing Supply (BITS) Office Clock. This might happen, if the NE forwards timing to the BITS and the same time receives a timing signal via one or both of the external timing input ports. If additionally the system clock is in the Locked Mode and derived from an external timing signal, **DUS** is forwarded to the timing outputs.

This parameter can take the values:

- **Enable (default)**

The **Regenerator Loop** functionality is enabled. Timing loops are considered.

- **Disable**

The **Regenerator Loop** functionality is disabled. Timing loops are not considered.

S_a bit Location

This parameter is only supported for framed 2 Mbit/s **SDH** signals.

Possible values are:

- S_{a4}
- S_{a5}
- S_{a6}
- S_{a7}
- S_{a8}
- **Disabled** (for unsupported signals)

Acceptance Quality Level for Output Threshold AIS

This parameter defines the provisioned quality acceptance level for external timing output signals. When the incoming signal is below this level the AIS or **DUS/DNU** will be inserted.

The possible values are:

SDH mode	SONET mode
PRC	PRS
SSUT	STU
SSUL	ST2
SEC (default)	ST3 (default)

AIS Mode This parameter is only supported for framed 2 Mbit/s output format signals (**SDH** mode) and **ESF** output format signals (**SONET** mode). It specifies what value will be sent when the signal is below quality acceptance or when forced **DNU/DUS** (Quality Level Mode) is set enabled.

The possible values are

- **AIS MODE**
- **QL MODE (default)**

**Sync Message Force
DUS/DNU**

This parameter defines whether Sync Message Force DNU (**SDH** mode) respectively Sync Message Force DUS (**SONET** mode) is inserted in the outgoing timing signal.

The following values are possible

- **Enable**
- **Disable (default)**

Output Quality Level

This information field shows the quality (the value of the Synchronization Status Marker, SSM) of the outgoing timing signal. It is greyed out, when the **Signal Format** is 2 MHz, as the SSM can only be provided for framed 2 Mbit/s (**SDH**) respectively ESF (**SONET**) signals.

The following values are possible (in order from highest to lowest quality):

- For **SDH** NEs
 1. **PRC** (Primary Reference Clock)
 2. **SSUT** (Synchronization Supply Clock (Transit node))
 3. **SSUL** (Synchronization Supply Clock (Local node))

4. **SEC** (SDH Equipment Clock)
5. **DNU** (Do not use for synchronization)
- For **SONET** NEs
 1. **PRS** (Primary Reference Source)
 2. **STU** (Synchronized Traceability Unknown)
 3. **ST2** (Stratum 2)
 4. **ST3** (Stratum 3)
 5. **DUS** (Do not use for synchronization)

Signal Format This parameter shows the signal format of the outgoing timing signal. **2 MHz** (default), **2 Mbit/s-framed** and **2 Mbit/s-unframed** are possible for **SDH** mode.

For **SONET** mode the possible values are **SF** (Super Frame) and **ESF** (Extended Super Frame) which is the default value.

Output Signal Status This parameter describes the Status of the outgoing timing signal.

It can take the values

- **Normal**
- **Disable**
- **Unacceptable**

ASAP Name Select the **Alarm Severity Assignment Profile** (ASAP). You can choose between a default and a specific ASAP. Via the push-button **ASAP Details...** you can retrieve more detailed information on the ASAPs.

Derived Output Timing Enable This parameter shows whether a timing signal is derived from the system clock and forwarded to the output port.

The values are

- **Enable**
- **Disable (default)**

Provisioned Derived Output Timing Source Selection This parameter shows from which source the external timing signal is derived.

Possible for **SDH** mode values are:

- **TLS** (Timing Link Switch)
The external timing signal is derived from one of the six timing references. The selection criteria are the same as for system timing apply except the following:
 - signals with derived output priority enabled
 - signals with derived output lockout status set to **No Lockout**.
- **SETG** (default)
The timing output is derived from the system clock

The possible values for **SONET** mode are:

- **line1** (for output 1)
- **line2** (for output 2)

Timing Output Equalization

This information field is available for **SONET** mode only.

The possible values are:

- **20%** (initial value)
- **40%**
- **60%**
- **80%**
- **100%**



The Timing Reference tabs

Overview The **Timing Reference** tab of the View**Synchronization Characteristics** window displays data on the configured timing reference source

Active Timing Reference In the group box **System Timing Reference**, the information field **Active Timing Reference** displays the reference timing signal which is currently selected. The timing reference is an external signal to which the internal **SDH/SONET** Equipment Clock is locked.

The following signals can be used as timing reference:

- external net clock input signals (2048 kHz, 2048 kbit/s acc. to ITU-T or DS1 acc. to Telcordia)
- 6 reference signals derived from the incoming STM-64, STM-16 or OC192, OC48 line signals.

Thus the following values can be displayed:

- **extref1** or **extref2** for the external net clock input signals
- **line1** to **line6** for the **SDH/SONET** signals

Settings The table on the tab gives an overview of the possible settings of the timing references.

Column	Possible values	Meaning
Incoming SSM value (SDH mode)	PRC, STUT, SSUL, SEC, DNU, SSM0, SSM1, SSM3, SSM5, SSM6, SSM7, SSM9, SSM10, SSM12, SSM13, SSM14, UNSTABLE, NONE	Indicates the QL value for the timing port
Incoming SSM value (SONET mode)	PRS, STU, ST2, ST3, DUS, NONE	Indicates the QL value for the timing port
Quality Level (SDH mode)	DNU, PRC, SSUT, SSUL, SEC	This parameter shows the synchronization messaging quality level value for timing references. This is the value which is forwarded to the timing output ports.

Column	Possible values	Meaning
Quality Level (SONET mode)	DUS, PRS, STU, ST2, ST3	This parameter shows the synchronization messaging quality level value for timing references. This is the value which is forwarded to the timing output ports.
Provisioned Quality Level (SDH mode)	PRC, SSUT, SSUL, SEC, AUTO	This parameter is the quality level SSM value which will be received on the timing references.
Provisioned Quality Level (SONET mode)	PRS, STU, ST2, ST3, AUTO	This parameter is the quality level SSM value which will be received on the timing references.
Input Quality Status	VALID, INVALID, NOT-SUPPORTED, NOT-APPLICABLE	This parameter shows if a valid timing input signal is available for the respective timing reference.
Assigned Port AID	exttmg0, exttmg1	An external net clock input signal is used as timing reference
	Not connected	The respective timing reference source is not used
	<port AID of an SDH/SONET timing reference>	The respective SDH/SONET timing reference signal is used as timing reference
System Timing Reference Priority	Disable (initial value), 1, 2,3, ..., 8	Configured priority of the timing reference signals
Timing Port Mode Monitoring	Monitored, Not Monitored	Specifies the monitoring status of the timing port
ASAP Name	Default, <ASAP Name>	Selection between a default and a specific Alarm Severity Assignment Profile (ASAP).
Signal Status	NORMAL	The timing reference signal is fault-free.
	FAILED	The timing reference signal failed.
	WAIT-TO- RESTORE	The timing reference signal has been failed and is now restored. A wait is made for a defined time (wait-to-restore time) to see whether the signal is stable, before the system switches back to it.
	NOT-CONNECTED	The timing reference is not used.
Lockout Status	LOCKOUT	The clock protection is deactivated
	NO-LOCKOUT	The clock protection is activated

Only one of the timing references at a time can be selected as the active one.



The System Timing Parameters tab

Overview The **System Timing** tab on the **Synchronization Characteristics** window displays data on the system timing state.

The tab consists of three group boxes **System Timing** and **System Timing Reference**.

The group box *System Timing* The following table lists the fields of the group box **System Timing**, the possible values and their meaning.

Information field	Possible value	Meaning
Wait to Restore	1 Minute ... 60 Minutes (1min steps)	Selected value of the wait-to-restore time which has to pass before the system switches to another timing reference signal.
Stratum Level Status	SEC (SDH) 3 (SONET)	Timing Quality of the internal equipment clock acc. to ITU-T Rec. G.813.
System Synchronization Status Messaging Mode	QL Enable, QL Disable	The reference selection process to use or not to use the incoming QL messages and the transmission of sync messaging on optical interfaces. If it set QL Disable the optical interface will transmit the message "do not use".
System Quality Level Status (SDH Mode)	PRC, SSUT, SSUL, SEC, DNU	The current quality level of the system clock.

Information field	Possible value	Meaning
System Quality Level Status (SONET Mode)	STU, ST2, ST3, PRS, DUS	The current quality level of the system clock.
Warm Up Status	Normal (default), Warming-Up	Show the status of the system. The system shall be in Warm up status for a temporary period of time before transition to Normal.
System Clock Mode Status	Holdover (SDH)	The current operating system clock mode is the holdover mode. The active timing generator enters the holdover mode if all timing reference signals fail. In the holdover mode, the active timing generator keeps its internal Stratum 3 clock at the point at which it was synchronized to the last known good reference signal.
	Autonomous Holdover (SONET)	
	Normal	
	Forced Holdover	
	Fast Start (SONET)	Fixed value.

Information field	Possible value	Meaning
Clock Mode	Free Running (initial value)	For the internal timing generator the Free Running Mode is selected. It is not locked to an external timing reference signal. The system clock is generated by an internal oscillator.
	Locked	The Locked Mode is selected. The internal timing generator is locked to an external timing reference signal.
ASAP Name	Default, <ASAP Name>	Selection between the default and a specific System Timing Alarm Severity Assignment Profile (ASAP).

System Timing Reference The table on the tab gives an overview of the possible settings of the system timing references.

Information field	Possible values	Meaning
System Timing Reference AID	exttmg0, exttmg1	AID of the System Timing Reference
Active Timing Reference	extref1, extref2; line1...line6	The currently active Timing Reference
Reference Switch Status	Forced, Manual, No Request	Value of the Switch Request activated by the user or initiated by the system.

Output Timing Reference The table on the tab gives an overview of the possible settings of the output timing references.

Information field	Possible values	Meaning
Active Output Timing Reference (SDH mode only)	Line1 ... Line 6	Selected value of the currently active Timing Output Reference if it is set to TLS (lines).

Information field	Possible values	Meaning
Output Timing Reference Switch Request Status (SDHmode only)	No Request, Manual, Forced	Value of the switch request activated by the user or initiated by the system.
Output Timing Reference AID	-	AID of the line port on the timing unit for external timing references or a STM-16, STM-64, OC48, OC192 port for a line timing reference.

Configuring the external timing output ports SDH mode

When to use Use the following procedures to configure the external timing output ports for **SDH** mode.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The External Timing Input Port tabs” (6-6)

Before you begin Prior to performing this task, you must connect the external timing output ports to an external timing network.

Required privilege code

You must have at least a privilege code of P3 to configure the external timing output ports.

Required equipment

The following is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to configure the external timing output ports:

- 1** Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronization Characteristics** appears.

- 2** Select a tab **External Timing Output Port**.
-

- 3** Select the timing output format in the group box **Signal Format** by clicking on the respective radio button. Select the format according to

the format which is required for the external network. The following values are possible:

- **2 MHz** (initial value)
 - **2 Mbit - framed**
For framed 2 Mbit/s signals, the generation and evaluation of timing marker information on the timing quality is supported as per ITU-T Rec. G.704. If you want to use the timing marker, select **2 Mbit - framed**.
 - **2 Mbit - unframed**
-

- 4 Enable the use of the external outputs in the group box **Derived Output Timing Enable**. Click on the radio button **Enable**.

Please note that there is only one timing output signal derived from the system clock or line signals which is forwarded in parallel to the two output ports which are physically available.

- 5 Select the timing output source in the group box **Provisioned Derived Output Timing Source Selection** from which the external timing signal is derived.

The following values are possible:

- **TLS** (Timing Link Switch)
The external timing signal is derived from one of the six timing references.
The selection criteria are the same as for system timing apply except the following:
 - signals with derived output priority enabled
 - signal with derived output lockout status set to **No Lockout**
 - **SETG** (default)
The external timing signal is derived from the system clock.
-

- 6 Set the parameter **Regenerator Loop** in order to avoid timing loops between the timing output ports and one or both of the timing inputs through a Stand-Alone Synchronization Equipment (SASE) Office Clock. This might happen, if the NE forwards timing to the SASE and at the same time receives a timing signal via one or both of the external timing input ports. If additionally the system clock is in the

Locked Mode and derived from an external timing signal, **DNU** is forwarded to the timing outputs.

The following values are possible:

- **Disable**
The Regenerator Loop functionality is disabled. Timing loops are not considered.
- **External Reference 1**
If the quality level of the incoming framed 2 Mbit/s timing signal at the exttmg0 input is equal to the quality level of the timing signal that is transmitted to the external timing output ports, DNU is inserted for the outgoing timing signal as the NE assumes that a timing loop is present.
- **External Reference 2**
If the quality level of the incoming framed 2 Mbit/s timing signal at the exttmg1 input is equal to the quality level of the timing signal that is transmitted to the external timing output ports, DNU is inserted for the outgoing timing signal as the NE assumes that a timing loop is present.
- **Both**
The Regenerator Loop functionality is applied to both external timing inputs.

-
- 7 Set the parameter **Loop Delay**. This parameter defines the delay during which DNU is transmitted from the timing outputs after the Regenerator Loop conditions are no longer present. You can select a value between **0 s** and **60 s**.
-

- 8 Set the parameter **Sync Message Force DNU**. Via this parameter you can define whether **DNU** is consistently transmitted from the timing output ports.

The following values are possible:

- **Enable**
- **Disable** (default)

-
- 9 Set individual location of the Sa bit in the group box **Sa bit Location**.

The following values are possible:

- S_{a4} (initial value)
- S_{a5}
- S_{a6}
- S_{a7}
- S_{a8}

This parameter is only supported for framed 2 Mbit/s signals.

-
- 10** Select the value that will be sent if the outgoing signal is below the quality acceptance or if forced **DNU** is enabled in the group box **AIS mode**.

The following values are possible

- **AIS mode**
- **QL mode**

This parameter is only supported for framed 2 Mbit/s signals.

-
- 11** In the group box **Acceptance Quality Level for Output Threshold AIS** you can select the provisioned quality acceptance level for the external timing output. When the incoming signal is below this level AIS or DNU is inserted into the external timing output port.

The possible values are:

- **PRC**
- **SSUT**
- **SSUL**
- **SEC** (default)

-
- 12** Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

Result:

If you have clicked on **OK** or **Cancel**, the **Synchronization Characteristics** window closes. If you have clicked on **Apply**, the window remains open and you can select another tab.

END OF STEPS



Configuring the external timing output ports SONET mode

When to use Use the following procedures to configure the external timing output ports for **SONET** mode.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The External Timing Input Port tabs” (6-6)

Before you begin Prior to performing this task, you must connect the external timing output ports to an external timing network.

Required privilege code

You must have at least a privilege code of P3 to configure the external timing output ports.

Required equipment

The following is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to configure the external timing output ports:

- 1 Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronization Characteristics** appears.

- 2 Select a tab **External Timing Output Port**.
-

- 3 Select the timing output format in the group box **Signal Format** by clicking on the respective radio button. Select the format according to

the format which is required for the external network. The following values are possible:

- **ESF** (initial value)
 - **SF**
-

- 4 Enable the use of the external outputs in the group box **Derived Output Timing Enable**. Click on the radio button **Enable**.

Please note that there is only one timing output signal derived from the system clock or line signals which is forwarded in parallel to the two output ports which are physically available.

- 5 Select the timing output source in the group box **Provisioned Derived Output Timing Source Selection** from which the external timing signal is derived.

This information field is greyed out, the following values are fixed:

- **line1** (for output 1)
 - **line2** (for output 2)
-

- 6 Set the parameter **Regenerator Loop** in order to avoid timing loops between the timing output ports and one or both of the timing inputs through a Building Integrated Timing Supply (BITS) Office Clock. This might happen, if the NE forwards timing to the BITS and at the same time receives a timing signal via one or both of the external timing input ports. If additionally the system clock is in the Locked Mode and derived from an external timing signal, **DUS** is forwarded to the timing outputs.

The following values are possible:

- **Disable**
The Regenerator Loop functionality is disabled. Timing loops are not considered.
- **Enable (default)**
The Regenerator Loop functionality is applied to both external timing inputs.

-
- 7 Set the parameter **Loop Delay**. This parameter defines the delay during which DUS is transmitted from the timing outputs after the Regenerator Loop conditions are no longer present. You can select a value between **0 s** and **60 s**.
-

- 8 Set the parameter **Sync Message Force DUS**. Via this parameter you can define whether **DUS** is consistently transmitted from the timing output ports.

The following values are possible:

- **Enable**
 - **Disable** (default)
-

- 9 Select the value that will be sent if the outgoing signal is below the quality acceptance or if forced **DUS** is enabled in the group box **AIS mode**.

The following values are possible

- **AIS mode**
- **QL mode**

This parameter is only supported for **ESF** output signals.

- 10 In the group box **Acceptance Quality Level for Output Threshold AIS** you can select the provisioned quality acceptance level for the external timing output. When the incoming signal is below this level AIS or DUS is inserted into the external timing output port.

The possible values are:

- **PRS**
 - **STU**
 - **ST2**
 - **ST3** (default)
-

- 11 Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

Result:

If you have clicked on **OK** or **Cancel**, the **Synchronization Characteristics** window closes. If you have clicked on **Apply**, the window remains open and you can select another tab.

END OF STEPS



Configuring the external timing input ports SDH mode

When to use Use the following procedures to configure the external timing input ports for **SDH** mode.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The External Timing Input Port tabs” (6-6)

Before you begin Prior to performing this task, you must connect the external timing input ports to an external timing source.

Requires privilege code

You must have at least a privilege code of P3, Provisioning, to configure the external timing input ports.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to configure the external timing input ports:

- 1 In the **System View** of the WaveStar CIT select **Configuration** → **Timing/Sync**.

Result:

The window **Synchronization Characteristics** appears with the active tab **External Timing Input Port 1**. For port 2 you select **External Timing Input Port 2**.

- 2 Select the timing input format in the group box **Input Signal Format** by clicking on the respective radio button. Select the format according

to the format of the external clock source. The following values are possible:

- **2 MHz**
- **2 Mbit - framed**
- **2 Mbit - unframed**

-
- 3 Select **Supported** in the **SSM support** tab. The SSM mode will be supported on the corresponding external timing input port (for framed 2 Mbit/s signals only). Otherwise the value will be **Not-Supported**.

-
- 4 Set individual location of the S_a bit in the group box **S_a bit Location**. The following values are possible:

- **S_{a4}** (initial value)
- **S_{a5}**
- **S_{a6}**
- **S_{a7}**
- **S_{a8}**

This parameter is only supported for framed 2 Mbit/s signals.

-
- 5 Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

Result:

If you have clicked on **OK** or **Cancel**, the window **Synchronization Characteristics** closes. If you have clicked on **Apply**, the window remains open and you can select another tab.

END OF STEPS



Configuring the external timing input ports SONET mode

When to use Use the following procedures to configure the external timing input ports for **SONET** mode.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The External Timing Input Port tabs” (6-6)

Before you begin Prior to performing this task, you must connect the external timing input ports to an external timing source.

Requires privilege code

You must have at least a privilege code of P3, Provisioning, to configure the external timing input ports.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to configure the external timing input ports:

- 1 In the **System View** of the WaveStar CIT select **Configuration** → **Timing/Sync**.

Result:

The window **Synchronization Characteristics** appears with the active tab **External Timing Input Port 1**. For port 2 you select **External Timing Input Port 2**.

- 2 Select the timing input format in the group box **Input Signal Format** by clicking on the respective radio button. Select the format according to the format of the external clock source. The following values are possible:
 - **ESF**
 - **SF**

-
- 3** Select **Supported** in the **SSM support** tab. The SSM mode will be supported on the corresponding external timing input port (for **ESF** signals only). Otherwise the value will be **Not-Supported**.
-

- 4** Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

Result:

If you have clicked on **OK** or **Cancel**, the window **Synchronization Characteristics** closes. If you have clicked on **Apply**, the window remains open and you can select another tab.

END OF STEPS



Configuring the timing references

When to use Use this procedure to configure the timing references.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The Timing Reference tabs” (6-12)

Before you begin Prior to performing this procedure, you must have completed the following provisioning tasks:

Administrative tasks, such as a setup of user profiles (cf. Chapter 2, “Security administration”) and provisioning of management communication via DCN (cf. Chapter 3, “Management communication setup”).

Select the synchronisation system mode (only possible in maintenance condition selectable via **Fault → Enter/Exit Maintenance Condition ... → Enter Maintenance Condition ...**)

Required privilege code

You must have at least a privilege code of P3 to configure the timing references.

Required equipment

The following equipment is required to perform this task:

- WaveStar[®] CIT

Instructions Complete the following steps to configure the timing references:

- 1 Select **Configuration → Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronization Characteristics** appears.

- 2 Select the **Timing Reference** source in the corresponding tab which you wish to configure. You can select the external timing signals

extref1 or **extref2** or an **SDH/SONET** signal via **line1 ... line6** for STM-N/OC-N line ports.

3 Select the port AID in the drop-down-list box **Assigned Port AID**.

IF	THEN
the selected timing reference shall not be used,	select NOT-CONNECTED
the selected timing reference is extref1	select exttmg0
the selected timing reference is extref2	select exttmg1
the selected timing reference is line1 ... line6 and the corresponding SDH/SONET port is not yet assigned,	click on Browse... and select the SDH/SONET port which shall be used as timing reference. You can either select one STM-16/OC48 or one STM-64/OC192 signal. Result: The window Select Line Timing Port AID opens.
the selected timing reference is line1 ... line6 and the corresponding SDH/SONET port is already assigned,	- Result: the respective port AID is displayed in the list box Assigned Port AID .
the selected timing reference is line1, line2, line3, line4, line5 or line6 and you want to assign a new SDH/SONET signal as timing reference,	select NOT-CONNECTED first in order to disable the currently assigned SDH/SONET port, and then select the new SDH/SONET port via Browse...

4 Select the timing quality belonging to the timing reference in the drop-down list box **Provisioned Quality Level**. For **line1 ... line6** select **AUTO**. This means that the timing marker is evaluated. For **extref1** and **extref2** assign the actual quality level of the external timing source.

Result:

The timing references are now used in the order of their quality level.

-
- 5 Select in the drop-down list box **System Timing Reference Priority** the priority of the selected timing reference. The values can be
- **Disable** (initial value)
 - **1, 2, 3, 4, 5, 6, 7, or 8**

Make sure that all configured timing references have different priorities assigned.

Result:

A priority list is created for the configured timing reference signals. Initially the signal with the highest quality level is used as timing reference signal. If it fails, the system switches to the signal with the next lower quality level. If there are several timing references with the same quality level, they are used according to the priority list. If all possible timing reference signals fail, the timing generator enters the holdover mode.

-
- 6 Select the **ASAP Name** Alarm Severity Assignment Profile. Via the push-button **Browse...** you can select the alarm in the drop-down list box. Click on **OK** to apply your setting.

By clicking on the push-button **ASAP Details...** you can call up a table with details on the ASAPs.

-
- 7 Apply the changes by clicking on **Apply**. If you wish to discard the changes click on **Cancel**.

-
- 8 Repeat Step 2 to Step 7 until all timing references are configured. Click on **OK** to close the window.

END OF STEPS



Configuring the system timing

When to use Use this procedure to configure the system timing.

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Viewing the timing configuration” (6-3)
- “The System Timing Parameters tab” (6-15)

Before you begin Prior to performing this procedure, you must have completed the following provisioning task:

Administrative tasks, such as a setup of user profiles (cf. Chapter 2, “Security administration”) and provisioning of management communication via DCN (cf. Chapter 3, “Management communication setup”).

Required privilege code

You must have at least a privilege code of P3 to configure the system timing.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to configure the system timing:

- 1 Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronization Characteristics** appears.

- 2 Select the **System Timing Parameters** tab.
-

- 3 Select the **System Timing** tab.

-
- 4 Select the clock mode in the group box **Clock Mode**. Click on the respective radio button. You can select the following values:
- **Free Running** (The system is synchronized to the internal oscillator.)
 - **Locked** (The system is synchronized to a timing reference signal.)

During normal operation in a network, the timing generator should be locked to a timing reference signal as far as available. Normally the free-running mode is used directly after the system start.

Result:

If you select **Free Running** a warning window appears.

“Switching the timing clock from locked to free running can temporarily result into transmission errors.”

- 5 Enable or disable the use of **System SSM Mode** by selecting **QL Disable** or **QL Enable**. This means that the selection of timing reference for the system timing is either determined only by the provisioned priority list or by the quality level given by the timing marker (SSM, Synchronization Status Message) and secondly by the priority list. Click on the respective radio button.
-

- 6 Select the wait-to-restore time in the group box **Wait To Restore**. Click on the respective radio button. The values can be:
- **0** (initial value)
 - **20 SEC**(SONET mode only)
 - **1 Minutes ... 60 Minutes** (selectable via a spin box)
 - **Infinite** (SONET mode only)

The wait-to-restore time is the wait which is made before every single switching from one timing reference to another.

- 7 Select the **ASAP Name** Alarm Severity Assignment Profile. Via the push-button **Browse...** you can select the alarm in the drop-down list box. Click on **OK** to apply your setting.
-

By clicking on the push-button **ASAP Details...** you can call up a table with details on the ASAPs.

.....

- 8 Apply the changes by clicking on **OK**. If you wish to discard the changes, click on **Cancel**.

END OF STEPS

.....



Forced Switching of the timing generator to the holdover mode

- When to use** Use this procedure to switch between different clock modes:
- **Clear Mode Switch**
This means that a current Forced Switch condition is reset.
 - **Force to Holdover**
The timing generator is switched to the holdover mode.

- Related information** For related information, see:
- Chapter 17, “Timing provisioning concepts”

- Before you begin** Prior to performing this task, verify that a *WaveStar*® CIT is connected and logged into the *LambdaUnite*™ MSS system.

Required privilege code

You must have at least a privilege code of M4 to change the system clock mode.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

- Instructions** Complete the following steps to change the clock mode:
-

- 1 Select **Clock Mode Switch** via **Fault** → **Timing/Sync Protection Switch** in the system view of the CIT.

Result:

The window **System Timing Clock Mode Protection Switch** appears.

- 2 Select the switch command in the field **Switch Type**. You can select the following values via a radio button:
 - **Clear Mode Switch**

This command clears the Forced Switch condition. If the system clock is switched to the holdover mode by the Forced Switch command, this will be reset. The **Clear Mode Switch** command does not affect the state of the automatic protection switching based on synchronization reference failure.

- **Force to Holdover**

The **Force to Holdover** command causes the system clock to be switched to the holdover mode regardless of the state of the timing references.

The mode switch is not carried out when the clock is provisioned for the free running mode.

-
- 3** Apply the changes by clicking on **OK**. If you wish to discard the changes, click on **Cancel**.

Important! After a switch to holdover or a clear mode switch, it takes the system about 7 minutes to stabilize the holdover filter. So don't do any further timing action during these 7 minutes.

Result:

The window **Clock Mode Switch** closes.

END OF STEPS



Switching to another timing reference

When to use Use this procedure to switch between different timing reference signals and to apply certain switch requests to a selected reference:

- **Clear Reference Switch**
- **Forced Switch**
- **Manual Switch**
- **Lockout**
- **Clear Lockout**

Related information For related information, see:

- Chapter 17, “Timing provisioning concepts”
- “Configuring the timing references” (6-31)

Before you begin Prior to performing this task,

- verify that a *WaveStar*[®] CIT is connected and logged into the *LambdaUnite*[™] MSS system.
- configure the timing references sources for the system via **Configuration → Timing/Sync → Timing Reference...** (see “Configuring the timing references” (6-31)).
- verify that the timing generator is in the locked mode via **View → Timing/Sync → System Timing Parameters** (see “Parameters of the “Synchronization Characteristics” window” (6-5))

Please note that the switch requests are only applicable if the timing generator is locked to a timing reference source. When the system is provisioned to the free running mode, all present requests are cleared.

Required privilege code

You must have at least a privilege code of P1+M4 to perform the switch commands.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to switch to another timing reference:

- 1 Select **System Timing Reference Switch** via **Fault → Timing/Sync Protection Switch** in the system view of the CIT.

Result:

The window **System Timing Reference Switch** appears.

- 2 Select the switch request you want to perform in the drop-down list box **Switch Type**. The following switch requests are possible:
 - **Clear Reference Switch**
removes any active external request (Lockout, Forced and Manual Switch). It cannot be denied. It can also be used to clear the Wait to Restore time. The Clear Reference Switch command does not affect the state of the automatic protection switching based on synchronization reference failure. If you select **Clear Reference Switch**, proceed to Step 4.
 - **Lockout**
allows manual selection of individual references, or manual disabling of individual references.
 - **Clear Lockout** disables the Lockout command.
 - **Manual Switch to Reference**
causes the system to be switched to the selected timing reference only if that timing reference is working fault free and no other external request is present.
 - **Forced Switch to Reference**
causes the system to be switched to the selected timing references regardless of the state of the timing reference. Only if a Clear Reference Switch or a Lockout command is present the Forced Switch is denied. A Forced Switch remains active until it is removed by a Clear Reference Switch or a Lockout command.
 - **Clear Wait to Restore**
disables the **Wait to Restore** command (see “Configuring the system timing” (6-34)).

-
- 3** Select the timing reference source to which you want to perform a switch request in the drop-down-list box **Timing Reference**. This can be:

- **extref1**
- **extref2**
- **line1 ... line6**

Result:

The AID of the respective timing reference is displayed in the **Port AID** information field. If no timing reference is defined, the drop-down list box and the information field are greyed out.

-
- 4** Apply the changes by clicking on **OK**. If you wish to discard the changes, click on **Cancel**.

Important! After a timing reference switch, it takes the system about 7 minutes to stabilize the holdover filter. So don't do any further timing action during these 7 minutes.

Result:

The window **System Timing Reference Switch** closes.

END OF STEPS





7 Traffic provisioning

Overview

Purpose This chapter describes the procedures which have to be performed for the traffic provisioning. This comprises basically the functions of the Cross Connection Wizard and the setup of network protections, such as MSP, MS-SPRing and SNCP.

Contents

Viewing existing cross-connections	7-3
Parameters of the window “View Cross Connections”	7-5
Retrieve Cross-connection Lists	7-8
Supporting information on the “Cross Connection List”	7-10
Substructuring of input and output signals	7-12
Creating a new cross-connection	7-16
Modifying a cross-connection	7-21
Rolling a cross-connection	7-23
Bridging a cross-connection	7-26
Deleting a cross-connection	7-29
Viewing an existing protection group	7-32

Parameters of the window “View Protection” for a 1+1 MSP or APS	7-34
Parameters of the window “View Protection” for a 2-Fiber MS-SPRing or 2-fiber BLSR	7-37
Parameters of the window “View Protection” for SNCP and UPSR	7-40
Creating a cross-connection in a 2-fiber MS-SPRing network environment	7-42
Creating a new 1+1 MSP or 1+1 APS (NE level)	7-46
Creating a new 2-fiber MS-SPRing (NE level)	7-49
Creating an SNCP or UPSR (NE level)	7-52
Deleting a protection group	7-56



Viewing existing cross-connections

When to use Use this procedure to query cross-connections in point-to-point, linear chain or ring applications. This also includes the protections on path level (SNCP, UPSR) belonging to the cross-connection.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Ring Protection” (18-20)
- “Line Protection” (18-18)
- “Configuring an optical SDH/SONET port” (4-16)
- “Configuring a tributary” (4-26)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P1, Provisioning, to query existing cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query existing cross connections:

- 1** Call up the window **View Cross Connections** via **View** → **Cross Connections...** in the **System View** of the *WaveStar* CIT.

- 2** Select in the tab **Ptn Grp** the required element for which you would like to query the cross-connection. This can be the shelf, a circuit pack, port or tributary. Activate the selection via double click or via the pushbutton **Select**.

Alternatively you can directly type the AID of the required element in the text box **Enter AID**.

Result:

The window **View Cross Connections for UNITE** opens. The displayed parameters are described in the chapter “Parameters of the window “View Cross Connections”” (7-5)

The window **View Cross Connections for UNITE** also can be reached via a right mouse on the respective port in the **System View** window.

END OF STEPS



Parameters of the window “View Cross Connections”

Overview	The window View Cross Connections consists of two tabs which are described in this chapter.
The <i>Equipment</i> tab	The window displays information on the inserted circuit packs, ports and tributaries.
Hierarchical structure	The network element components are organized in a tree structure from the system level down to the tributaries. Components of a lower level become visible by clicking on the “+” in front of a higher level component. You can select the components according to the following hierarchy: <i>system-bay-shelf-circuit pack/slot-port-tributary</i> This hierarchy is also used for the AIDs (cf. “Overview of access identifiers” (15-8))
The <i>Ptn. Grp</i> tab	The tab Ptn. Grp. is very similar to the tab Equipment . The shelf, circuit packs, ports and tributaries can also be selected on this tab. Additionally the tab contains information about the participation of a port in a protection group. For further information on protection, please refer to “Protection mechanisms” (18-12).
The <i>View Cross Connections for UNITE</i> window	After the selection of the required element the window View Cross Connections for UNITE opens. In this window all cross-connections belonging to the selected network element component are displayed.

Data in the information field In the information field the following values are displayed:

Value	Meaning
Src	The AID(s) for the source tributary/tributaries
Src Node NE Name	20-character TID which has been assigned to the Source Node TID (cf. Chapter 14, “Management communication setup concepts”). If a TID has not been associated with the source, “.” is displayed.
Role	The values Wkg and Prot are possible. This parameter shows whether a cross-connection is the working or the protection leg of a path protected cross-connection.
Type	The cross-connection type. The values 1-Way , 2-Way and UPSR/SNCP Ring Add, Drop are possible.

Value	Meaning
Rate	The rate associated with the cross-connection. The values STS1 , STS3 , STS12 , STS48 , STS192 , VC3 , VC4 , VC44c , VC416c and VC464c are possible.
Dest.	The AID(s) for the destination tributary/tributaries
Dest. Node NE Name	The 20 character TID which has been assigned to the Destination Node TID (cf. Chapter 14, “Management communication setup concepts”). If a TID has not been associated with the destination, “-” is displayed.

A certain cross-connection can be selected in the information field. Then further information on that cross-connection is displayed in the group boxes below.

The *Loopback* information field

The information field **Loopback** reflects the loopback status of a cross-connection. It indicates if any of the tributaries of the cross-connections is involved in a loop. Thus the values **Yes** or **No** are possible.

The *Output Mode Source to Destination* information field

The following values for the provisioned **Output Mode** are possible:

- **NORM** refers to a cross-connection which is carrying “normal” traffic.
- **AIS** is a test and maintenance setting. An AIS is transmitted via the respective cross-connection.
- **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.

The *Output Mode Destination to Source* information field

The following values for the provisioned **Output Mode** are possible:

- **NORM** refers to a cross-connection which is carrying “normal” traffic.
- **AIS** is a test and maintenance setting. An AIS is transmitted via the respective cross-connection.
- **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.

In the case of a 1-way cross connection this field is greyed out.

XC Num information field

The information field **Source to Destination Cross Connection Number** respectively **Destination to Source Cross Connection Number** displays an up to 9 digit number which is associated with the cross connection

XC Appl information field The information field **Source to Destination Cross Connection Application** respectively **Destination to Source Cross Connection Application** displays the application associated with the cross connection.

The possible values are:

- Unknown
- 2-Way Point-to Point
- 1-Way Point-to Point
- UPSR/SNCP Ring Add, Drop

Pushbuttons The pushbutton **Browse** leads back to the window **View Connection** where you can select a shelf, circuit pack, port or tributary.

The pushbutton **Refresh** updates the window.

Via the pushbutton **Save As** it is possible to save the displayed data in a text file.

Via the pushbutton **View Graphic** the selected cross-connection is graphically displayed.

Via the pushbutton **Print** the information about the selected cross-connection will be printed.

Via the pushbutton **Close** the window is closed.



Retrieve Cross-connection Lists

When to use	Use this procedure to retrieve information on existing protection cross connections in point-to-point, linear chain or ring applications. This also includes the protections on path level (SNCP, UPSR) belonging to the cross-connection.
Related information	For related information, see: • “Cross-connection management” (18-2) • “Ring Protection” (18-20) • “Line Protection” (18-18) • “Configuring an optical SDH/SONET port” (4-16) • “Configuring a tributary” (4-26)
Before you begin	Prior to performing this task, you must be logged into the <i>WaveStar</i>® CIT and the respective network element. Required privilege code You must have at least a privilege code of P1, Provisioning, to query existing cross connections. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Complete the following steps to query existing cross connections: 1 Call up the window CrossConnection List via Reports → Cross Connection List... in the System View of the <i>WaveStar</i> CIT. 2 Select in the tab Ptn Grp the required element for which you would like to query the cross-connection. This can be the shelf, a circuit pack, port or tributary. Activate the selection via double click or via the pushbutton Select. Alternatively you can directly type the AID of the required element in the text box Enter AID.

Result:

The **CrossConnection List** opens. The displayed parameters are described in the chapter “Supporting information on the “Cross Connection List”” (7-10)

END OF STEPS



Supporting information on the “Cross Connection List”

Overview The **CrossConnection List** displays information on the selected cross connection.

Displayed Data The following data are displayed:

Value	Meaning
Src	The AID(s) for the source tributary/tributaries
Src Node NE Name	20-character TID which has been assigned to the Source Node TID (cf. Chapter 14, “Management communication setup concepts”). If a TID has not been associated with the source, “-” is displayed.
Role	The values Wkg and Prot are possible. This parameter shows whether a cross-connection is the working or the protection leg of a path protected cross-connection.
Type	The cross-connection type. The values 1-Way , 2-Way and UPSR/SNCP Ring Add, Drop are possible.
Rate	The rate associated with the cross-connection. The values STS1 , STS3 , STS12 , STS48 , STS192 , VC3 , VC4 , VC44c , VC416c and VC464c are possible.
Dest.	The AID(s) for the destination tributary/tributaries
Dest. Node NE Name	The 20 character TID which has been assigned to the Destination Node TID (cf. Chapter 14, “Management communication setup concepts”). If a TID has not been associated with the destination, “-” is displayed.
Source to Destination Cross Connection Application	Displays the application associated with the cross connection. The possible values are: • Unknown • 2-Way Point-to Point • 1-Way Point-to Point • UPSR/SNCP Ring Add, Drop
Source to Destination Cross Connection Number	Displays an up to 9 digit number associated with the cross connection.
Destination to Source Cross Connection Application	Displays the application associated with the cross connection. The possible values are: • Unknown • 2-Way Point-to Point • 1-Way Point-to Point • UPSR/SNCP Ring Add, Drop
Destination to Source Cross Connection Number	Displays an up to 9 digit number associated with the cross connection.

Value	Meaning
Source to Destination Output Mode	The following values for the provisioned Output Mode are possible: • NORM refers to a cross-connection which is carrying “normal” traffic. • AIS is a test and maintenance setting. An AIS is transmitted via the respective cross-connection. • IDLE/UNEQ is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.
Destination to Source Output Mode	The following values for the provisioned Output Mode are possible: • NORM refers to a cross-connection which is carrying “normal” traffic. • AIS is a test and maintenance setting. An AIS is transmitted via the respective cross-connection. • IDLE/UNEQ is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.
Loopback Status	Reflects the loopback status of a cross-connection. It indicates if any of the tributaries of the cross-connections is involved in a loop. Thus the values Yes or No are possible.

Pushbuttons The pushbutton **Refresh** updates the window.

Via the pushbutton **Save As** it is possible to save the displayed data in a text file.

Via the pushbutton **Print** the information about the selected cross-connection will be printed.

Via the pushbutton **Close** the window is closed.



Substructuring of input and output signals

When to use Use this procedure to create a substructure for input and output signals of one or more optical port(s) of the same type for the operation of a *LambdaUnite*[™] MSS system. This procedure is part of the cross-connection switching. Before a cross-connection can be created the substructure of the input and output signals must be defined.

Related information For related information, see:

- “Port and tributary provisioning” (15-15)
- “Reassigning a circuit pack” (4-14)

Before you begin Prior to performing this task, you must insert the optical port unit you want to configure into the correct slot of the shelf. Furthermore, the circuit pack provisioning must be completed before a certain port can be configured (cf. “Slot/circuit pack provisioning” (15-14) and “Reassigning a circuit pack” (4-14)).

You must be logged into the *WaveStar*[®] CIT and the respective network element.

You have to know which cross-connection are to be switched. The outgoing signal of a port must have the same substructure like the incoming signal of the port to which it is connected.

Required privilege code

You must have at least a privilege code of P3+M1 to create a substructure.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps in order to create the substructure for input and output signals of one or more optical port(s):

- 1 In the **System View** of the *WaveStar* CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window.

Result:

On the left side of the window, the equipment selection tab becomes visible. The shelf belonging to the system is listed.

- 2 Double click on the shelf or click on the **+** in front of the shelf name.

Result:

The list of circuit packs and slots which are available becomes visible.

- 3 Select the desired optical port unit. Double click on the port unit or click on the **+** in front of the unit name.
-

- 4 Select the desired port (type). Click on the **Provision** pushbutton.

Result:

On the right side of the window the provisionable parameters are displayed.

- 5 For substructuring the input signal click on the button **Use Form** next to the text box **Input Signal Rate List**.

Result:

The window **Signal Rate Entry Form for Input Signal Rate List** opens.

The substructuring is a prerequisite for the cross-connection switching. Configure the substructure according to the cross-connection plan for the respective network element.

First select a signal rate, then select all tributaries which are necessary to fill the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**.

Substructuring should be made by clustering tributaries, i.e. using subsequent time slots in the signal. The following tributaries can be selected:

- VC-3, VC-4, VC4-4C, VC4-16C and VC-4-64C for STM-16 and STM-64 (in SDH Standard)
- STS-1c, STS-3c, STS-12c, STS-48c, STS-192c for OC-48 and OC-192 (in SONET Standard)

The final substructure is displayed in the text box **Input Signal Rate List**. The final substructure is displayed in the text box **Input Signal Rate List** in the following form **<NX-NX-NX-...>**. X= **3, 4, 4C, 16C, 64C** in SDH Standard. In SONET Standard X= **1, 3, 12, 48, 192**. X is the transmission rate. N is the number of subsequent X.

- 6 For substructuring the output signal click on the button **Use Form** next to the text box **Unequipped Output Signal**.

Result:

The window **Signal Rate Entry Form for Unequipped Output Signal** opens.

First select a signal rate, then select all tributaries which are necessary for the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**.

Substructuring should be made by clustering tributaries, i.e. using subsequent time slots in the signal. The following tributaries can be selected:

- VC-3, VC-4, VC4-4C, VC4-16C and VC-4-64C for STM-16 and STM-64 (in SDH Standard)
- STS-1c, STS-3c, STS-12c, STS-48c, STS-192c for OC-48 and OC-192 (in SONET Standard)

The final substructure is displayed in the text box **Unequipped Output Signal**. The final substructure is displayed in the text box **Unequipped Output Signal** in the following form **<NX-NX-NX-...>**. X= **3, 4, 4C, 16C, 64C** in SDH Standard. In SONET Standard X= **1, 3, 12, 48, 192**. X is the transmission rate. N is the number of subsequent X.

-
- 7 Select the destination port(s) in the **Apply To:** drop-down listbox. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack or to all ports on this type in the shelf. By using the latter options, you can decrease your provisioning time significantly.
-
- 8 Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.
-

END OF STEPS

Example

64–303 for an STM-16 port designates a substructure of 6 VC-4 (timeslots 111 to 221) and 30 VC-3 (timeslots 231 to 443).

The following figure shows the **Signal Rate Entry Form for Input Signal Rate List** window. It shows the substructure of an STM-16 signal with 33 VC-3, 1 VC-4 and 1 VC-4-4c.

The image shows a software window titled "Signal Rate Entry Form for Input Signal Rate List". Inside the window, there is a text box that says "Select a signal rate, then choose the tributary. By holding down the shift key while selecting, you may choose a range of tributaries." Below this, there are three sections: "Rate Selection", "Tributaries", and "Selections".

The "Rate Selection" section contains three radio buttons: "VC3" (selected), "VC4", and "VC4-4c". There are also small colored bars (green, blue, red) next to each radio button.

The "Tributaries" section shows a horizontal bar with a grid of small squares. The squares are colored green, blue, and red. The numbers 111, 131, 211, 231, 311, 331, 411, 431, and 443 are displayed below the bar.

The "Selections" section contains three lines of text: "Selected Rate: VC3", "Selected Tributary:", and "Current Rate List: 93-14-14c-243".

At the bottom of the window, there are two buttons: "OK" and "Close".

Creating a new cross-connection

When to use Use this procedure to provision unprotected cross-connections in point-to-point, linear-chain or ring applications.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Ring Protection” (18-20)
- “Line Protection” (18-18)
- “Configuring an optical SDH/SONET port” (4-16)
- “Configuring a tributary” (4-26)
- “Creating a cross-connection in a 2-fiber MS-SPRing network environment” (7-42)
- “Creating an SNCP or UPSR (NE level)” (7-52)

Before you begin Prior to performing this task, you must complete the port provisioning, including protection provisioning, for any port which is involved in the cross-connection.

Generally, an end-to-end link requires that a series of cross-connections (involving multiple ports and NEs) have to be provisioned for pre-service testing or re-arrangements. It is recommended to complete the cross-connections starting from:

1. One of the add/drop NEs,
2. continuing sequentially through all intermediate NEs, and
3. ending with the alternate add/drop NE.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.(For some fields privilege code M1 is required).

Required equipment

The following equipment is required to perform this task:

- WaveStar[®] CIT

Instructions

**CAUTION**

cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.

Complete the following steps to create a new cross-connection:

- 1 Call up the **Cross-Connection Wizard** via **Configuration → Cross-Connections...** in the **System View** of the *WaveStar* CIT.
- 2 Click on the radio button **Create a new cross-connection** and click on **Next>**.

Result:

Screen 1 appears.

- 3 Define the cross-connection rate in the drop-down list box **Rate:**. The following values are possible:
 - **VC-3**(default value)
 - **VC-4**
 - **VC-4-4c**
 - **VC-4-16c**
 - **VC-4-64c**
 - **STS-1**
 - **STS-3**
 - **STS-12**
 - **STS-48**
 - **STS-192**

Please note that it is not possible to proceed to the next window before selecting the cross-connection rate.

-
- 4 Define the type of cross-connection by clicking on the respective radio button in the group box **Type of Cross-connection**. The following values are possible:

- **2-Way Point-to-Point** (default value)
- **1-Way Point-to-Point**
- **UPSR/SNCP Ring Add, Drop**

If you are creating 1-way or 2-way cross-connections within a ring which is protected by a 2-fiber MS-SPRing please note the additional hints in “Creating a cross-connection in a 2-fiber MS-SPRing network environment” (7-42).

If you are creating a cross-connection which is protected by a Sub-Network Connection Protection (SNCP) or Unidirectional Path-Switched Ring (UPSR) please refer to “Creating an SNCP or UPSR (NE level)” (7-52).

-
- 5 Click on **Next>** to proceed to the next window.

Result:

Screen 2 of 3 opens.

-
- 6 Click on **Select...** to select the source tributary.

Result:

The **Ptn Grp** selection tab appears. In the list box of the **Ptn Grp** selection tab the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted.

-
- 7 Select one port in the list or enter the AID in the text box **Enter AID:** above.

Result:

In the list box **Tributary** on the right, the AIDs of all VCs/STSs belonging to the respective port are displayed.

-
- 8 Select the VC/STS which shall be used as the source and click on the **Select...** button.
-

- 9 Select the destination port in the **Ptn Grp** selection tab and the corresponding VC/STS in the **Tributary** list box and click on the **Select...** button.

Result:

On **Screen 2 of 3** both, the source and destination tributary, are displayed.

- 10 Click on the **Next>** button.

Result:

The **Screen 3 of 3** opens.

The current data of the cross connection are displayed.

If you are creating an unprotected cross-connection you can set the values of the provisionable parameters of the specified cross-connection via this window. Configuration data is described in “Parameters of the window “View Cross Connections”” (7-5).

- 11 The fields **XC Application**, **Source NE Name** and **Destination NE Name** are view only and display the previous decisions.
-

- 12 Select the **Output Mode** in the group boxes **Source to Destination** and **Destination to Source**. The following values are possible:

- **NORM**
- **AIS**
- **IDLE/UNEQ**

Result:

The selected settings have the following consequences:

- With the setting **NORM**, a normal payload signal is transmitted.
- With the setting **AIS**, an AIS is inserted in the signal for test and maintenance purposes.
- With the setting **IDLE/UNEQ**, an unequipped signal is transmitted for test and maintenance purposes.

-
- 13** Type a number for the cross connection in the field **XC Number** or use the automatically generated one.
-

- 14** Click on the **Finish** button to apply your settings.

Result:

In case of one (or two) unprotected ports, a confirmation window appears. If you are sure, confirm.

END OF STEPS

.....



Modifying a cross-connection

When to use Use this procedure to modify existing cross connections in point-to-point, linear-chain or ring applications.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Viewing existing cross-connections” (7-3)

Before you begin Check the parameters of the cross-connection you wish to modify in the window **View Cross-Connections**. (cf. “Viewing existing cross-connections” (7-3))

Required privilege code

You must have at least a privilege code of P3 to modify cross-connections. (For some fields privilege code M1 is required).

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions



CAUTION

cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.

Complete the following steps to modify a cross-connection:

- 1 Call up the **cross-connection Wizard** via **Configuration** → **Cross-Connection...** in the **System View** of the WaveStar CIT.
 - 2 Click on the radio button **Modify parameters on an existing Cross-Connection** and click on **Next>**.
-

Result:

Screen 1 appears.

In the list box of the **Equipment** selection tab, the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs and ports is depicted.

- 3** Select one port in the list or enter the AID in the text box **Enter AID:** above.

Result:

In the list box on the right the AIDs of all sources and destinations of cross-connections belonging to the respective port are displayed.

- 4** Select the cross-connection which shall be modified and click on the **Next>** button.

Result:

Screen 2 opens. If you have selected a one-way cross-connection, go to Step 6.

- 5** Select the desired leg (two-way cross-connections have two legs) and click on the **Next>** button.

Result:

Screen 3 opens. In this window you can set the values of the provisionable parameters of the specified cross-connection.

- 6** Modify the desired parameters and click on the **Finish** button to apply your changes.

END OF STEPS



Rolling a cross-connection

When to use Use this procedure to “roll” a cross connection leg from one tributary source to another. This means you can choose a new source for an existing cross connection.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Configuring an optical SDH/SONET port” (4-16)
- “Configuring a tributary” (4-26)

Before you begin Prior to performing this task, you must complete the port provisioning, including protection provisioning, for any port which is involved in the cross-connection.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to roll cross-connections. (For some fields privilege code M1 is required.)

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions



CAUTION

cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.

Complete the following steps to roll a cross-connection:

- 1 Call up the **cross-connection Wizard** via **Configuration** → **cross-connection...** in the **System View** of the WaveStar CIT.

-
- 2 Click on the radio button **Roll a cross-connection leg from one tributary source to another** and click on **Next>**. Via the check box **Signal Rate Auto Set** you can select whether the signal rate of the existing cross-connection is also used for the new one. As default value **Signal Rate Auto Set** is activated.

Result:

Screen 1 appears.

- 3 Select the desired port on the **Ptn Grp** tab.

Result:

All cross-connections belonging to the respective port are displayed on the table on the right side of the window. The type and signal rate are of the cross-connections are also displayed.

- 4 Select a cross-connection on the right table. Finally click on **Next>**.

Result:

Screen 2 appears

- 5 Click on the cross-connection leg you want to roll. You may only choose one leg. Then click on **Next>**.

Each leg of a two-way cross-connection is treated as a one-way cross-connection. If the roll function is applied for one leg, first this leg is removed and a new one is created with another tributary source. The second leg remains untouched.

Result:

The **New Source Tributary** window appears

- 6 Select a new source for the cross-connection. First select a port on the **Ptn Grp** tab.

Result:

The AID of all VCs belonging to this port are displayed on the table on the right side of the window. Furthermore it is shown

whether a VC is already involved in a cross-connection and if it is protected.

-
- 7 Select the tributary which shall be used as a new source and click on the **Next>** button.

Result:

Screen 3 opens. In this window you can set the values of the provisionable parameters of the specified cross-connection. The **Screen 3** also contains a view of the configured changes. Furthermore configuration data is displayed.

-
- 8 Select the source and the destination TID in the drop-down list boxes **New Src NE Name:** and **Destination NE Name:**

This field only applies to a leg which is part of an MS-SPRing (Multiplex Section Shared Protection Ring).

-
- 9 Click on the **Finish** button to apply your settings.

END OF STEPS



Bridging a cross-connection

When to use Use this procedure to bridge a cross-connection leg of an existing cross-connection from the tributary source to a second destination tributary. This means you can create a broadcast from one source to two destination tributaries.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Configuring an optical SDH/SONET port” (4-16)
- “Configuring a tributary” (4-26)

Before you begin Prior to performing this task, you must complete the port provisioning, including protection provisioning, for any port which is involved in the cross-connection.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to bridge cross-connections. (For some fields privilege code M1 is required.)

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions



CAUTION

cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.

Complete the following steps to roll a cross-connection:

- 1 Call up the **Cross-Connection Wizard** via **Configuration** → **Cross-connection...** in the **System View** of the WaveStar CIT.

-
- 2 Click on the radio button **Bridge a cross-connection from a source tributary** and click on **Next>**. Via the check box **Signal Rate Auto Set** you can select whether the signal rate of the existing cross-connection is also used for the new one. As default value **Signal Rate Auto Set** is activated.

Result:

Screen 1 appears.

- 3 Select the desired port on the **Ptn Grp** tab.

Result:

All cross-connections belonging to the respective port are displayed on the table on the right side of the window. The type and signal rate are of the cross-connections are also displayed.

- 4 Select a cross-connection on the right table. Finally click on **Next>**.

Result:

Screen 2 appears

- 5 Click on the cross-connection you want to bridge. You may only choose a one-way cross-connection. Then click on **Next>**.

Result:

The **New Destination Tributary** window appears.

- 6 Select a new destination for the cross-connection. First select a port on the **Ptn Grp** tab.

Result:

The AID of all VCs or STSs belonging to this port are displayed on the table on the right side of the window. Furthermore it is shown whether a VC or STS is already involved in a cross-connection and if it is protected.

- 7 Select the tributary which shall be used as a new destination and click on the **Next>** button.
-

Result:

Screen 3 opens. In this window you can set the values of the provisionable parameters of the specified cross-connection. The **Screen 3** also contains a view of the configured changes. Furthermore configuration data is displayed.

-
- 8** Select the source and the destination TID in the drop-down list boxes **Src NE Name:** and **New Destination NE Name:**

This field only applies to a leg which is part of an MS-SPRing (Multiplex Section Shared Protection Ring) or BLSR (Bidirectional Line-Switched Ring).

-
- 9** Click on the **Finish** button to apply your settings.

END OF STEPS



Deleting a cross-connection

When to use Use this procedure to delete cross connections in point-to-point, linear-chain or ring applications.

Related information For related information, see:

- “Cross-connection management” (18-2)
- “Creating a new cross-connection” (7-16)
- “Configuring an optical SDH/SONET port” (4-16)
- “Configuring a tributary” (4-26)

Before you begin In order to prevent a service interruption, the traffic provided on the respective path must have previously been removed (e.g. rerouted to another path) before deleting any of the cross-connections included in that path. The recommendation is that cross-connections be deleted starting from

1. one of the add/drop NEs,
2. continuing sequentially through all intermediate NEs, and
3. ending with the alternate add/drop NE.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to delete cross-connections. (For some fields privilege code M1 is required).

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Complete the following steps to delete a cross-connection:

- 1 Call up the **cross-connection Wizard** via **Configuration** → **cross-connection...** in the **System View** of the WaveStar CIT.

- 2 Select the option **Delete leg(s) of an existing cross-connection** and then click on the **Next>** button.

Result:

The **Screen 1** appears.

In the list box of the **Equipment** selection tab the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs and ports is depicted.

- 3** Select one port in the list or enter the AID in the text box **Enter AID:** above.

Result:

In the list box on the right the AIDs of all sources and destinations of cross-connections belonging to the respective port are displayed.

- 4** Select the cross-connection which shall be deleted and click on the **Next>** button.

Result:

Bidirectional cross-connection → **Screen 2** opens. Proceed with next step.

Unidirectional cross-connection → **Screen 3** opens. It contains the parameters of the cross-connection that is to be deleted. Go to step 6.

- 5** Select the leg(s) of the cross-connection you want to delete and click on the **Next>** button

Result:

Screen 3 opens. This window contains the parameters of the cross-connection which is to be deleted.

- 6** Review the data. Click on **<Back** to make any corrections, click on **Cancel** to discard your changes or click on **Finish>** to delete the cross-connection.

Result:

If you have clicked on the **Finish>** button a **Confirm** box opens.

-
- 7** Review the accuracy of the entries in the **Confirm** box and, as appropriate, check **Yes** or **No**.

END OF STEPS



Viewing an existing protection group

When to use Use this procedure to query the current status of a protection group. It can be used for all kinds of protection.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Line Protection” (18-18)
- “Ring Protection” (18-20)
- “Path Protection” (18-13)

Before you begin Prior to performing this task you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of M4, Maintenance, to view an existing protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the status of a protection group:

- 1 Call up the window **View Protection** via the menu **View** → **Protection...** in the **System View** of the *WaveStar* CIT.

- 2 Select the components of the required protection group in the tab **Ptn Grp** on the left side of the window.

Reference:

The displayed parameters are described in “Parameters of the window “View Protection” for a 1+1 MSP or APS” (7-34).

END OF STEPS

**Alternative instruction for
SNCP and UPSR**

- 1 Call up the window **Path Protection Group Names** via the menu **View → Path Protection Group Names** and select the desired path protection group.

END OF STEPS



Parameters of the window “View Protection” for a 1+1 MSP or APS

Status data The following table shows the status data which is shown in the **View Protection** window for an optical port protection (MSP or APS).

Information field	Possible value	Meaning
Protection Group AID	cf. “Overview of access identifiers” (15-8)	The AID defined for the selected protection group.
Protection Type	1+1 Optical Port Protection	SDH: 1+1 MSP, SONET: 1+1 Automatic Protection Switching
Optical Line Rate	SDH: STM16 SONET: OC48	
Protocol	Unidirectional	Each transmission direction is monitored separately and switched over if necessary. This can lead to a situation in which only one direction is transmitted via the main section and the other direction via the standby section.
SDH: Working AID SONET: Working 1 AID	cf. “Overview of access identifiers” (15-8)	The port AID which has been assigned to be the working port.
SDH: Protection AID SONET: Working 2 AID	cf. “Overview of access identifiers” (15-8)	The port AID which has been assigned to be the protection port.
Protection Group Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm status associated with the protection group. The alarm format (CR/MJ/MN or PR/DF/INF) is configurable via the Preferences window (cf. Chapter 22, “WaveStar® CIT Tutorial”).
SDH: Working Port Alarm Status SONET: Working 1 Port Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm status associated with the working port. The alarm format (CR/MJ/MN or PR/DF/INF) is configurable via the Preferences window (cf. Chapter 22, “WaveStar CIT Tutorial”).
SDH: Working Fault Status SONET: Working 1 Fault Status	Signal Failure, Signal Degrade, None	Switch initiation reason associated with the working port
SDH: Protection Port Alarm Status SONET: Working 2 Port Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm status associated with the protection port. The alarm format (CR/MJ/MN or PR/DF/INF) is configurable via the Preferences window (cf. Chapter 22, “WaveStar CIT Tutorial”).
SDH: Protection Fault Status SONET: Working 2 Fault Status	Signal Failure, Signal Degrade, -	Switch initiation reason associated with the protection port
Active Port	Working (<port AID>), Protection (<port AID>)	Indicates which port is carrying traffic

Information field	Possible value	Meaning
Switch Request State	Lockout, Forced Switch , Signal Failed, Signal Degraded, Manual Switch, No Request, Do Not Revert, Failure of Protocol	Indicates whether a manually or automatically initiated switch has occurred and whether the MSP is activated. For the meaning of the Switch Requests please refer to “Switch request state” (7-41).
Near-End Outgoing APS Message	Lockout, Forced Switch, No Request, Signal Failed, Signal Degraded, Manual Switch, Do Not Revert, Reverse Request	The outgoing Automatic Protection Switch Message, please refer to “Switch request state and APS messages” (7-35).
Near-End Outgoing Request Selection	Working/Working 1(<port AID>), Protection/ Working 2 (<port AID>), None	
Far-End Incoming APS Message	Lockout, Forced Switch, No request, Signal Failed High, Signal Failed Low Signal Degraded High, Signal Degraded Low, Manual Switch, Do Not Revert, Reverse Request	cf. “Switch request state and APS messages” (7-35)
Far-End Incoming Request Selection	Working/Working 1 (<port AID>), Protection/Working 2 (<port AID>), Invalid, None	
Alarm Severity Assignment Profile	<24-character string>	Designation of the corresponding ASAP

Important! If the protection line is interrupted the K1/K2 byte
protocol is no longer transmitted. Thus messages from the Far End
might be incorrect. In this case the network element on the receive
side marks the Far End Messages as **Invalid**.

Switch request state and APS messages

The following table shows the meaning of the switch request state and
the APS (Automatic Protection Switch) messages.

Switch Request State	Meaning
Lockout	Protection switching is deactivated. Traffic is carried on the working section. No switchover occurs in the event of a section fault.

Switch Request State	Meaning
Forced Switch	A forced switchover has been made from one section to the other (user action). This action can also be carried out to a faulty section. Automatic protection switching is deactivated as long as the Forced Switch is activated.
Signal Failed High	Signal failure on a section. An automatic switchover has been carried out. This state is valid for the SDH area (MSP), acc. to ETSI EN 300417.
Signal Failed Low	Signal failure on a section. An automatic switchover has been carried out. This state is valid for the SONET area (APS), acc. to Telcordia GR-253.
Signal Degraded High	The signal quality on a section is degraded. An automatic switchover has been carried out. This state is valid for the SDH area (MSP), acc. to ETSI EN 300417.
Signal Degraded Low	The signal quality on a section is degraded. An automatic switchover has been carried out. This state is valid for the SONET area (APS), acc. to Telcordia GR-253.
Manual Switch	A manual switchover has been made from one section to the other (user action). This action can be carried out to a fault-free section only. Automatic protection switching remains activated.
No Request	No switchover request exists
Do Not Revert	Can occur as the MSP operates in non-revertive mode. The working section is restored, but traffic remains on the protection section.
Failure of Protocol	Includes all other possible errors, which are not initiated by a user switch or a signal failure.
Invalid	The Far End APS messages are no longer valid as the protection line has failed.



Parameters of the window “View Protection” for a 2-Fiber MS-SPRing or 2-fiber BLSR

Description The **View Protection** window consists of five tabs, each describing a set of parameters:

- Protection Group
- Alarm Status
- Provisionable Parameters
- West Side
- East Side

Status data The following table shows the status data which is shown in the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
The tab Protection Group		
Protection Group AID	<two-digit character string> (cf. “Overview of access identifiers” (15-8))	The AID defined for the selected protection group.
Protection Type	SDH: 2-Fiber MS-SPRING SONET: 2-Fiber BLSR	
Optical Line Rate	SDH: STM16, STM64 SONET: OC48, OC192	SDH or SONET line-rate associated with the port
Interworking Type	SDH, SONET	-
Ring-ID	<ASCII character string> (up to 15 characters)	Ring ID for the selected protection group
West Port AID/East Port AID	cf. “Overview of access identifiers” (15-8)	Port AID of the west/east side which has been provisioned for the protection group
Ring Node APS State	Idle, Switching, Passthrough, Suspended-Idle, Suspended-Switching, Suspended-Passthrough	Switch status of the NEs of the respective MS-SPRing
The tab Alarm Status		
Protection Group Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm level of the protection group. The alarm format (CR/MJ/MN or PR/DF/INF) is configurable via the Preference window (cf. Chapter 22, “WaveStar® CIT Tutorial”).
West Port AID/East Port AID	(cf. “Overview of access identifiers” (15-8))	The AID defined for the West and the East Port of the respective NE

Information field	Possible value	Meaning
West AID Alarm Status/East AID Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm level for the West/East port. The alarm format (CR/MJ/MN or PR/DF/INF) is configurable via the Preference window (cf. Chapter 22, “WaveStar CIT Tutorial”).
The tab Provisionable Parameters		
Wait To Restore	0 ... 12 minutes, infinite	Displays the selected Wait-to-Restore time of the selected protection group.
Alarm Severity Assignment Profile	<24-character string>	The selected Alarm Severity Assignment Profile.
The tabs West Side and East Side		
East/West Switch Request State	LP-S Lockout of Prot. FS-R Forced Switch-Ring SF-R Signal Fail-Ring SD-R Signal Degrade-Ring MS-R Manual Switch-Ring WTR Wait to Restore RR-R Reverse Request - Ring NR No Request	Switch request for the outgoing west/east side
East/West Last Protection Switch Attempt Status	Success, Denied, Failed	Status of the last switch action.
East/West Switch Priority	LP-S Lockout of Prot. FS-R Forced Switch-Ring SF-R Signal Fail-Ring SD-R Signal Degrade-Ring MS-R Manual Switch-Ring WTR Wait to Restore RR-R Reverse Request - Ring NR No Request	K1 byte, bits 1-4.
East/West Destination Node ID	0 ... 15	Node ID associated with the protection group. K1 byte, bits 5-8
East/West Source Node ID	0 ... 15	Node ID associated with the Far End of the fiber. K2 byte, bits 1-4
East/West Protection Path	Short, Long	K2 byte, bit 5. The path of the rerouted traffic from the point of view of the regarded NE.

Information field	Possible value	Meaning
East/West Channel Status	Idle	The current channel status of the node.
	Bridged	
	Bridged and Switched	
	Not Used	
	RDI-L	
	AIS-L	

After the deletion of an MS-SPRing protection group and the following creation of a new group with the same ports in the K-Bytes to the neighbouring NEs, not the default values are sent, as would be expected, but some old values from the deleted group. After the ring recovery has been completed, the K-Byte information will be aligned to the new group.



Parameters of the window “View Protection” for SNCP and UPSR

Status data The following table shows the status data which is shown in the **View Protection** window for SNCP and UPSR.

Information field	Possible value	Meaning
Protection Group AID	cf. “Overview of access identifiers” (15-8)	The AID defined for the selected protection group.
Protection Type	Path	
Path Protection Group Name	<ASCII string with up to 24 characters>	
Cross Connection Rate	VC-3, VC-4, VC-4-4c, VC-4-16c	
Working Path	<source tributary AID>, <destination tributary AID>	Source and destination of the working path
Protection Path	<source tributary AID>, <destination tributary AID>	Source and destination of the protection path
Protection Group Alarm Status	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) or Prompt (PR), Deferred (DF), Info (INF)	The highest alarm status associated with the protection group.
Constituent Signal Type	VC-3, VC-4, VC-4-4c, VC-4-16c, STS-1, STS-3c, STS-12c, STS-48c	Cross-connection rate
Active Constituent	Working, Protection	Shows which path is actually active
Working Constituent	<source tributary AID>, <destination tributary AID>, cf. “Overview of access identifiers” (15-8)	
Protection Constituent	<source tributary AID>, <destination tributary AID>, cf. “Overview of access identifiers” (15-8)	
Switch Request State	cf. “Switch request state” (7-41)	
Working Fault Status	Signal Failed (SF), Signal Degraded (SD), None	Displays the failure condition of the working path
Protection Fault Status	Signal Failed (SF), Signal Degraded (SD), None	Displays the failure condition of the protection path
Revertive Mode	Enabled, Disabled	
Wait To Restore time	0 ... 60 minutes	Defines the time interval before the system switches back to the working path after restoration
Holdoff Timer	Enabled, Disabled	

Information field	Possible value	Meaning
Protection Type	SNC-I, SNC-N	This field is only applicable for an SDH path protection. It displays the type of path protection.
Alarm Severity Assignment Profile	<ASCII string with up to 24 characters>	Displays the Path Protection Switch Alarm Severity Assignment Profile

Switch request state The following table shows the meaning of the switch request state:

Switch Request State	Meaning
Lockout	Protection switching is deactivated. Traffic is carried on the working path. No switchover occurs in the event of a section fault.
Forced Switch	A forced switchover has been made from one path to the other (user action). This action can also be carried out to a faulty path. Automatic protection switching is deactivated as long as the Forced Switch is activated.
Signal Failed	Signal failure on a path. An automatic switchover has been carried out.
Signal Degraded	The signal quality on a section is degraded. An automatic switchover has been carried out.
Manual	A manual switchover has been made from one section to the other (user action). This action can be carried out to a fault-free section only. Automatic protection switching remains activated.
Wait To Restore	The working path is operable again. Traffic is still carried on the protection path. A wait is made for a defined time (wait-to-restore time) to see whether the working path is stable before traffic is switched back. Automatic switchback is carried out only if the protection group operates in revertive mode. Only in this case can a wait to restore time be defined.
No Request	No switchover request exists.



Creating a cross-connection in a 2-fiber MS-SPRing network environment

When to use Use this procedure to create cross-connections for traffic which is protected via a 2-fiber MS-SPRing.

Before you begin You must have a detailed knowledge on the network topology of the respective ring.

If you are creating cross-connections within a 2-fiber MS-SPRing, you have to create through-connections in each network element which is part of the protected route, as shown in the example below.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.

Required equipment

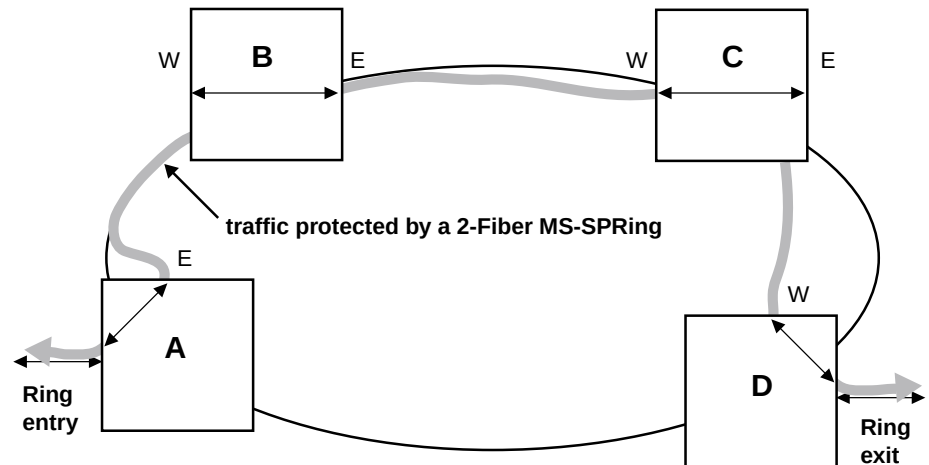
The following equipment is required to perform this task:

- WaveStar® CIT

Related information For related information, see:

- “Creating a new cross-connection” (7-16)
- “Creating a new 2-fiber MS-SPRing (NE level)” (7-49)

Example A bidirectional route which is protected by an MS-SPRing is established between NE A and NE D. In each NE in between a bidirectional cross-connection has to be created in order to route the traffic from NE A to NE D.



In order to avoid confusion with the source and destination of the cross-connection, which might cause traffic loss in case of a protection switch, it is highly recommended to start at one end of the route with the creation of the cross-connections and proceed from NE to NE and to keep always the same view of source and destination for the through-connection. This means that you should always switch the cross-connection, for example, from a tributary of the west port to a tributary of the east port, even if you are creating a bidirectional cross-connection. Of course you could also select source and destination the other way round, but you should keep the same view for all NEs on the protected route.

Instructions

- 1 **NE at ring entry:** Select a cross-connection **Source**. In the example the ring entry is NE A.
- 2

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection Destination the AID of a tributary belonging to an STM-64 port.

IF	THEN
the NE belongs to an STM-16 ring,	select as cross-connection Destination the AID of a tributary belonging to the STM-16 port which is interface to the MS-SPRing.

Result:
The **Source NE Name** is greyed out.

-
- 3** Select the **Destination NE Name**. It must be the TID of the NE at the end of the MS-SPRing route.

In the example the cross-connection switching is started at the NE A, the **Destination NE Name** is D.

-
- 4** Repeat Step 1 to Step 3 for all cross-connections which have to be created in the NE at the ring entry.

-
- 5** ***Intermediate NEs:***
- Create all cross-connections in the neighbour network element by keeping the same view of source and destination or east and west, respectively. First select the **Source** AID, then the **Destination** AID of the cross-connection. Proceed to the next window and select the **Source NE Name** and **Destination NE Name** of the protected route.
- In the example all cross-connections are switched from the cross-connection **Source** on the west port to the cross-connection **Destination** on the east port. Thus in NE B and NE C the **Source NE Name** is A and the **Destination NE Name** is D.

-
- 6** Repeat Step 5 for all NEs on the protected route.

-
- 7** ***NE at ring exit:***

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection Source the AID of a tributary belonging to an STM-64 port. In the example the ring exit is NE D.
the NE belongs to an STM-16 ring,	select as cross-connection Source the AID of a tributary belonging to the STM-16 port which is interface to the ring.

.....

8 Select a cross-connection **Destination**.

Result:

The **Destination NE Name** is greyed out.

.....

9 Select the **Source NE Name**. In the example it is A.

.....

10 Repeat Step 7 to Step 9 for all cross-connections in the NE at the ring exit.

END OF STEPS

.....



Creating a new 1+1 MSP or 1+1 APS (NE level)

When to use Use this procedure to create a new 1+1 Multiplex Section Protection (MSP) in an SDH network element or a new 1+1 Automatic Protection Switching (APS) in a SONET network element. The MSP can be established for optical STM-16 ports. The APS can be established for optical OC-48 ports. The MSP or APS is unidirectional and non-revertive.

Before you begin Prior to performing this task, you must:

- Verify that all required circuit packs are installed (cf. “Shelf configuration” (15-6), “Creating a new circuit pack” (4-11) and “Reassigning a circuit pack” (4-14)).
- Complete the port provisioning for any optical port which is involved in the protection group (cf. “Configuring an optical SDH/SONET port” (4-16) and “Configuring a tributary” (4-26)).
- Verify that no failure (Loss of Signal, LOS) is present on the working line (cf. *LambdaUnite*™ MSS Alarm Messages and Trouble Clearing Guide, chapter “Retrieving a list of current alarms”).

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create a new protection group.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Configuration rules An MSP can only be established between two separate circuit packs (which are of the same type), i.e. it is not allowed to establish an MSP between 2 ports on the same circuit pack. An MSP between different ports on different circuit packs can be configured independently, e.g. one port of circuit pack 1 can be protected with one port of circuit pack 2 while the second port on circuit pack 1 is protected by circuit pack 3.

Lockout In case of establishment of an 1+1 uni-directional MSP group, the received traffic at the near-end will be lost unexpectedly if it was selected from protection (with existing WD/WF condition) until also the MSP group has been established at the far end.

In a normal way of operation, the operator will at first switch back the traffic to working. This can be done with an external lockout request. The provisioning of the MSP architecture and the operation in near-end and far-end shall be chosen to be the same.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Line Protection” (18-18)

Instructions Complete the following steps to create a new MSP:

- 1 Call up the window **Create New Protection Group** via **Configuration** → **Create New...** → **Protection Group** in the **System View** of the CIT.

Result:

On the left side of the window the tab **Ptn Grp** appears. The selected system and bay and the available shelf are displayed.

- 2 Double-click on the shelf or select the shelf and click on the pushbutton **Select I/O Shelf**.

Result:

On the right side of the window the **Protection Type Selection** menu appears.

- 3 Select the type **1+1 MSP** (SDH) or **1+1** (SONET) in the drop-down list box **Protection Type**.

Result:

The parameter fields for the 1+1 MSP or 1+1 APS appear.

- 4 Define the last digit(s) of the **Protection Group AID** in the respective text box. Insert a value from **1** to **999**.

-
- 5 Select the **AIDs of the Working Port** and the **Protection Port** in the respective drop-down list boxes in the group box **Group Member**. The values correspond to the slot designations.
-

- 6 Select the **Alarm Severity Assignment Profile**.
-

- 7 Click on **Apply** then click on **Close**.

Result:

The window **Create New Protection Group** closes.

END OF STEPS



Creating a new 2-fiber MS-SPRing (NE level)

When to use Use this procedure to create a new 2-fiber Multiplex Section Shared Protection Ring (MS-SPRing) in an SDH network element or a new Bidirectional Line-Switched Ring (BLSR) in a SONET network element..

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Ring Protection” (18-20)
- Chapter 3, “Management communication setup”

Before you begin Prior to performing this task, you must:

- Verify that all required circuit packs are installed (cf. “Shelf configuration” (15-6), “Creating a new circuit pack” (4-11) and “Reassigning a circuit pack” (4-14)).
- Complete the port provisioning for any optical port which is involved in the protection group (cf. “Configuring an optical SDH/SONET port” (4-16) and “Configuring a tributary” (4-26)).
- Verify that no cross-connections have been made on any port to be included in the protection group (cf. “Viewing existing cross-connections” (7-3)).
- Enable the DCC channels and check in the OSI Neighbor Map that all neighbor network elements have connection (cf. Chapter 3, “Management communication setup”).

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create a new protection group.

Required equipment

The following equipment is required to perform this task:

- WaveStar[®] CIT

Instructions Complete the following steps to create a new MS-SPRing:

- 1 Call up the window **Create New Protection Group** via **Configuration** → **Create New...** → **Protection Group** in the **System View** of the CIT.

Result:

On the left side of the window the tab **Ptn Grp** appears. The selected system and bay and the available shelf are displayed.

- 2 Select the shelf and click on the pushbutton **Select I/O Shelf**.

Result:

On the right side of the window the **Protection Type Selection** menu appears.

- 3 Select in the drop-down list box **Protection Type** the type **2 Fiber MS-SPRing** (SDH) or **2 Fiber BLSR** (SONET).

Result:

The parameter fields for the 2-fiber MS-SPRing or BLSR appear.

- 4 Define the **Protection Group AID** by typing the last digit(s) in the respective text box. This can be max. two digits, a value from **1** to **99** is possible. Please note that you have to choose different AIDs for different protection groups within one network element. Within the whole ring equal Protection Group AIDs may exist.
-

- 5 Enter the Ring ID. The Ring ID must be defined for the whole ring. For all MS-SPRing protection groups which are defined in network elements belonging to one ring always the same Ring ID has to be inserted.
-

- 6 Select the AIDs of **East Port** and **West Port** in the respective drop-down list boxes in the group box **Group Member**. The values correspond to the slot designations (cf. "Shelf configuration" (15-6) and "Overview of access identifiers" (15-8)).
-

-
- 7** Set the Wait-To-Restore time in the drop-down list box **Wait to Restore:**.

Values between **1** and **12** minutes in steps of one minute are possible. Also the value **INFINITE** can be selected.

-
- 8** Select the **MS-SPRing Alarm Severity Assignment Profile** (SDH) or the **BLSR Alarm Severity Assignment Profile** (SONET).

-
- 9** Verify that all parameters are correct. Click on **Apply** to make the changes.

Result:

If the creation of the MS-SPRing protection group was successful, a DCC Termination Provisioning message appears indicating that the LAPD role has been set at User Side (default). This setting can be modified (cf. “Configuring data communication channels” (3-36)). If there are insufficient DCC channels available for termination, a denial message appears.

-
- 10** If the creation of the MS-SPRing/BLSR protection group was successful click on **Apply**, then click on **Close**.

Otherwise delete one or two DCC terminations in order to create the MS-SPRing. Two free LAPD channels are necessary (cf. “Configuring data communication channels” (3-36)).

-
- 11** Repeat Step 1 to Step 10 for each network element in the ring.

END OF STEPS



Creating an SNCP or UPSR (NE level)

When to use Use this procedure to create a bidirectional SNCP (Sub-Network Connection Protection) in an SDH network element or a UPSR (Unidirectional Path-Switched Ring) in a SONET network element. The SNCP can be used to protect an SDH signal. The UPSR can be used to protect a SONET signal within one ring. Both protection schemes are realized via a broadcast in transmission direction and the protection switch in receive direction on time slot level. Configure the SNCP/UPSR for the two NEs between which the protected cross connection is to be established.

Related information For related information, see

- “Path Protection” (18-13)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to create a new cross-connection protected with a bidirectional single-ring SNCP:

- 1 Call up the **Cross-connection Wizard** via **Configuration** → **cross-connection...** in the **System View** of the *WaveStar* CIT.
 - 2 Click on the radio button **Create a new cross-connection** and click on **Next>**.
-

Result:

Screen 1 appears.

-
- 3 Define the cross-connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

- **VC-3**(default value)
- **VC-4**
- **VC-4-4c**
- **VC-4-16c**
- **VC-4-64c**
- **STS-1**
- **STS-3**
- **STS-12**
- **STS-48**
- **STS-192**

-
- 4 Select **UPSR/SNCP Ring Add, Drop** by clicking on the respective radio button in the group box **Type of Cross-connection**.
-

- 5 Click on **Next>** to proceed to the next window.

Result:

Screen 2 appears. A depiction of the cross-connection in the NE to which you are connected and for which you are creating the SNCP/UPSR is displayed.

- 6 Select the Path 1 tributary (A), the Add/Drop (B) and the Path 2 tributary (C) as described in the window via the buttons **Select....**. Proceed as described in the windows **Path 1 Tributary**, **Add/Drop Tributary** and **Path 2 Tributary**.
-

- 7 Define the working path and the protection path by clicking on the respective check box.
-

- 8 Click on the **Next>** button.
-

Result:**Screen 3** opens.

-
- 9** Select the **Path 1 NE TID**, the **Add/Drop NE TID** and the **Path 2 NE TID** in the respective drop-down list boxes. This is necessary if the network element is part of an MS-SPRing. Otherwise proceed to Step 10.
-
- 10** Select the **Output Mode** for the bidirectional cross-connection. The following values are possible:
- **NORM** refers to a cross-connection which carries “normal” traffic.
 - **AIS** is a test and maintenance setting. An AIS is transmitted via the respective cross-connection.
 - **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.
-
- 11** Select the **Protection Type**:
- For a UPSR select **NA**.
 - For an SNCP you can select **SNC/N** (using non-intrusive monitoring) or **SNC/I** (using inherent monitoring).
SNC/I protection, generally, protects against failures in the server layer. The protection process and the defect detection process are performed by two adjacent layers. The server layer performs the defect detection process, and forwards the status to the client layer by means of the **Server Signal Fail (SSF)** signal. This means AU-4 or STS-1 defects are defects and the switch is triggered by the SSF signal.
SNC/N protection, generally, protects against failures in the server layer **and** against failures and degradation in the client layer. This means the non-intrusive monitor function on the receive side detects Signal Fail (SF) and Signal Degrade (SD) events on the incoming signal and triggers the switch.
-
- 12** Select the **Holdoff Timer**. Values between **0** and **10000 msec** are possible.
-

Note that the hold-off time should be configured in such a way that an interaction with other protection schemes (equipment protection or MS-SPRing /BLSR) is taken into consideration. Via different hold-off times it can be defined which protection should switch first. Thus double switches can be avoided.

-
- 13** Insert a name with up to 24 characters for the protection group in the text box **PPG Name**.
-

- 14** Define whether the SNCP shall operate in revertive or non-revertive mode.
-

- 15** Select the **Wait To Restore Time** if the SNCP/UPSR is working in revertive mode. Values between **0** and **60 min** are possible.
-

- 16** Click on the **Finish** button to apply your settings.

END OF STEPS

.....

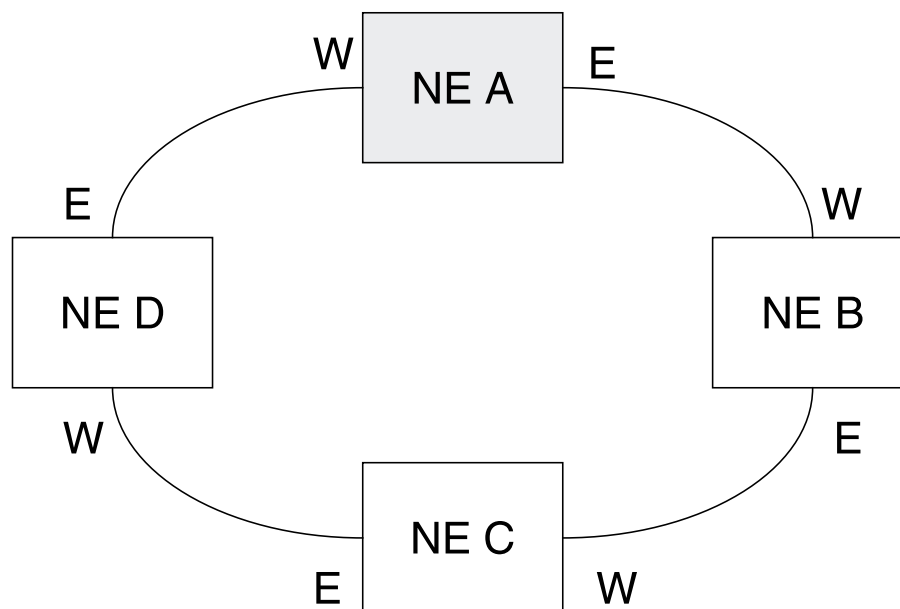


Deleting a protection group

When to use Use this procedure to delete protection groups which have been provisioned for the system. This can be 1+1 MSPs/APSs or 2-fiber MS-SPRings/2-fiber BLSRs.

Before you begin If you intend to remove an NE completely (i.e., physically) from an MS-SPRing or BLSR protected ring, perform the following actions before deleting the protection groups in this NE and removing circuit packs or cables in order to isolate the NE from the rest of the ring first, so that traffic cannot be lost:

In the adjacent NEs (NE B and NE D in the example, see figure below) of the NE you want to remove (here NE A), perform a forced switch to protection (cf. “Switching a 2-fiber MS-SPRing or 2-fiber BLSR” (8-4)). In NE B, the direction for the forced switch is East, in NE D the direction is West.



Required privilege code

You must have at least a privilege code of M4, Maintenance, to remove protection groups from the system.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Lockout The near-end can still be MSP protected at the moment the MSP group at the far-end is deleted. At unpairing, the K1 byte and K2 bits 1-5 is set to all 0s. For SONET, the operation indication in K2 bits 5-8 is removed.

As a result, the unpairing operation at the far-end can cause APS defects at the near-end. This will results into release of the selector and also to APS failure(s) after 2.5 sec.

In case of 1+1 uni-directional operation, the received traffic at the near-end will be lost unexpectedly if it was selected from protection. Because in this the case, the selector is controlled by the local request only.

In a normal way of operation, the operator will at first switch back the traffic to working. This can be done with an external lockout request. If MSP in uni-directional operation, it should be done at both near-end and far-end NEs.

Instructions Complete the following steps to remove equipment from the system:

- 1 Call up the window **Delete** via **Configuration** → **Delete...** in the **System View** of the WaveStar CIT.
- 2 Select the tab **Ptn Group**.
- 3 Select the shelf in which the protection group is located.
- 4 Select the protection group
- 5 Click on **Select** to apply your changes. A confirmation window opens containing the name of the protection group, the protection type and the current group members. Click on **Yes** to confirm your changes. Click on **No** to discard your changes.

Deletion of a protection group which has a cross connection established of an active protection switch on one or more of the involved ports will be denied by the network element.

END OF STEPS





8 Traffic maintenance

Overview

Purpose This chapter describes the traffic maintenance procedures. This comprises the manual and forced switch of network protections.

Contents

Switching an MSP or APS	8-2
Switching a 2-fiber MS-SPRing or 2-fiber BLSR	8-4
Switching a UPSR or SNCP	8-6
Clearing a protection switch request	8-8
Retrieve protection switch reports	8-10
Supporting information on the “BLSR Protection Switch List”	8-11
Supporting information on the “NE Protection Switch Activity Log”	8-12



Switching an MSP or APS

When to use	Use this procedure to switch from one section to the other in a 1+1 MSP or from one line to the other in a 1+1 APS.
Related information	For related information, see: • “Protection mechanisms” (18-12) • “Line Protection” (18-18)
Before you begin	Prior to performing this task, you must be logged into the <i>WaveStar</i>® CIT and the respective network element. Required privilege code You must have at least a privilege code of M4, Maintenance, to switch a 1+1 MSP. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Complete the following steps to switch a 1+1 MSP or APS: 1 Call up the Protection Switch window either in the System View via Fault → Protection Switch, or in the Shelf View, clicking with the right mouse button on a specific circuit pack and then selecting Protection Switch. 2 Select the the desired protection group in the tab Ptn Group on the left side of the window. Result: Some data of the protection group are displayed. 3 Select the desired switch request in the field Switch Type. The following options are possible: • Clear • Lockout of Protection

- **Forced to Working**
- **Forced to Protection**
- **Manual to Working**
- **Manual to Protection**

Important! A forced switch to a faulty section could cause a traffic interruption. Perform a forced switch only to a section which is working fault-free.

4 Click on **Apply.**

END OF STEPS



Switching a 2-fiber MS-SPRing or 2-fiber BLSR

When to use	Use this procedure to switch from one section to the other in a 2-fiber MS-SPRing or from one line to the other in a 2-fiber BLSR.
Related information	For related information, see: • “Protection mechanisms” (18-12) • “Ring Protection” (18-20)
Before you begin	Check in the menu View → Rings → Ring Map whether the ring discovery is finished and the ring is complete. Please note that you do not execute manual switch commands while the ring is incomplete! Required privilege code You must have at least a privilege code of M4, Maintenance, to switch a 2-fiber MS-SPRing. Required equipment The following equipment is required to perform this task: • WaveStar® CIT
Instructions	Complete the following steps to switch a 2-fiber MS-SPRing or 2-fiber BLSR: 1 Call up the Protection Switch window either in the System View via Fault → Protection Switch, or in the Shelf View, clicking with the right mouse button on a specific circuit pack and then selecting Protection Switch. 2 Select the respective MS-SPRing/BLSR in the tab Ptn Grp on the left side of the window. Result: Some data of the protection group are displayed.

.....

3 Select the transmission direction to which the traffic shall be switched in the field **Direction**. The following options are possible:

- **East**
 - **West**
-

4 Select the desired switch request in the field **Switch Type**. The following options are possible:

- **Clear**
 - **Lockout of Protection, Span**
 - **Forced to Protection, Ring**
 - **Manual to Protection, Ring**
-

5 Click on **Apply**.

.....

END OF STEPS

.....



Switching a UPSR or SNCP

When to use	Use this procedure to switch from one path to the other in a UPSR or SNCP.
Related information	For related information, see: • “Path Protection” (18-13)
Before you begin	Prior to performing this task, you must be logged into the <i>WaveStar</i>® CIT and the respective network element. Required privilege code You must have at least a privilege code of M4, Maintenance, to switch a UPSR or SNCP. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Complete the following steps to switch a UPSR or SNCP: 1 Call up the Protection Switch window either in the System View via Fault → Protection Switch, or in the Shelf View, clicking with the right mouse button on a specific circuit pack and then selecting Protection Switch. 2 Select the desired UPSR or SNCP in the tab Ptn Grp on the left side of the window. Result: The window Path Protection Switch opens. 3 Select the desired switch request in the field Switch Type. The following options are possible: • Clear • Lockout of Protection • Forced to Working

- **Forced to Protection**
 - **Manual to Working**
 - **Manual to Protection**
-

4 Click on **Apply**.

END OF STEPS



Clearing a protection switch request

When to use Use this procedure to perform a Clear command to a protection group. This means that the currently applied switch request is abolished.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Path Protection” (18-13)
- “Parameters of the window “View Cross Connections”” (7-5)
- “Ring Protection” (18-20)
- “Switching an MSP or APS” (8-2)
- “Switching a 2-fiber MS-SPRing or 2-fiber BLSR” (8-4)
- “Switching a UPSR or SNCP” (8-6)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of M4, Maintenance, to perform a switch command on a protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to perform a clear command.

- 1 Call up the **Protection Switch** window either in the **System View** via **Fault → Protection Switch**, or in the **Shelf View**, clicking with the right mouse button on a specific circuit pack and then selecting **Protection Switch**.

- 2 Select the desired protection group (MS-SPRing/BLSR, MSP/APS or SNCP/UPSR) in the tab **Ptn Grp** on the left side of the window.

Result:

Some data of the selected protection group are displayed on the right side of the window.

- 3** Select the switch request **Clear** in the field **Switch Type**.

Result:

The currently applied switch request is cleared.

- 4** Click on **Apply**.

END OF STEPS



Retrieve protection switch reports

When to use Use this procedure to retrieve information on the status of existing protection groups in the network element.

Related information For related information, see:

- “Protection mechanisms” (18-12)
- “Ring Protection” (18-20)
- “Switching an MSP or APS” (8-2)
- “Switching a 2-fiber MS-SPRing or 2-fiber BLSR” (8-4)
- “Switching a UPSR or SNCP” (8-6)

Before you begin Prior to performing this task, you must be logged into the *WaveStar*® CIT and the respective network element.

Required privilege code

You must have at least a privilege code of M1, Maintenance, to retrieve the **BLSR Protection Switch List** and a privilege code of S1, Security, to retrieve the **NE Protection Switch Activity Log**.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to retrieve the protection switch reports.

- 1 Call up the window **BLSR Protection Switch List** or the window **NE Protection Switch Activity Log** via **Reports** in the System View of the *WaveStar* CIT.

END OF STEPS



Supporting information on the “BLSR Protection Switch List”

Purpose	The BLSR Protection Switch List allows the user to see the status of all BLSR or MS-SPRing protection groups.
Displayed data	The following data are displayed • Ring ID • Port AID This is the AID of each port (east and west) in the MS-SPRing/BLSR protection group • Direction This is either East or West. • Lockout Here * or (R) can be displayed or both. The * indicates the switch request which is derived from the K1 byte for the respective port. The (R) indicates the currently active switch request state of the port. • Forced Here * or (R) can be displayed or both. The * indicates the switch request which is derived from the K1 byte for the respective port. The (R) indicates the currently active switch request state of the port. • Manual Here * or (R) can be displayed or both. The * indicates the switch request which is derived from the K1 byte for the respective port. The (R) indicates the currently active switch request state of the port. • Automatic WTR, SD, SF, WTR (R), SF (R), SD (R) or a combination of two conditions can be displayed. The (R) indicates the currently active switch request state of the respective port. The other values indicate the switch request which is derived from the K1 byte for the port.

□

Supporting information on the “NE Protection Switch Activity Log”

Purpose The **NE Protection Switch Activity Log** provides details on manual and autonomous protection switches.

Displayed data The following values are displayed:

Value	Description
Pack/Port AID	The AID of the pack or port in which the protection switch occurred.
AID Type	The type of AID in the protection group, e.g. OC3 , 2F , EQPT
Occurrence Date	Year, month and day of the protection switch.
Occurrence Time	Hours, minutes and seconds of the protection switch.
Switch Type	Switch to Working , Switch to Protection , Lockout or Lockout Cleared
Switch Description	Displays the kind of switch request.





9 Performance monitoring

Overview

Purpose This chapter describes the procedures for configuring the performance monitoring functions of *LambdaUnite*[™] MSS systems.

Related information Please also refer to Chapter 19, “Performance monitoring concepts”.

Contents	
Enabling or disabling performance monitoring data collection	9-2
Retrieving performance monitoring settings for individual ports or tributaries	9-6
Retrieving performance monitoring reports	9-9



Enabling or disabling performance monitoring data collection

Purpose Use this procedure to enable or disable the performance monitoring data collection for selected ports or tributaries.

Before you begin Prior to performing this task, you must:

- Identify the ports or tributaries related to the task:
 - To enable or disable Regenerator Section and/or Multiplex Section performance monitoring, you need to select an SDH port.
 - To enable or disable Section and/or Line performance monitoring, you need to select a SONET port.
 - To enable or disable path performance monitoring, you need to select an SDH or SONET tributary.
- Log into the NE with the *WaveStar*® CIT and be familiar with the functions of the *WaveStar* CIT.
- Make sure that the port or tributary to be monitored has been established properly.

Required privilege

You must have a security privilege code of at least **P3** and **S1** to perform this task.

Required equipment

WaveStar CIT.

Instructions Complete the following steps to enable or disable performance monitoring data collection for selected ports.

1	IF you want to enable performance monitoring data collection you want to disable performance monitoring data collection	THEN continue with Step 2. continue with Step 7.

-
- 2 Before enabling performance monitoring data collection, make sure that the port monitoring mode for the required port or in case of path performance monitoring the monitoring mode for the required tributary is set to “monitored”. Therefore, from the **System View** main menu, select **Configuration** → **Provision...**

Result:

The **Provision Parameters** window opens.

- 3 In the **Provision Parameters** window, open the required bay and shelf details then select the required port or tributary.
-

- 4 Click **Provision**.

Result:

The **Provision Parameters for Protection Group or Equipment** window opens for the port or tributary selected. The type of window depends on your selection.

- 5 In the **Transmission** area, select in the **Port Mode** drop-down list (for port) or the **Tributary Monitoring Mode** drop-down list (for tributary) the **Monitored** option.
-

- 6 Click **Apply**.
-

- 7 From the **System View** main menu, select **Performance** → **Provision Ports**.

Result:

The **Provision Parameters for Port Performance Monitoring** window with the **Equipment Selection** window opens.

- 8 In the **Equipment Selection** window, open the required bay and shelf details, then select the required port or tributary.
-

- 9 Click **Provision**.
-

Result:

The right-hand side of the **Provision Parameters for Port Performance Monitoring** window is populated with the performance monitoring provisioning options for the port or tributary selected. The type of window depends on your selection.

10 Proceed as follows, depending on your selection in Step 8:

IF	THEN
you selected an SDH port	Enable or disable Regenerator Section and Multiplex Section performance monitoring data collection by selecting Enable or Disable respectively for Regenerator-Near End Multiplex Section PM Activation and Far End Multiplex Section PM Activation .
you selected a SONET port	Enable or disable Section and Line performance monitoring data collection by selecting Enable or Disable respectively for Section and Near End Line PM Activation and Far End Line PM Activation .
you selected an SDH or SONET tributary	Enable or disable path performance monitoring data collection by selecting Enable or Disable respectively for Path PM Activation .

11 From the **Apply to** list, select the required application:

- Apply to this port (trib) only
Enables or disables the selected performance monitoring data collection to only the port (tributary) you have selected.
- Apply to all tribs, this port
Enables or disables the selected performance monitoring data collection to all the tributaries on the port that contains the tributary you have selected.
- Apply to all ports (tribs) this pack

Enables or disables the selected performance monitoring data collection to all the ports (tributaries) on the circuit pack that contains the port (tributary) you have selected.

- **Apply to all ports (tribs) this type, this shelf**
Enables or disables the selected performance monitoring data collection to all the ports (tributaries) on all the circuit packs on a shelf that have the same type port (tributary) as the one you have selected.

12 Click **Apply**, then click **Close** to exit.

END OF STEPS



Retrieving performance monitoring settings for individual ports or tributaries

Purpose Use this procedure to retrieve performance monitoring settings made for a selected port or tributary.

- Before you begin** Prior to performing this task, you must:
- Identify the ports or tributaries related to the task:
 - To retrieve Regenerator Section and/or Multiplex Section performance monitoring settings, you need to select an SDH port.
 - To retrieve Section and/or Line performance monitoring settings, you need to select a SONET port.
 - To retrieve path performance monitoring settings, you need to select an SDH or SONET tributary.
 - Log into the NE with the *WaveStar*[®] CIT and be familiar with the functions of the *WaveStar* CIT.

Required privilege code

You must have a security privilege code of at least PM1 to perform this task.

Required equipment

WaveStar CIT.

Instructions Complete the following steps to retrieve the performance monitoring settings for selected ports or tributaries.

- 1 From the **System View** main menu, select **Performance** → **View PM Ports**.

Result:

The **View Parameters for Port Performance Monitoring** window with the **Equipment Selection** window opens.

- 2 In the **Equipment Selection** window, open the required bay and shelf details then select the required port or tributary.

3 Click **Select.**

Result:

The right-hand side of the **View Parameters for Port Performance Monitoring** window is populated with the performance monitoring information for the port or tributary selected. The type of window depends on your selection.

If an SDH port has been selected, the following parameters can be viewed:

Parameter	Meaning
Regenerator-Near End Multiplex Section PM Activation	Indicates whether Regenerator Section performance monitoring and near-end Multiplex Section performance monitoring is enabled or not.
Far End Multiplex Section PM Activation	Indicates whether far-end Multiplex Section performance monitoring is enabled or not.
Multiplex Section Near End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end Multiplex Section performance monitoring.
Multiplex Section Far End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for far-end Multiplex Section performance monitoring.
Regenerator Section Near End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for Regenerator Section performance monitoring.

If a SONET port has been selected, the following parameters can be viewed:

Parameter	Meaning
Section and Near End Line PM Activation	Indicates whether Section performance monitoring and near-end Line performance monitoring is enabled or not.

Far End Line PM Activation	Indicates whether far-end Line performance monitoring is enabled or not.
Line Near End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end Line performance monitoring.
Line Far End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for Line performance monitoring.
Section Near End SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end Section performance monitoring.

If a tributary has been selected, the following parameters can be viewed:

Parameter	Meaning
Path PM Activation	Indicates whether path performance monitoring is enabled or not.
Higher-order Path Far-end SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for far-end path performance monitoring.
Higher-order Path Near-end SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end path performance monitoring.

4 Click **Close** to exit.

END OF STEPS



Retrieving performance monitoring reports

Purpose Use this procedure to retrieve the performance monitoring register values for the following performance monitoring parameter groups when available:

- SONET Section
- SONET Line
- SONET Path
- SDH Regenerator Section
- SDH Multiplex Section
- SDH Path

Before you begin Prior to performing this task, you must fulfill the following requirements:

Required privilege code

You must have a security privilege code of at least **PM1** to perform this task.

Required equipment

WaveStar® CIT.

Instructions Complete the following steps to retrieve, display, and/or save performance monitoring register values.

- 1 Log into the system using the *WaveStar* CIT.

- 2 Select one of the following from the System View main menu to display the performance monitoring register values associated with the listed parameter group:
 1. **Performance → Reports → SONET Section...**
 2. **Performance → Reports → SONET Line...**
 3. **Performance → Reports → SONET Path...**
 4. **Performance → Reports → SDH Regenerator Section...**
 5. **Performance → Reports → SDH Multiplex Section...**
 6. **Performance → Reports → SDH Path...**

Result:

The corresponding ... **PM Parameters Selection** window opens with the **Equipment Selection** window.

- 3 Open the bay and shelf details, then select the port or tributary for which you want to receive a report. Click **Select**.

Result:

The right-hand side of the ... **PM Parameters Selection** window is populated with the related information and provisioning options.

- 4 Select the **Time Period**, **Monitored Date**, **Monitor Time**, **Monitor Level** and the performance monitoring parameters you want to be included in the performance monitoring report.

Reference:

For related information concerning these configuration options and the selectable performance monitoring parameters, please refer to “Performance measurements” (19-6) and “Performance monitoring reports” (19-12).

- 5 Click **Apply**.

Result:

The corresponding ... **PM Report** window opens.

- 6 View the report, then perform one of the following options:

IF	THEN
you want to save the results to a file,	Continue with the next step.
you want to print the results to a printer connected to your PC,	Click Print .
you want to refresh the screen display,	Click Refresh .

IF	THEN
you do not want to dismiss the window,	Click Close to exit.
7 Select the Save As control option.	
Result:	
The file name selection window opens.	
8 Enter a file name where you want to save the report.	
9 Click Apply .	
10 Click Close to exit.	
END OF STEPS	

Validity flag The validity flag shows the validity of the register whose value is reported. The validity flag is set to “1” if the corresponding value is valid. Otherwise, the validity flag is omitted.

The validity flag is omitted (the corresponding value is invalid) if:

- the elapsed time deviation is greater than 10 seconds, or
- the SES declaration threshold has been changed.





10 Software upgrade

Overview

Purpose This chapter describes the procedures which have to be carried out for the software upgrade of the *LambdaUnite*[™] MSS.

Contents

Performing an initial software download using the CIT	10-2
Performing a software download for upgrade purposes using the <i>WaveStar</i> [®] CIT	10-7
Activating an NE software generic	10-12
Retrieving NE software generic information	10-14
Supporting information for “Retrieving NE software generic information”	10-15



Performing an initial software download using the CIT

Purpose Use this procedure to install a software generic in the NE for the first time.

The software is initially delivered to the customer on a CD-ROM (ComCode 108687013). The software generic has to be copied from the CD-ROM to the *WaveStar*® CIT PC and then to the empty *CompactFlash*™ card via *WaveStar* CIT. Afterwards, the *CompactFlash* card is inserted into the NE.

It is essential that the *CompactFlash* card has to remain in the CTL circuit pack during normal operation!

Before you begin Prior to performing this task, you must:

1. Have a valid login on both the *WaveStar* CIT and all subject NE(s) within the ring.
2. Acquire the CD-ROM that contains the new generic/version of the NE software (“*LambdaUnite*™ MSS Release 2.1 NE Software”, ComCode 108687013).
3. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.

Required privilege code

You must have at least a privilege code of S4 .

Required equipment

The following equipment is required to perform this task:

- Empty 220 Mb *CompactFlash* card (as delivered from manufacturer)
- CD-ROM that contains the new generic/version of the NE software
- *WaveStar* CIT with *CompactFlash* slot

Safety precautions To assure both personal safety and the proper functioning of the *LambdaUnite* MSS product, it is imperative to observe the following precaution.

Related information

For related information, please refer to:

- Chapter 20, “Software upgrade concepts”
- Chapter 22, “WaveStar CIT Tutorial”.



CAUTION

Electrostatic discharge damage to sensitive components

Handling circuit packs or working on a WaveStar CIT can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar CIT, to prevent electrostatic discharge damage to sensitive components.

Instructions



CAUTION

Improper removal of a CompactFlash card can result in damaged files and the generation of information messages such as “lost clusters” and/or “missing/damaged sectors”.

Do not ever remove a CompactFlash card.

To initially download the NE software (delivered on a CD-ROM) proceed as follows:

- 1 Power up the WaveStar CIT PC and log into Windows NT as Administrator. If you are already logged into Windows NT, close any open window.
.....
- 2 Install the NE software on your PC. To do this, use one of the following two methods (automatic or manual installation).
.....
- 3

IF	THEN
You use the automatic installation method	proceed with the next step.
You use the manual installation method	proceed with Step 5

4 Automatic Installation:

Insert the *LambdaUnite* CD-ROM with the new NE software and wait for the welcoming screen to appear. If your PC does not start the CD-ROM automatically, perform the following:

- Double-click **My Computer** on your desktop.
 - Right-click on your CD-ROM drive's icon.
 - Click **Auto Play**.
If Auto Play is not available in this menu list, you have to start the *setup.exe* file in the root directory of your CD-ROM.
Click the **Next** button.
Wait for the software transfer to complete. You will notice that the "Decompressing Files in ..." message and also the InstallShield Wizard disappears when the operation has completed.
Continue with Step 13.
-

5 Manual Installation: Insert the *LambdaUnite* CD-ROM with the new NE software. If the welcoming screen appears, select **Cancel** to exit from the automatic installation procedure.

6 Open the Windows NT Explorer on your desktop.

7 Select the hard disk drive where *WaveStar* CIT is installed (in most cases **C:**) and click through to **Program Files** → **Lucent Technologies** → **WaveStar CIT** → **generics**.

Please note that, if the subdirectory **generics** does not exist, you must create it!

- 8 In the **generics** directory, create a new folder, preferably stating the new software version in its name.
- 9 In the Windows NT Explorer, right-click the CD-ROM drive of your computer and select **Explore**. Go to the **generics** directory. This directory contains two subdirectories: **p** and **up**.
- 10 Select the complete **up** and **p** directories and copy it to the folder you created in Step 8.
- 11 To install Acrobat Reader on your system, go to the *AcrobatReader* subdirectory on your CD-ROM drive and double-click the *AcrobatReader40.exe* file.
- 12 The Software Release Description (SRD) is located in the *Documentation* subdirectory of the CD. You can read it by double-clicking the *.pdf* file in this subdirectory.
- 13 Insert the empty *CompactFlash* card into the *CompactFlash* slot of the *WaveStar* CIT PC.
- 14 Format the *CompactFlash* card by performing the following:
 - Double click the **My Computer** icon on your desktop
 - Select **Cards** → **Format...** in the PC card control window.
 - Select **FAT** in the **File System** selection box.
 - Select **Quick Format**
 - Click **Start**.
- 15 Start Window Explorer.
- 16 Copy all files in the directory *..\Program Files\Lucent Technologies\WaveStar CIT\generics\xx.xx.xx\up* to the *CompactFlash* card.

Result:

The file copy function begins and you see a “Copying files...” message.

.....

17 After copying, **power off** the flash disk slot.

.....

18 Eject the *CompactFlash* card from the *CompactFlash* slot of the PC.

.....

19 Insert the *CompactFlash* card with the new software version into the CTL circuit pack. Make sure that it is firmly seated in the CTL.

Result:

The system automatically starts the download.

Also note that the *CompactFlash* card has to remain in the CTL circuit pack during normal operation.

END OF STEPS

.....



Performing a software download for upgrade purposes using the *WaveStar*[®] CIT

When to use Use this procedure to download a new version of the NE software generic. A prerequisite for this is that a software generic is already available in the NE. If this is not the case, please refer to the task “Perform an initial software download using *WaveStar* CIT”.

Related information For related information, please refer to:

- Chapter 20, “Software upgrade concepts”
- Chapter 22, “*WaveStar* CIT Tutorial”.

Before you begin Prior to performing this task, you must:

1. Have a valid login on both the *WaveStar* CIT and all subject NE(s) in the ring.
2. Acquire the CD-ROM that contains the new generic/version of the NE software (“*LambdaUnite*[™] MSS Release 1.0 NE Software”, ComCode 109088708)
3. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.
4. Carry out a backup of the NE database (recommended; cf. “Manually backup database to the *WaveStar* CIT” (11-3)).
5. Make sure that there is no configuration (write) access to the NE from other CITs or management systems during the software download.

Required privilege code

You must have at least a privilege code of S4.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT
Please make sure that you always use the *WaveStar* CIT version corresponding to the NE release you are upgrading to. If not yet done, install *WaveStar* CIT Release 6.0.0 on your PC (cf. *WaveStar* CIT Tutorial).

Instructions Complete the following steps to download a new version of the NE software generic.

.....

1 Power up the *WaveStar* CIT PC and log into Windows NT as Administrator. If you are already logged into Windows NT, close any open window.

.....

2 Install the NE software on your PC. To do this, use one of the following two methods (automatic or manual installation).

.....

3	
IF	THEN
You use the automatic installation method	proceed with the next step.
You use the manual installation method	proceed with Step 5

.....

4 Automatic Installation:

Insert the *LambdaUnite* CD-ROM with the new NE software and wait for the welcoming screen to appear. If your PC does not start the CD-ROM automatically, perform the following:

- Double-click **My Computer** on your desktop.
 - Right-click on your CD-ROM drive's icon.
 - Click **Auto Play**.
If Auto Play is not available in this menu list, you have to start the *setup.exe* file in the root directory of your CD-ROM.
Click the **Next** button.
Wait for the software transfer to complete. You will notice that the "Decompressing Files in ..." message and also the Install Shield Wizard disappears when the operation has completed.
Continue with Step 13.
-

5 Manual Installation: Insert the *LambdaUnite* CD-ROM with the new NE software. If the welcoming screen appears, select **Cancel** to exit from the automatic installation procedure.

6 Open the Windows NT Explorer on your desktop.

7 Select the hard disk drive where WaveStar CIT is installed (in most cases **C:**) and click through to **Program Files** → **Lucent Technologies** → **WaveStar CIT** → **generics**.

Please note that if the subdirectory **generics** does not exist, you must create it!

8 In the **generics** directory, create a new folder, preferably stating the new software version in its name.

9 In the Windows NT Explorer, right-click the CD-ROM drive of your computer and select **Explore**. Go to the **generics** directory. This directory contains two subdirectories: **p** and **up**.

10 Select the complete **up** and **p** directories and copy it to the folder you created in Step 8.

11 To install Acrobat Reader on your system, go to the *AcrobatReader* subdirectory on your CD-ROM drive and double-click the *AcrobatReader.exe* file.

12 The Software Release Description (SRD) is located in the *Documentation* subdirectory of the CD. You can read it by double clicking the *.pdf* file in this subdirectory.

13 Log into the WaveStar CIT.

14 At the WaveStar CIT, connect to the network element.

15 From the WaveStar CIT **System View**, select the **Configuration** → **Software** → **Download Software** menu option.

Result:

The **Download Generic** window appears.

- 16** In the **Download from** drop down list box select **CIT**.

Result:

A file selection screen appears showing that the software will be downloaded from C:\Program Files\Lucent Technologies\Wavestar CIT\generics. The directory of the file selection screen is automatically pre-populated.

- 17** In the file selection window, double click the version of network element software you are upgrading to (i.e. if manual installation has been done, the name of the folder you created in Step 8), double click the **p** directory.
-

- 18** Click the **Download** push-button.

Result:

A warning screen appears.

- 19** Read the text in the warning screen and if you are sure, confirm with **OK**.

Result:

A second warning screen appears.

- 20** Read the text in the second warning screen and confirm with **Yes**.

Result:

The new software generic is being downloaded to the NE.

A progress indicator window is shown. When the download is finished successfully, the progress indicator disappears.

Please note that downloading a full generic will take approx. 1 hour 10 minutes.

-
- 21** The new software generic is now available in the “PREVIOUS” area of the NE’s non-volatile memory (NVM). It is not yet activated. For activating the new software, please refer to the task “Activating an NE software generic” (10-12).

END OF STEPS



Activating an NE software generic

When to use Use this procedure to activate a downloaded new version of NE software generic.

Related information For related information, please refer to:

- Chapter 20, “Software upgrade concepts”
- Chapter 22, “ *WaveStar*® CIT Tutorial”.

Before you begin Prior to performing this task, you must:

1. Have a valid login on both the *WaveStar* CIT and all subject NE(s) within the ring.
2. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.
3. Have performed a software download to the non-volatile memory of the NE before.

Required privilege code

You must have at least a privilege code of S4.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to activate a new version of the NE software generic.

- 1 Log into the *WaveStar* CIT.

- 2 At the *WaveStar* CIT, connect to the network element where you want to activate the software currently located in the “PREVIOUS” area of the non-volatile memory (NVM).

- 3 In the *WaveStar* CIT **System View**, select the menu option **Configuration → Software → Activate Software**.

-
- 4 The **Software Generic Activate** window appears. The window shows the currently inactive software generic in the “PREVIOUS” area of the non-volatile memory. Select the generic in the list.
-

- 5 Click **OK**.

Result:

A confirmation window appears.

- 6 If you are sure you want to activate the software, confirm by clicking **Yes**.
-

- 7 The new software generic is activated. The activation is not traffic affecting. The NE performs a reset and it takes approx. 10 minutes until the NE is reachable by *WaveStar* CIT again.

END OF STEPS



Retrieving NE software generic information

When to use Using the *WaveStar*[®] CIT you can retrieve the current software version ID. Software updates, or patches, are identified and included in the current version, if appropriate.

NE active software The **About NE** window which displays the currently active NE software version in the form explained above, is invoked by selecting **Help** → **About This Network Element** from the NE **System View** menu bar.

Instructions To invoke the **CIT/NE Software** display window proceed as follows.

- 1 Select **View** → **Software Generic** from the NE **System View** menu bar.

Result:

A file selection window is displayed.

With this invocation of the file selection screen, only NE software type files stored on the CIT or on the NE are selectable.

- 2 Select a file or files or directory.

Reference:

The displayed parameters are described in “Supporting information for “Retrieving NE software generic information”” (10-15).

END OF STEPS



Supporting information for “Retrieving NE software generic information”

NE software display window

WaveStar[®] CIT allows the user to view the current status of the various copies and releases of the NE software as they reside on the NE non-volatile memory (NVM). The display includes the currently active release and may include either the previous release or a newly downloaded release which might not yet be applied.

Elements of the NE software display window

The following information is displayed in the window for each file selected by the user:

Object	Description/Behavior
Current generic	Software release which is currently active for the system.
File	Selected file. If resident on the NE, the file description indicates whether the file is • Current • Previous Otherwise it gives the directory tree and name of the specific file.
NE Type	Product type of alphanumeric characters
Release	Software release, for example: 01.03.00, which signifies the 00 patch release to the 03 point release associated with the 01 release, corresponds to the successive edits for the first release.
Supplier	Name of the supplier, currently Lucent.
Delivered	Date and end time that the software release was downloaded onto the NE, if this is an NE file, or the date and time the file was last modified if the file is not on the NE.
Installed	Date and start time that the software release was installed onto the NE. If this release has not yet been applied, this field is empty.
Size	Size of the software in bytes.

Object	Description/Behavior
Source	Source of the original download. Examples at this time include CIT and EMS along with a file path and file name. If the source system is either CIT or EMS and if the file is on the NE, the field additionally includes the psel, ssel, tsel, and NSAP values for those systems (for further explanation, refer to “DCN protocols and services” (14-16) and “NSAP address format” (14-19)).
Software State	State of this software release. It may take the values: • Corrupt • Downloaded • In Progress • Failed • Previous • Running • Initial.
Free NVM Space	Displays the free space available on the storage device in bytes.
Unavailable NVM Space	Displays the unavailable space available on the storage device in bytes.
Software version numbering	The version number of a software generic (e.g., new, point, or patch) is identified by a numeric scheme by which a new release and its subsequent point and patch releases can unambiguously be identified and related. Each field in the version numbering has two digits. As an example of version numbering, 01.03.00, which signifies the 00 patch release to the 03 point release associated with the 01 release, corresponds to the successive edits for the first release. □



11 Database backup

Overview

Purpose This chapter describes the procedure which has to be carried out for a NE database backup of the *LambdaUnite*[™] MSS. Furthermore, the procedure for retrieving information on the current NE database is provided.

Contents

Limiting the number of saved backups	11-2
Manually backup database to the <i>WaveStar</i> [®] CIT	11-3
Retrieving NE database information	11-5
Supporting information for “Retrieving NE database information”	11-6

□

Limiting the number of saved backups

Purpose Use this procedure to specify the maximum number of backup directories to be saved.

Before you begin Before you begin this task:

- Obtain the work instructions for this task.
- Verify that a *WaveStar*® CIT is connected and logged into the *LambdaUnite*™ MSS system.

Required equipment

The following equipment is required to perform this task.

- *WaveStar* Customer Interface Terminal (*WaveStar* CIT)

Instructions Complete the following steps to manually backup the network element database (current program and data) to the *WaveStar* CIT.

- 1 At the *WaveStar* CIT, select **Configuration**→ **Software** → **Remote Backup**.
-

- 2 In the **Backup Database** window select **Setup**.

Result:

The **Provision Backup Number** screen appears.

- 3 In the **Provision Backup Number** screen specify the maximum number of backups to CIT per system.

The parameter can be set to a number from 1 to 10, or it can be set to infinite by clicking the radio button **Infinite**.

- 4 Click on **OK**.

END OF STEPS



Manually backup database to the WaveStar® CIT

- When to use** Use this procedure to manually backup the network element database (current program and data) to the WaveStar Customer Interface Terminal (WaveStar CIT):
- after initial software installations/upgrades/changes
 - after major provisioning data changes
 - periodically according to local policy
 - before software upgrades/changes
 - before major provisioning data changes
- Safety precautions** To assure both personal safety and the proper functioning of the LambdaUnite™ MSS system, it is imperative to review and understand these warnings and precautions prior to performing this task.
- Related information** For related information, see:
- Chapter 21, “Database backup concepts”
 - LambdaUnite MSS Alarm Messages and TroubleClearing Guide, “Manually Restore Database from the WaveStar CIT to an NE”
- Before you begin** Before you begin this task:
- Obtain the work instructions for this task.
 - Verify that a WaveStar CIT is connected and logged into the LambdaUnite MSS system.
- Required equipment**
- The following equipment is required to perform this task.
- WaveStar Customer Interface Terminal (WaveStar CIT)



CAUTION

Electrostatic discharge damage to sensitive components

Use a static ground wrist strap whenever handling circuit packs or working on a LambdaUnite MSS system, to prevent electrostatic discharge damage to sensitive components.

Instructions Complete the following steps to manually backup the network element database (current program and data) to the WaveStar CIT.

- 1 At the WaveStar CIT, select **Configuration**→ **Software** → **Remote Backup**.

- 2 In the **Backup To** drop down list box select **CIT**.

Result:

A file selection screen appears showing that the database will back up to C:\Program Files\Lucent Technologies\Wavestar CIT\backups\backupfoldernumber. The directory of the file selection screen is automatically pre-populated.

- 3 Record the path/destination of the backup folder/files and click on **Backup**.

Result:

The NE Data Backup in Progress Screen appears.

- 4 When the NE Data Backup in Progress screen disappears and the backup is complete, select **View** → **NE Data...**

Result:

The File Selection Screen appears.

- 5 Select CIT in the Look in: field and double click on C:, Program Files, Lucent Technologies, WaveStar CIT, and Backups. Then click on the backupfoldernumber and on OK.

Result:

The Database Info Screen appears.

- 6 Verify the Last Backup Time and Last Backup Destination parameters and click on Close.

END OF STEPS



Retrieving NE database information

When to use Via the *WaveStar*® CIT you can retrieve the NE Backup status as reported by the NE as well as showing the release number of NE Data backup files resident on the CIT.

Related information For related information, see Chapter 21, “Database backup concepts”.

Instructions To invoke the **Database Info** window proceed as follows.

- 1 Select **View** → **NE Data** from the **System View** menu bar.

Result:

A file selection window is displayed.

- 2 Select a file or files or directory.

Reference:

The displayed parameters are described in “Supporting information for “Retrieving NE database information”” (11-6).

END OF STEPS



Supporting information for “Retrieving NE database information”

Elements of the *Database Info* window

The **Database Info** window displays the following information for the file(s) selected by the user:

Object	Description/Behavior
Current Generic	Version number of current NE software generic
TID	TID of the NE from which the configuration data was stored on this NVM.
Software Release	Software release corresponding to the data.
Size	Size of the file in bytes.
State	State of this data. It may take the values: • Backup • Corrupt • Failed • Initial • In Progress • Previous • Running.
Last/Previous Backup Time	Date and time when the data was backed up from the NE. If there has been no backup, this field is blank.
Last/Previous Backup Destination	Destination of the most recent backup. Examples at this time include SEC, EMS, and CIT and a file name/path. If there has been no backup, this field is blank.
Last/Previous Restore Time	Date and time when the data was restored to the NE. If there has been no restoral, this field is blank. This field only applies to files on the NE.

Object	Description/Behavior
Last/ Previous Restore Source	Source of the most recent restore. Examples at this time include EMS and CIT plus a file name/path. If there has been no restoral, this field is blank.





12 Periodic activities

Overview

Purpose This section describes periodic activities for maintaining the system.

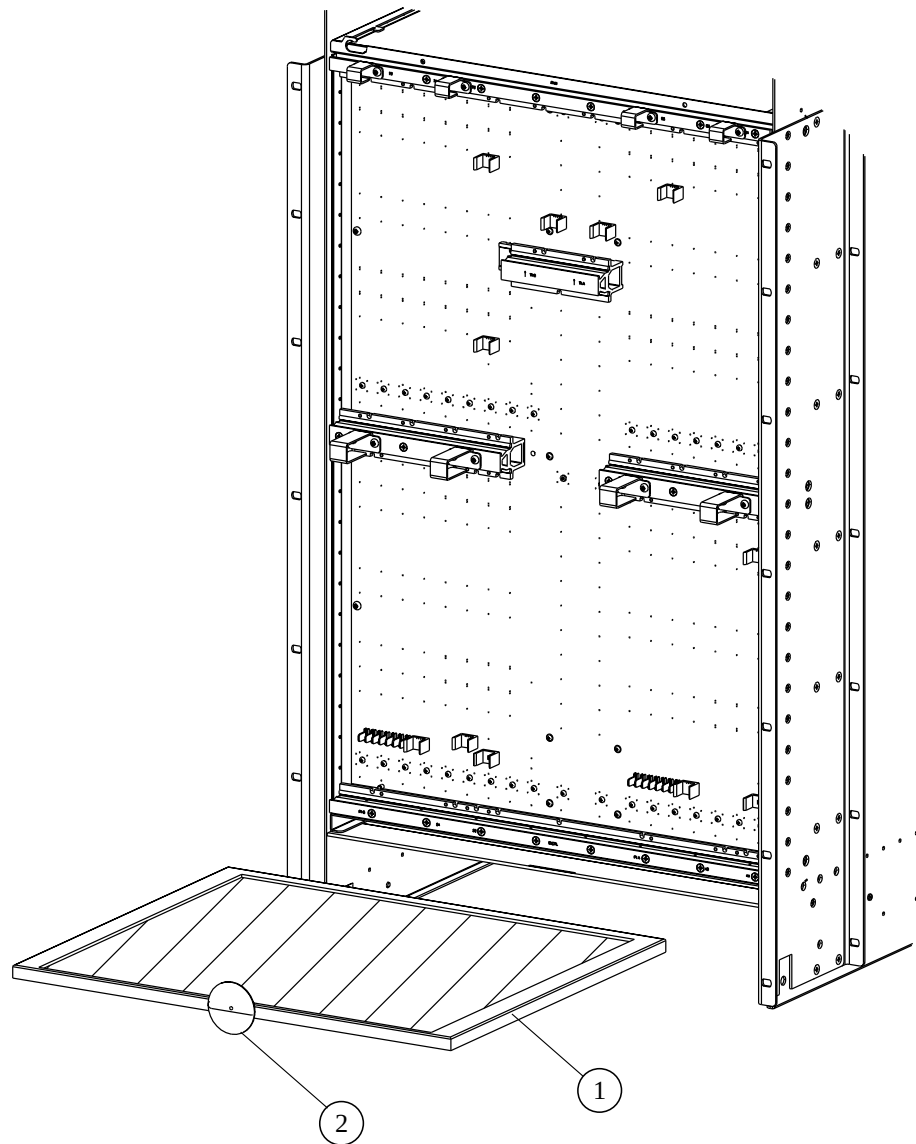


Replacing the air filter

When to use Use this procedure:

- Every 6 months, as a part of routine fan maintenance.
- When instructed to do so as a part of a trouble-clearing task.

Air filter position The following figure illustrates the position of the air filter (1) and its locking/pull tab (2) in the NE rack:



- Air filter types** Two air filter types can be used
- Filter washable — DC1002025
 - Filter disposable — DC1002027

- Before you begin** The following equipment is required to perform this task:
- A replacement air filter (either a new or a cleaned air filter)

Instructions Complete the following steps to replace the air filter.

- 1 Rotate the (one) locking/pull tab (in the middle of the filter) to a horizontal position.
- 2 Remove the air filter by grasping the locking/pull tab and pulling the air filter out of the subrack.
- 3 Insert the replacement air filter into the shelf so that the locking/pull tab is positioned at the rear of the subrack.
- 4 Rotate the locking/pull tab until the air filter is locked in place.
- 5 Discard or clean the dirty air filter.

There are four easy ways recommended to clean Universal's Windowpane, Quadrafoam and Uni-Foam Air Filters:

1. Cleaning using a vacuum cleaner
A few passes of a vacuum cleaner will remove accumulated dust and dirt in seconds.
2. Cleaning using compressed air
Point compressed air nozzle in opposite direction of operating air flow (blow from exhaust side toward intake side).
3. Cleaning using cold water
Under normal conditions the foam media used in Universal's Windowpane, Quadrafoam and Uni-Foam filters require no oily adhesives. Collected dirt is washed away quickly and easily using just a standard hose nozzle with plain water.
4. Cleaning using warm, soapy water

Where stubborn air-borne dirt is present, the filter may be dipped in a solution of warm water and mild detergent. Then simply rinse in clear water, let stand until completely dry and free of moisture, and return to service.

END OF STEPS





13 Security and administration concepts

Overview

Purpose This chapter provides information on security and administration concepts.

Contents

Security management	13-2
User administration	13-3
History logs	13-12

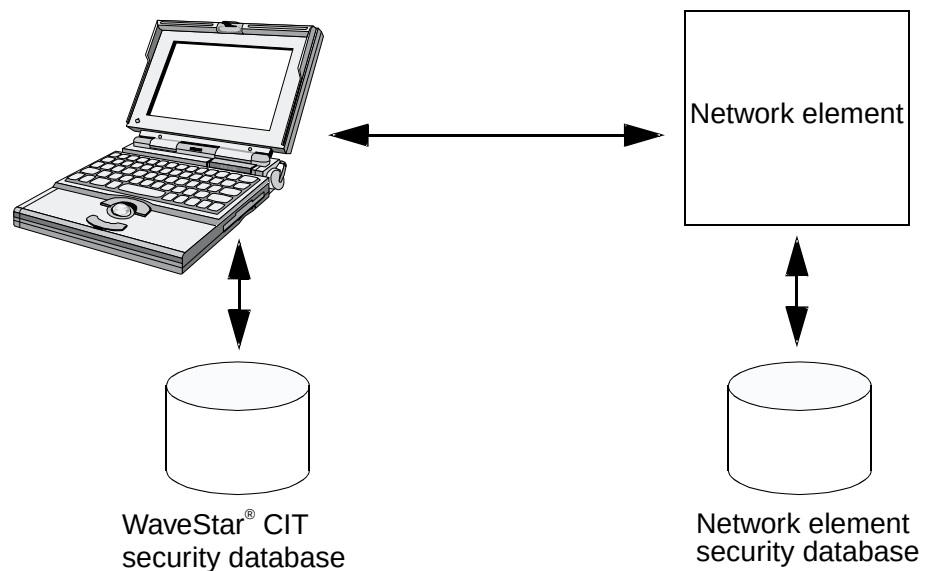


Security management

Access control Access to the *WaveStar*[®] CIT and to *LambdaUnite*[™] MSS network elements is controlled by user logins and associated passwords. User access privileges are defined by authorization levels assigned when the user logins are created.

Security databases A decentralized database concept is used to manage the related security information. The *WaveStar* CIT and the *LambdaUnite* MSS network elements have separate security databases.

The following figure illustrates the decentralized database concept.



Important! Due to the decentralized database concept it is possible that a user may have different passwords for the *WaveStar* CIT and for an NE. The *WaveStar* CIT, however, may “learn” settings from an NE security database.

Simultaneous user sessions Per network element a maximum of 16 sessions are currently possible. □

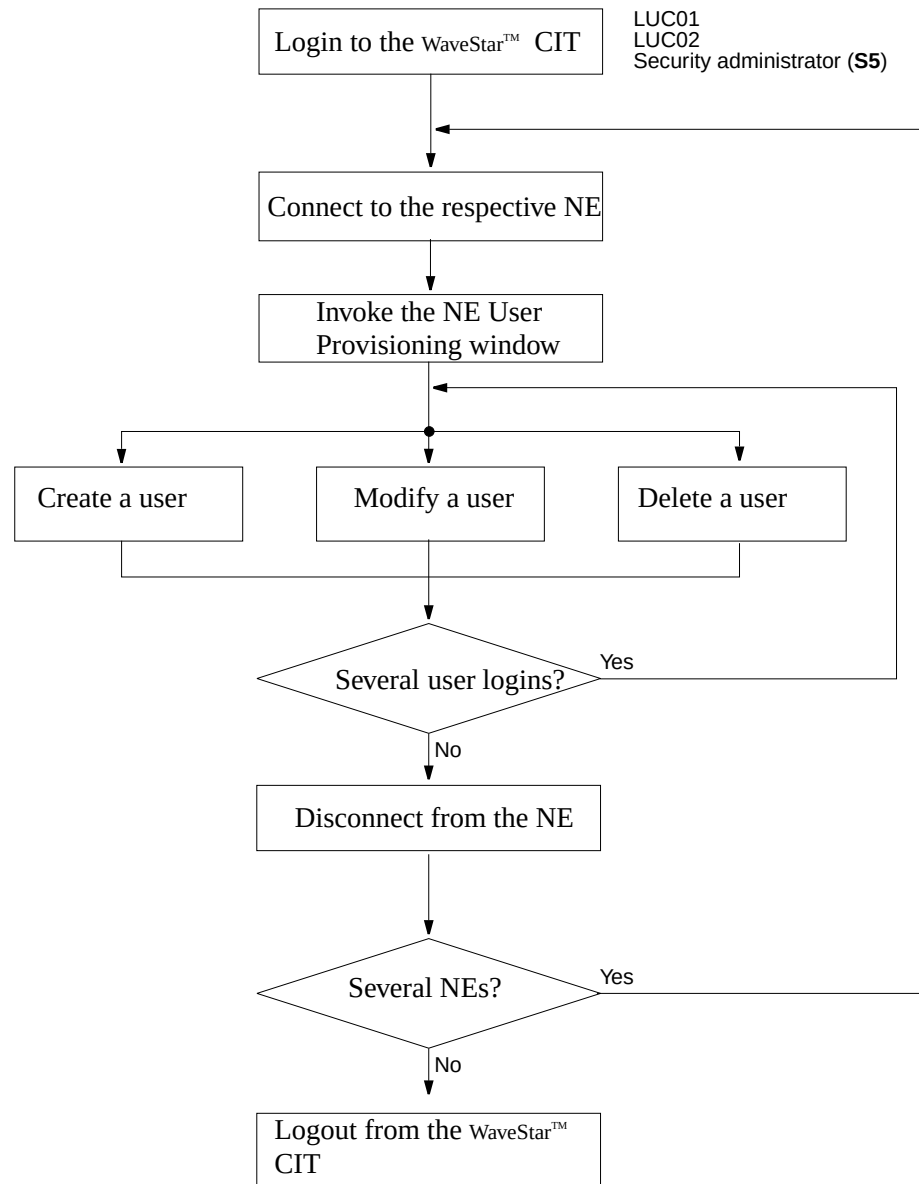
User administration

- Overview** User administration (please refer to “Administering user logins” (2-3)) comprises the following:
- Creating, modifying or deleting user logins,
 - Specifying associated passwords,
 - Assigning access privileges,
 - Enabling/disabling/logging out users,
 - Viewing user details.

User permission Administration on the security databases can only be performed by a security administrator, i.e. a super user login or at least a user login with a security privilege code of ‘S5’ is required.

User administration diagram The following figure gives an outline of the main points of user administration as an overview. The diagram is based on the assumption that a new user or an existing user has or shall have access to both the *WaveStar*[®] CIT and the NEs.

User administration for the *WaveStar* CIT can be done by means of the *WaveStar* CIT **User Provisioning** window (cf. “The NE User Provisioning window” (2-18)).



User login and password Each user must enter a user identification (user login) and a password to gain access to the *WaveStar* CIT or to a *LambdaUnite*™ MSS NE.

To connect to a *LambdaUnite* MSS NE, firstly a login attempt with the same user login and password used for the *WaveStar* CIT login will be made.

Valid user login

The following characters are allowed in a user login:

- Upper-case letters ('A' .. 'Z')
- Lower-case letters ('a' .. 'z')
- Digits ('0' .. '9')

A valid user login consists of a sequence of one to ten characters and is case -sensitive.

Important! The reserved word “ALL” in any combination of uppercase or lowercase letters cannot be used for a valid user login.

Valid password

The following characters are allowed in a password:

- Upper-case letters ('A' .. 'Z')
- Lower-case letters ('a' .. 'z')
- Digits ('0' .. '9')
- Special characters:
 - ' apostrophe
 - % percent sign
 - # number sign
 - - hyphen
 - (left parenthesis
 -) right parenthesis
 - . period, full stop
 - / slash
 - + plus sign
 - ! exclamation mark
 - * asterisk
 - [left square bracket
 -] right square bracket
 - ^ caret
 - ' grave accent
 - { left curly brace

- | vertical bar
- } right curly brace
- < less than
- > greater than
- ~ tilde

The following characters are **not allowed** in a password:

- space
- @ commercial at
- , comma
- : colon
- = equal sign
- " quotation mark
- ; semicolon
- & ampersand
- _ horizontal bar, underscore
- ? question mark

Furthermore, a valid password ...

- consists of a sequence of six to ten characters.
- must start with a letter.
- must contain at least two non-alphabetic characters and at least one special character.

Important! Passwords are case sensitive.

User privilege codes

Users are given access privileges by means of user privilege codes when the user login is created or modified. The user privilege codes determine the tasks a user is permitted to perform. They consist of a combination of one or two letters representing the functional category and a one-digit number representing the authorization level within that functional category.

The following user privilege codes are defined:

Maintenance	M0	M1	M2	M3	M4	M5
Provisioning	P0	P1	P2	P3	P4	P5
Performance Monitoring	PM0	PM1	PM2	PM3	PM4	PM5

Security	–	S1	S2	S3	S4	S5
Test	T0	T1	T2	T3	T4	T5

If a particular authorization level is '0', then there are no access privileges granted for the corresponding functional category, i.e. execution of any of the related tasks is not allowed. Notice that a user privilege code of 'S0' is not allowed and therefore not defined.

A user can be assigned any combination of user privilege codes with the only exception that apart from the two predefined super users (cf. "Super user logins and passwords" (13-10)) no other user can have an authorization level of '5' for all functional categories.

Predefined user types

User types are categorized depending on the task to perform. Some users may have full access to all functions while other users have restricted access.

The six predefined user types with associated user privilege codes are as follows:

Super user	M5	P5	PM5	S5	T5
Privileged user	M5	P5	PM5	S3	T5
General user	M4	P3	PM4	S1	T4
Maintenance user	M4	P3	PM1	S1	T4
Reports only (user)	M1	P1	PM1	S1	T1
Default user	M0	P0	PM0	S1	T0

Priority level

By means of the priority level a priority for the execution of commands can be assigned. For example, if two commands are executed at the same time for the same NE, the command originating from the user with the highest priority level will be executed first.

The priority level range of values is from one to five. The highest priority level is five, the default priority level is one.

Notification list	The notification list indicates the type of notifications a user may receive. The following settings are possible: • Database changes (DBCHG) (only if User receives his/her own command response only is not selected in the Change Notification form.) • State changes (STCHG) (only if User receives his/her own command response only is not selected in the Change Notification form.) • Protection switching changes (PSCHG) (only if User receives his/her own command response only is not selected in the Change Notification form.) • Alarm notifications (ALARMS) (only if User receives his/her own command response only is not selected in the Change Notification form.) • Combinations of the above (only if User receives his/her own command response only is not selected in the Change Notification form.) • Responses to commands initiated by the user (OWN) Responses to commands initiated by the user are always included. • ALL (only if User receives his/her own command response only is not selected in the Change Notification form.)
Inactivity time-out period	The inactivity time-out period indicates the number of minutes of inactivity before a user is logged off. The number of minutes ranges from 0 to 999. The default is 30. A value of zero disables this function.
User class	This is the class of the user, and can have the following values • OTHER This is the default class. For users in this class, command privileges and notifications are controlled only by their UPCs and their Notification Registration List. For users in this class, the ATAG sequence starts with 000 when they log in. Each user session has a unique ATAG sequence. • MEMADMIN

This is a special user class for TL1 Memory Administration OS users. For users IDs assigned to this user class, a special handling of DBCHG notifications is used. The only autonomous messages that MEMADMIN users will receive are DBCHG messages. The ATAG sequence for the autonomous messages is maintained for the entire MEMADMIN user class. In other words, the same ATAG value is used for the same autonomous message sent to all users in the MEMADMIN user class that are logged in. For MEMADMIN users, the ATAG sequence continues during an interruption.

The ATAG sequencing continues:

- across NE/OS loss of communication
- across NE resets
- or if autonomous message reporting is inhibited with the INH-MSG command.

If MEMADMIN is selected, then the User Notification Registration List is set to ***not applicable***. The Modify button in the *WaveStar* CIT **User Provisioning** window is disabled.

Password aging Password aging is the interval before you have to change your password stored on an NE. The password aging interval range is from 7 to 999 days. The default value is 90 days. Select disable to switch off this function.

User id lockout threshold The ***User Id Lockout Threshold*** indicates the number of sequential invalid login attempts after which the user id will be locked out and an ***Intruder Alert Alarm*** will be raised. This parameter is defined for the whole NE. The default value is 5. The number of invalid login attempts ranges from 2 to 99.

User id lockout period The ***User Id Lockout Period*** indicates the number of minutes a user id will be locked out after the number of sequential login attempts exceeds the ***User Id Lockout Threshold***. This parameter is defined for the whole NE. The default is 10. The number of minutes ranges from 0 to 99.

Important! Setting this parameter to 0 will eliminate User Id Lockout.

User id lockout aging period The *User Id Lockout Aging Period* indicates the number of minutes before the NE resets a user’s invalid login attempt count. This is the time period within which the counter of invalid sequential attempts are counted and starts at the first invalid login attempt. For example, if the user has 4 sequential invalid login attempts within this aging period, the invalid attempts counter is 4 and the user has not exceeded the threshold of 5 (i.e., the *User ID Lockout Threshold*). If the user then has another invalid login attempt within this aging period, the threshold will have been exceeded and the user will be locked out for the period defined by the *User Id Lockout Period*. However, if the user does not attempt another login within the lockout aging period, e.g., 60 minutes, the invalid attempts counter is reset to zero. Thus, after 60 minutes from the first invalid login attempt, the user gets another 5 attempts to login before being locked out. Note that both the invalid attempts counter and the aging period are reset to zero whenever a login attempt is successful. This parameter is defined for the whole NE. The default value is 60 minutes. The number of minutes ranges from 1 to 999 minutes.

User id aging period The *User Id Aging Period* is a system-wide parameter. The NE provides the capability to modify this parameter. Its default value is 10 days, with a settable range from 0 days to 999 days, in increments of 1 day. The value 0 disables user ID aging.

History logs The history logs a user can retrieve are defined by the settings in the *registration list* for the specific user.

The following table shows the correlation between the entries in the history logs and the settings in the notification registration list.

History log	DBCHG	STCHG	PSCHG	ALARMS	RESPONS
NE alarm log	–	–	–	✓	–
NE protection switch activity log	–	–	✓	–	–

Super user logins and passwords Two super user logins are preinstalled: “LUC01” and “LUC02”.

The associated passwords are:

- For the *WaveStar* CIT:
 - “LUC+01” and “LUC+02”, if the current *WaveStar* CIT release is the first *WaveStar* CIT installation on the respective PC,
 - the previously defined passwords, if previous releases of the *WaveStar* CIT have already been installed on the respective PC.
- For *LambdaUnite* MSS NEs: “UNITE+01” and “UNITE+02”.

A super user has an authorization level of ‘5’ in all functional categories (cf. “Predefined user types” (13-7)).

The user privilege codes cannot be changed and no other user can be assigned authorization levels of ‘5’ for all functional categories. The super user logins cannot be renamed or removed, and no other super user logins can be added. However, the default passwords can be changed.

Important! If both super user passwords are forgotten, the software containing the logins must be reloaded to recover the preinstalled logins.

□

History logs

Types of history logs	The <i>LambdaUnite</i>[™] MSS system provides the following history logs: • NE alarm log • NE protection switch activity log History logs are used to display history data that is maintained in the network element database.
User dependency	Which history logs will be retrievable by a user depends on the settings in the notification registration list defined during user provisioning; please refer to “Notification list” (13-8).
NE alarm log	The NE alarm log provides a chronological history of all of the most recent anomalous behaviour detected by a <i>LambdaUnite</i> MSS network element. The NE alarm log may contain up to 1024 entries. The NE alarm log can be invoked via Reports → NE Alarm Log... from the System View or Shelf View main menu of the <i>WaveStar</i>[®] CIT.
NE protection switch activity log	The NE protection switch activity log provides a chronological history of all of the most recent manual and automatic protection switching activities. The NE protection switch activity log may contain up to 512 entries. The NE protection switch activity log can be invoked via Reports → NE Protection Switch Activity Log... from the System View or Shelf View main menu of the <i>WaveStar</i> CIT.





14 Management communication setup concepts

Overview

Purpose This chapter deals with the basic theoretical background of Data Communication Networks (DCNs) and provides DCN configuration guidelines for *LambdaUnite*[™] MSS systems.

Contents

Basic DCN principles	14-2
DCN configurations	14-6
DCN configuration guidelines	14-11
Partition repair guidelines	14-12
DCN protocols and services	14-16
NSAP address format	14-19
Data communication channels	14-24
LAN access	14-31
Name-to-address translation	14-32
NE name administration	14-37
System provisioning	14-38



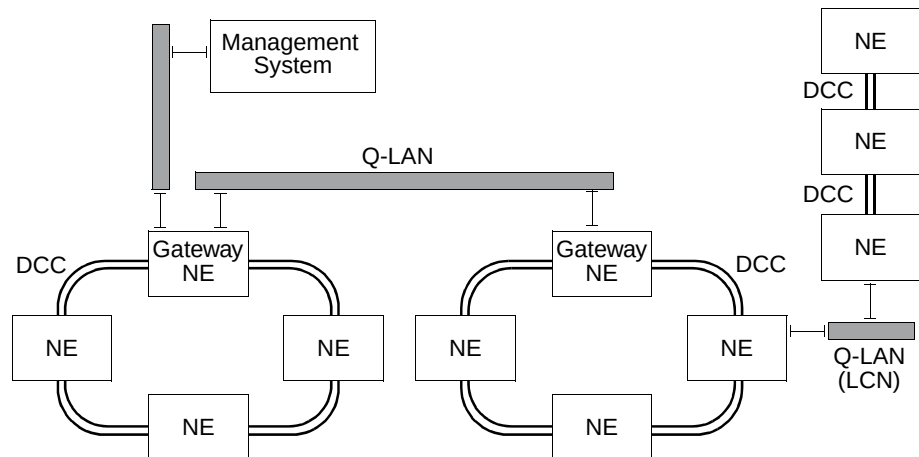
Basic DCN principles

Overview This subsection serves as an entry point, it describes the basic DCN principles. The following subsection describes common DCN configurations. DCN configuration guidelines for *LambdaUnite*[™] products, NSAP address formats and other related information are provided thereafter.

Purpose of a data communication network A Data Communication Network (DCN) is used for the exchange of management data. This section provides an overview of the Data Communication Network and describes the type of communication between the nodes in the network and the used protocols.

SDH/SONET management network The SDH/SONET management network is an overlay network of the transmission network. A management system and the network elements together are the nodes of this network. The Q-LAN and Data Communication Channels (DCCs; cf. “Data communication channels” (14-24)) provide the physical connection between the nodes.

DCN physical components The following figure illustrates an OSI-DCN. The illustration only gives the physical components and connections in the DCN, it does not give the logical configuration.



The illustration of the OSI-DCN consists of 2 Q-LANs and a number of Data Communication Channels (DCCs) in an SDH transmission network (point-to-point configuration and two ring configurations

shown), with a management system (Element Management System (EMS) or Customer Interface Terminal) connected to it. The management system is connected to the transmission network via gateway network elements (GNEs) and the Q-LAN. The network elements are connected to each other by DCCs.

In the case where there is no DCC connectivity between nodes (see the right part of the illustration), a Local Communication Network (LCN) can be used to connect the nodes to each other.

“NE” versus “Node”

Network elements can be identified by their target identifier (TID), i.e. their NE name (“NE name” and “TID” are used synonymously throughout this User Operations Guide), whereas a node is identified by its Network Service Access Point (NSAP) address or its Network Entity Title (NET). Each NSAP address or NET within a network constitutes a node which can individually be addressed. A node represents an End System (ES) (represented by the NSAP address) and/or an Intermediate System (IS) (represented by the NET) in a Data Communications Network (DCN).

DCN protocols

The Protocols used in the DCN between the nodes include:

- Media access protocols:
 - Ethernet on the Q-LAN
 - LAPD on the DCCs
- OSI network routing protocol (DCN wide)
The OSI network routing protocol (OSI-DCN) is used for routing management data between nodes in the DCN.

ISO-OSI network protocols

The network protocols used between nodes are the ISO-OSI network protocols:

- Connectionless Network Service/Connectionless Network Protocol (CLNS/CLNP) acc. to ISO 8473,
- ES-IS routing protocol acc. to ISO 9542,
- IS-IS routing protocol acc. to ISO 10589.

According to these protocols a node in the network can behave as an end system (ES) or as an intermediate system (IS, sometimes also called a router).

End systems	Nodes behaving as end systems perform no forwarding of data packets. They communicate with each other on an end-to-end basis via intermediate systems. End systems (ESs) periodically generate ES Hellos (ESHs) to announce their presence. These ESHs are received and recorded by neighboring intermediate systems. The interval between two ESHs is determined by the End System Configuration Timer (ESCT).
Intermediate systems	Intermediate systems (ISs) are used for routing data between nodes and networks or parts of a network. The end system to intermediate system protocol (ES-IS protocol) is responsible for the exchange of data between an end system and an intermediate system. A network element can act both as an end system as well as an intermediate system. However, a management system, for example, can only act as an end system. Comparable to ESs, ISs periodically generate IS Hellos (ISHs). The interval between two ISHs is determined by the Intermediate System Configuration Timer (ISCT).
ES - IS protocol	The end system to intermediate system protocol (ES-IS protocol) provides information to ISs on the existence of ESs within an area. This information is sent periodically to the ISs via a broadcast mechanism. The ES-IS protocol permits ESs to discover the existence and reachability of ISs and vice versa. Furthermore, the ES-IS protocol provides information to ISs supporting the computation of the shortest path first (SPF) algorithm. <i>LambdaUnite</i> products make use of the ES-IS protocol acc. to ISO 9542.
IS - IS protocol	The intermediate system to intermediate system protocol (IS-IS protocol) is used between intermediate systems in the DCN. The IS-IS protocol maintains the IS Routing Information Base (RIB). The information in the RIB is used by the SPF algorithm for the routing of management data packets in the DCN by the intermediate systems. <i>LambdaUnite</i> products make use of the IS-IS protocol acc. to ISO 10589.
Routing information base and LSPs	Each Routing Information Base comprises a number of routing tables containing information on NSAP addresses of nodes in the network and ports of the IS through which these nodes can be reached.

Intermediate systems exchange routing information regularly with one another as part of the IS-IS protocol by the use of Link State PDUs (Link State Protocol Data Units, LSPs). A Link State PDU contains information about the node itself, about its neighboring ES nodes, and about its neighboring IS nodes.

LSPs exchanged within a level-1 area are called L1-LSPs, LSPs exchanged accross level-2 areas are called L2-LSPs.

OSI routing map and OSI neighbor map

The **OSI Routing Map** and the **OSI Neighbor Map** information that can be retrieved by using the *WaveStar*[®] CIT is derived from a node's internal routing tables and the LSP databases. The LSP database contents are equal in all nodes within an area (distributed database concept).

Please note that when a DCN controller (DCF) is restarted then the LSP databases and the internal routing tables may temporarily contain inconsistent information. As a consequence, the information displayed in the **OSI Routing Map** and the **OSI Neighbor Map** may also be inconsistent. After the DCC controller restart has finished Link State PDUs are exchanged to resynchronise the databases.

Management protocol: TL1

The management of *LambdaUnite* products is based on the use of the Transaction Language 1 (TL1, defined by Telcordia Technologies, formerly Bellcore, standards) on the OSI application layer.

Please also refer to the *LambdaUnite* MSS **TL1 Reference Manual**.

□

DCN configurations

Hierarchical routing Hierarchical routing is used for large networks when the number of NSAP entries in the RIB databases of the intermediate systems becomes too large. When this happens, it causes an exponential increase of exchanged LSPs between intermediate systems. This in turn causes the performance of the DCN to decrease due to the computation of the shortest path first (SPF) algorithm.

Definition of hierarchical routing:

In hierarchical routing, the addressing domain of the DCN is divided into a number of areas. Each area is assigned a unique area identifier. The value of the area identifier of the NSAP address of each node is set according to which area a node belongs (cf. “NSAP address format” (14-19)).

Level-1 IS and level-2 IS Each area contains a number of end systems as well as level-1 and level-2 intermediate systems. Level-1 intermediate systems (level-1 ISs) provide interconnectivity between nodes in an area. Level-2 intermediate systems (level-2 ISs) provide interconnectivity between areas.

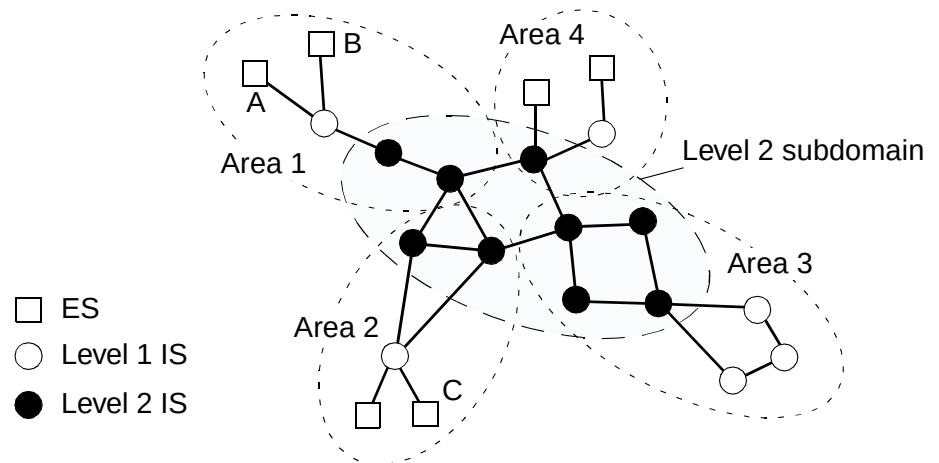
Level-2 subdomain The adjacent set of level-2 ISs is also referred to as the level-2 subdomain. All areas in a network are connected via the level-2 subdomain.

Area-divisioning of a DCN Divisioning is configuring the DCN in such a way that the exchange of LSPs between intermediate systems is limited.

When networks are divided into areas, the RIB databases in the systems are much smaller and hence the routing overhead is significantly reduced. Intermediate systems in an area only exchange information (L1-LSPs) on nodes with other systems in their own area. Information on other areas is exchanged by level 2 ISs only and maintained by the level-2 ISs of the area.

In this way, the load of management data in the network is strongly reduced, while keeping the dynamic re-routing capabilities of intermediate systems in case of failures intact. It is important to notice that although the DCN is divided into areas, ES-ES communication between all nodes in the DCN is still possible.

The following figure illustrates how a network can be divided into areas, connected by level-2 ISs. Each area has at least one level-2 IS assigned and can have a number of level-1 intermediate systems and end systems.



Divisioning at network protocol level

Divisioning of the DCN is usually done at the network protocol level. Communication between intermediate systems is disabled or enabled using different techniques, but this does not necessarily have to affect the physical DCN topology. The SDH/SONET transmission network should in general not be affected by DCN engineering.

Example: Routing of management data

Suppose a node “A” wants to send messages to another node. If this node is in the same area (determined by means of the area identifier of the node’s NSAP address), the messages from “A” to this particular node (“B” in “Area-divisioning of a DCN” (14-7)) are routed directly using a level-1 intermediate system.

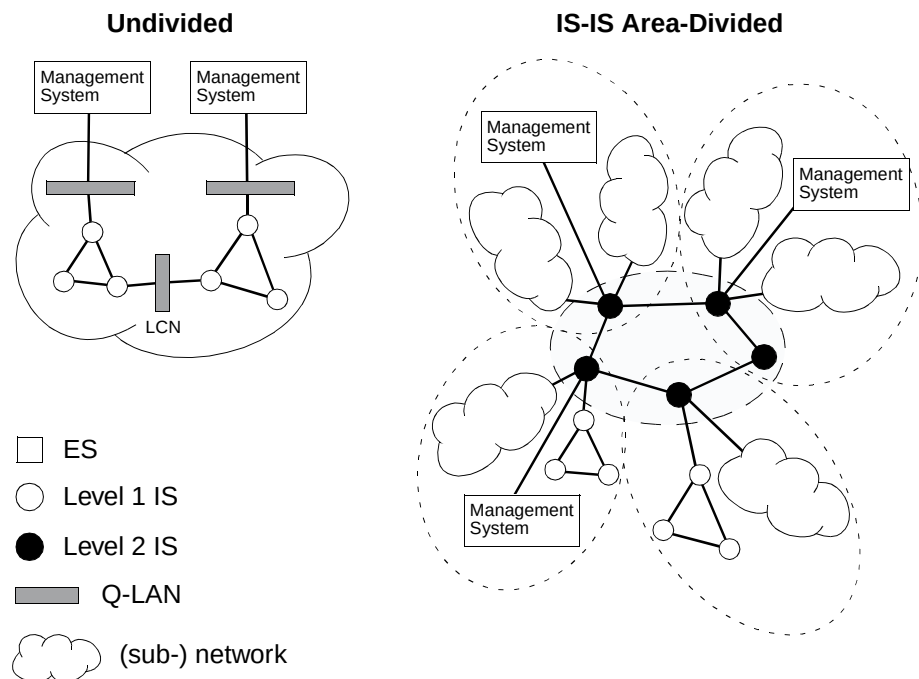
Alternatively, if the desired destination is in a different area (“C” in “Area-divisioning of a DCN” (14-7)), the messages are sent to a second, higher level (level-2) intermediate system. This level-2 IS routes the messages coming from node “A” to other level-2 ISs until they reach a level-2 intermediate system attached to the destination area of “C”. From there, the messages are routed to “C” within the area using one or more level-1 ISs.

Types of OSI-DCN networks

In general the OSI-DCN network can be classified in two types:

- Undivided DCN (single node architecture), or
- IS-IS area-divided DCN (multiple node architecture).

These two types of OSI-DCN network are illustrated in the following figure.



Undivided DCN

An undivided DCN consists of a single area. There is no division between the nodes on network protocol level. All nodes in the network and especially the intermediate systems can exchange routing information with each other. Although a network element can only be managed by one management system at a time, the IS-IS protocol is running between all nodes in the network. This leads to the exchange of LSPs between all intermediate systems in the network.

IS-IS area-divided DCN

The divisioning of the DCN into areas can be accomplished by introducing level-2 intermediate systems (cf. "Area-divisioning of a DCN" (14-6)).

Advantages of areas

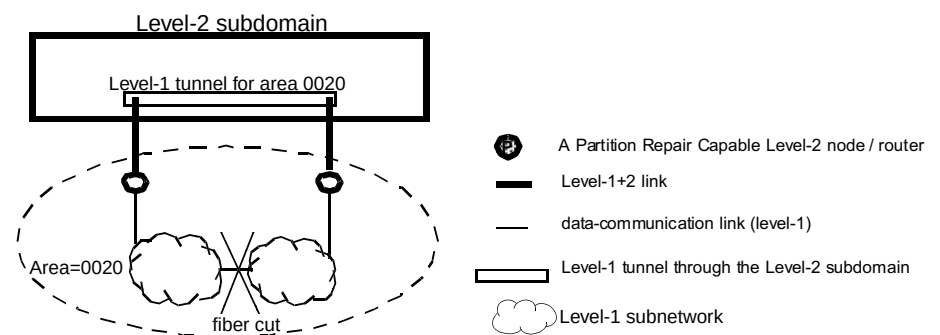
Among others, areas have the following advantages:

- Management systems can be connected to any point in the DCN. As a rule, management systems should be connected to the backbone of the DCN, i.e. to a level-2 intermediate system in the center of their management domain, to prevent them from being overloaded with too much data in the case of a failure resulting in re-routing data traffic.
- The exchange of data is still possible between **all** nodes in the DCN (cf. “Example: Routing of management data” (14-7)).

Partition repair

(Area) Partition repair provides a way to enhance the robustness of the DCN by providing the capability to repair intra-area routing using connections via nodes outside the area. This is done by creating a path outside the area, between two level-2 nodes (which are provisioned to be Partition Capable level-2 nodes) that belong to distinct partitions of the same IS-IS area. Level-1 IS-IS PDUs and CLNP PDUs are encapsulated and transferred over the level-2 path.

Note that network element types that do not support the Partition Repair feature can exist in the “repaired” areas; however, they cannot be part of the level-2 repair path (they are not able to be part of the level-1 tunnel through the level-2 domain).



The terminology that is used in combination with the Partition Repair functionality requires some explanation. A node can be Partition

Repair Capable, Partition Repair Compatible, and Partition Repair Designated. These terms are described below.

- A node is **Partition Repair Capable** if it is provisioned as such. Only possible end points of **Partition Repair** tunnels need to be provisioned as **Partition Repair Capable**. Such possible end points must be **attached** level-2 nodes. (A level-2 node is called **attached** if it is able to forward packets to a different area, even if the level-2 node itself is not on an area boundary.)
- A node is **Partition Repair Compatible** if a partition repair path can pass through the node. No provisioning is needed or required to make a node **Partition Repair Compatible**; this is a property of the stack software.
- A node is **Partition Repair Designated** if all other nodes of its area that are still connected to it via a level-1 path elect it as such. The election is done by choosing one node from the set of still-connected **Partition Repair Capable** nodes. If a **Partition Repair Designated** node of a certain area learns (by listening to level-2 communication) that there is another **Partition Repair Designated** node in the same area, both of these nodes conclude that their area is partitioned. They will then establish a partition repair path between each other.
- The **partition repair path** is a virtual level-1 connection between the two **Partition Repair Designated** nodes that runs through the level-2 domain. Level-1 packets are tunnelled through this virtual connection; this removes the area partitioning.

□

DCN configuration guidelines

- Background information** Please refer to “Basic DCN principles” (14-2) and to “DCN configurations” (14-6). These two sections provide theoretical background information on data communication networks.
- Guidelines** Please observe the following engineering guidelines when configuring a DCN with *LambdaUnite*[™] MSS systems involved:
- A maximum of 50 nodes (i.e. NSAP addresses) is supported in an area.
Notice that a *LambdaUnite* MSS network element can contain one or more **nodes** (please refer to ““NE” versus “Node”” (14-3)).
 - A maximum of 10 areas is supported in a subnetwork.
 - All nodes in an area must have the same area address (cf. “ISO-DCC NSAP address format” (14-20)).
 - All nodes in an area must have DCC connectivity **within the area** to all other nodes in the same area.
 - At least one level-2 IS is required per area in area-divided DCNs for communication accross area boundaries. Two level-2 ISs are recommended in each area for DCC communications redundancy to/from each area.
 - All level-2 ISs must have DCC connectivity, either directly or indirectly via other level-2 ISs, to all other level-2 ISs in the subnetwork to form a single level-2 subdomain that provides connectivity to all areas.
 - To distribute the load of management data in a subnetwork, it is recommended, when feasible, but not required that:
 - all area sizes be approximately the same,
 - and the number of level-2 ISs be about the same as the average area size.

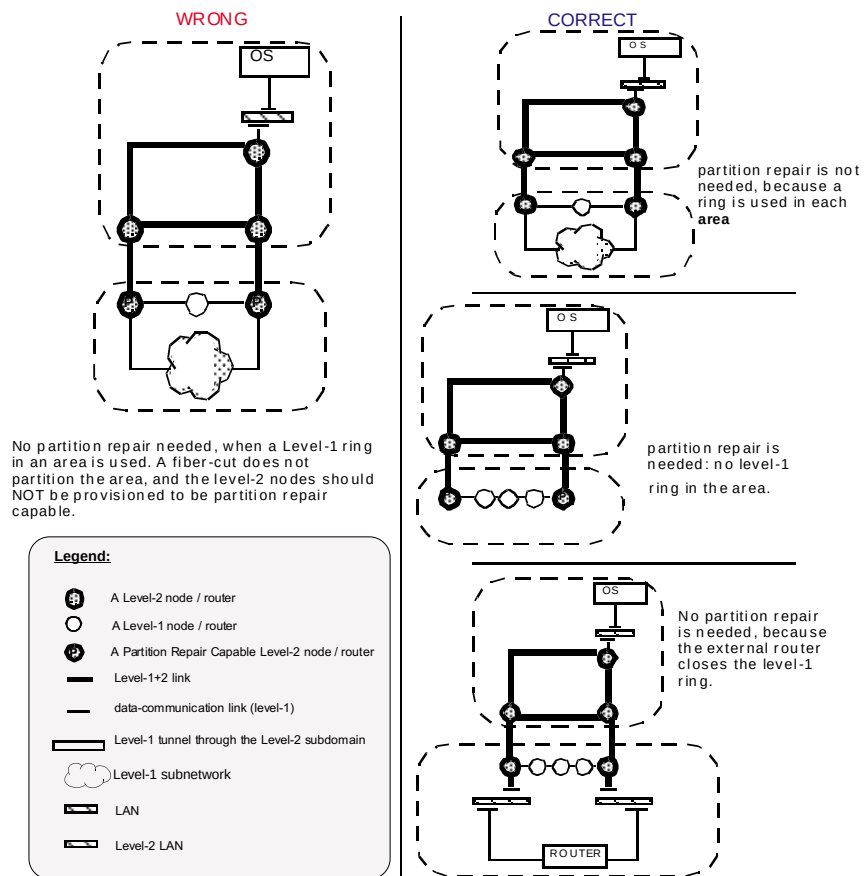
For example, a perfectly balanced subnetwork of 200 nodes would include 20 nodes per area in each of 10 areas and 20 level-2 ISs in the level-2 subdomain (two level-2 ISs per area).
- Related information** Please refer to “NSAP address format” (14-19) and to “Data communication channels” (14-24) for further information.



Partition repair guidelines

When to use partition repair

Only provision nodes to be **Partition Repair Capable** in an area, if a Single Point of Failure can otherwise not be avoided for that area. If more than one Level-2 entry into an area is used, partition repair is a valid mechanism.



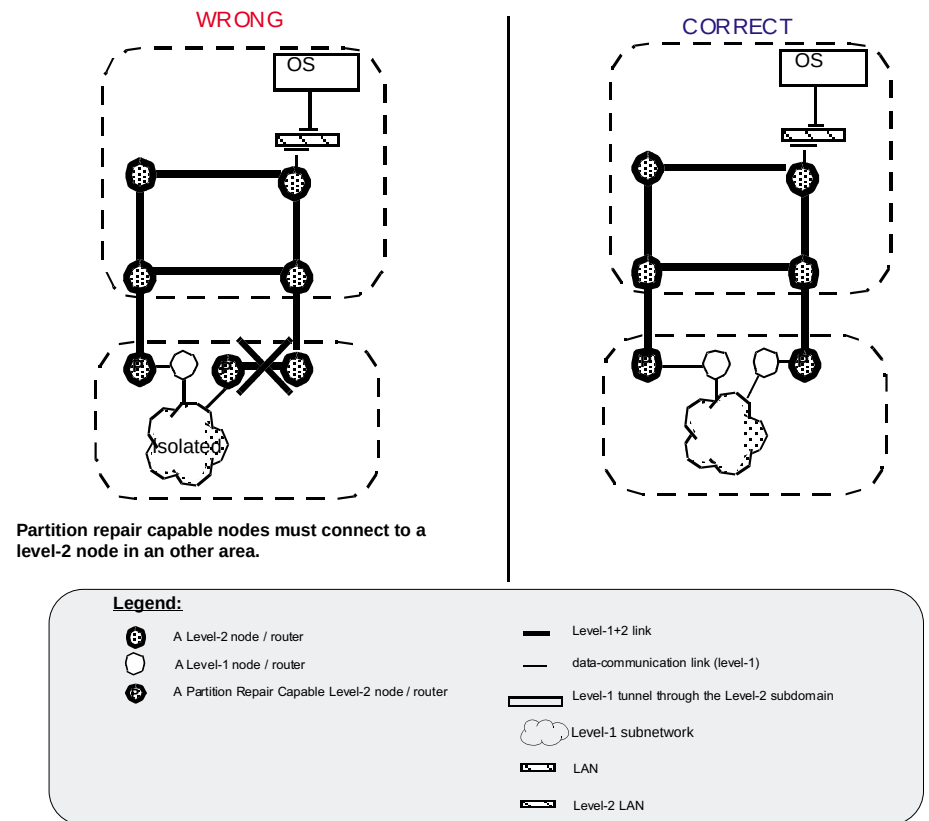
How to use partition repair

To allow the healing of a partitioned area, two nodes must be provisioned as Partition Repair Capable as follows:

- At the area boundary, connecting Level-2 node(s) in (an) other area(s)
- The potential virtual link (tunnel) should reduce the SPoF's in the area to a minimum.

In case an area is partitioned due to a single failure, the two partition repair capable level-2 nodes in each partition will establish a level-1

tunnel through the level-2 subdomain, in order to repair level-1 connectivity between all nodes in the two related partitions.



NE type restrictions

Observe the following NE type restrictions:

- All NE-types, managers and other OSI nodes (like external OSI-routers) are allowed as Level-1 IS nodes or as ES-only nodes, in an area with Partition Repair Capable NE's. When a repair tunnel is established, the partition repair designated NE's will advertise information such, that the tunnel is identified as a normal level-1 route within the area.
- All NE-types and other OSI nodes (like external OSI-routers) are allowed as Level-2 nodes in the Level-2 subdomain, as long as they are not part of the shortest inter-area path between two Partition Repair Capable NE's in an area.

The network is expected to be designed for full management connectivity in case of a single failure. In case of two failures, including a partitioned area and a failure in the shortest potential tunnel route, the network is allowed to drop management connections. Therefore not all OSI-nodes in the Level-2 subdomain need to be partition compatible.

Large network restrictions

Observe the following restrictions regarding large networks:

- The manager (OS/SNMS) connections that are tunnelled through a Level-2 node in case of a single failure, are counted as connections and must therefore be subtracted (like all other rerouted connections through this node) from the maximum number as specified in S-111 in order to identify the maximum number of acceptable connections in the case that the network is in its normal (failure-free) state.

If 50 manager connections can be tunnelled in case of a failure, and 150 manager connections are forwarded in a failure-free network, through one of the nodes in the potential tunnel, the related node must be capable of forwarding 200 manager connections.

The total number of managed NE's in an area can be tunnelled through the Level-2 subdomain with regard to the maximum number of manager connections that can be forwarded by a node. Only the shortest inter-area route between two Partition Repair Capable nodes in an area has to be taken into account.

- The manager (WaveStar[®] CIT/SNMS) connections that are received, encapsulated and forwarded into a partition-repair tunnel, are counted as normal connections. If 100 manager connections can be tunnelled in case of a failure, the related partition designated node must be capable of forwarding 100 manager connections.
- All areas can be provisioned to have one or more Partition Repair Capable node(s).
Each area with one or more Partition Repair Capable nodes requires an extra entry in the routing table (RIB), because of initial selection of a partition repair designated node per area..
- Avoid the use of partition repair capable NE's in large areas.

A DCN network design that selects small level-1 areas to use partition repair, while the large areas are rings that need no partition repair, will be easier to understand. Also it is easier to check that all rules are obeyed.

- The maximum number of Partition Repair Capable NE's in a network is 10.

All partition designated nodes in the level-2 subdomain require an additional entry in the routing table of the other partition designated nodes. Upto 49 additional entries are available, which are all used after a single failure when all 40 areas have Partition Capable nodes and one of those areas is partitioned.

Partitioning restrictions

A maximum of 10 partition repair capable NEs per area is allowed. This implies that the partition repair capable NEs can terminate a maximum of 9 partition repair tunnels. A single cable cut may imply many fiber cuts, of which more than 9 of those fiber cuts may imply partitioning of the same area. A fiber cut between two DWDM nodes may imply a cut of many DCC channels. The Network design shall not use partition repair to cover such topologies.

□

DCN protocols and services

Overview

LambdaUnite[™] MSS network elements support the exchange of management information over DCC or OSI LAN. This network operations capability uses the section DCC bytes in the SDH/SONET overhead of the optical signals. *WaveStar*[®] CIT dialogues and OS messages are transmitted in these DCC bytes.

The *LambdaUnite* MSS OS interface is accessed through one of the 10 of 100 BaseTX Ethernet IAO LAN rear panel connectors. The *LambdaUnite* MSS interface supports Transaction Language 1 (TL1) for commands/messages, and File Transfer and Access Management (FTAM) for software downloads and provisionable data backup and restore.

The *LambdaUnite* MSS OS interfaces supported include the following:

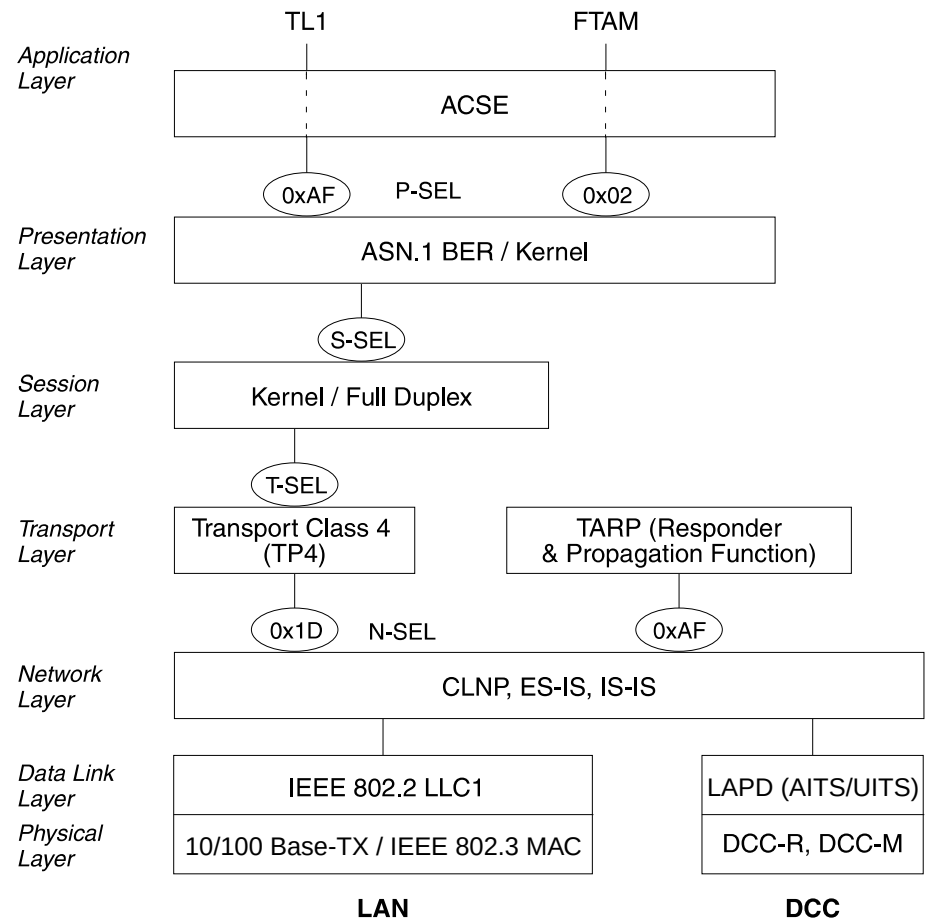
- OSI LAN/WAN
- FTAM (for software download, etc.)

Standard 7-layer OSI stack

LambdaUnite MSS network elements support the exchange of management information over the standard 7-layer OSI protocol stack over Local Area Networks (LAN) and over Data Communication Channels (DCC) acc. to the Telcordia Technologies (formerly Bellcore) GR-253 standard.

Protocols and services

The following figure shows how *LambdaUnite* MSS network elements support the protocols and services.

**FTAM**

File Transfer, Access and Management (FTAM), defined by ISO 8571, is an Application Service Element (ASE). FTAM facilitates file transfer and allows file manipulation across a network. The FTAM protocol is used for *LambdaUnite* MSS software management purposes, such as software download, backup or restoration.

IAO LAN access

The IAO LAN serves two main purposes:

- It provides a standard means of connecting a network element into a central office (CO) data communications network (DCN) to provide OS access
- It provides an alternate path for data communications channel (DCC) communications to travel within a subnetwork.

The *LambdaUnite* MSS IAO LAN is internally connected to the DCC subnetwork so that operations messages on the IAO LAN can be seamlessly delivered to a remote network element by the DCC and vice-versa (DCC to IAO LAN).



NSAP address format

Related information Please refer to “Basic DCN principles” (14-2) and to “DCN configurations” (14-6). These two sections provide theoretical background information on Data Communication Networks.

For related task-oriented procedures, please refer to Chapter 3, “Management communication setup”.

UNITE NE addressing A UNITE NE that runs OSI has at least one node, which is referred to as node-1.

When a node acts as an intermediate system (all nodes), $SEL = 0$, and this implies that we are concerned with the Network Entity Title alone. When a node acts as an end system (node-1), which is where the network services are provided, $SEL \neq 0$, and this implies we are concerned with the NSAPs.

Summarizing, a node is known by its unique NET (see “Network entity title NET” (14-22)). If it provides multiple services, then each service has a unique access point, the NSAP ($NSAP = NET + SEL$). One NSAP differs from the other only in the SEL value.

NSAP address The Network Service Access Point (NSAP) address is used by the network protocol for location information.

The Network Service Access Point (NSAP) Address is the access point where the Network Layer services are available to network service users.

NSAP addresses take on three properties:

1. they must identify a unique entity,
2. they must be globally unique across the network, and
3. routing information cannot be derived from the NSAP address.

Several formats for the NSAP, each with its own syntax and semantics, are possible. GR-253 requires the use of the ISO DCC syntax (20 octets long) for NSAP addresses for SONET nodes. Non-SONET nodes are not restricted to this NSAP format. The syntax selected has no bearing on the routing strategy of the routing protocols used.

ISO-DCC NSAP address format

Although different NSAP formats exist, preferably all nodes in a network should use the same address structure. The *LambdaUnite*[™] MSS supports the 20-byte ISO Data Country Code (DCC) NSAP address format in accordance with ISO 8348.

The figure below represents both the "SONET ISO-DCC" format and the "default SDH ISO-DCC" format. The value of the IDI field is the only difference between the two formats.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
IDP			DSP																
Area Address																			
High Order DSP																			
AFI	IDI + pad		DFI	ORG			RES		RD	AREA		SYSTEM (MAC)						SEL	

The NSAP address consists of the Initial Domain Part (IDP) and the Domain Specific Part (DSP).

The ISO_DCC IDP defines the DSP to be 17 octets long, all coded in direct binary, not preferred binary. The DSP values are allocated by the ISO member body to which the ISO DCC value has been assigned. For the US, ANSI picks the specific DSP format. The DSP is further broken down into the High Order DSP (HO-DSP), followed by the SYSTEM (SysID) and SEL fields.

The first 13 bytes ("AFI" to "AREA" fields) of the NSAP address make up the area address.

The meaning of the individual fields of the ISO-DCC NSAP address is explained in "NSAP address fields" (14-20).

NSAP address fields

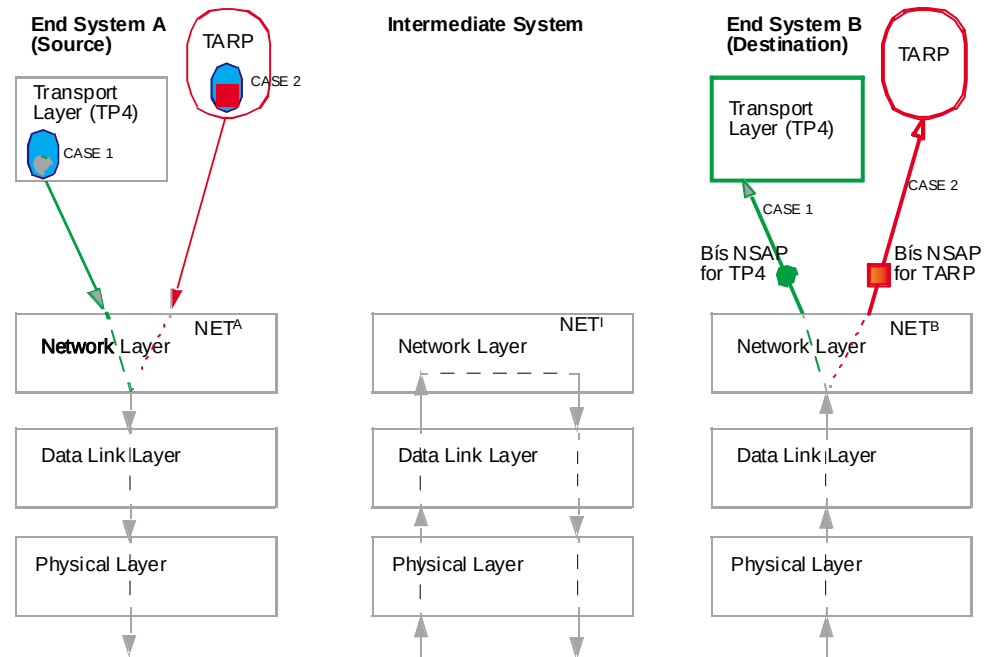
The following table lists the NSAP address fields and describes their meaning.

Field	Meaning	Description
Initial Domain Part (IDP):		
AFI	Authority and Format Identifier specifying the NSAP address format.	The predefined value is 0x39 (hex.), indicating that the ISO Data Country Code (ISO-DCC) is the address format. This field is configurable.
IDI	Initial Domain Identifier specifying the country code.	The predefined value is 0x840F (hex.). This field is configurable.

Field	Meaning	Description
Domain Specific Part (DSP):		
DFI	DSP Format Identifier specifying the DSP format.	The predefined value is 0x80 (hex.). This field is configurable.
ORG	Organization identifier (or Operator identifier) representing the Network Service Provider (NSP).	The predefined value is 0x000000 (hex.). This field is configurable.
Reserved	Reserved portion of the NSAP.	The predefined value is 0x0000 (hex.). This field is configurable.
RD	Routing Domain	The predefined value is 0x0000 (hex.). This field is configurable.
AREA	Area identifier indicating the routing area to which a node belongs (cf. "Hierarchical routing" (14-6)).	The predefined value is 0x0000 (hex.). This field is configurable.
SYSTEM	System identifier representing the node. The IEEE 802.3 MAC address.	A range of 9 subsequent IEEE-MAC numbers is reserved for every UNITE NE, and only one number is physically stored in the backplane SEEPROM of the NE. This field is not configurable .
SEL	The selector field is used to direct the Protocol Data Units (PDUs) to the correct destination making use of the CLNP network layer service.	The predefined value is: • 0x00 (hex.): For the "Network Entity Title", used for exchanging PDUs in the ES-IS and IS-IS routing exchange protocols. • 0x04 (hex.): For the NSAP of CLNP PDUs, containing encapsulated IP packets. • 0x1D (hex.) for PDUs to be processed via the OSI stack • 0xAF (hex.) for PDUs to be processed via the TID Address Resolution Protocol (TARP; cf. "Name-to-address translation" (14-32)). This field is not configurable .

Relationship between NSAP and NET

The figure below describes the relationship between NSAPs and NETs and their roles in PDU transfer between peer Transport/TARP layers. The SONET network SEL for TP4 is used in the example.



NETs define the network entities uniquely from an addressing point of view. They are used for routing decisions by the network layer. NSAPs are only relevant for end systems, because that's where the services are that can be "accessed". The network SEL defines the specific access point, if more than one.

Case 1

The Transport Layer of End System A wishes to communicate with its peer Transport Layer of End System B. A should launch a TP4 PDU containing B's NSAP for TP4 which is: B's NET + SEL=0x1D.

Case 2

TARP of End System A wishes to communicate with its peer TARP of End System B. A should launch a TARP PDU containing B's NSAP for TARP which is: B's NET + SEL=0xAF.

Network entity title NET

The area address together with the system identifier (SYSTEM field) of the NSAP address is also called the Network Entity Title (NET; cf. "ISO-DCC NSAP address format" (14-20)).

The SYSTEM field in the NET of each node has the following value:

- Node-2: the IEEE-MAC address of LAN1 +1
- Node-3: the IEEE-MAC address of LAN1 +2
- Node-4: the IEEE-MAC address of LAN1 +3
- Node-5: the IEEE-MAC address of LAN1 +4
- Node-6: the IEEE-MAC address of LAN1 +5
- Node-7: the IEEE-MAC address of LAN1 +6
- Node-8: the IEEE-MAC address of LAN1 +7
- Node-9: the IEEE-MAC address of LAN1 +8

DCC controller reset All parameters related to DCC communication including all fields of the NSAP address are retained over a DCC controller reset. All parameters are kept in non-volatile memory.

Configuring the NSAP address You can configure the NSAP address on each node-1 in each NE. individually.

Important! Changing the NSAP address causes the DCC controller to be restarted, thus causing momentary loss of communication with the system via that circuit pack.

Additional information For information on how to change the configurable fields of the network element's NSAP address, please refer to "Configuring the basic DCN parameters for an NE" (3-28).



Data communication channels

Exchange of network management information

Network management information can be exchanged between SONET/SDH network elements via Data Communication Channels (DCCs) using the D1-D12 Section Overhead (SOH) bytes of the first STM-1 frame within an STM transmission signal.

The DCC bytes in the overhead of the SONET/SDH signal provide an embedded operations channel at the physical layer. It carries operations traffic, a combination of application messages and protocol management messages, between optically connected NEs.

This makes it possible to set up a Data Communication Network (DCN; cf. “Basic DCN principles” (14-2)) which uses SDH/SONET connections for exchanging network management data.

The DCC uses OSI protocols.

Please note that all nodes in an area must have DCC connectivity **within the area** to all other nodes in the same area (cf. “DCN configuration guidelines” (14-11)).

DCC-R (Section DCC)

The Regenerator Section Data Communication Channel (DCC-R or Section DCC) makes use of the RSOH bytes D1-D3 thus providing a transmission channel with a capacity of 192 kbit/s. The DCC-R is automatically set as the default DCC for provisioned (configured) or pre-provisioned optical interface ports.

MS-DCC (Line DCC)

The Multiplex Section Data Communication Channel (DCC-M or Line DCC) uses the MSOH bytes D4-D12 thus providing a transmission channel with a capacity of 576 kbit/s.

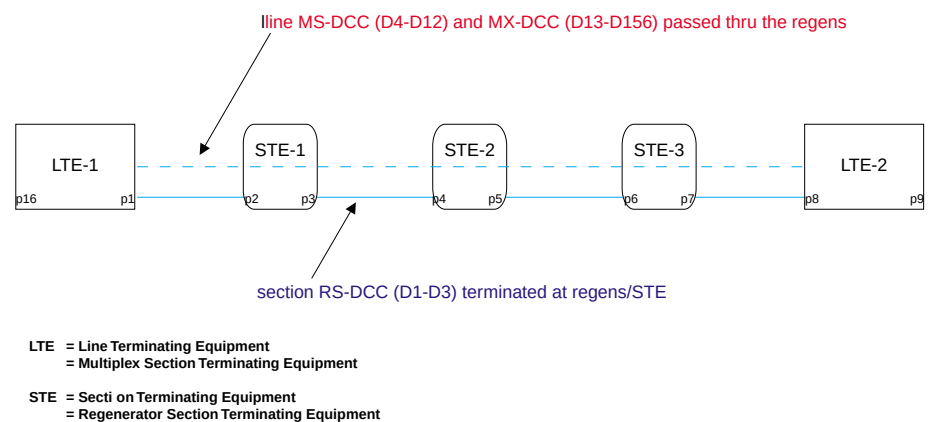
Termination of Data Communication Channels

The *LambdaUnite*[™] MSS system supports the 7-layer OSI protocol stack over the DCC links which terminate on the DCC controller DCF. The controller (DCF and SCF in one circuit pack) circuit pack provides the source and sink of the DCC bytes to and from the active DCC links via LAPD devices. The LAPD protocol acc. to ITU-T Rec. Q.921 is used. You can define DCC links by assigning DCC terminations to optical interface ports.

The NE provides the capability to terminate and originate

- the Section RS-DCC (D1-D3) overhead bytes for all SONET optical interfaces according to ANSI-T1.105.04 and for all SDH optical interfaces according to ITU-T G.784. The SONET optical interfaces include OC-768, OC-192, OC-48. The SDH optical interfaces include STM-256o, STM-64o, STM-16o. The transmit and receive rate for the Section/RS-DCC (SONET/SDH) access is a single bandwidth of 192 Kbit/s in each direction.
- the Line/ MS-DCC (D4-D12) overhead bytes for all SONET optical interfaces according to ANSI-T1.105.04 and for all SDH optical interfaces according to ITU-T G.784. The transmit and receive rate for the Line MS-DCC channel is a single message-based channel of 576 Kbit/ss in each direction.

The following figure illustrates the functional principle.



Max. number of active DCC links

The maximum number of simultaneously supported MS/RS-DCC channels per NE is 64. Each DCC controller thus can support up to 64 active DCC links.

When a circuit pack is inserted into a slot, the RS/MS/MX-DCC on a port are left in disabled state.

The User has to explicitly enable the RS/MS/MX-DCC on a port.

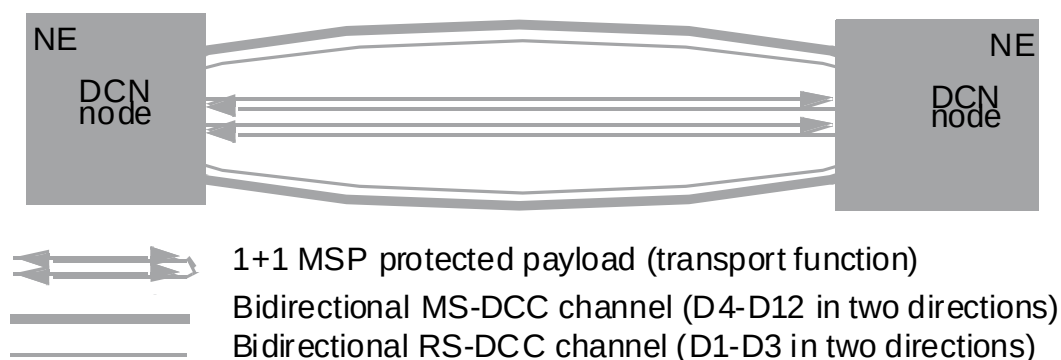
DCC provisioned state A Data Communication Channel (RS/MS/MX-DCC) can be in one of the following provisioned states:

- **Enabled**
 - The corresponding DCC bytes are allocated to an optical interface port.
 - The DCC is assigned a LAPD channel.
- **Disabled**
 - The corresponding DCC bytes are no longer allocated to an optical interface port.
 - The DCC is no longer accessed by a LAPD channel.

The provisioned state of a DCC as well as the LAPD channel assignments are persistent over a DCC controller or NE reset.

DCC protection switching The DCC channels in an APS/MSP protection group are independent of the MS-protection and there is no DCC protection facility in an APS/MSP-pair, other than the layer-3 re-routing facilities of the protocol stack.

The figure below shows the APS/MSP protection of the transport channels (payload), while the two bidirectional MS-DCC channels (subnets) and the two bidirectional RS-DCC channels (subnets) are independent from APS/MSP.



Mandatory DCC access for BLSR/MS-SPRing

The DCC channels are used by the BLSR/MS-SPRING protection facilities to exchange information between the nodes in the BLSR/MS-SPRING ring. The BLSR/MS-SPRING protection is only available after exchange of information via DCC (building a ring map and cross-connect representation).

Node addition/deletion in a 4-fiber ring

The node addition/deletion in a 4-fiber ring requires procedures whereby the DCC is disabled on the affected span to prevent a ring discovery of the new neighbor. In the 4-fiber ring, traffic is forced onto the protection line of a span before the node is added to (deleted from) the working line. DCC is disabled on the working line so that a new ring map is not discovered until the forced span switch is released and the active traffic is on the working line again, and the NE is added to (deleted from) the protection line.

The node addition/deletion scenario in a 4-fiber ring include the following steps:

- FS-R on both adjacent nodes to force the traffic to the protection lines
- All DCC off for the working line on both adjacent nodes
- node insertion into/ deletion from the working line
- Clear to bring the traffic back to the working lines
- node insertion into/ deletion from the protecting line
- enable DCC for the working lines.

The RCS and therefore the ring map discovery only registers to the LinkID neighbour information from the working line. The DCC of the protection line is not used for ring map discovery. If a new neighbor is detected, the ring map is invalidated and protection switching is suspended. Protection switching is resumed after the new map is successfully discovered.

Important! Data Communication Channels used for MS-SPRing management cannot be disabled as long as the MS-SPRing protection group exists and the MS-SPRing management mode is “automatic discovery”.

Creating a BLSR/MS-SPRING protection group

The BLSR/MS-SPRING protection group can only be created when a DCC channel is enabled on the ports in the protection group. For a BLSR/ MS-SPRING ring protection group at least one DCC channel (MS-DCC or RS-DCC or MX-DCC) must be enabled on each working line. See below for the related requirements on enabling/disabling. Only DCC-channels on the working-line of a 4-fiber ring are not used for ring map discovery.

Requirements on enabling/disabling DCC channels

The following requirements have to be observed for enabling/disabling DCC channels in BLSR/MS-SPRING protection groups:

- If there is no DCC (MS-DCC or RS-DCC or MX-DCC) enabled on each port of a 2-fiber BLSR/MS-SPRING protection group, the creation of the protection group is denied.
- If there is no DCC (MS-DCC or RS-DCC or MX-DCC) enabled on each working-line port of a 4-fiber BLSR/MS-SPRING protection group, the creation of the protection group is denied.
- DCC-disabling on a port of a 2-fiber BLSR/MS-SPRING protection group is denied if no other DCC channel (MS-DCC or RS-DCC) is available on that port.
- DCC-disabling on the port of the working line of a 4-fiber BLSR/MS-SPRING protection group is denied if no other DCC channel (MS-DCC or RS-DCC or MX-DCC) is available on that port.

Enabling of DCCs

When a circuit pack is inserted into a slot, the RS/MS on a port is in disabled state. Each RS/MS/MX-DCC has to be enabled explicitly on each port.

The Section/RS-DCC and/or Line/MS-DCC channels of any optical interface port can be enabled, as long as

- the optical port is (pre-)provisioned
- DCC channels are available.

A Data Communication Channel can be enabled manually by user provisioning. Please refer to “Configuring data communication channels” (3-36).

A DCC will be successfully enabled if an LAPD channel exists that can be assigned to this DCC in the unprotected mode.

DCC pre-provisioning

A DCC can be pre-provisioned to be enabled for a provisioned or pre-provisioned optical interface port even if the port is not physically equipped.

Disabling of DCCs

A Data Communication Channel (RS-DCC or MS-DCC) can be disabled in either of the following ways:

- Automatically when an optical interface port is de-provisioned via *WaveStar*® CIT.

When an optical interface port is provisioned to be removed physically (de-provisioned), then all enabled DCCs will be disabled, and the corresponding LAPD channels will be released.

- Manually by user provisioning.
Please refer to “Configuring data communication channels” (3-36).

Important! Disabling a previously enabled DCC at a local NE needs to be coordinated with disabling the same DCC at the opposite end of the DCC link (remote NE) to avoid persistent communication alarms from the remote NE.

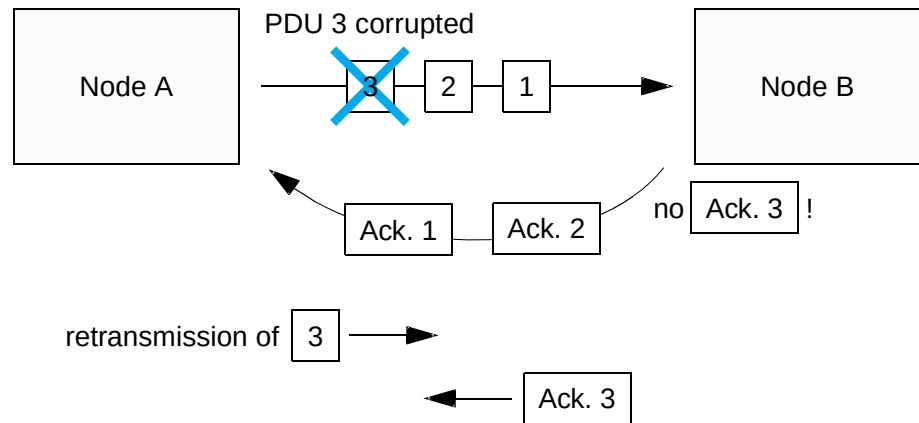
AIMS and UITS supported

LambdaUnite MSS network elements support the Acknowledged Information Transfer Service (AIMS) and the Unacknowledged Information Transfer Service (UITS) as the basis for the LAPD protocol with the UITS mode being the default mode of operation. AIMS should only be used if required by other NE types. UITS is furthermore used for link protocol at the same time when AIMS is chosen.

AIMS and UITS functional principles

In the LAPD protocol, all PDUs are sent with a checksum to verify that the data has not been corrupted during the transmission over the DCC link. If a PDU is received with a bad checksum, it is not acknowledged and will be resent:

- In the ***Unacknowledged Information Transfer Service*** (UITS) (default), corrupted PDUs are ignored and no further actions taken. Upper layers of the OSI stack are responsible for recovery actions.
- In the ***Acknowledged Information Transfer Service*** (AIMS), PDUs are numbered and transmitted sequentially, and acknowledgement PDUs are sent back from the receiver to the sender. If a PDU is lost, that is, if the sender gets no acknowledgement, the PDU is retransmitted.

Functional principle of the AITS

Routing metric The shortest-path-first (SPF) algorithm calculates the preferred route between two nodes based on the cost of a route. The cost of a route is described by a single dimensionless routing metric.

The *LambdaUnite* MSS system makes use of the default routing metric as defined in ISO 10589.

□

LAN access

Overview 4 LAN ports with automatic 10/100BASE-T selection are supported. All LANs have an own MAC address. No hub is supported in HW on the CTL/DCF.

The 4 LAN ports are available as follows:

1. LAN1: Internally connected via the CIP [8] to the CTL/DCF. Accessible on User Panel (UPL), intended for CIT access.
2. LAN2: Internally connected via the CIP to the CTL/DCF. Accessible on LAN I/O-Panel at the rear, intended for EMS access.
3. LAN3: Internally connected via the CIP to the CTL/DCF. Accessible on LAN I/O-Panel at the rear, reserved for future applications (e.g. SNN, or as backup port for the EMS).
4. LAN4: Internally connected via the CIP to the CTL/SCF. Accessible on LAN I/O-Panel at the rear, intended for interworking with Xtreme. This LAN interface is HW-prepared only. There is no protocol definition available yet.

LAN connectors The RJ-45 LAN connectors are located on the User Panel (connector labelled “CIT (LAN)”) and on the LAN I/O-Panel at the rear (connector labelled “LAN 2”).

□

Name-to-address translation

Overview The communication between *LambdaUnite*[™] MSS network elements and their management systems, such as the *WaveStar*[®] CIT, is established by using TL1 command messages.

A TL1 message addresses a network element by its “name”, also referred to as its target identifier (TID), whereas nodes within an OSI network are identified by their NSAP address. Hence a name-to-address translation becomes necessary.

Naming conventions “NE name” and “TID” are used synonymously throughout this User Operations Guide.

TID to NSAP-address translation *LambdaUnite* MSS offers two possible ways to accomplish the TID to NSAP-address translation:

1. A static routing table; please refer to “Static routing” (14-32) (starting below).
2. The TID Address Resolution Protocol (TARP); please refer to “TARP” (14-33).

To establish a management association to a remote NE, the *WaveStar* CIT first evaluates the static routing table. If the corresponding name/address pair cannot be found in the table, the TARP will automatically be used.

Static routing The complete area address part of the NE’s NSAP address is configurable (cf. “NSAP address format” (14-19)). Therefore, the *WaveStar* CIT allows static routing, i.e. the TID-to-NSAP-address translation is realized by using a static routing table (Name/Address List) stored in the *WaveStar* CIT.

The Address List is used to provision the TIDs and NSAPs for NEs that might be connected to the CIT via OSI.

For systems that have no access to an SDS database and which do not support TARP for Name/Address resolution, it is necessary to provide a mechanism to manually enter a list of TID/NSAP pairs.

Static routing table

The static routing table

- must be constructed and maintained manually by a system administrator and
- must be synchronized in **all** *WaveStar* CITs managing the network elements.

TARP

The TID Address Resolution Protocol (TARP) acc. to Telcordia Technologies (formerly Bellcore) GR-253 standard provides a means to perform the TID to NSAP address translation dynamically by means of TARP Protocol Data Units (TARP PDUs), originating from an end system such as the *WaveStar* CIT.

Three basic TARP functionalities can be distinguished:

- TARP propagation functionality
- TARP responder functionality

TARP propagation functionality

The TARP propagation functionality means the ability to evaluate a received TARP PDU type 1, 2 or 5 query and to further broadcast it over the OSI network if the requested TID or NSAP address does not match the NE's TID or NSAP address, and if the requested TID or NSAP address could not be found in the TARP Data Cache (TDC; cf. "TARP data cache" (14-35)).

A TARP propagator decrements the lifetime of a received TARP PDU by one and broadcasts the modified PDU to all of its network neighbors (with the exception of the previous PDU sender). When the TARP PDU lifetime becomes zero, then no further propagation takes place.

TARP responder functionality.

The TARP responder functionality means the ability to respond to a TARP PDU type 1, 2 or 5 query via a type 3 response (cf. "Types of TARP PDUs" (14-33)).

Types of TARP PDUs

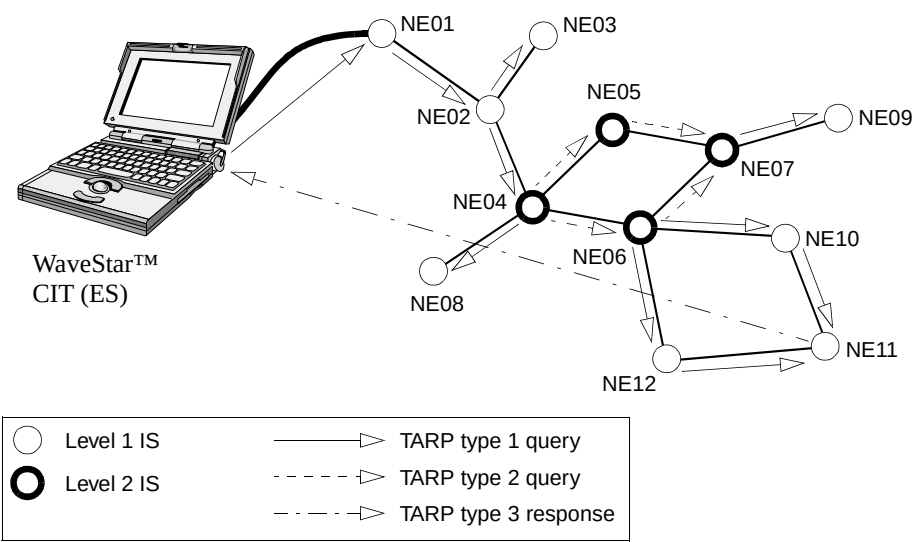
The following table shows the five defined types of TARP PDUs.

Type	Characteristic	Description
1	Query	Given an NE name (TID), the corresponding NSAP address is requested (restricted to IS-IS level-1 area).

Type	Characteristic	Description
2	Query	Given an NE name (TID), the corresponding NSAP address is requested (IS-IS level-1 and 2 areas).
3	Response	Response to a TARP Query.
4	Autonomous notification	Autonomous notification of a TID or NSAP address change, or a reset indication.
5	Query	Given an NSAP address, the corresponding NE name (TID) is requested.

Supported TARP functionality *LambdaUnite* MSS network elements support the TARP propagation and TARP responder functionalities. These functionalities can be either enabled or disabled.

TARP example The following figure shows an example to illustrate the TARP functional principle.



When a user requests to establish a management association to NE11 and the corresponding NSAP address cannot be found in the static routing table, then the *WaveStar* CIT originates a TARP type 1 query. This query will be propagated over the network until it reaches NE11.

NE11 then sends a TARP-type-3 response directly back to the *WaveStar* CIT.

Please note that the TARP Data Cache (TDC; cf. “TARP data cache” (14-35)) was not taken into consideration for this example.

Network services/protocols

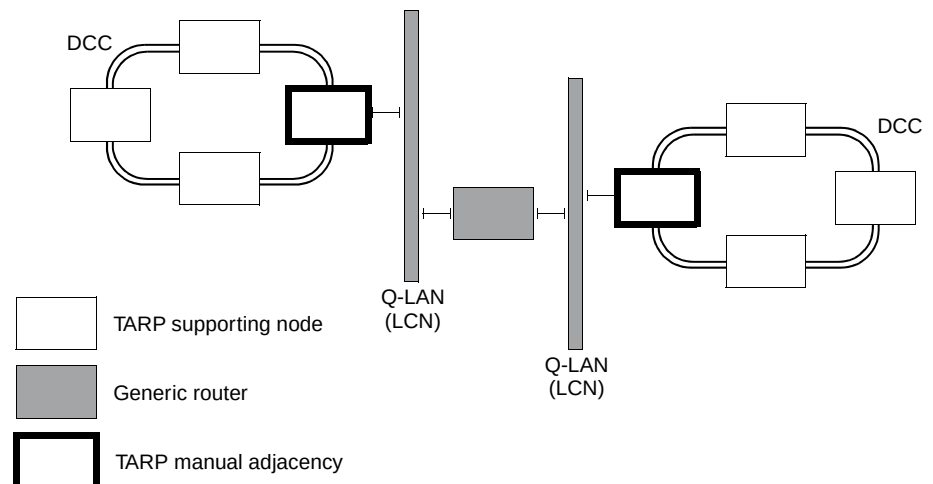
TARP depends on the network layer services and protocols provided by the Connectionless Network Service/Connectionless Network Protocol (CLNS/CLNP) and the ES-IS and IS-IS routing protocols (cf. “ISO-OSI network protocols” (14-3)) to obtain information about the network neighbors of an NE.

TARP data cache

A local database, the TARP Data Cache (TDC), is used in each NE to store information on the NE’s adjacencies, i.e. its direct neighbors in the network. Hence an NE may be able to respond to a TARP query, even if the requested TID or NSAP address does not match the NE’s own TID or NSAP address. Thus, the network performance can be enhanced.

TARP manual adjacencies

By using TARP manual adjacencies it is possible to route TARP PDUs over subnetworks which do not support the TARP functionality. However, a precondition is that the nodes within the non-TARP subnetwork are “generic routers”. A TARP manual adjacency is simply the Network Entity Title (NET; cf. “Network entity title NET” (14-22)) of a node that supports TARP.



Loop detection *LambdaUnite* MSS nodes provide a loop detection mechanism to prevent a repeated processing of previously processed TARP PDUs. A loop detection buffer (LDB) in conjunction with an LDB entry timer and an LDB flush timer is used for this purpose. A previously processed and again received TARP PDU is discarded.

Configuration of TARP parameters For information on the configuration of TARP parameters, please refer to the following procedures:

- “Configuring the TARP parameters for an NE” (3-44),
- “Assigning TARP manual adjacencies” (3-47),
- “Configuring the LDB timers for the *WaveStar* CIT” (3-15).

□

NE name administration

Definition **NE Name (TID)** The NE name, also referred to as the NE's target identifier (TID), is an alphanumeric string of up to 20 characters, used to uniquely identify a network element within the network. "NE name" and "TID" are used synonymously throughout this User Operations Guide.

Configuration rules The following NE name configuration rules must be observed:

- Each NE name must be unique within the network.
- The following characters are allowed in an NE name:
 - Upper-case letters ("A" .. "Z"),
 - Lower-case letters ("a" .. "z"),
 - Special characters("-", "+", "_", ".", "/"),
 - Digits ("0" .. "9").
- An NE name must not end and begin with an special character.
- Each NE name must be maximally 20 characters in length.
- The NE name may contain segments separated by hyphens ("-") or slashes ("/"), but each segment must begin with a letter.

Please note that NE names are case insensitive.

Examples:

The following are examples for valid and invalid NE names.

- "NE-A1", "CHICAGO7" or "NY-B3/C5" are valid NE names.
- "NE-01", "CHICAGO-7" or "NY-3/5" are invalid NE names.

Changing the NE name For information on how to change the NE name, please refer to "Changing the NE name (TID)" (3-3).



System provisioning

Overview System provisioning allows you to configure parameters associated with the entire system.

Parameters The following parameters can be set:

- ***Date***
Selection of year, month and day.
- ***Time***
The time can be displayed in a format specific to the country in which the *WaveStar*[®] CIT is being used.





15 Equipment provisioning concepts

Overview

Purpose This chapter gives you an overview of the hardware components of the *LambdaUnite*[™] MSS network elements which have to be configured.

Contents

Equipment provisioning and autoprovisioning	15-2
<i>WaveStar</i> [®] CIT methods to perform provisioning	15-3
Provisioning of new components	15-5
Shelf configuration	15-6
Overview of access identifiers	15-8
Shelf provisioning	15-13
Slot/circuit pack provisioning	15-14
Port and tributary provisioning	15-15
Gigabit Ethernet (GE1/SX4) Interface	15-16
Equipment protection	15-18



Equipment provisioning and autoprovisioning

What does equipment provisioning mean?

Equipment provisioning is the pre-configuration of network element components before protection groups and cross-connections can be defined.

Provisioning can take place for the first time after the installation of the equipment (initial provisioning) or when re-configuration of the *LambdaUnite*[™] MSS in an existing SDH or SONET network is necessary.

The following components have to be provisioned initially:

- System
- Slots/circuit packs
- Optical ports
- Tributaries

Equipment provisioning can be carried out with the *WaveStar*[®] CIT. The configuration data is placed in the NE and stored in a non-volatile memory (NVM) on the **CompactFlash**[™] card.

Autoprovisioning

Some of the components are autoprovisioned. This means some system parameters are assigned automatically after installation and system start. These are:

- System control and DCC control circuit pack
- Plugged-in Switch circuit packs with timing generator functions
- Synchronization default mode (free running)
- Equipment protection (if two XC320 are available)
- DCC default modes: LAPD role is set automatically via auto-negotiation, DCC_R (Section DCC) and DCC_M (Line DCC) are disabled, AITS mode
- All mandatory circuit packs in the shelf and all circuit packs which are already plugged-in during system start.

A modification of the autoprovisioned parameters is possible.

□

WaveStar[®] CIT methods to perform provisioning

Overview The *WaveStar* CIT supports two different methods, graphical and windows-style explorer, to perform provisioning tasks. You may choose to use only one of the methods or a combination of the two. Generally, you can switch from one method to the other at any time.

Graphical The following steps demonstrate the graphical method.

1 A graphic drawing of the shelf 1-1 is displayed. Note that each port unit has a light-emitting diode (LED) associated with each port. Each LED displays the alarm status (for example, green = no alarm, red = critical alarm, yellow = major alarm, cyan= minor alarm) for the associated port.

2 Place the cursor anywhere on a circuit pack and right-click to select the circuit pack.

3 Place the cursor on a port-unit LED and right-click to select a port on the circuit pack.

4 Select **Provision Circuit Pack** or **Provision Port #** in the pop-up menu to provision the selected circuit pack or port.

All provisionable parameters for the selected circuit pack or port are displayed in the pop-up dialogue box. You can select each parameter and display or change the parameter for a specific application.

END OF STEPS

Windows-style explorer The following steps demonstrate the windows-style method:

- 1 Select **Configuration** → **Provision** in the *WaveStar* CIT Shelf 1-1 window.

Result:

A Windows-style explorer window opens.

- 2 Do one of the following:
 - Enter the AID (for example, 1-1-#-#-1-1) of the desired component in the **Enter AID:** field, or
 - In the left side of the window, click the “+” symbol left to bay 1 to expand bay information.
 1. Select shelf 1-1 in the bay to expand shelf information.
 2. Select the desired circuit pack or slot location.
 3. Select the desired port.
-

- 3 Select the **Provision** button at the bottom of the window.

The provisionable parameters of the selected port are displayed in the right portion of the window. You can select each parameter and display or change the parameter for a specific application.

END OF STEPS



Provisioning of new components

Overview You can add new components to an existing system. This can be necessary during reconfiguration or after installation. The following components can be added:

- Circuit packs
- Protection groups

Invocation Select in the main menu **Configuration** → **Create New**. In the pop-up menu you can select the desired component.

Parameters Already while creating a component you can define some parameters of the respective component:

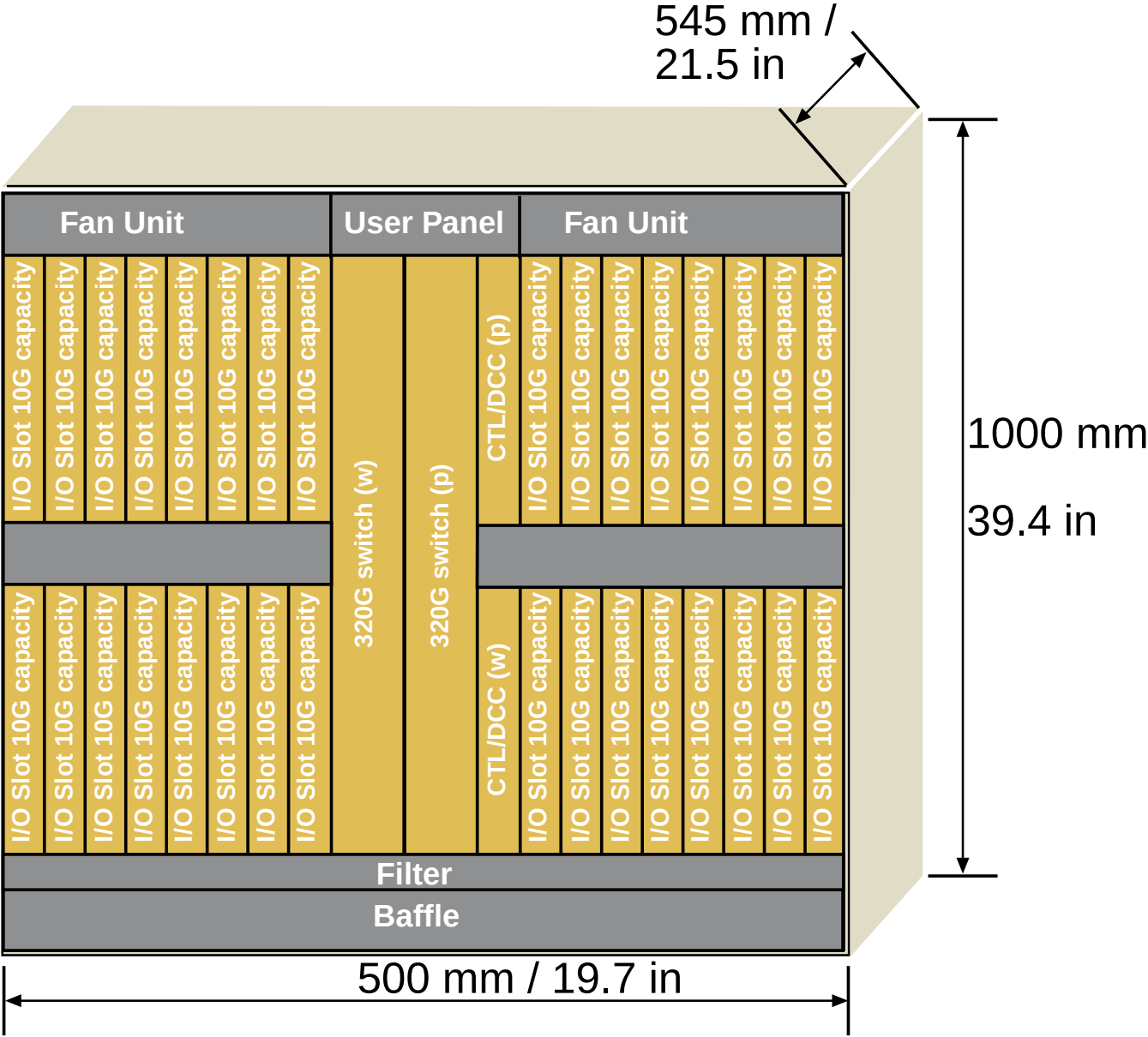
- Circuit Pack
New circuit packs can be established. The circuit pack types can be selected. In the selection window for new circuit packs only the circuit packs, which are suitable for the respective slot can be selected.
- Protection Group
LambdaUnite[™] MSS supports both, SDH and SONET protection features. All entities which are necessary for the creation of a new protection group can be selected. They can be part of the following protection types:
 - 1+1 MSP/1+1 APS
 - MS-SPRing/BLSRFor further information on the protections please refer to “Protection mechanisms” (18-12).

□

Shelf configuration

Overview This chapter describes the configuration of the shelf of the *LambdaUnite™* MSS.

Layout (front view) The following figure depicts the *LambdaUnite* MSS shelf circuit pack slots.



Minimum Complement of Circuit Packs

The minimum complement of circuit packs required for an operational *LambdaUnite* MSS shelf is

- Working XC320 circuit pack (switch and timing functions)
- CTL circuit pack (controller functions)
- Any interface circuit packs in the universal slots

A shelf equipped with these circuit packs would be fully functional. Other essential parts of the system which always have to be installed in the shelf are the Power Interfaces (PI), the fan unit, the User Panel and a CI-CTL.

Circuit Pack Slots

The following table identifies the circuit packs used in the *LambdaUnite* MSS shelf.

Slot Designation	Slot Equipage
universal slots (32)	Any mix of transmission interface circuit packs: • 155 Mbit/s port units (future release) • 622 Mbit/s port units (future release) • 2.5 Gbit/s port units • 10 Gbit/s port units • 40 Gbit/s port units (future release) • 1 Gigabit Ethernet interface • 10 Gigabit Ethernet interface (future release)
Controller slot (working)	CTL circuit pack. System controller including non-volatile memory and DCC controller for the whole network element.
Controller slot (protection)	Reserved for future use.
320G switch slot (working)	The switching circuit pack in this slot can make cross-connections for 6144 STS-1 / 2048 VC-4 equivalent circuits. This switch is paired with 320G switch (protection) in a 1+1 non-revertive protection mode configuration. Furthermore, this circuit pack contains the timing generator function for the NE.
320G switch slot (protection)	The switching circuit pack in this slot can make cross-connections for 6144 STS-1 / 2048 VC-4 equivalent circuits. This switch is paired with 320G switch (working) in a 1+1 non-revertive protection mode configuration. Furthermore, this circuit pack contains the timing generator function for the NE. After initial power up of the system this circuit pack is in standby mode.

Overview of access identifiers

Overview Access identifiers (AIDs) are used for addressing particular components within a *LambdaUnite*™ MSS system, like a shelf, circuit pack, slot or port, for example. An AID is case-insensitive, but AID values are usually given in lower case.

Hierarchical structure AIDs are hierarchically structured. The following table provides an overview of the general AID structure by presenting some examples.

Entity	Format	Example
Network element	bay	1
Shelf	bay-shelf	1-1
Protection group	bay-shelf- protection group	1-1-t001
Slot	bay-shelf-##-slot	1-1-##-1
Circuit pack	bay-shelf-##-slot-cp	1-1-##-1-cp
Port	bay-shelf-##-slot-port	1-1-##-1-1
Tributary	bay-shelf-##-slot-port-trib	1-1-##-1-1-1

The entity network element refers to a logical unit which can be composed of up to the shelf.

The “#” character serves as a wildcard if a particular AID field cannot be specified, instead of leaving the field empty.

General AID structure The general AID structure is based on the assumption that there is a hierarchy associated with the system entities in the order of bay, shelf, protection group, line/side, slot, port/circuit pack and tributary. Therefore, the general structure consists of these entities separated by “-”:

- ***bay-shelf-protection group-line/side-slot-port/circuit pack-tributary***

Some entities such as the system itself fall out of this hierarchy and are handled separately.

An AID may not exceed 20 characters in length (including “-”).

Simple and compound AIDs

Access identifiers can be distinguished into simple and compound AIDs. For example, “system” or “estgrp” are simple AIDs. Compound AIDs follow the general AID structure given in the previous paragraph.

Please refer to “Overview of AIDs” (15-9) for an overview of *LambdaUnite* MSS AIDs.

The “all” AID entry

Access identifiers allow for the specification of a range of entities by using the term **all**. The **all** AID entry may be used in the bay, shelf, slot, port, and tributary fields. It can neither be used in the protection group field nor in the side/line field.

If **all** is used in the bay and/or shelf AID fields, it cannot be used in any other AID fields.

Overview of AIDs

The following table gives an overview of the access identifiers defined for *LambdaUnite* MSS. If there are several values possible for an entry, they are given in curly braces ({ }).

Entity	Access Identifier
System	
system	system
Nodes	
OSI Nodes	osinode{1-9} osinodeall
Bay	
Bay	1 all
Shelf	
Shelf	1-1 1-all
Protection Group	
1+1 Facility Protection Group	1-1-o{001-999} 1-1-oall
1:N Facility Protection Group	1-1-n{001-999} 1-1-nall
2-F BLSR Facility Protection Group	1-1-t{001-999} 1-1-tall

Entity	Access Identifier
4-F BLSR Facility Protection Group	1-1-f{001-999} 1-1-fall
1+1 Switch and Timing Equipment Protection Group	1-1-estgrp
1+1 System Controller Equipment Protection Group	1-1-ectlgrp
Slot	
All slots	1-1-#-#-all
Universal Slots	1-1-#-#-{1-8, 12-19, 21-28, 32-39} 1-1-#-#-all 1-1-#-#-usall
Cross-Connect Slots	1-1-#-#-xcp 1-1-#-#-xcw 1-1-#-#-xcall
Controller Slots	1-1-#-#-ctlp 1-1-#-#-ctlw 1-1-#-#-ctlall
Circuit Packs	
Universal Slots Circuit Packs	1-1-#-#-{1-8, 12-19, 21-28, 32-39}-cp 1-1-#-#-all-cp
Cross-Connect Circuit Packs	1-1-#-#-xcp-cp 1-1-#-#-xcw-cp 1-1-#-#-xcall-cp
Controller Circuit Packs	1-1-#-#-ctlp-cp 1-1-#-#-ctlw-cp 1-1-#-#-ctlall-cp
NVM	
NVM	1-1-#-#-ctlp-nvm 1-1-#-#-ctlw-nvm 1-1-#-#-ctlall-nvm
Port	
I/O Port (Generic type)	1-1-#-#-{1-8, 12-19, 21-28, 32-39}-{1-4} 1-1-#-#-{1-8, 12-19, 21-28, 32-39}-all
LAN Ports	1-1-lan{1-3} 1-1-lanall

Entity	Access Identifier
Virtual Concatenation Group (VCG)	1-1-#-#-{1-8, 12-19, 21-28, 32-39}-v{1-4} 1-1-#-#-{1-8, 12-19, 21-28, 32-39}-vall
<i>Tributary</i>	
AU-3/STS-1 Tributary	1-1-#-#-{1-8, 12-19, 21-28, 32-39}-{1-4}-{1-768} 1-1-#-#-{1-8, 12-19, 21-28, 32-39}-{1-4}-all
VCG Tributary	1-1-#-#-{1-8, 12-19, 21-28, 32-39}-v{1-4}-{1-21} 1-1-#-#-{1-8, 12-19, 21-28, 32-39}-v{1-4}-all
<i>Interfaces</i>	
Power Interfaces	1-1-pia 1-1-pib 1-1-piall
Timing Interfaces	1-1-tia 1-1-tib 1-1-tiall
Backplane	1-1-backpl
User panel	1-1-usrpnl
CI-CTL	1-1-cictl
<i>Fans</i>	
Fan unit	1-1-fan 1-1-fanall
<i>External Timing References</i>	
External Timing reference	extref1 extref2 extrefall
Line Timing references	line1 line2 line3 line4 line5 line6 lineall
<i>Timing Ports</i>	
External Timing Input Port	exttmg0 exttmg1 exttmgall

Entity	Access Identifier
External Timing Output Port	exttmg0_out
	exttmg1_out
	exttmgall_out
Timing Output	outtmg

Shelf provisioning

Overview Shelf provisioning allows the user to configure parameters associated with the shelf.

Parameters The following parameter can be viewed:

- ***Shelf AID***

The following parameter can be set:

- ***Alarm Severity Assignment Profile*** (cf. “Alarm severity assignment profiles” (16-25))

An Alarm Severity Assignment Profile (ASAP) is a list of alarms that can occur in an NE and which have each an alarm severity assigned. Several ASAPs for different functional categories are predefined for the *LambdaUnite*[™] MSS system.

□

Slot/circuit pack provisioning

Slot provisioning Slot provisioning allows the user to configure parameters associated with a specific slot.

Parameter The *Alarm Severity Assignment Profile* (cf. “Alarm severity assignment profiles” (16-25)) can be selected.

Circuit pack provisioning Circuit pack provisioning allows the user to configure parameters associated with a specific circuit pack.

Parameters The *Alarm Severity Assignment Profile* (cf. “Alarm severity assignment profiles” (16-25)) can be selected.

ASAPs An Alarm Severity Assignment Profile (ASAP) is a list of alarms that can occur in an NE and which have each an alarm severity assigned. Several ASAPs for different functional categories are predefined for the *LambdaUnite*[™] MSS system.

□

Port and tributary provisioning

Optical ports Optical port provisioning allows the user to configure parameters associated with a specific optical port (cf. “Configuring an optical SDH/SONET port” (4-16)).

Tributary provisioning Tributary provisioning allows the user to configure parameters associated with a specific tributary belonging to a port (cf. “Configuring a tributary” (4-26)).



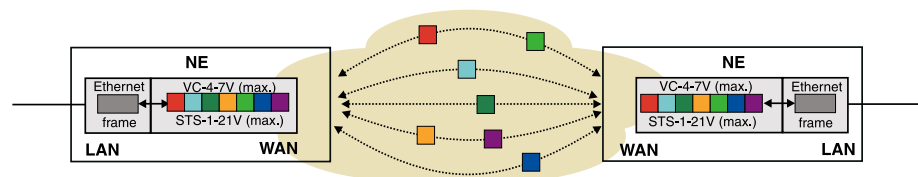
Gigabit Ethernet (GE1/SX4) Interface

Overview *LambdaUnite*[™] MSS supports a Gigabit Ethernet interface. The GE1/SX4 interface conforms to the standards outlined in IEEE 802.3, and supports the 1000BASE-SX protocol.

Capabilities The GE1/SX4 interface supported by the *LambdaUnite* MSS allows you to transport Gigabit Ethernet (GbE) signals over SONET/SDH networks by encapsulating ethernet packets in virtually concatenated SPEs/VCs. Each GE1/SX4 port unit offers four 1000BASE-SX Ethernet LAN ports. The GbE interface supports point-to-point connectivity. The capacity per GbE line is 21 STS-1s/7 VC-4s.

Virtual concatenation STS-1/VC-4 concatenation can be used for the transport of payloads that do not fit efficiently into the standard set of synchronous payload envelopes (SONET) or virtual containers (SDH). Virtual concatenation splits the contiguous bandwidth into individual SPEs/VCs, transports these SPEs/VCs and recombines them to a contiguous functionality only at the path termination equipment, i.e. the GE1/SX4 Gigabit Ethernet circuit pack.

The following figure shows the principle of virtual concatenation in a point-to-point Gigabit Ethernet (GbE) network application example. Protection of the STS-1-Kv/VC-4-kv traffic is possible via UPSR/SNCP and in ring topologies via BLSR/MS-SPRing protection schemes.



The H4 POH byte is used for the sequence and multi-frame indication specific for virtual concatenation.

Due to different propagation delay of the STS-1s/VC-4s a differential delay will occur between the individual STS-1s/VC-4s. This differential delay has to be compensated and the individual STS-1s/VC-4s have to be re-aligned for access to the contiguous

payload area. The *LambdaUnite* MSS re-alignment process covers at least a differential delay of 32 ms.

Operation The *LambdaUnite* MSS operates in point-to-point LAN bridge promiscuous mode. In promiscuous mode all Ethernet packets forwarded without address filtering. Provisioning of the Gigabit Ethernet interface is not necessary.

□

Equipment protection

Principle An equipment protection always involves one or more plug-in units which carry traffic (**working** plug-in unit) and one plug-in unit which will assume the function of a plug-in unit that has failed (**protection** plug-in unit). Together they form a **protection group**.

Types For the following objects, equipment protection is supported:

- Cross-connect and timing generator circuit pack XC320: 1+1
- Redundant power supply

Cross-connect and timing generator unit protection

A XC320 can be protected 1+1 by another XC320. Both the cross-connect function as well as the timing function are protected on this way and build a single protection object. The equipment protection process of the XC320 will be fully performed by a central process in the CTL.

The standby XC320 works in the so called hot-standby modus, which means both XC320 work in parallel. The whole configuration of the XC320 is broadcasted by the CTL to both the active as well as the standby unit.

Creation

The equipment protection group is created automatically if the second XC320 unit is plugged in the shelf.

Operation

The XC320 equipment protection operates in non-revertive mode.

Redundant power supply

The power feed is maintained duplicated throughout the system. Two redundant power supply inputs are available per shelf. The A (working) and B (protection) power inputs are supervised individually by the system controller circuit pack (CTL). The input voltage is below a threshold of $39.0\text{ V} \pm 1.0\text{ V}$, an alarm message will be sent to the CTL.

□



16 Alarm management concepts

Overview

Purpose

Contents

<i>LambdaUnite</i>[™] MSS fault management	<u>16-2</u>
<i>LambdaUnite</i> CIT alarm presentation formats	<u>16-9</u>
Alarm severities	<u>16-10</u>
Alarm format preferences	<u>16-12</u>
Signalling of alarms	<u>16-17</u>
<i>WaveStar</i> [®] CIT visual alarm indicators	<u>16-19</u>
NE local indications	<u>16-21</u>
Impact of state changes on the signalling of alarms	<u>16-22</u>
Alarm provisioning	<u>16-24</u>
Operations interfaces	<u>16-38</u>
The <i>LambdaUnite</i> MSS user panel	<u>16-39</u>
ACO interaction with an alarm test	<u>16-42</u>
Circuit pack status indicators	<u>16-44</u>
Office alarm interfaces	<u>16-48</u>



LambdaUnite[™] MSS fault management

Overview

Purpose The present section describes the behaviour of *LambdaUnite* MSS network elements with respect to fault management.

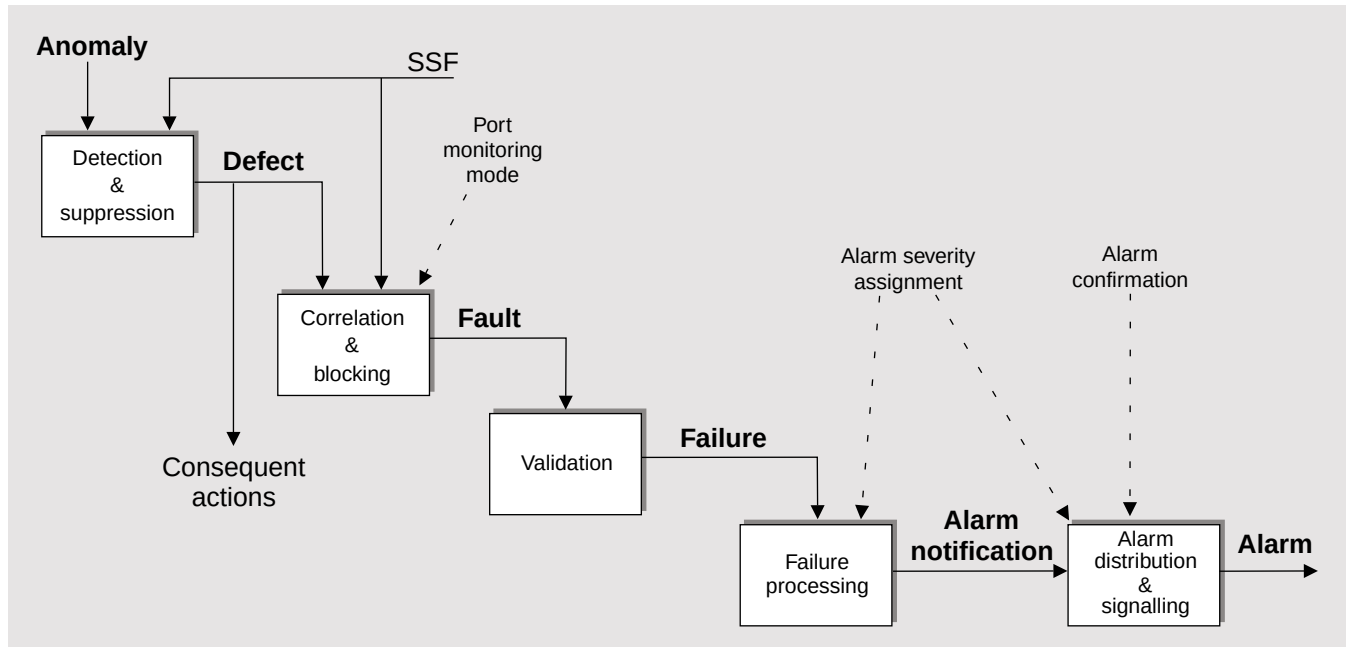
Fault management deals with the detection and the reporting of particular degraded conditions by the network elements and the resulting actions.



Basic fault management concepts

Fault management process

The following figure illustrates the fault management process in conjunction with the main influencing factors (visualized by means of dashed lines), such as the port monitoring mode for example.



Occurrences of degraded conditions are detected by the functional system components (a circuit pack for example) of a *LambdaUnite™* MSS network element (NE) as defects, derived from anomalies.

Faults may be generated as a consequence of evaluating existing defects. The evaluation of defects comprises correlation and blocking. When a fault persists for a pre-defined observation period (“raise validation time”), a corresponding failure is declared and reported to the management systems and to the local alarm interfaces by means of an alarm notification.

When the defect is absent for a pre-defined observation period (“clear validation time”), then the failure is cleared, and an appropriate alarm clear notification is sent.

Definitions

Anomaly An anomaly is the smallest observable discrepancy between the actual and the desired characteristic of a system

component. The occurrence of a single anomaly does not interrupt the ability to perform a required function.

SSF A Server Signal Fail (SSF) indicates that a Signal Fail (SF) condition is present on a server layer. A Signal Fail condition exists when the server signal contains AIS, or when a defect is detected which leads to the insertion of AIS.

Defect A defect is the limited interruption of a system component's ability to perform a required function. An anomaly becomes a defect when it persists for a significant amount of time (persistency check). For transmission defects this can be three signal frames in sequence for example. The detection of defects is suppressed when the corresponding server layer indicates a signal fail condition (SSF). Local indications via the "FAULT" LED on the circuit pack faceplate and the insertion of consequent actions, for example insertion of an Alarm Indication Signal (AIS) or a Remote Defect Indication (RDI), are controlled by defects.

Correlation Correlation means the calculation of faults based on the existence of defects.

The relation between defects and faults can be either

- 1:1, i.e. one defect corresponds exactly to one fault, or
- n:1, i.e. several defects lead to the same fault.

Blocking Blocking is closely related to correlation. It means the suppression of faults due to the existence of specific defects.

Fault A fault (or "correlated fault cause") is the inability of a system component to perform a required function. Faults may be declared dependent on the evaluation of defects.

Validation Validation is the mechanism that prevents alarming of faults whose presence, or absence in the case of alarm clearing, is shorter than the relevant observation period (validation time).

Failure A failure is the termination of a system component's ability to perform a required function. If a fault is present for at least its raise validation time it becomes a failure. There is a 1:1 relation between faults and failures.

Alarm notification Alarm notifications are used to inform management systems and local alarm interfaces on the presence or absence of alarms. An alarm notification is a system message

containing information on a failure condition, such as the probable cause, the alarm category, the time of occurrence, the alarm severity, the affect on service etc.

Alarm An alarm is a human observable alerting indication, visually or acoustically for example, to a condition that may have immediate or potential negative impact on the state of the monitoring network element.

Port monitoring mode Please refer to “Port monitoring mode” (16-34).

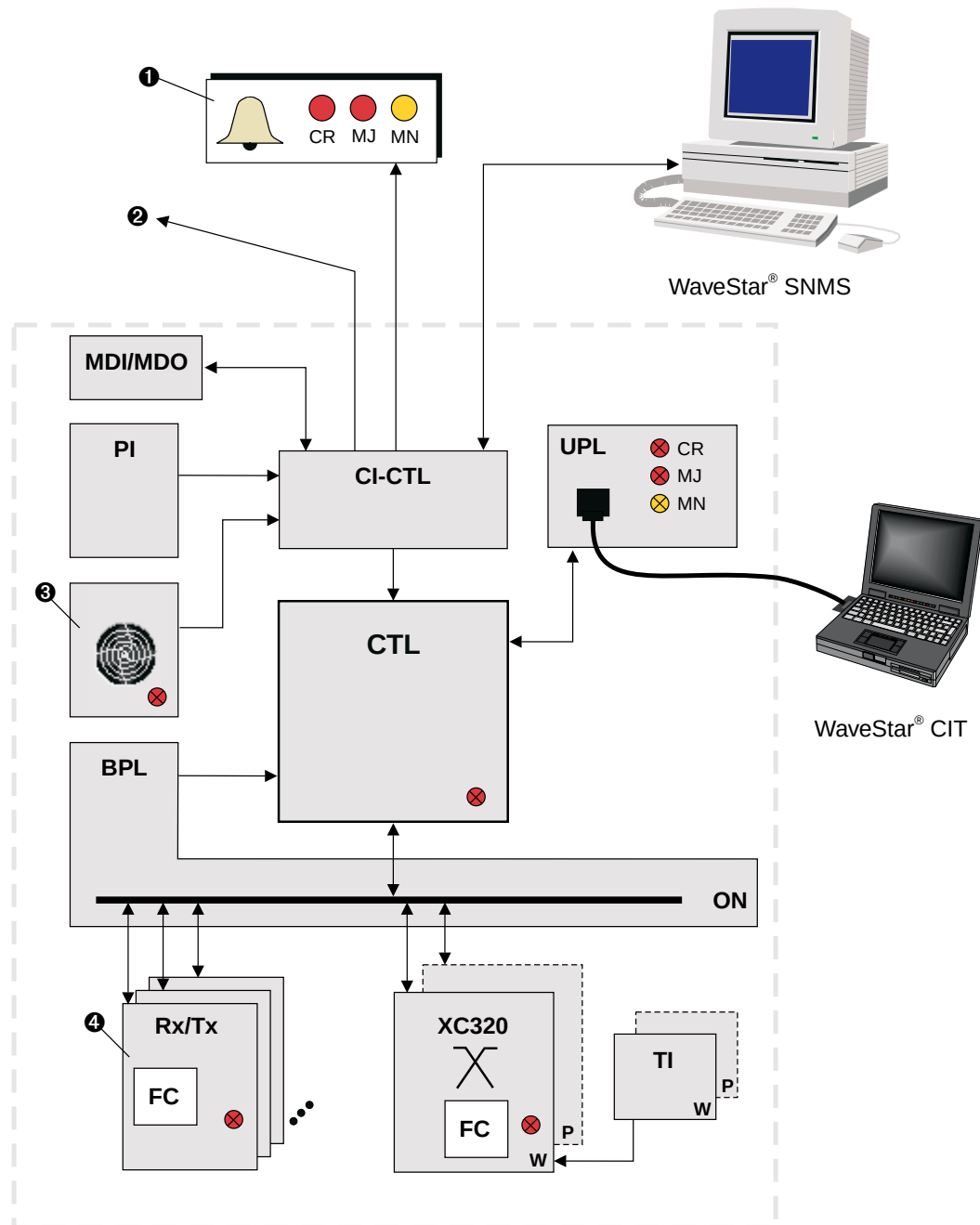
Alarm severity assignment Please refer to “Alarm severities” (16-10) and “Alarm severity assignment profiles” (16-25).

Alarm confirmation Please refer to “Alarm acknowledgment” (16-40).



LambdaUnite™ MSS fault management principle

System context The following figure provides an architectural overview of a LambdaUnite MSS system with regard to fault management.



Legend:

CTL	Controller
1	Rack alarming
2	Central office alarming (Station alarm interface)
MDI/MDO	Miscellaneous discrete inputs and outputs ¹
PI	Power Interface
3	Fan unit
BPL	Backplane (ON=Operations Network)
4 Rx/Tx ²	Transceiver units (FC=Function Controller) For example optical port units (OP...) or Gigabit Ethernet port unit (GE...)
XC320 ²	Cross connection unit with a switching capacity of 320 Gbit/s, (FC=Function Controller, W=Working, P=Protecting)
TI	Timing Interface (W=Working, P=Protecting)
UPL	User panel
CI-CTL	Connection Interface for the Controller
	Red LED: "FAULT" LED on the circuit pack faceplate and "CR" and "MJ" alarm LED on the user panel.
	Yellow LED: "MN" alarm LED on the user panel.

Notes:

1. Miscellaneous discrete inputs and outputs are prepared for future applications. The corresponding functionality is not supported in LambdaUnite MSS Release 1.0.
2. Circuit packs with an integrated function controller are referred to as "subsystems".

Related information

Please also refer to "Operations interfaces" (16-38).

***LambdaUnite* MSS fault processing**

Each subsystem (circuit pack with integrated function controller) contributes to the *LambdaUnite* MSS fault processing (cf. “Fault management process” (16-3)) to the extend of its limited system view:

- Defects are detected and possibly suppressed (for example due to the existence of a Server Signal Fail (SSF) condition) by the subsystem that detected the underlying anomaly.
- Consequent actions as well as the red “FAULT” LED on the circuit pack faceplate are controlled by the subsystem that detected the defect. The red “FAULT” LED on the faceplate of the fan unit, which is not a subsystem, is driven by hardware signals.
- Correlation and blocking:
 - If a subsystem is able to detect **all** defects required to determine a particular correlated fault cause, then correlation and blocking is performed completely by that subsystem.
 - If a subsystem is able to detect several, but not all defects required to determine a particular correlated fault cause, then it performs a partial correlation with the defects it can detect and reports this to the Controller (CTL). The Controller collects the missing fault data and completes the correlation.
 - If a subsystem is able to detect only one out of several defects required to determine a particular correlated fault cause, then it reports the defect to the Controller (CTL). The CTL collects the missing fault data and completes the correlation.
- Validation and reporting (i.e. the generation of alarm notifications) is controlled centralized by the CTL.

□

LambdaUnite[™] CIT alarm presentation formats

Overview

Purpose In the following, the available *LambdaUnite* CIT alarm presentation formats are explained.

This includes

- the severity of an alarm as displayed in the list of current alarms or the alarm history log,
- the severity of an alarm as part of an alarm severity assignment profile (ASAP),
- the numbering of tributaries in an alarm displayed in the list of current alarms or the alarm history log.

Contents

Alarm severities	16-10
Alarm format preferences	16-12



Alarm severities

Possible alarm severities An alarm can have one of the following alarm severities (alarm levels), in descending order of priority, in accordance with the Telcordia Technologies (formerly Bellcore) standards:

- 1. Critical (CR),
- 2. Major (MJ),
- 3. Minor (MN),
- 4. Not alarmed (NA),
- 5. Not reported (NR).

These alarm severities are used for the internal alarm processing of the network elements.

Please note that you can specify the alarm display format by means of the *LambdaUnite*™ CIT to influence how alarm severities will be presented in the *LambdaUnite* CIT **NE Alarm List** or **NE Alarm Log**, please refer to “Alarm format preferences” (16-12).

Meaning of the alarm severities The alarm severities have the following meanings:

Alarm severity	Meaning
Critical (CR)	“Critical” and “Major” represent prompt maintenance conditions. Immediate action is required by maintenance personnel to remove defective equipment from service for the purpose of restoring good service and effecting repair of the failed equipment.
Major (MJ)	
Minor (MN)	“Minor” represents a deferred maintenance condition. No immediate action is required by maintenance personnel, for example, when performance falls below standard but the effect does not warrant removal from service, or generally, if automatic changeover to standby equipment has been used to restore service.

Alarm severity	Meaning
Not alarmed (NA)	Alarm conditions having the “Not-alarmed” alarm severity assigned will not be signalled by the user panel LEDs or the office alarm interfaces (cf. “Signalling of alarms” (16-17)). However, alarm signalling by the management systems is possible because an event notification is generated by the NE and reported to the management systems.
Not reported (NR)	No alarm notification will be generated for alarm conditions having the “Not-reported” alarm severity assigned. Therefore, no alarm signalling is possible.

Assigning alarm severities

The assignment of alarm severities (alarm levels) can be accomplished by means of alarm severity assignment profiles (ASAPs); please refer to “Alarm severity assignment profiles” (16-25).



Alarm format preferences

Introduction By means of the *LambdaUnite™* CIT, preferences can be specified for presenting alarm severities:

- in the alarm status display and in alarm lists, and
- in alarm severity assignment profiles (ASAPs).

These presentation format preferences can be set by invoking the **Preferences** window from the main menu of the **System View** window via **View** → **Preferences** and specifying the alarm severity presentation format in the **Alarm Format** group box.

Alarm formats A preference for presenting alarm severities in the alarm status display and in alarm lists and alarm severity assignment profiles (ASAPs) in either of the following two alarm formats can be specified:

- Critical/Major/Minor (**CR/MJ/MN**),
- Prompt/Deferred/Info (**PR/DF/INF**).

In principle, the same preferences for the alarm presentation format can be set for *WaveStar®* SNMS sessions. However, the procedure for accomplishing this setting is out of the scope of the present manual. Please refer to the *WaveStar* SNMS user documentation.

Alarm severity representation How alarm severities are represented in the *WaveStar* CIT alarm status display and in alarm lists or alarm severity assignment profiles (ASAPs) depends on the selected alarm format:

- When the **CR/MJ/MN** alarm format is selected, then alarm severities are presented in the SONET format.
- When the **PR/DF/INF** alarm format is selected, then alarm severities are presented in the SDH format. This is the default setting for *LambdaUnite* MSS systems.

Alarm severity representation in alarm lists

The following table demonstrates the alarm severity representation in alarm lists:

Alarm severities acc. to the Telcordia Technologies standards	Alarm severity representation in alarm lists	
	SDH format ¹ (PR/DF/INF)	SONET format (CR/MJ/MN)
Critical (CR)	Prompt (PR)	Critical (CR)
Major (MJ)		Major (MJ)
Minor (MN)	Deferred (DF)	Minor (MN)
Not alarmed (NA)	Info (INF)	Not alarmed (NA)
Not reported (NR)	Alarm signalling is not possible.	

Notes:

1. This is the default setting for *LambdaUnite* MSS systems.

Alarm severity representation in ASAPs

The following table demonstrates the alarm severity representation in alarm severity assignment profiles (ASAPs):

Alarm severities acc. to the Telcordia Technologies standards	Alarm severity representation in alarm severity assignment profiles (ASAPs)	
	SDH format ¹ (PR/DF/INF)	SONET format (CR/MJ/MN)
Critical (CR)	Prompt, Critical	Critical
Major (MJ)	Prompt, Major	Major
Minor (MN)	Deferred	Minor
Not alarmed (NA)	Info	Not Alarmed
Not reported (NR)	Not Reported	Not Reported

Notes:

1. This is the default setting for *LambdaUnite* MSS systems.

**Tributary numbering
format preference**

A preference for presenting tributary AIDs can be specified. These are the selectable preferences:

- **SONET**
All tributary AIDs are displayed in SONET format whether they are from SONET or SDH ports.
- **SDH**

All tributary AIDs are displayed in SDH format (cf.) whether they are from SONET or SDH ports.

- **Mixed Tributary**
Tributary AIDs from SONET ports are displayed in SONET format. Tributary AIDs from SDH ports are displayed in SDH format.

SONET and SDH tributary numbering format A special numbering format is used for SDH tributaries (VC-3, VC-4, VC-4-4C, VC-4-16C and VC-4-64C) whereas the SONET tributary numbering format is relatively straight-forward:

Interface port rate	Tributary rate	Tributary AID	
		SONET format	SDH format
OC-3/STM-1	STS-3/VC-4	1	0
	STS-1/VC-3	1, 2, 3	1, 2, 3
OC-12/STM-4	STS-12/VC-4-4C	1	00
	STS-3/VC-4	1, 4, 7, 10	10, 20, 30, 40
	STS-1/VC-3	1, 2, 3, 4, ... , 12	11, 12, 13, 21, 22, 23, 31, 32, 33, 41, 42, 43
OC-48/STM-16	STS-48/VC-4-16C	1	000
	STS-12/VC-4-4C	1, 13, 25, 37	100, 200, 300, 400
	STS-3/VC-4	1, 4, 7, 10, ... , 46	110, 120, 130, 140, 210, 220, ... , ... , 430, 440
	STS-1/VC-3	1, 2, 3, 4, ... , 48	111, 112, 113, 121, 122, 123, ... , 441, 442, 443

Interface port rate	Tributary rate	Tributary AID	
		SONET format	SDH format
OC-192/STM-64	STS-192/VC-4-64C	1	0000
	STS-48/VC-4-16C	1, 49, 97, 145	1000, 2000, 3000, 4000
	STS-12/VC-4-4C	1, 13, 25, 37, ... , 181	1100, 1200, 1300, 1400, 2100, 2200, ... , ... , 4300, 4400
	STS-3/VC-4	1, 4, 7, 10, ... , 190	1110, 1120, 1130, 1140, 1210, 1220, ... , ... , 4430, 4440
	STS-1/VC-3	1, 2, 3, 4, ... , 192	1111, 1112, 1113, 1121, 1122, 1123, ... , 4441, 4442, 4443
	STS-1/VC-3	1, 2, 3, 4, ... , 192	1111, 1112, 1113, 1121, 1122, 1123, ... , 4441, 4442, 4443
OC-768/STM-256 ¹	STS-768/VC-4-256C	1	00000
	STS-192/VC-4-64C	1, 193, 385, 577	10000, 20000, 30000, 40000
	STS-48/VC-4-16C	1, 49, 97, 145, ... , 721	11000, 12000, 13000, 14000, 21000, 22000, ... , ... , 43000, 44000
	STS-12/VC-4-4C	1, 13, 25, 37, ... , 757	11100, 11200, 11300, 11400, 12100, 12200, ... , ... , 44300, 44400
	STS-3/VC-4	1, 4, 7, 10, ... , 766	11110, 11120, 11130, 11140, 11210, 11220, ... , ... , 44430, 44440
	STS-1/VC-3	1, 2, 3, 4, ... , 768	11111, 11112, 11113, 11121, 11122, 11123, ... , 44441, 44442, 44443

Interface port rate	Tributary rate	Tributary AID	
		SONET format	SDH format
1 Gbit/s (Ethernet)	STS-3/VC-4	1, 4, 7, 10, 13, 16, 19, 22	110, 120, 130, 140, 210, 220, 230, 240
	STS-1/VC-3	1, 2, 3, 4, ... , 24	111, 112, 113, 121, 122, 123, ... , 241, 242, 243

Notes:

1. STM-256 and OC-768 ports are not supported in *LambdaUnite* MSS Release 1.0
- The tributary numbering format is of particular importance in respect of the display of tributary alarms, especially in the case of SDH tributaries.
- Please also refer to “Identifying SDH tributaries in alarm messages” (5-10).



Signalling of alarms

Overview

Purpose	This section provides information about the signalling of alarms via the various management interfaces available.
Management interfaces for alarm signalling	<i>LambdaUnite</i>[™] MSS systems provide the following management interfaces for alarm signalling: • Management systems: - <i>WaveStar</i>[®] SNMS - <i>WaveStar</i> CIT Please notice that administration, maintenance and provisioning activities via <i>WaveStar</i> SNMS are described in the separate <i>WaveStar</i> SNMS documentation set. • Alarm LEDs on the user panel • “FAULT” LED on the circuit pack faceplate • Office alarm interfaces: - Rack alarm interface - Station alarm interface
Control of alarm signalling	Alarm signalling is influenced and controlled by the following factors: • Alarm severity Signalling via the management systems, the alarm LEDs on the user panel and the office alarm interfaces corresponds to the currently assigned alarm severity. • Alarm configuration Office alarms can be enabled or disabled by means of the <i>WaveStar</i> CIT. • Alarm confirmation Please refer to “Alarm acknowledgment” (16-40).

Contents

WaveStar CIT visual alarm indicators

[16-19](#)

NE local indications	16-21
Impact of state changes on the signalling of alarms	16-22

□

WaveStar[®] CIT visual alarm indicators

Kinds of alarm indicators

The *WaveStar* CIT provides the following visual alarm indicators to display the current NE alarm status:

- Latest alarm display,
- Alarm status display,
- **System View** alarm indicators,

Alarm status display

The alarm status display, permanently displayed in the lower left corner of the **System View** window, reflects the current alarm status of the entire NE. It shows a count of all alarms currently present on the NE, sorted by alarm severity (alarm level), for Critical (CR), Major (MJ) and Minor (MN) or Prompt (PR) and Deferred (DF) alarm severities, depending on the alarm format preferences setting.



Update of the alarm status display

The alarm status display is automatically updated as soon as the NE alarm status varies. The date and time of the last update is indicated on the right hand side of the alarm status display.

The **Update Alarms** button beside the **Alarm List** button can be used to manually refresh the alarm status display.

System view alarm indicators

In the **System View**, each shelf is functionally depicted with a shelf level alarm LED which serves to indicate the highest level of alarm for that shelf.

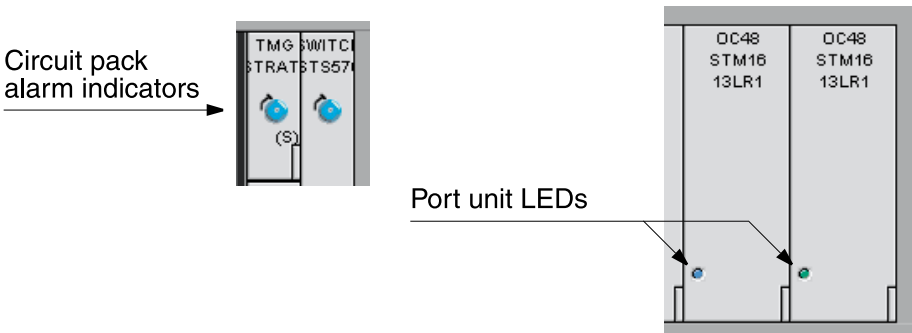
Shelf view alarm indicators

In the **System View**, each circuit pack may have two different types of alarm indicators:

- Circuit pack alarm indicators

Each circuit pack has a bell symbol to indicate the circuit pack’s current alarm status. Notice that a bell symbol will only be visible if at least one deferred alarm is present for the circuit pack.

- Port unit LEDs
 Furthermore, each port unit has an LED associated with each port which serves to indicate the alarm status for the associated port.



Color scheme Indication of alarms is according to the following color scheme:

Alarm severity		Color
SONET	SDH	
Critical	Prompt	Red
Major		Yellow
Minor	Deferred	Blue
Not alarmed	Info	White

The WaveStar CIT NE Alarm List

The WaveStar CIT **NE Alarm List** can be used to retrieve detailed information about the current alarm status of a *LambdaUnite™* MSS network element (NE).

 Please refer to “The WaveStar CIT NE Alarm List” (5-5).



NE local indications

Alarm LEDs on the user panel

Alarms are signalled via the alarm LEDs on the user panel according to the currently assigned alarm severity:

Assigned alarm severity	Alarm LED
Critical	Red LED (CR)
Major	Red LED (MJ)
Minor	Yellow LED (MN)
Not alarmed	No indication via the user panel alarm LEDs
Not reported	

Please also refer to “The *LambdaUnite*[™] MSS user panel” (16-39).

Fault LED on circuit packs

A red “FAULT” LED is located on all *LambdaUnite* MSS circuit packs to indicate failures attributable to the circuit pack.

The possible Fault LED states are shown in the following table.

Fault LED State	Meaning
On	indicates a circuit pack failure
Off	indicates no failures
Flashing	indicates an incoming signal failure, an external timing failure or a memory corruption

Office alarm interfaces

The office alarms interface is a set of discrete alarm outputs controlling audible and visible office alarms via the rack or station alarm facilities. Separate alarm outputs handle critical, major and minor alarms. If desired, critical and major alarm outputs can be wired so that either, neither, or both of the outputs control the prompt office alarm.

Please also refer to “Office alarm interfaces” (16-48).



Impact of state changes on the signalling of alarms

State changes

State changes may be the result of provisioning activities, a changed alarm severity for example, or they may be caused by changed attributes that are processed by the system, such as the affect-on-service attribute (SA/NSA) for example.

Alarm severity

The following distinction of cases is based on the assumption that an alarm is currently present (not necessarily reported), and then the severity of the alarm is changed.

These cases can be distinguished:

The alarm severity is changed ...		Impact on the alarm signalling
from	to	
Any severity other than “Not reported”	Any other severity (other than “Not reported”)	No change of alarm signalling
	“Not reported”	The corresponding alarm will be cleared.
“Not reported”	Any other severity	The corresponding alarm will be reported with the new severity.

Autonomous alarm forwarding

In the default configuration, the forwarding of autonomously generated alarm notifications to management systems is enabled.

It is possible to inhibit, temporarily, the forwarding of autonomously generated alarm notifications to management systems (please refer to “Enabling or disabling autonomous alarm forwarding” (5-41)).

If the autonomous alarm forwarding is disabled then no alarm notifications will be reported to the management systems. Alarms and events that were not forwarded to the management systems due to the disabling of autonomous alarm forwarding will not be resent to the management systems after enabling the autonomous alarm forwarding again.

Local alarm indications such as the signalling of alarms by means of the red “FAULT” LED on the circuit pack faceplate, the alarm LEDs on the user panel and the signalling of alarms at the rack and station alarm interfaces are not affected.

Affect-on-service attribute

If the affect-on-service attribute (SA/NSA) changes for a present alarm with an alarm severity other than “Not reported” then the alarm will be reported as cleared and raised again with the new affect-on-service attribute.



Alarm provisioning

Overview

Purpose This section on alarm provisioning deals with the provisioning activities related to the generation and display of alarms.

Alarm provisioning includes:

- assigning alarm severities,
- setting the port monitoring mode,
- enabling or disabling office alarm signalling,
- configuring thresholds for bit error monitoring, and
- enabling or disabling consequent actions in case of an excessive bit error ratio.

□

Alarm severity assignment profiles

Overview An alarm severity assignment profile (ASAP) is a list of alarms which can occur in a network element and which each have an alarm severity assigned.

ASAPs can be assigned to *LambdaUnite*[™] MSS functional system components (a circuit pack or a specific port for example) during provisioning.

Each ASAP can be uniquely identified by its type and its name.

Basic ASAP variants Depending on their affect-on-service attribute (not service-affecting (NSA) or service-affecting (SA)), two types of alarms can be distinguished, service-dependent and service-independent alarms. Accordingly, the following two basic ASAP variants can be distinguished:

- **Service-independent ASAP**
The ASAP consists of assigning an alarm severity to each alarm. No distinction is made concerning the affect-on-service attribute.
- **Service-dependent ASAP**
The ASAP consists of assigning alarm severities to each alarm dependent on the value of the affect-on-service attribute (SA or NSA).

Notes:

“Service” always means the transmission service.

In the case of a service-dependent ASAP, the SA alarm severity cannot be less than the NSA alarm severity.

If the affect-on-service attribute (SA or NSA) changes for a present alarm with an alarm severity other than not reported then the alarm will be cleared and reported again with the new affect-on-service attribute.

Alarm severities These alarm severities are used in the following description of the ASAP types:

1. Critical (CR),
2. Major (MJ),
3. Minor (MN),

- 4. Not alarmed (NA),
- 5. Not reported (NR).

Please note that the display of alarm severities on the WaveStar® CIT graphical user interface depends on the specified alarm format; please refer to “Alarm format preferences” (16-12).

ASAP types These ASAP types, listed in alphabetical order according to their *LambdaUnite* CIT representation, are defined for *LambdaUnite* MSS network elements:

ASAP Type ¹	Functional category
Automatic Protection Switch	Alarms related to Automatic Protection Switching (APS)
BLSR/MS SPRing Protection Switch	Ring protection switching alarms (BLSR/MS-SPRing)
DCN	Alarms related to the Data Communication Network (DCN)
Equipment without SA/NSA	Circuit pack and other equipment alarms (unprotected components)
Equipment with SA/NSA*	Circuit pack and other equipment alarms (protected components)
Ethernet*	Alarms related to the transport of Ethernet data
MSA/NIM*	Path-related alarms (path monitoring)
Path Protection SNCP_UPSR	Path protection switching alarms (SNCP/UPSR)
Path terminating SDH*	Path-related alarms (path termination)
Port*	SDH/SONET port-related alarms
System Timing	Synchronization system alarms

Notes:

- 1. The service-dependent ASAP types are marked with an asterisk (“*”). The remaining ASAP types are service-independent.

Default ASAPs For each of the available ASAP types, there exists a default ASAP containing meaningful factory settings. The default ASAPs are named “Default” for all ASAP types. In the following, the composition and the alarm severity assignments of these default ASAPs are given.

“Automatic Protection Switch” ASAP

The following table lists the default alarm severity assignments of the “Automatic Protection Switch” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
PAMARCH	Prot. Arch. Mismatch	Major
PAMOPER	Prot. Arch. Operation Mismatch	Major
PAMMODE	Prot. Arch. Mode Mismatch	Major
PSBUNACC	Prot. Switch Byte Unacceptable	Major
PSBI-NAPPR	Prot. Switch Byte Inappropriate	Major
SCM	Switch Channel Mismatch	Major
FESF	Far End Signal Fail	Major

“BLSR/MS SPRing Protection Switch” ASAP

The following table lists the default alarm severity assignments of the “BLSR/MS SPRing Protection Switch” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
APSC	Inconsistent APS Codes	Major
IMAPS	Improper APS Codes	Major
NID-CONFL	Node ID Mismatch	Major
DKB	Default K-bytes	Major
RNG-PSS	Ring Protection Switch Suspended	Major
TS	Traffic Squelched	Major
DUPL-RNG	Duplicate Ring Node	Major
SQMAP-CONFL	Local Squelch Map Conflict	Major
RNG-INC	Ring Incomplete	Major
RNG-URT	Unknown Ring Type	Not alarmed
RNG-IRPM	Inconsistent Ring Protection Mode	Major
RNG-DSCVY	Ring Discovery in Progress	Not alarmed

Probable cause	Alarm text	Alarm severity
ET-PREEMPT	Extra Traffic Preempted	Not alarmed
LCONDINS	Line Condition Instable	Major
RNG-OPEN	Open Ring	Major

“DCN” ASAP The following table lists the default alarm severity assignments of the “DCN” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
PARARREP	Partitioned Area Repair	Minor
PROVINVAL	DCN Provisioning Not Valid	Major
ADDROV	Address List Overflow	Major
TUNOV	Tunnels Overflow	Major

“Equipment without SA/NSA” ASAP The following table lists the default alarm severity assignments of the “Equipment without SA/NSA” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
CSDWF	Worker Clock Input Fail	Minor
CSDPF	Protection Clock Input Fail	Minor
SYNCCLK	NE Clock Failure	Critical
CPDEGR	Unit Cooling Degraded	Minor
CPCOMF	Circuit Pack Comm Failure	Minor
ONIF	ONI Failure	Minor
BPEF	Backplane Read Failure	Major
PROCROVLD	Resource Overload	Minor
SYSCOMF	Comm Channel Failure	Major
CTLCOMF	CTL Comm Failure	Minor
BKUPMEMP	IDE Flash Card Access Fail	Major
BKUPMEMO	NVM Shortage	Minor

Probable cause	Alarm text	Alarm severity
CIPWRDWN	CICTL Powered Down	Minor
TIMM	TI Mismatch	Minor
CIMISS	CICTL not Present	Minor
CIF	CICTL Failure	Minor
CICOMF	CICTL Comm Failure	Minor
FANUNITMISS	Fan Unit not Present	Critical
FANUNIT-COMF	Fan Unit Comm Failure	Minor
FANUNITF	Fan Unit Failure	Critical
FANF	Fan Failure	Major
FEEDAF	Fan Voltage Feed A Failure	Minor
FEEDBF	Fan Voltage Feed B Failure	Minor
UPMISS	User Panel not Present	Minor
UPCOMF	User Panel Comm Failure	Minor

“Equipment with SA/NSA” ASAP The following table lists the default alarm severity assignments of the “Equipment with SA/NSA” ASAP (service-dependent).

Probable cause	Alarm text	Alarm severity	
		NSA	SA
EQPT	Circuit Pack Clock Failure	Minor	Critical
CPDEGR	Temperature degrades MTBF	Minor	Major
PRCDRERR	Circuit Pack Type Mismatch	Minor	Major
REPLUNITMISS	Circuit Pack not Present	Minor	Critical
TXInF ¹	TXI Failure	Minor	Critical
CPFAIL	Circuit Pack Failure	Minor	Critical
PIMISS	Power Interface not Present	Minor	Major
POWF	System Power Failure	Minor	Major

Notes:

1. “n” (=1, 2, ...) represents the failed TXI bus line. The number of TXI bus lines depends on the circuit pack.

“Ethernet” ASAP The following table lists the default alarm severity assignments of the “Ethernet” ASAP (service-dependent).

Probable cause	Alarm text	Alarm severity	
		NSA	SA
VCGLOA	Loss of Alignment	Minor	Critical
VCGLOPC	Partial Transport Capacity Loss	Minor	Major
VCGLOTC	Total Transport Capacity Loss	Minor	Critical
VCGFOPT	Source End Failure of Protocol	Minor	Major
VCGFOPR	Sink End Failure of Protocol	Minor	Major
VCGSSF	Server Signal Fail	Not reported	Not reported
VCGPLM	Payload Mismatch	Minor	Critical
GFPLOF	GFP Loss of Frame	Minor	Critical
LANLOS	LAN Loss of Signal	Minor	Critical
LANANM	LAN Auto Negotiation Mismatch	Minor	Not alarmed

“MSA/NIM” ASAP The following table lists the default alarm severity assignments of the “MSA/NIM” ASAP (service-dependent).

Probable cause	Alarm text	Alarm severity	
		NSA	SA
AIS-P	Alarm Indication Signal	Not reported	Not reported
LOP-P	Loss of Pointer	Minor	Critical
SRM-P	Signal Rate Mismatch	Minor	Major
UNEQ-P	Unequipped	Minor	Critical
TIM-P	Trace Identifier Mismatch	Minor	Critical
EXC-P	Excessive Bit Error Ratio	Minor	Critical
DEG-P	Degraded Signal	Minor	Major
SSF-P	Server Signal Fail	Not reported	Not reported
RFI-P	Remote Defect Indication	Not reported	Not reported
PDI-P	Payload Defect Indication	Minor	Major

“Path Protection SNCP_UPSR” ASAP The following table lists the default alarm severity assignments of the “Path Protection SNCP_UPSR” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
PSI	Path Switch Inhibit	Not alarmed
FAILTOSW	Path Switch Denial	Not alarmed

“Path terminating SDH” ASAP

The following table lists the default alarm severity assignments of the “Path terminating SDH” ASAP (service-dependent).

Probable cause	Alarm text	Alarm severity	
		NSA	SA
THPLOP	Loss of Pointer	Minor	Critical
THPSSF	Server Signal Fail	Not reported	Not reported
THPUNEQ	Unequipped	Minor	Critical
THPTIM	Trace Identifier Mismatch	Minor	Critical
THPEXC	Excessive Bit Error Ratio	Minor	Critical
THPDEG	Degraded Signal	Minor	Major
THPRDI	Remote Defect Indication	Not reported	Not reported
VCLOM	Loss of Multiframe	Major	Critical
VCSQM	Sequence Number Mismatch	Major	Critical

“Port” ASAP

The following table lists the default alarm severity assignments of the “Port” ASAP (service-dependent).

Probable cause	Alarm text	Alarm severity	
		NSA	SA
TF	Transmit Failure	Minor	Major
BIASHIGH ¹	LASER bias too high	Minor	Major
OCHLOF	OCh Loss of Frame	Minor	Critical
RECOV ²	Input Power too high	Minor	Critical
LOS	Loss of Signal	Minor	Critical
LOF	Loss of Frame	Minor	Critical
RSTIM	Trace Identifier Mismatch	Minor	Critical
DCCRSE	DCC Failure	Major	not applicable
LIDRSM	Protocol Version Mismatch	Major	not applicable

Probable cause	Alarm text	Alarm severity	
		NSA	SA
MSEXC	Excessive Bit Error Ratio	Minor	Critical
MSDEG	Degraded Signal	Minor	Major
AIS-L	Alarm Indication Signal	Minor	Critical
MSSSF	Server Signal Fail	Not reported	Not reported
RFI-L	Remote Defect Indication	Not reported	Not reported
MSPSSF	Server Signal Fail	Not reported	Not reported
DCCMSF	DCC Failure	Major	not applicable
LIDMSM	Protocol Version Mismatch	Major	not applicable

Notes:

1. Although the LASER bias too high alarm is part of the “Port” ASAP, it has no relevance for the present *LambdaUnite* MSS release because the detection of the alarm is not supported.
2. Although the Input Power too high alarm is part of the “Port” ASAP, it has no relevance for the present *LambdaUnite* MSS release because the detection of the alarm is not supported.

“System Timing” ASAP The following table lists the default alarm severity assignments of the “System Timing” ASAP (service-independent).

Probable cause	Alarm text	Alarm severity
RF	Timing Reference Failure	Major
SyncLoss	Loss of Synchronisation	Major
T4out	T4 quality insufficient	Major

Maximum number of ASAPs A maximum number of 64 ASAPs may exist per *LambdaUnite* MSS system, including the default ASAPs.

ASAP name The ASAP name is used to distinguish different ASAPs of the same type.

The following provisioning rules apply to the ASAP name:

1. The “Default” ASAPs cannot be renamed.
2. The ASAP name is an alphanumeric string of up to 24 characters.

3. The following characters are permitted in an ASAP name:
 - Upper case letters (A ... Z),
 - Lower case letters (a ... z),
 - Digits (0 ... 9),
 - Special characters (separated by comma):
' , - , (,) , . , / , + , ! , * , [,] , ^ , { , } , | , < , > , ~ , % , # , _
 4. These characters are **not** permitted:
 - Comma,
 - Special characters (separated by comma):
@ , : , = , " , ; , & , ?
- Spaces in an ASAP name will be ignored.

Non-reporting ASAPs Non-reporting ASAPs, named “NonReporting”, can be created for all ASAP types. Non-reporting ASAPs have an alarm severity of “Not reported” (NR) assigned to each alarm and may be useful to suppress undesired alarm messages during provisioning activities for example.

Provisioning ASAPs Please refer to the following procedures for information on how to provision alarm severity assignment profiles:

- “Creating a new ASAP” (5-18)
- “Creating non-reporting ASAPs” (5-21)
- “Modifying an existing ASAP” (5-23)
- “Setting ASAPs for a shelf” (5-26)

□

Port monitoring mode

Introduction The setting of the port monitoring mode determines whether an incoming port signal will be monitored for defects. By means of the WaveStar® CIT, you can configure the port monitoring mode of each incoming port to “automatic” (**Auto**), **Monitored** or **Not Monitored**.

Meaning of the port monitoring modes The meaning of the different port monitoring modes is as follows:

- **Auto**
Port monitoring is disabled. However, as soon as a valid input signal is detected, the port monitoring mode is automatically switched to **Monitored**. **Auto** is the default setting.
- **Monitored**
The incoming port signal is monitored for defects.
- **Not Monitored**
Port monitoring is disabled, the incoming port signal is not monitored for defects.

Setting the port monitoring mode For information on how to set the port monitoring mode for a particular port, please refer to “Setting the port monitoring mode” (5-29).



Forward error correction

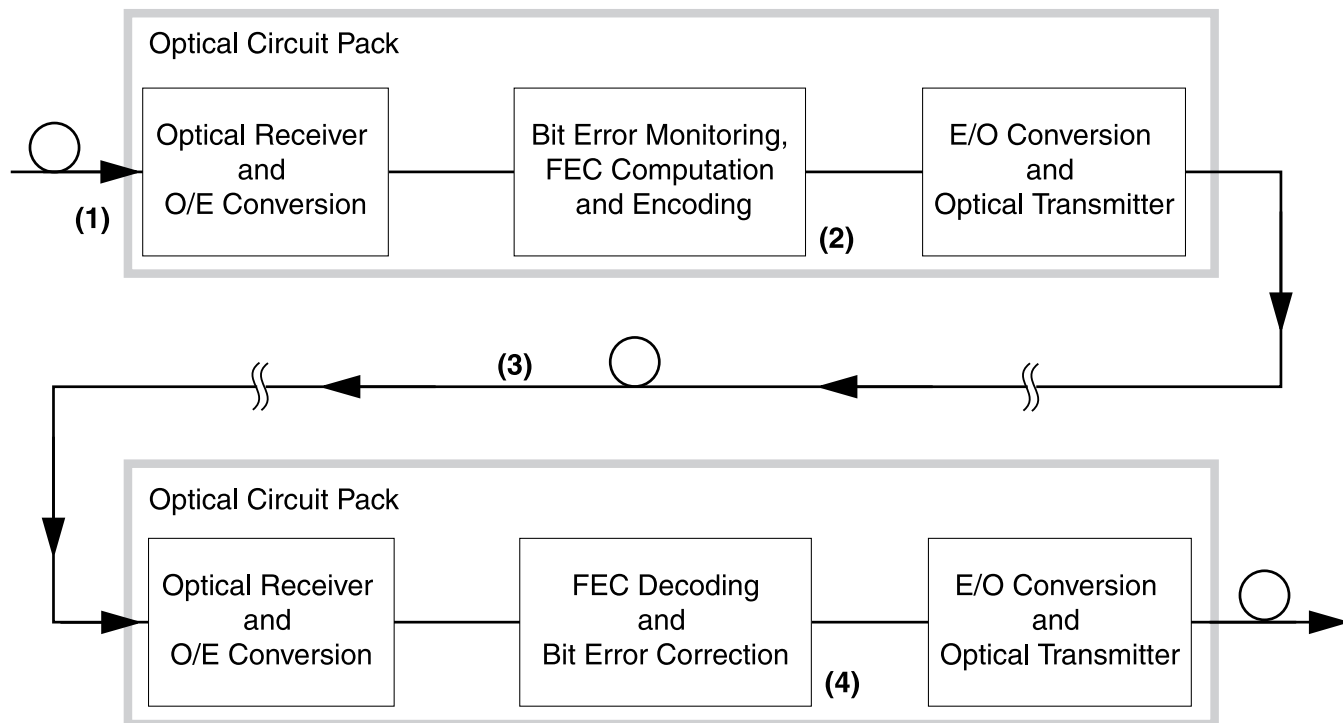
Overview Forward Error Correction (FEC) makes it possible to improve the optical signal-to-noise ratio (OSNR), and thus to lower the bit error ratio, of an optical line signal by adding redundant information. This redundant information can then be used to correct bit errors that unavoidably occur when an optical line signal is transmitted over longer distances over an optical fiber.

Two types of forward error correction

LambdaUnite[™] MSS systems support two types of Forward Error Correction:

- In-band FEC (also referred to as “multibit FEC”)
The redundant information is stored and transported in previously unused overhead bytes, the framing structure as well as the bit rate remain unchanged.
- Out-of-band FEC (also referred to as “strong FEC”)
The redundant information is appended to the original signal resulting in an optical signal with a modified framing structure and extended bit rate. The bit rate is increased by approx. 7%. The new signal format is referred to as “Optical Channel” at the corresponding bit rate.

Functional principle The following figure depicts the functional principle of the Forward Error Correction.



Following an opto-electrical conversion, the bit error ratio in the incoming optical signal (1) is calculated. The FEC algorithm is computed and the redundant information added to the signal (2).

The modified transmit signal is then transported over a transmission line (3) after an electro-optical conversion. The quality of the optical transmit signal is usually decreased by interfering noise, caused among others by chromatical dispersion for instance.

The again opto-electrically converted receive signal is evaluated in the receiver circuit pack, and the FEC information is extracted. Bit errors can now be corrected by using this information (4).

The resulting signal is characterized by a significantly improved BER.

FEC support in LambdaUnite MSS systems

LambdaUnite MSS systems support Forward Error Correction for STM-64 signals:

- ***In-band FEC***

LambdaUnite MSS systems make use of a proprietary BCH-2 algorithm for in-band FEC. The BCH-2 algorithm is a 4-times bit-interleaved 2-bit error correcting BCH algorithm on a row-by-row basis using a block size of 2^{16} .

In-band FEC yields an OSNR improvement of approx. 3 dB at a BER of 10^{-12} . It is primarily used to compensate insufficiencies of optical components.

- ***Out-of-band FEC***

LambdaUnite MSS systems make use of an RS(255,239) Reed-Solomon code for out-of-band FEC in acc. with ITU-T Rec. G.975. The RS(255,239) Reed-Solomon code is a 16-times byte-interleaved systematic linear cyclic block code.

Out-of-band FEC yields an OSNR improvement of approx. 5 dB at a BER of 10^{-12} . It enables high-speed transmission more reliably and for longer distances.



Operations interfaces

Overview

Purpose This chapter provides information about the operations interfaces of *LambdaUnite*[™] MSS network elements.

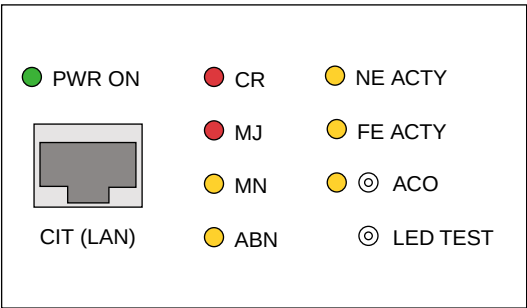
Contents

The <i>LambdaUnite</i> MSS user panel	16-39
ACO interaction with an alarm test	16-42
Circuit pack status indicators	16-44
Office alarm interfaces	16-48

□

The *LambdaUnite*[™] MSS user panel

User panel The user panel of a *LambdaUnite* MSS network element provides visual status indicators, test and control buttons and a connector for connecting the *WaveStar*[®] CIT.



Visual indicators Each user panel is equipped with the following LEDs:

LED	Function
PWR ON (green)	Indicates that power is applied to the shelf. The LED is lit if either 48V feeder is on.
CR (red)	Indicates that at least one critical alarm is present. Please refer to “User panel alarm LEDs” (16-40).
MJ (red)	Indicates that at least one major alarm is present. Please refer to “User panel alarm LEDs” (16-40).
MN (yellow)	Indicates that at least one minor alarm is present. Please refer to “User panel alarm LEDs” (16-40).
ABN (yellow)	Indicates abnormal conditions – temporary conditions that may potentially be service affecting. Please refer to “Abnormal Conditions” (16-40).
NE ACTY (yellow)	Indicates that at least one near-end transmission alarm is present. Transmission alarms are all alarms of the category “Communication (Transport)” except Remote Defect Indication.
FE ACTY (yellow)	Indicates that at least one far-end transmission alarm (Remote Defect Indication) is present.

LED	Function
ACO (yellow)	Indicates that the alarm cut-off button (ACO button) was pressed. Please refer to “Alarm acknowledgment” (16-40).

Controls and connectors In addition to the LEDs, the user panel is equipped with two buttons and a connector:

Button/connector	Function
LED TEST	An LED test button for testing all shelf LEDs (except PWR ON on the user panel and the fan unit LEDs). Please refer to “LED test” (16-41).
ACO	An alarm cut-off button to suppress both visual and audible alarm indications. Please refer to “Alarm acknowledgment” (16-40).
CIT	An RJ-45 connector for connecting a <i>WaveStar</i> CIT.

User panel alarm LEDs There are three alarm LEDs on the user panel, Critical (CR), Major (MJ), and Minor (MN). They indicate that alarms of the corresponding severity are present. Alarms having a different alarm severity than CR, MJ or MN cannot be indicated via the user panel alarm LEDs.

An alarm LED (CR, MJ or MN) is lit, if at least one alarm of the corresponding severity is present.

Alarm acknowledgment Alarms can be acknowledged (confirmed) by pushing the alarm cut-off button (“ACO” button). The alarm LEDs currently lit are switched off when the “ACO” button is pushed. Simultaneously the “ACO” LED is lit as a reminder of the alarms confirmed. If a new alarm is detected afterwards, then the “ACO” LED is switched off, and the alarm LEDs are lit according to the current alarm status.

Abnormal Conditions The purpose of the “ABN” LED is to indicate any potentially service-affecting abnormal conditions, but not to report failures. The user panel alarm LEDs (CR, MJ, MN) are used for the latter purpose.

The “ABN” LED is lit when the control system detects manually initiated maintenance activity that could affect service or potentially mask the reporting of service affecting failures.

Abnormal conditions are:

- The timing generator is configured to operate in hold-over or free running mode
- A forced switch or a lockout of a protection scheme.
- Any cross connection or facility loopback.
- Autonomous event forwarding from NE to EMS is inhibited.

LED test You can test the user panel and circuit pack LEDs by pushing the LED TEST button on the user panel.

During a test cycle the LEDs are activated for 2 seconds and then deactivated for 2 seconds three times in sequence. The LEDs return to their actual state after the test.

Important! The “PWR ON” LED on the user panel and the fan unit LEDs are not affected by the LED test. After an LED test, the restoration of the LED state before the test may be delayed for some seconds on single circuit packs.



ACO interaction with an alarm test

Overview The alarm indicators activated by an alarm test are the visual and audible office alarm outputs and the “CR”, “MJ” and “MN” LEDs on the user panel.

Alarm test sequence When an alarm test is being performed, the following sequence of indications occurs:

-
- 1** All alarm indicators mentioned above are switched off for five seconds.

If the “ACO” LED was lit before the test, it goes off. Pushing the “ACO” button has no effect.
 - **2** The “CR” and “MJ” LEDs on the user panel and the rack alarm lamp for prompt alarms are switched on for five seconds.

The indicators can be switched off and the “ACO” LED be switched on by pushing the “ACO” button. The indicators as well as the “ACO” LED are switched off automatically when the five-seconds interval has elapsed.
 - **3** The “MN” LED on the user panel and the rack alarm lamp for deferred alarms are switched on for five seconds.

The indicators can be switched off and the “ACO” LED be switched on by pushing the “ACO” button. The indicators as well as the “ACO” LED are switched off automatically when the five seconds interval has elapsed.
 - **4** Stage 2 to Stage 3 are repeated according to the specified number of iterations.
 - **5** All alarm indicators as well as the “ACO” LED (if previously lit) are switched off for five seconds.

Pushing the “ACO” button has no effect.
-

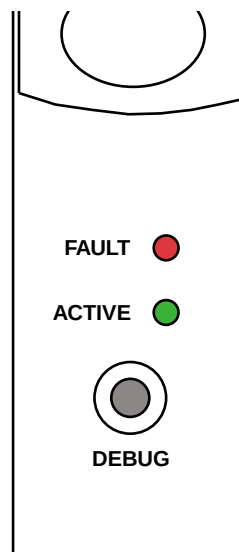
-
- 6** The control of the alarm indicators is returned to the control system to reflect the actual system status.



Circuit pack status indicators

LEDs on the circuit pack faceplate

Each circuit pack is equipped with a red fault LED labelled “FAULT” and a green activity LED labelled “ACTIVE” located on the circuit pack faceplate. The green activity LED on the fan unit is labelled “PWR ON”.



Activity LED The green activity LED is used to indicate the activity state of an operational circuit pack. An operational circuit pack can be either in service or in the standby mode. A flashing activity LED indicates that a circuit pack is in the initialization or self-test phase, or that a software download is ongoing.

Fault LED The red fault LED is used to indicate failures attributable to the relevant circuit pack. Please refer to “Circuit pack status indications” (16-46) or “Fault LED on circuit packs” (16-21).

Indications on insertion of circuit packs

The following sequence of indications will occur when you insert a circuit pack into its slot:

1. The red “FAULT” LED is lit.
2. The red “FAULT” LED goes off, and the green “ACTIVE” LED flashes as the circuit pack is initialized, self-tests are performed and software is downloaded.
3. The “ACTIVE” LED stops flashing and
 - a. is lit after the circuit pack or at least one port on a multi-port circuit pack becomes active.
or
 - b. goes off if the circuit pack is in the standby mode.

The green “ACTIVE” LED will be switched off and the red “FAULT” LED switched on if a failure is detected during initialization, self-test or software download.

The reason why the red “FAULT” LED is lit immediately after circuit pack insertion is that if you insert a circuit pack with a defective controller the red LED remains lit.

Circuit pack status indications

The following table provides an overview of the *LambdaUnite*[™] MSS circuit pack status indications.

Operational State	Status	“FAULT” LED	“ACTIVE” LED
Circuit pack not yet operational	Powering-up (immediately after circuit pack insertion) (This circuit pack state may not be clearly recognizable depending on the duration of the power-up cycle and the time needed to start initialization.)	●	–
	Initialization	–	✱
	Self-test		
	Software download		
	Failure detected during initialization, self-test or software download	●	–
Active	No failure	–	●
	Failure of the circuit pack hardware	●	●
	Failure of an input signal	✱	●
Standby	No failure	–	–
	Failure of the circuit pack hardware	●	–
	Failure of an input signal	✱	–

Explanation:

● LED is continously lit; – LED is off; ✱ LED flashes (0.5 s on, 0.5 s off)

Important! A failure of an input signal is a failure detected at the input of at least one of the input ports of the circuit pack. A circuit

pack input port may be a power supply, timing, control or transmission port.

References For more information on *LambdaUnite* MSS circuit packs, please refer to the *LambdaUnite MSS Applications, Planning, and Ordering Guide*.



Office alarm interfaces

Overview *LambdaUnite*[™] MSS network elements provide the following two alarm interfaces to support office alarm signalling:

- rack alarm interface,
- station alarm interface.

Rack alarm facility Three rack alarm lamps are located at the front and at the rear side on the top of the rack to indicate critical, major and minor alarms:



The rack alarm lamps have the following meaning:

- The red “Critical” lamp is lit when there is at least one critical alarm present which has not been acknowledged yet by means of the alarm cut-off (ACO) function.
- The red “Major” lamp is lit when there is at least one major alarm present which has not been acknowledged yet by means of the alarm cut-off (ACO) function.
- The yellow “Minor” lamp is lit when there is at least one minor alarm present which has not been acknowledged yet by means of the alarm cut-off (ACO) function.

Rack alarm interface Rack alarm signalling is controlled via the rack alarm interface on the connection interface for the controller (CI-CTL) at the rear side of a *LambdaUnite* MSS network element. The alarm interface provides individual alarm outputs for each of the three alarm severities “Critical”, “Major” and “Minor”. The rack-top alarm interface cable to connect the rack alarm lamps is prefabricated when ordered, please also refer to the *LambdaUnite MSS Installation Guide*.

As there may be up to two network elements installed in a rack, the rack alarm lamps may be connected to more than one network element. In this case the sum of all alarms is indicated. The rack alarm lamps match the “CR”, “MJ” and “MN” LED display on the user panel if only one network element is connected.

Furthermore, by corresponding wiring it is also possible to realize a two-lamp arrangement to indicate prompt and deferred alarms.

Station alarm interface

A station alarm interface is located on the connection interface for the controller (CI-CTL) at the rear side of a *LambdaUnite* MSS network element to connect a central office alarm facility.

The station alarm interface provides alarm outputs for critical, major and minor alarms, both visual and audible.

Related information

Please also refer to the *LambdaUnite MSS Installation Guide*.





17 Timing provisioning concepts

Overview

Purpose This chapter describes the timing features *LambdaUnite*[™] MSS provides.

LambdaUnite MSS synchronizes all add, drop and through signals to one timing source which is normally locked to an external reference signal. This reference signal is configurable. Various signals can be used as a timing reference signal. Furthermore *LambdaUnite* MSS provides different timing modes (see “Timing operational modes” (17-2). Timing protection can also be established by using two timing generator circuit packs within one shelf.

More detailed information on the timing concept is given in the section “**Synchronization**” in the *LambdaUnite* MSS **Applications and Planning Guide, chapter 4, “Product Description”**.

Contents

Timing generator	17-2
Timing configuration	17-3
Timing quality	17-4
Timing protection	17-8



Timing generator

Function of the timing generator

LambdaUnite[™] MSS synchronizes all add, drop and through signals by using one timing source. The timing is ensured by the XC320 circuit pack which generates one common internal clock. If two XC320 circuit packs are present in the NE, an 1+1 non-revertive protection of the timing sources is provided.

The timing generator and the timing distribution within the network elements is described in more detail in the section **“Synchronization”** in the *LambdaUnite* MSS ***Applications and Planning Guide, chapter 4, “Product Description”***.

Timing operational modes

The *LambdaUnite* MSS can run in the following timing modes:

- Free-running mode
The active timing generator circuit pack is not locked to an external timing reference, but the standby timing generator is locked to the active one.
This mode may especially be needed for the initial startup of an NE to allow the system being installed without a valid external timing reference.
- Holdover mode
The active timing generator circuit pack enters the holdover mode if all timing reference signals fail. The active timing generator keeps its internal oscillator at the point at which it was synchronized to the last known good reference signal. The standby timing generator remains locked to the active one.
- Locked mode, system time-base is locked to:
 - One of the two external netclock inputs (each of them configurable for 2048 kHz or 2 Mbit/s or DS1 signals)
 - One of all STM-64/OC-192 line input (choice of input is provisionable)
 - One optical STM-16/OC-48 tributary input (choice of input is provisionable)

□

Timing configuration

Querying timing configuration

The *WaveStar*[®] CIT allows you to query the timing configuration of the *LambdaUnite*[™] MSS. Please refer to “Viewing the timing configuration” (6-3).

Timing configuration

In the menu **Configuration** → **Timing/Sync...** it is possible to change the timing configuration.

This includes:

- the configuration of the external timing input ports (cf. “Configuring the external timing input ports SDH mode” (6-27) and “Configuring the external timing input ports SONET mode” (6-29))
- the configuration of the external output port (cf. “Configuring the external timing output ports SONET mode” (6-23)) and “Configuring the external timing output ports SDH mode” (6-19))
- the selection and configuration of the timing references (cf. “Configuring the timing references” (6-31))
- the configuration of the system timing, this means the configuration of the master timing generator (cf. “Configuring the system timing” (6-34))

□

Timing quality

- Optical line timing** In the locked mode, the timing functions on the XC320 circuit packs can be provisioned to accept a timing reference signal from an incoming optical signal (10 Gbit/s, 2.5 Gbit/s), the timing functions accept a timing reference signal from one port unit (40 Gbit/s, 10 Gbit/s, or 2.5 Gbit/s) and derive the timing signals used to synchronize the transmission port units.
- The timing reference signal is continuously monitored for error-free operation. If the reference signal becomes degraded or unavailable, the timing function selects the timing reference signal that is next in the priority list. If all configured timing reference signals are degraded or unavailable, the timing function enters the holdover mode.
- External Nclock Timing Mode** In the external nclock timing mode, the timing function on the active XC320 circuit pack receives a 2.048-MHz, 2.048-Mbit/s ITU-T or a DS1 Telcordia (B8ZS, SF and ESF format) reference signal from the external nclock inputs. The reference signals should be based on a Stratum 1 clock. The timing function on the active circuit pack synchronizes its internal Stratum 3 clock to the reference signal. The timing function on the standby XC320 circuit pack synchronizes its internal Stratum 3 clock to the active circuit pack. Then the timing functions distribute the clock signals to all circuit packs in the shelf.
- Timing Protection** *LambdaUnite™* MSS uses non-revertive 1+1 protection switching to protect its timing function. If the active XC320 circuit pack fails and causes a switch to the standby circuit pack, the standby circuit pack becomes the active circuit pack. It remains the active circuit pack, even when the failed circuit pack is replaced. The replaced circuit pack becomes the standby circuit pack. Thus bit errors can be avoided.
- If the active timing generator fails while the system is in holdover mode, the standby timing generator would become the active timing generator and would switch to holdover mode (before switching, it was fed by the active timing generator) until the reference signal is restored to an acceptable quality.

Timing Provisioning The *LambdaUnite* MSS synchronization mode can be set to locked or free running by using *WaveStar*® CIT. Additionally, either timing generator circuit pack can be switched to be the active timing generator. However, when *LambdaUnite* MSS is provisioned for the locked mode, the holdover mode is entered automatically upon loss of all reference signals. The holdover mode can be entered intentionally by the operator command “Forced Holdover”.

Control and Status The behavior of the timing generators is controlled by switching them among several defined states. As commands are issued or as failures occur and are cleared, the timing system switches from one state to another. The status of the timing is retrievable for user observation. You can issue commands to obtain status reports or to manually change the synchronization state from one to another.

There are three categories of commands

- Modify – to provision operating parameters
- Retrieve – to obtain parameter values, states and statuses
- Operate – to lockout a switch, force a switch or holdover mode or clear a state

Timing marker The timing quality of the 10 Gbit/s and 2.5 Gbit/s data signals is coded in the timing marker (Synchronization Status Message, SSM) as per ITU-T Rec. G.783 and G.707. The timing marker is located in the lower four bits of the S1 byte of the STM-N signal SOH (SDH) or of the first STS-1 of a STS-N (SONET).

The bit combinations are listed in the following table. The remaining combinations are reserved for future use.

S1 Bits	Quality level (SDH)	Quality level (SONET)
0000	—	Synchronized - Traceability Unknown (STU)
0001	—	Primary Reference Source (PRS), acc. to Bellcore TR-1244
0010	Primary Reference Clock (PRC), acc. to ITU-T Rec. G.811	—

S1 Bits	Quality level (SDH)	Quality level (SONET)
0100	Transit Node Clock (SSU-T), acc. to ITU-T Rec. G.812	—
0111	—	Stratum-2 clock (ST2), acc. to Bellcore TR-1244
1000	Local Node Clock (SSU-L), acc. to ITU-T Rec. G.812	—
1010	—	Stratum-3 clock (ST3), acc. to Bellcore TR-1244
1011	SDH Equipment Clock (SEC), acc. to ITU-T G.81s	—
1100	—	—
1110	—	—
1111	Do not use for Synchronization (DNU)	Do not use for Synchronization (DUS)

The quality level “DUS/DNU” is inserted if AIS, LOS or LOF is detected in the incoming signal. Insertion of “DUS/DNU” in an outgoing timing signal can also be configured by the operator in order to avoid timing loops in the network.

SSM of lower quality than the internal system clock

If the SSM of a reference clock source indicates a lower quality than the internal clock (SEC), this reference is considered to be failed and the system switches to the reference with the next lower priority. When all assigned references are considered to be failed, the system enters the holdover mode.

No SSM available

As long as no SSM value has been accepted and evaluated at STM-N/OC-M interfaces, “DUS/DNU ”is assumed. This also applies at the initial system start-up.

SSM for 2 Mbit/s synchronization signals

LambdaUnite MSS supports the interpretation and generation of SSM values for framed 2 Mbit/s timing input and output ports (“G.703.9 ports”). The coding conforms to ITU-T Rec. G.704. One set of the S_{a4} to S_{a8} bits can be allocated for the Synchronization Status Message (SSM). The message set is similar to the SSM messages defined for bits 5 to 8 of the byte S1 belonging to an SDH signal.

User operation You can define whether the SSM is evaluated for the selection of the timing reference from which the system timing is derived. Furthermore, you can define the quality level of the outgoing timing signal.



Timing protection

Timing reference protection switching

During configuration of the timing references, a priority list is created for the configured timing reference signals. The signal with the highest priority is initially used as the timing reference signal. If it fails, the system switches to the signal with the next lower priority. If all possible timing reference signals fail, the timing generator enters the holdover mode.

The following signals can be used as a timing reference:

- 2 external netclock input signals (2048 kHz or 2 Mbit/s acc. to G.703)
- 6 reference signal derived from the incoming STM-16/OC-48, STM-4/OC-12 or STM-1/OC-3 tributary signals or the incoming STM-64/OC-192 line signals.

The following alarms cause a protection switch from a G.703 2 Mbit/s signal to another timing reference signal (acc. to the priority list):

- LOS (Loss of Signal)
- AIS (Alarm Indication Signal)
- LOF (Loss of Frame)
- LOM (Loss of Multiframe)

The following alarm causes a protection switch from a G.703 2048 kHz signal to another timing reference signal (acc. to the priority list):

- Loss of Signal

The following alarms and fault criteria cause a protection switch from an SDH/SONET signal to another timing reference signal (acc. to the priority list):

- LOS
- AIS
- LOF
- LOM
- EXC (Excessive Bit Error Ratio)

Timing equipment protection switching

A network element can contain two timing circuit packs (XC320) on which the timing function (TF) is located. If there are two TFs, Timing equipment protection switching is possible.

When two timing circuit packs are present the timing is derived from one circuit pack, called the **active** timing circuit pack. The other timing circuit pack is standby. It produces the same timing signal as the active one but is not used, unless the active timing circuit pack fails.

For the initial start-up of the system and initial provisioning of the 1+1 protection group the free running mode is used. For the system reset after the 1+1 protection was in operation, the system restores the timing circuit pack as the active one which was active before the system reset operation.

Wait-to-restore time

The timing reference protection is working in a revertive mode. If a timing reference is restored the system has to make a wait for a defined time (wait-to-restore time, WTR) to see whether the signal is stable, before the system switches back to it.

□



18 Traffic provisioning concepts

Overview

Purpose This chapter gives important background information on the cross-connection management and the Cross-Connection Wizard of the *LambdaUnite*[™] MSS.

Contents

Cross-connection management	18-2
Cross-connection wizard	18-6
Protection mechanisms	18-12
Path Protection	18-13
Line Protection	18-18
Ring Protection	18-20
Protection configurations	18-24



Cross-connection management

Overview The *LambdaUnite*[™] MSS add/drop multiplexer in its basic configuration is a single shelf that interfaces optical STM-16/OC-48 and optical STM-64/OC-192 lines to an SDH/SONET-standard 2-fiber MS-SPRing protected ring. It has 32 universal slots that support flexible optical port unit mixing.

Definitions **Port** A physical transmission interface, consisting of both an input and an output, which may be used to carry traffic between network elements. Operational differences between ports determined by port provisioning include pointer processing, fault and performance monitoring, path maintenance (e.g. Unequipped, AIS, RDI), cross-connections (supported rates), and protection switching.

Port protection group A user-provisioned association of optical interface ports which is used for protection in a particular type of network configuration. Four types of port protection groups are defined:

- 2-fiber MS-SPRing port protection group used for STM-64 and STM-16 1+1 MS-SPRing
- 1+1 MSP port protection group used for STM-16 1+1 Multiplex Section Protection (MSP)
- 2-fiber BLSR port protection group used for OC-192 and OC-48 1+1 BLSR
- 1+1 APS port protection group used for OC-48 1+1 Automatic Protection Switching (APS) The operations on a port protection group include the provisioning, control, and status of the protection switching.

Tributary A path-level unit of bandwidth within a port, or the signal(s) being carried in this unit of bandwidth, e.g. a VC-3 or VC-4 within an STM-N port.

Cross-connection A reconfigurable SDH/SONET path-level interconnection within a network element between input and output tributaries of specific ports.

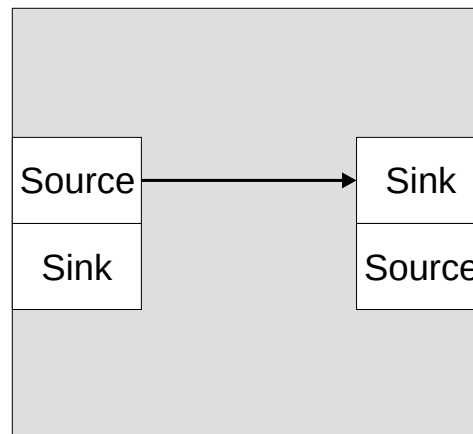
Cross-connection leg A one-way connection provisioned from one input tributary to one output tributary. Each leg is identified

as an entity by its input and output tributaries, its cross-connection rate, and the type of cross-connection it is part of. A leg pair is a pair of cross-connection legs which are reported as a two-way connection between two tributaries.

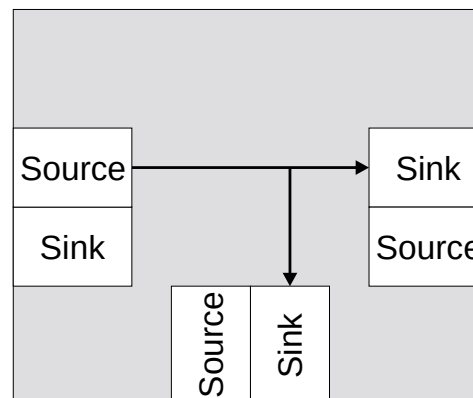
Cross-connection types

All meaningful cross-connection types can be reduced to three basic types:

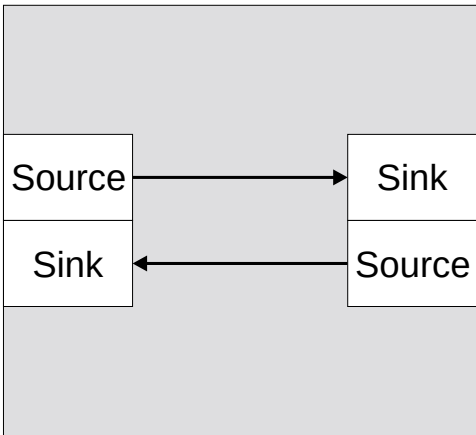
- Unidirectional point-to-point connection



- Unidirectional point-to-multipoint connection (broadcasting/bridging)



- Bidirectional connection



You can provision and reconfigure cross-connections. *LambdaUnite* MSS provides an STM-1 rate time-slot-assignment capability that supports the following types of cross-connections, which are derived from the three basic types introduced above:

- 1-way point-to-point
- 2-way Point-to-Point (default)
- SNCP/UPSR Ring Add, Drop

Transmission interfaces *LambdaUnite* MSS includes the following optical port units:

Interface type	Transmission rate	Wavelength
Optical	STM-64/OC-192	1.5 μm (long reach)
		1.5 μm (intermediate reach)
		1.3 μm (intra office)
		OLS 800 G compatibel
		passive WDM compatible
	STM-16/OC-48	1.3 μm (short reach / intra office)
	GE1/SX4, 1Gigabit Ethernet	—

Switch capacity The total full non-blocking switch capacity is 320 Gbit/s (6144 STS-1/2048 VC-4s).

Additionally also overhead information from SDH/SONET I/O ports may be transparently switched. The switch is based on a bit sliced architecture providing this very high capacity on a single pack.

Cross-connection levels	The following cross-connection levels are supported in <i>LambdaUnite</i> MSS: • VC-3 • VC-4 • VC-4-4c (Concatenated VC-4) • VC-4-16c (Concatenated VC-4) • VC-4-64c (Concatenated VC-4) • STS-1 • STS-3 • STS-12 • STS-48 • STS-192
Output mode	The cross-connection output mode is a provisionable parameter • for the destination-to-source direction, and/or • for the source-to-destination direction. If some of the facilities are not in place whenever the cross-connection is being established, then you can provision this field as Terminated-AIS or Terminated-IDLE (DS3) / Unequipped(SDH/SONET) and a Terminated-AIS or Terminated-IDLE (DS3) / Unequipped(SONET) signal will be inserted to function as a keep-alive signal. If all of the involved facilities are in place when the cross-connection is established, the field should be provisioned as NORMAL. The end-to-end signal path is then established and the signal can be passed.
Interworking	<i>LambdaUnite</i> MSS is a member of the suite of next generation transport products which have the prefix “Lambda” in their name. The system can be deployed together with other Lucent Technologies transport products, for example <i>WaveStar</i>® TDM 10G, <i>WaveStar</i> ADM-16/1, <i>WaveStar</i> BandWidth Manager, <i>Metropolis</i>™ DMX, <i>WaveStar</i> OLS 1.6T, <i>WaveStar</i> LambdaXtreme and <i>WaveStar</i> LambdaRouter systems today and in the future.



Cross-connection wizard

Overview Cross-connections may be configured using the WaveStar® CIT Cross-Connection Wizard. The Cross-Connection wizard is opened by selecting the menu sequence **Configuration** → **Cross Connection** from the shelf view of the CIT. The wizard will lead you through a series of windows in which you can identify all the attributes of the cross-connection.

Cross-connection sequence Creating or modifying a cross-connection involves the following sequence:

1. Complete all port provisioning and protection provisioning before creating a cross-connection.
2. Some of the steps involved in setting up a cross-connection will have already been made if a reservation has been made on one or more of the tributaries involved in the cross-connection.
3. Select the rate, cross-connection type, and ports involved in the cross-connection.
4. Identify the tributaries for the cross-connection from a display of tributaries corresponding to the selected ports.
5. Complete the cross-connection by selecting cross-connection parameters and the source and destination TIDs needed for a ring squelch map.

Cross-connection wizard action window The cross-connection action selection window appears when the Cross-Connection Wizard is opened. The cross-connection action selection window allows you to select whether you want to create, modify, or delete a cross-connection. The window options include:

- **Create New** - The Create New option causes the Create New Cross Connection windows to open where you can make the choices necessary to create a new cross-connection.
- **Modify Parameters** - The Modify Parameters option causes the Modify Cross Connection Parameters windows to open where you make the choices necessary to modify a cross-connection.
- **Delete** - The Delete option causes the Delete Cross Connection windows to open where you make the choices necessary to delete a cross-connection or one leg of a protected cross-connection.

- **Roll** - The Roll option causes the Roll Cross Connection Leg windows to open where you can change the source of an existing cross connection.
- **Bridge** - The Bridge option causes the Bridge Cross Connection Leg windows to open where you can select a second destination for an existing cross-connection.

Access Identifiers

For any action on cross-connections you need the Access Identifiers (AID) of the source and destination port of the cross-connection. Please refer to “Overview of access identifiers” (15-8) for the structure of the AIDs.

Create new cross connection windows

The following Cross-Connection Wizard window flow allows you to create new cross-connections:

1. The **Rate/Type** window - The **Rate/Type** window allows you to select the cross-connection rate and the cross-connection type.
2. **Source Tributary** window - The **Source Tributary** window allows you to select the source port and tributary for a cross-connection.
3. **Destination Tributary** window - The **Destination Tributary** window allows you to select the destination port and tributary for a cross-connection.
4. **Cross Connection Parameter** window - The **Cross Connection Parameter** window allows you to establish or modify the provisionable parameters for an existing or new cross-connection.

Rate/Type window

The **Rate/Type** window allows you to select the cross-connection rate and the cross-connection type. The selection of cross-connection rates may include rates such as VC-3, VC-4, VC-4-4c, VC-4-16c, VC-4-64c, STS-1, STS-3, STS-12, STS-48 or STS-192. The cross-connection types are described in “Cross-connection types” (18-3).

Source Tributary window

The Source Tributary window allows you to select the source port and tributary for a cross-connection. Port selection is confined to the ports which support the previously chosen cross-connection rate. Protection ports of a 1+1 protection group are not selectable. Protection ports or tributaries of an MS-SPRing may be selected.

Tributaries associated with the selected port are displayed according to the selected cross-connection rate. The following is also displayed for each tributary:

- AIDs of the tributaries belonging to the selected port are displayed.
- Availability of the tributaries to be used for the cross-connection source is displayed. Availability (**Avbl**) is **Yes** or **No**.
- An indication of whether the tributary is a protection tributary is displayed. The indication (**Prot**) is **Yes** or **No**.

Destination Tributary window

The **Destination Tributary** window allows you to select the destination tributary for a cross-connection. The Destination Tributary window is the same as the Source Tributary window.

Cross Connection Parameter window

The **Cross Connection Parameter** window allows you to modify provisionable parameters for an existing or new cross-connection. The window may already be populated with defaults or current settings are displayed.

The Parameter window includes the following parameters. Some parameters may not apply to the cross-connection selection and will be greyed out on the window.

- **Src. Ring ID** - The Source Ring ID displays the Ring ID associated with the source tributary on a port which is part of an MS-SPRing.
- **Dest. Ring ID** - The Destination Ring ID field lists the Ring ID of a Destination tributary on a port which is part of an MS-SPRing.
- **Existing Src AID** - The Source AID applies to a cross-connection leg which is part of an MS-SPRing. This field displays or lists AIDs you may select to assign as the Source AID.
- **Existing Dest. AID** - The Destination AID applies to a cross-connection leg which is part of an MS-SPRing.
- **New Src. AID(s)** - The New Source AID applies to a new cross-connection.
- **New Dest. AID(s)** - The New Destination AID applies to a new cross-connection

- **Src. Node NE Name** - Applies to legs which are part of a BLSR ring only. It displays a list of valid TIDs from which you can select one to assign as the Source Node TID for this leg of the cross connection.
- **Dest. Node NE Name** - Applies to legs which are part of a BLSR ring only. It displays a list of valid TIDs from which you can select one to assign as the Destination Node TID for this leg of the cross connection.
- **Source to Destination Output Mode** - This field allows you to set or display the provisioned output mode for the Source to Destination leg and has the values of **NORM**, **AIS** and **IDLE/UNEQ**.
 - **NORM** refers to a cross-connection which is carrying “normal” traffic.
 - **AIS** is a test and maintenance setting. AIS is transmitted via the respective cross-connection.
 - **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.
- **Destination to Source Output Mode** - This field allows you to set or display the provisioned output mode for the Destination to Source leg and has the values of **NORM**, **AIS** and **IDLE/UNEQ**.
- **XC Type** - This field displays the selected cross-connection type such as 1-way point to point.
- **XC Rate** - This field displays the selected cross-connection rate such as VC-4 or STS-12, etc.
- **XC Number** - This field displays the 9 digit number of the cross-connection.
- **Action** - This field displays the action you chose to perform, e.g. create or delete.
- **Range** - This field displays the selected range for the cross connection.
- **New Path Protection Group Name** - In this field you can type an up to 24 characters alphanumeric string name for the new path protection group.

TID	The Target Identifier (TID) of a network element is its name which can be assigned by the user during the configuration of a network element.
Schematic view	The Cross Connection Parameter window provides a schematic view of the selected cross-connections. It displays the cross-connection rate, such as VC-3, VC-4, STS-1 or STS-3 etc. Furthermore, it displays the source and destination AIDs of the cross-connection within a schematic diagram which represents the cross connection type by one (1-way) or two (2-way) arrows.
Modify Cross Connection Parameters	The Modify Cross Connection Parameters selection invokes the following sequence of wizard windows: 1. Existing Cross Connection Selection window 2. Leg Selection window for any point-to-point or path-protection cross-connection. 3. Cross Connection Parameter window.
Delete Cross Connection	The Delete Cross Connection selection invokes the following sequence of wizard windows: 1. Existing Cross Connection Selection window 2. Cross Connection Leg Selection window to allow you to select one or more cross-connection legs for deletion, if applicable. 3. Cross Connection Parameter window.
Roll Cross Connection	The Roll Cross Connection selection invokes the following sequence of wizard windows: 1. Existing Cross Connection Selection window 2. Leg Selection window for any point-to-point or path-protection cross-connection. 3. Roll to Tributary Selection window to allow you to select a new source for an existing cross-connection. 4. Cross Connection Parameter window.

Bridge Cross Connection

The **Bridge Cross Connection** selection invokes the following sequence of wizard windows:

1. Existing Cross Connection Selection window
2. Leg Selection window for any point-to-point or path-protection cross-connection.
3. Bridge to Tributary Selection window to allow you to select a new destination for an existing cross-connection.
4. Cross Connection Parameter window.



Protection mechanisms

Overview The reliability of a transmission system can be considerably increased by means of redundant transmission routes. In the event of a transmission error, e.g. if LOS (Loss of Signal) is signalled due to a cable break, or in the event of an excessive bit error ratio, the signals can be switched to a protection line.

Types The following types of network protection switching can be realized:

- STM-64/STM-16 2-fiber Multiplex Section-Shared Protection Ring (MS-SPRing) or OC-192/OC-48 Bidirectional Line Switched Rings (BLSR)
- Multiple MS-SPRing/BLSR protection
- Sub-Network Connection Protection (SNCP) or Unidirectional Path Switched Rings (UPSR)
- STM-16 1+1 Multiplex Section Protection (MSP) or OC-48 1+1 Automatic Protected Switch (APS)
- Multiple MSP/APS 1+1 protection



Path Protection

Overview The principle of a path protection is based on the duplication of the signals to be transmitted and the selection of the best signal available at the path connection termination. The two (identical) signals are routed over two different path segments, one of which is defined as the main path and the other as standby path. The same applies to the opposite direction. The system only switches to the standby path if the main path is faulty.

LambdaUnite[™] MSS supports both, SONET and SDH path protection features.

- SDH: Subnetwork Connection Protection (SNCP)
- SONET: Unidirectional Path-Switched Ring (UPSR)

SNCP SNCP providing path-level protection for individual VC-N circuits that are routed independently across any network (meshed, rings or mixed). It may be applied at any path layer in a layered network. It can be used to protect a portion of a path between two Connection Points (CPs) or between a CP and a Termination Connection Point (TCP), or the full end-to-end path between two TCPs.

SNCP is a dedicated 1+1 protection architecture in which the traffic is permanently bridged onto two SNCs at the transmit end, carried through any number of facilities of any type, and selected from one of the two SNCs at the receive end. One SNC is called the working SNC and the other, the protection SNC.

LambdaUnite MSS supports two types of SNCP:

- Inherently monitored subnetwork connection protection (SNC/I) SNC/I protection, generally, protect against failures in the server layer. The protection process and the defect detection process are performed by two adjacent layers. The server layer performs the defect the defect detection process, and forwards the status to the client layer by means of the Server Signal fail (SSF) signal. This means AU-4 or STS-1 defects are defects and the switch is triggered by the SSF signal.
- Non-intrusively monitored subnetwork connection protection (SNC/N)

SNC/N protection, generally, protects against failures in the server layer **and** against failures and degradation in the client layer. This means the non-intrusive monitor function on the received side detects Signal Fail (SD) and Signal Degrade (SD) events on the incoming signal and triggers the switch.

UPSR The UPSR is typically a SONET ring architecture. It provides path-level protection for STS-N circuits within in physical ring network. The ring is usually comprised of unprotected lines at the same OC-N rate which are connected in a ring topology. Typically all (or most) of the circuits within the ring are path-protected. The UPSR provides redundant bandwidth to protect services against node failures or other failures conditions. UPSR operate by bridging an identical STS-N path signal in both directions around the ring, and then selecting the better of the two signals to drop from the ring, based on a signal quality hierarchy. As for SNCP, the path selection is based on purely local information, i.e. on path layer indications including path layer defects and maintenance signals.

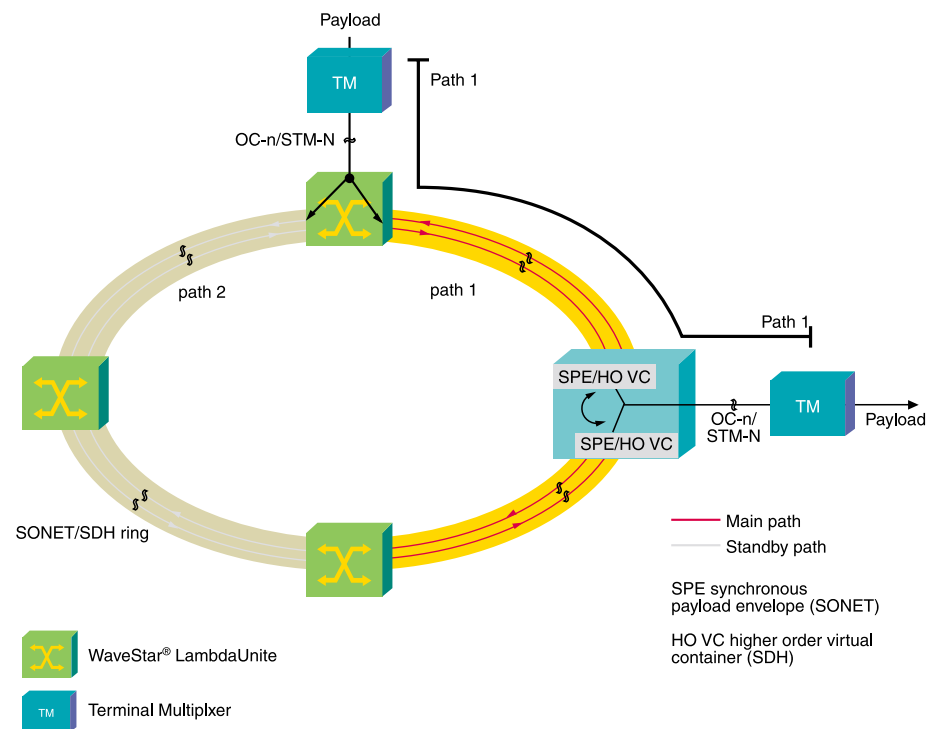
LambdaUnite MSS supports UPSR protection, also within logical ring applications.

A Logical Ring is formed by bridging the incoming signal at a source node, diversely routing the two paths through a SONET network, and selecting the “better” of the two diversely routed paths at the destination node. The paths may traverse over any type of physical linear, mesh or ring network.

Topologies The *WaveStar*® CIT Cross-Connection Wizard supports the creation of SNCP/UPSR protected paths in single rings and in connected rings (ring-to-ring configuration, i.e., one NE connects to two rings). Please note that in the ring-to-ring configuration the full SNCP/UPSR is available within each ring. The connection between the rings, this means the connection within the network element, is unprotected, because there is no dual node ring interworking.

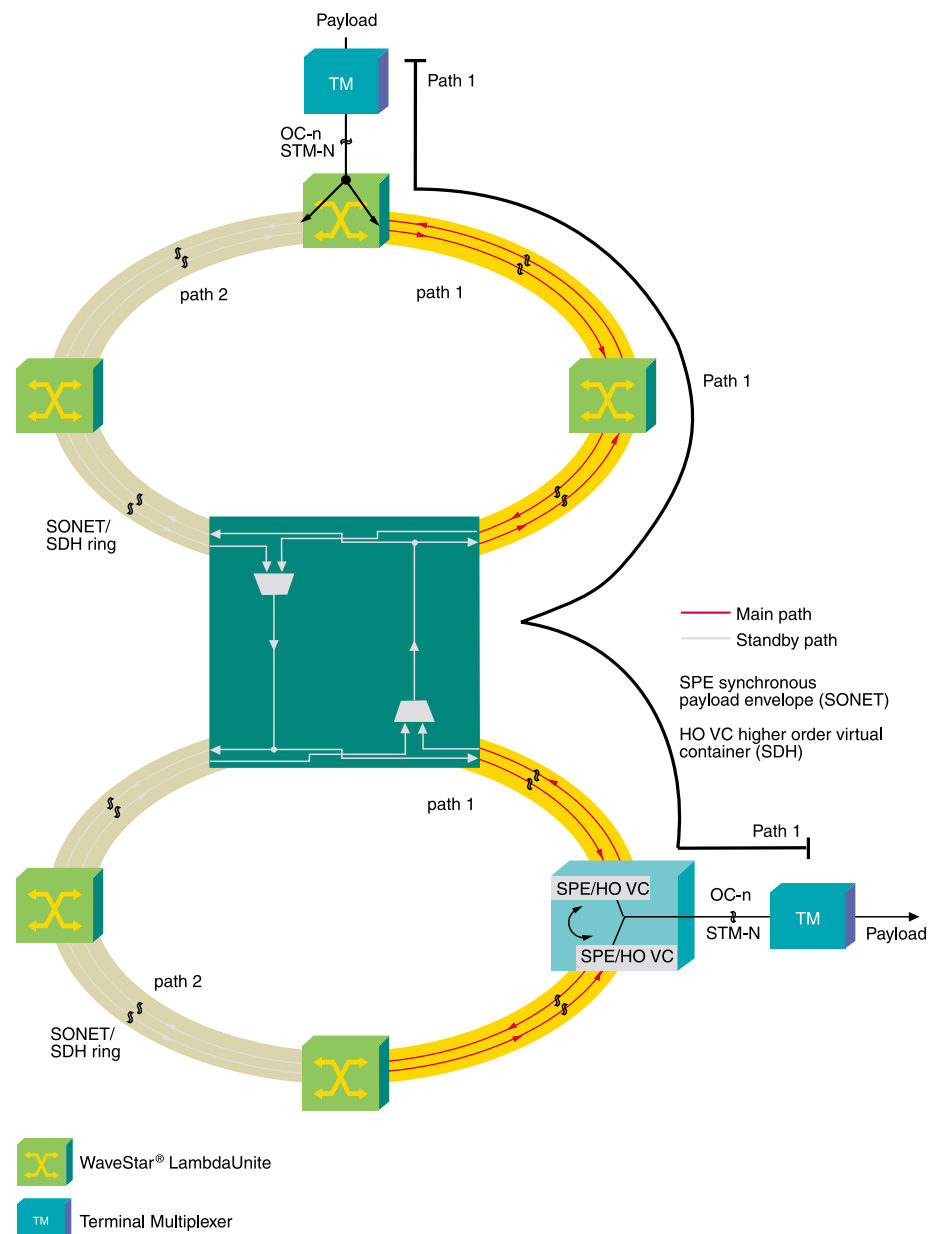
The following figure shows an example of a single ring UPSR/SNCP application. Path 1 is the working (main) path, path 2 is the protection (standby) path in this example. The path termination is always outside

the *LambdaUnite* MSS. For simplification, the UPSR/SNCP switch is only shown for an unidirectional connection.



The following figure shows an example of a ring-to-ring UPSR/SNCP configuration. Here, the UPSR/SNCP also consists of a broadcast in transmit direction. The signal then moves through the first ring via path 1 (working) and path 2 (protection). The ring is connected to

another ring via one single NE. For simplification, the UPSR/SNCP switch is only shown for an unidirectional connection.



Switching criteria Two types of events can trigger a switch action.

- failure detection
- external request

Controller failures in the NE do not affect the capability of automatic SNCP/UPSR protection switching.

SNCP/UPSR protection switching can be configured revertive or non-revertive with *WaveStar* CIT. When revertive switching is configured, a wait-to-restore time can be defined. The default configuration is non-revertive.

Manual switch

The following manual switching actions are possible with *WaveStar* CIT or *WaveStar* SNMS:

- manual to working: switches the traffic to the main path if it is not faulty
- manual to protection: switches the traffic to the standby path if it is not faulty
- forced to working: causes switchover to the main (working) path (even if this path is faulty)
- forced to protection: causes forced switchover to the standby (protection) path (even if this path is faulty)
- clear: clears any active manual switch request, clear will also release the wait-to-restore timer when provided for revertive switching

□

Line Protection

Overview In line protection switching, the complete (physical) transmission path between two multiplexers is duplicated. This means that a separate Optical Interface Unit is connected in each multiplexer for the main (working) and standby (protection) section.

LambdaUnite[™] MSS supports both, SONET and SDH line protection features.

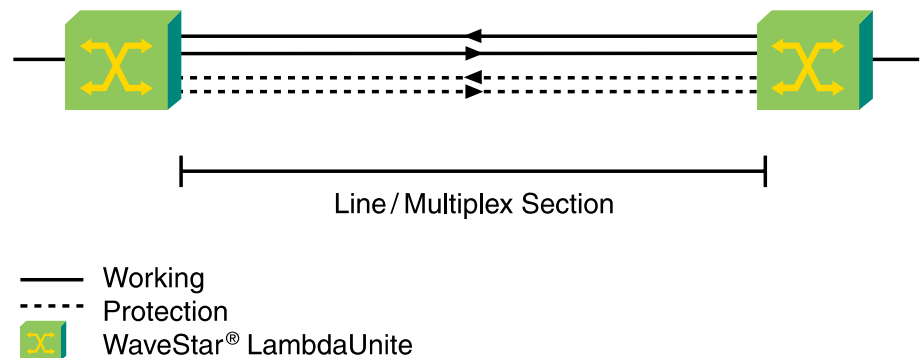
- SDH: 1+1 Multiplex Section Protection (MSP) on STM-16 interfaces
- SONET: 1+1 Linear Automatic Protection Switch (APS) on OC-48 interfaces

MSP The SDH multiplex section protection scheme complies with the ITU-T G.841.

APS The SONET Linear Automatic Protection Switch scheme complies with the ANSI T 1.105.01 APS.

1+1 MSP/APS In case of a 1+1 MSP/APS each main line is assigned to one standby line. As for other types of protection switching the signals are duplicated in the transmit direction. In the receive direction, this type of switching either selects, depending on the signal quality, the input signals of the main section or that of the standby section for transmission. The network elements are equipped with an MSP function which carries out the selection and changeover processes. The switching activities are monitored by the K1-K2 byte. This takes place in the receive direction on the circuit pack, which is connected to the standby section.

The following figure illustrates the schematic diagram of a 1+1 line protection.



Switching criteria

The switchover is triggered by the following switching criteria, which are generated by the MST functional block after evaluation of the SOH:

- **Signal Degrade (SD)**
Bit error ratio (BER) in the range $10^{-3} \dots 10^{-9}$
- **Loss of Signal (LOS)**
- **Loss of Frame (LOF)**
- **Multiplex Section Excessive Bit Error Ratio (MS-EXC)**
Bit error ratio $\geq 10^{-3}$
- **Multiplex Section Alarm Indication Signal (MS-AIS)**

Mode of operation

In the *LambdaUnites* MSS systems the 1+1 MSP/APS operate unidirectional in non-revertive mode.

□

Ring Protection

Overview A Ring Protection is a self-healing ring configuration in which traffic is bidirectional between each pair of adjacent nodes and is protected by redundant bandwidth on the bidirectional lines that interconnect the nodes in the ring. Because traffic flow is bidirectional between nodes, traffic can be added at one node and dropped at the next without traveling around the entire ring. This leaves the spans between other nodes available for additional traffic. Therefore, with many traffic patterns a bidirectional ring can carry much more traffic than the same facilities could carry if configured for a unidirectional ring.

LambdaUnite[™] MSS supports both, SONET and SDH ring protection features.

- SDH: Multiplex Section Shared Protection Ring (MS-SPRing)
- SONET: Bidirectional Line Switched Ring (BLSR)

MS-SPRing The following protection Schemes can be configured by *LambdaUnite* MSS network elements.

- 2-fiber MS-SPRing on STM-64 interfaces
- 2-fiber MS-SPRing on STM-16 interfaces

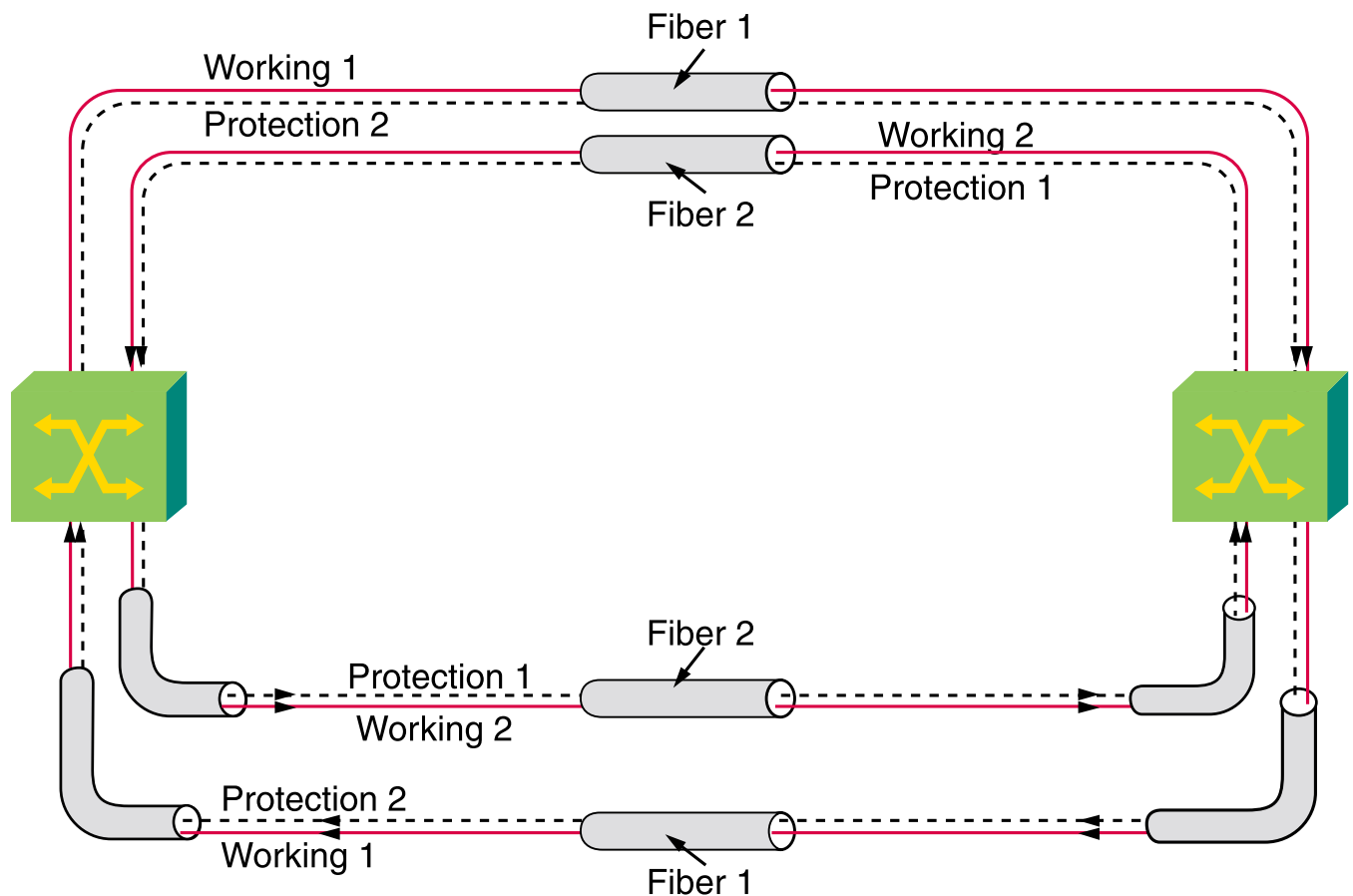
The STM-64 and STM-16 2-fiber MS-SPRing complies with the ITU-T G.841.

BLSR The following protection Schemes can be configured by *LambdaUnite* MSS network elements.

- 2-fiber BLSR on OC-192 interfaces
- 2-fiber BLSR on OC-48 interfaces

The OC-48 and OC-192-fiber BLSR complies with the ANSI T1.105.01 APS.

Traffic disposition The following figure shows working and protection traffic disposition in a *LambdaUnite* MSS 2-fiber MS-SPRing/BLSR.



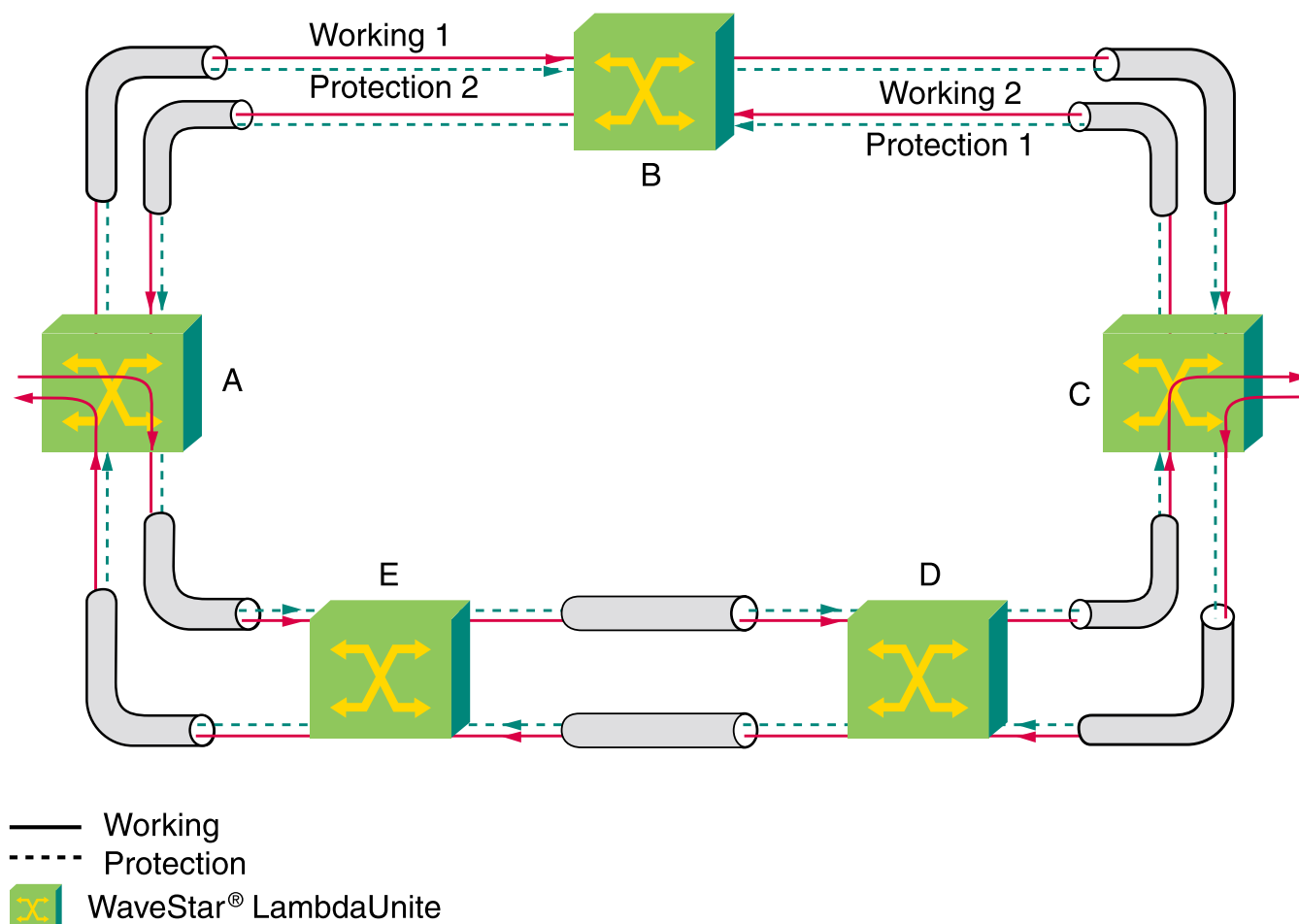
Self-healing rings *LambdaUnite* MSS MS-SPRings/BLSRs are self healing, that means transport is automatically restored after node or fiber failures.

In case of a 2-fiber 10Gbit/s MS-SPRing/BLSR, each line carries 32 VC-4/STS-3c equivalent timeslots of working capacity plus 32 VC-4/STS-3c equivalent timeslots of protection capacity. For 2-fiber 2.5 Gbit/s MS-SPRing/BLSR, the working and protection capacity is 8 VC-4/STS-3c equivalents timeslots.

In the event of a fiber or node failure, service is restored by switching traffic from the working capacity of the failed line to the protection

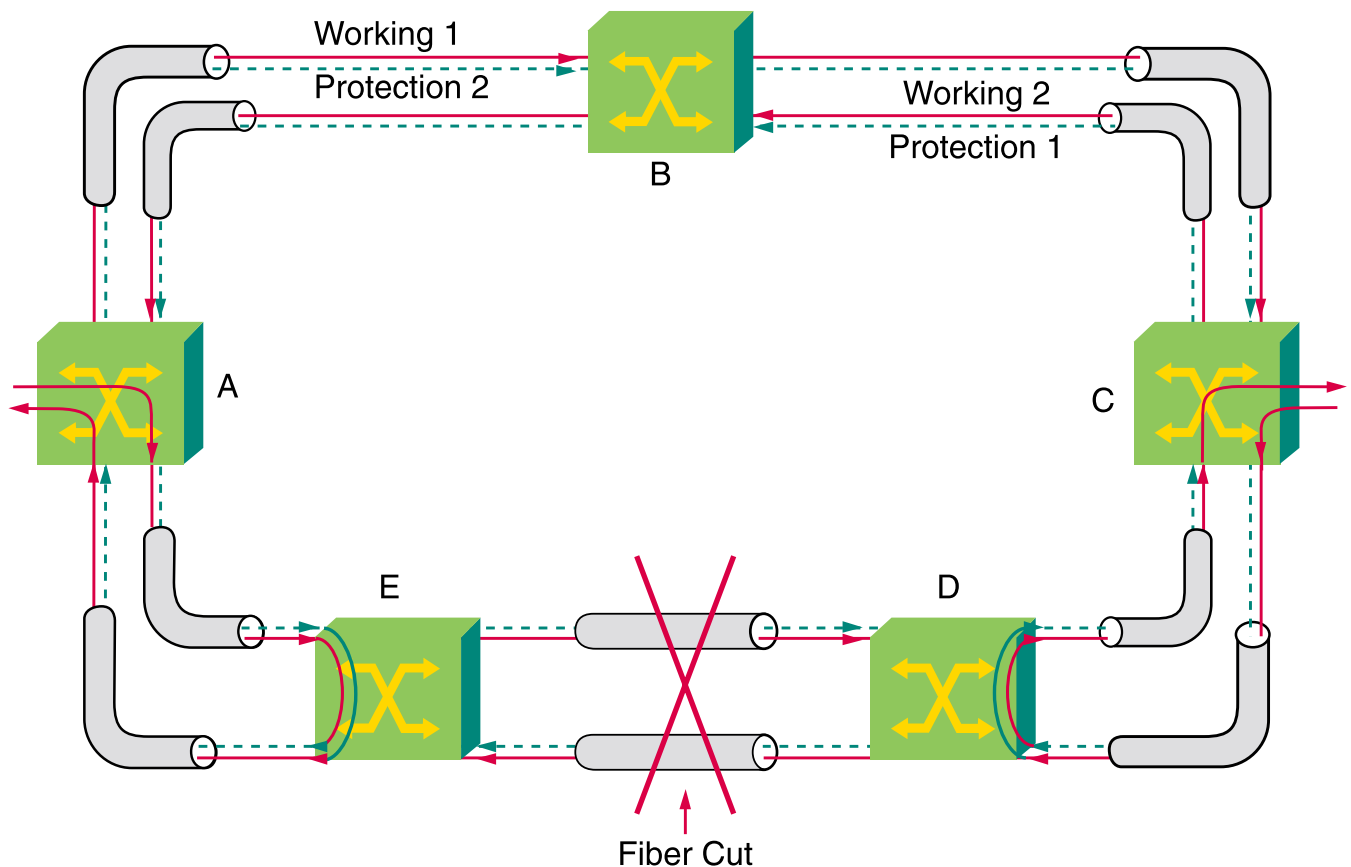
capacity in the opposite direction around the ring. (See “Traffic flow example” (18-22) and “Fiber cut example” (18-23).)

Traffic flow example The following figure shows normal (non-protection-switched) traffic flow in a *LambdaUnite* MSS 2-fiber MS-SPRing/BLSR.



Protection switching When a line-level event triggers a protection switch, the affected nodes switch traffic on to protection capacity and transport it to its destination by looping it back the other way around the ring. (See “Fiber cut example” (18-23).) Service is reestablished on the protection capacity in less than 50 milliseconds after detection of the failure (for signal fail conditions in rings without existing protection switches or extra traffic).

Fiber cut example The following figure illustrates a 2-fiber MS-SPRing/BLSR protection switch that results from a fiber cut.



 WaveStar® LambdaUnite

Protection traffic flow In “Fiber cut example” (18-23), traffic going from Node A to Node C that normally passed through Node E and Node D on “working 2” capacity, is switched onto the “protection 2” capacity of the line leaving Node E in the opposite direction. The traffic loops back around the ring via Node B, C, and D (where the loopback switch is active) to Node C. Similarly, traffic going from Node C to Node A that normally passed through Node D and Node E on “working 1” capacity is switched on to the “protection 1” capacity of the line leaving Node D in the opposite direction.

The same approach is used for a node failure. For example, if Node D were to fail, Nodes C and E would perform loopback protection switches to provide an alternate route for ring traffic.

□

Protection configurations

Overview This section describes the shelf configuration guidelines that have to be observed for the following protection mechanisms:

- 2-fiber MS-SPRing/BLSR
- 1+1 MSP/ 1+1 APS.

MS-SPRing/BLSR The MS-SPRing/BLSR related STM-16/OC-48 and STM-64/OC-192 circuit packs have to be plugged into any universal slot.

MSP/APS MSP/APS can only be established between two separate circuit packs (which are of the same type), i.e. it is not allowed to establish MSP/APS between 2 ports on the same circuit pack. MSP/APS between different ports on different circuit packs can be configured independently, e.g. one port of circuit pack 1 can be protected with one port of circuit pack 2 while the second port on circuit pack 1 is protected by circuit pack 3.

For STM-16/OC-48 port units, any pair combination of universal slot positions can be applied.

□



19 Performance monitoring concepts

Overview

Purpose This chapter describes the underlying performance monitoring concepts of the *LambdaUnite*[™] MSS systems.

Contents

Introduction	19-2
The performance monitoring process	19-5
Performance measurements	19-6
Performance monitoring reports	19-12
Impact of configuration changes on performance monitoring	19-18



Introduction

Purpose of performance monitoring

The purpose of performance monitoring is:

1. to detect degraded performance of the transport functionality in order to support pro-active maintenance activities, for example replacing equipment before the impact of the performance degradation on service becomes unacceptable (maintenance-oriented performance monitoring).
2. to collect performance data over a long period (typically months) in order to verify the quality of the transport service (quality-of-service-oriented performance monitoring).

Near-end and far-end performance monitoring

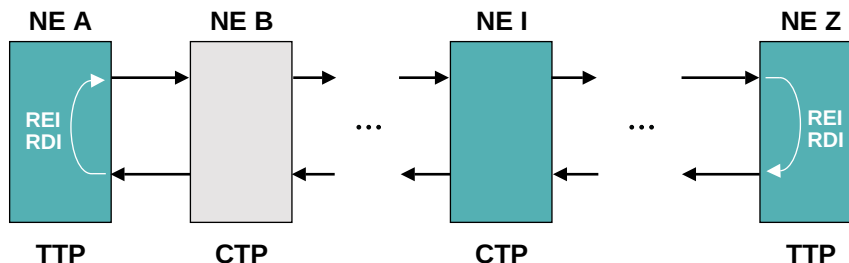
In principle, two kinds of performance monitoring can be distinguished:

- Near-end performance monitoring
Performance parameters are derived from bit errors and defects in the incoming signal.
- Far-end performance monitoring
Performance parameters are derived from the remote information (REI/RDI) in the incoming signal. The meaning of the remote information will be explained in more detail afterwards in this chapter.

Performance monitoring of a bidirectional path

To monitor the performance of a bidirectional path, near-end and far-end performance monitoring information is correlated. The bidirectional path is considered unavailable if at least one of the directions is unavailable.

The following figure shows an example of a bidirectional path:



At NE A, the near-end information represents the performance of the unidirectional trail from NE Z to NE A, while the far-end information represents the performance of the unidirectional trail from NE A to NE Z.

At NE Z, the near-end information represents the performance of the unidirectional trail from NE A to NE Z, while the far-end information represents the performance of the unidirectional trail from NE Z to NE A.

At an intermediate NE I, the near-end information in the direction from NE A to NE Z represents the performance of the unidirectional trail segment from NE A to NE I, while the far-end information represents the performance of the unidirectional trail from NE Z to NE A. The near-end information in the direction from NE Z to NE A represents the performance of the unidirectional trail segment from NE Z to NE I, while the far-end information represents the performance of the unidirectional trail from NE A to NE Z.

At either end of the trail (NE A or NE Z) the combination of near-end and far-end information represents the performance of the two directions of the trail. At an intermediate NE I, the combination of far-end information in the trail signal from NE A to NE Z and far-end information in the trail signal from NE Z to NE A presents the performance of the two directions of the trail.

Selection between SDH and SONET behaviour

The selection between SDH and SONET behaviour of performance monitoring is made by setting the interface standard of a port. Depending on that SDH/SONET selection, there is a different collection of performance parameters associated to a monitoring point (cf. "Performance measurements" (19-6)).

Bit errors and block errors

A distinction has to be made between SDH and SONET concerning the underlying performance monitoring concepts. SONET performance monitoring is based on the evaluation of bit errors (code violations) while SDH performance monitoring is based on the evaluation of block errors.

SONET performance monitoring

In SONET performance monitoring, at each of the transmission layers (section, line, path) a bit-interleaved parity (BIP) word is calculated at the transmitter and forwarded downstream to the receiver. At the receive side, the BIP is re-calculated and compared on a bit-by-bit basis with the BIP received from the transmit side. The number of mismatches between the re-calculated BIP and the BIP received is the code violations (CV) count. On the line and path layer, the CV count is then sent upstream to the far end, where it is evaluated as the Remote Error Indication (REI).

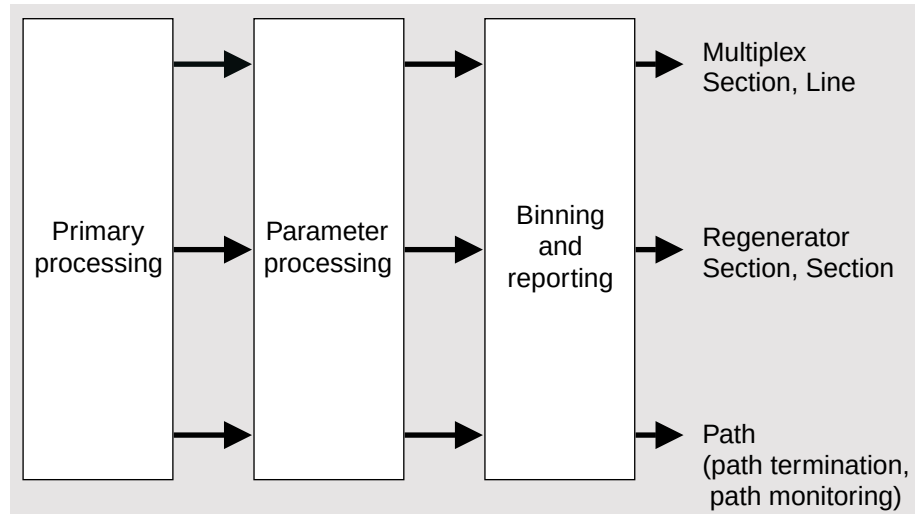
SDH performance monitoring

SDH performance monitoring is based on the evaluation of block errors, where the block size depends on the transmission layer. At the Regenerator Section (RS) layer, a block is equivalent in size to an SDH frame. Therefore, the number of bits in an RS block is dependent on the signal rate. The BIP comparison is performed on a per-byte basis. Therefore, one or more errored bits in the RS parity byte (B1 byte in the RSOH) constitutes a single RS block error. At the Multiplex Section (MS) layer, the number of bits in a block is always 801. The BIP comparison is performed on a per-bit basis. Therefore, a single bit error in the MS parity bytes (three B2 bytes in the MSOH) constitutes a single MS block error. At the higher order path layer, a block is equivalent in size to an SDH path. Therefore, the number of bits in a VC-n block is dependent on the signal rate. The BIP comparison is performed on a per-byte basis. Therefore, one or more errored bits in the parity byte of the higher order path (B3 byte in the VC-n POH) constitutes a single VC-n block error. Concerning the Remote Error Indication (REI), the same approach as used for SONET performance monitoring is also used for SDH performance monitoring.

□

The performance monitoring process

Process description The performance monitoring process is a three-stage process:



Primary processing

Fundamental parameters are derived from errors detected in the transport signal, classified into bit errors and defects, and accumulated over one-second periods.

Parameter processing

Near-end and far-end performance parameters are calculated based on the evaluation and correlation of the fundamental parameters obtained during the primary processing. Please refer to “Near-end performance parameters” (19-6) and “Far-end performance parameters” (19-8).

□

Performance measurements

Performance monitoring points Performance monitoring points can be any trail termination point (TTP) or connection termination point (CTP) in the network element.

Possible TTPs and CTPs are:

- Trail termination points (TTPs)
 - SDH: Regenerator Section Termination (RST),
SONET: Section termination
 - SDH: Multiplex Section Termination (MST),
SONET: Line termination
 - SDH and SONET: Path termination
- Connection termination points (CTPs)
 - SDH and SONET: Path monitoring at non-intrusive monitoring (NIM) points.

Maximum number of performance monitoring processes

Simultaneously, up to 2000 performance monitoring processes can co-exist.

The number of performance monitoring processes depends on the number of enabled performance monitoring points. For each enabled performance monitoring point,

- near-end performance monitoring is counted as one process, and
- far-end performance monitoring is counted as one process.

Please note that in the adaptive-rate tributary operation of a port, the transport capacity of the port is counted as a number of performance monitoring points equal to its bandwidth (in STS-1 equivalents). An OC-48 port for example, would consume 48 performance monitoring processes.

Near-end performance parameters The following near-end performance parameters are supported by the *LambdaUnite*[™] MSS systems:

Parameter	SDH	SONET
Errored seconds (ES) A near-end errored second is a one-second interval with one or more block errors (SDH) or bit errors (SONET) or one or more defects ($\neq$ RDI) in the incoming signal. Errored seconds are not declared during a period of unavailability (cf. unavailable seconds).	X	X
Severely errored seconds (SES) A near-end severely errored second is a one-second interval in which the amount of block errors (SDH) or bit errors (SONET) has exceeded the near-end SES threshold, or in which at least one defect has been detected ($\neq$ RDI) in the incoming signal.	X	X
Background block errors (BBE) The BBE count is the accumulated number of block errors not occurring as part of a severely errored second.	X	–
Code violations (CV) Code violations are the SONET equivalent to the SDH background block errors.	–	X
Unavailable seconds (UAS) Near-end unavailable seconds determine the period of time during which the transmission route in the receive direction is in the unavailability state. A period of unavailability begins at the onset of ten consecutive near-end severely errored seconds. These ten seconds are considered to be part of the unavailability period. A new period of availability begins at the onset of ten consecutive non-severely-errored seconds. These ten seconds are considered to be part of the availability period.	X	X
Loss of signal seconds (LOSS) A loss of signal second is a second in which a loss of signal condition has been detected in the incoming signal.	–	X

Parameter	SDH	SONET
Severely errored framing seconds (SEFS) A severely errored framing second is a second in which frame alignment has temporarily been lost (out-of-frame (OOF) condition).	–	X
Failure count (FC) The near-end failure count is incremented each time a near-end defect (not RDI) has been detected in the incoming signal. The near-end failure count is reset to “0” at the end of each one-second interval.	–	X
AIS seconds (AISS) An AIS second is a second in which AIS has been detected in the incoming signal.	–	X
Forward Error Correction – corrected (FECC) The FECC count is the accumulated number of detected and corrected FEC code violations per frame.	X	X

Far-end performance parameters

The following far-end performance parameters are supported by the *LambdaUnite* MSS systems:

Parameter	SDH	SONET
Errored seconds (ES) A far-end errored second is a one-second interval with one or more block errors (SDH) or bit errors (SONET) or one or more defects at the far end. ¹ Far-end errored seconds are not declared when other defects than RDI are present at the near end.	X	X
Severely errored seconds (SES) A far-end severely errored second is a one-second interval in which the amount of block errors (SDH) or bit errors (SONET) at the far end has exceeded the far-end SES threshold, or in which at least one defect has been detected at the far end. ¹	X	X

Parameter	SDH	SONET
Background block errors (BBE) The BBE count is the accumulated number of block errors not occurring as part of a severely errored second.	X	–
Code violations (CV) Code violations are the SONET equivalent to the SDH background block errors.	–	X
Unavailable seconds (UAS) Far-end unavailable seconds determine the period of time during which the transmission route in the transmit direction is in the unavailability state. A period of unavailability time begins at the onset of ten consecutive far-end severely errored seconds. These ten seconds are considered to be part of unavailability time. A new period of availability time begins at the onset of ten consecutive non-severely-errored seconds. These ten seconds are considered to be part of availability time.	X	X
Failure count (FC) The near-end failure count is incremented each time an RDI defect has been detected in the incoming signal. The far-end failure count is reset to “0” at the end of each one-second interval.	–	X

Notes:

1. The number of block errors or bit errors at the far end is indicated at the near end by means of the Remote Error Indication (REI), the presence of defects at the far end is indicated by the Remote Defect Indication (RDI). Please also refer to “Near-end and far-end performance monitoring” (19-2) and “Performance monitoring of a bidirectional path” (19-2). In SONET, the remote information for defects is called “Remote Failure Indication (RFI)”.

SES declaration threshold

The SES declaration threshold is a configurable parameter defining the threshold for the detection of Severely Errored Seconds (SES).

The SES declaration threshold can be set individually for:

- Near-end
 - SDH Regenerator Section performance monitoring (please note that there is no far-end Regenerator Section performance monitoring)
 - SDH Multiplex Section performance monitoring
 - SDH path performance monitoring
 - SONET Section performance monitoring (please note that there is no far-end Section performance monitoring)
 - SONET Line performance monitoring
 - SONET path performance monitoring
- Far-end
 - SDH Multiplex Section performance monitoring
 - SDH path performance monitoring
 - SONET Line performance monitoring
 - SONET path performance monitoring

SDH performance parameters

The following overview shows the available SDH performance parameters and their association to the monitoring points Regenerator Section (RS), Multiplex Section (MS) and path (path termination and path monitoring at non-intrusive monitoring (NIM) points):

Parameter	Regenerator Section	Multiplex Section	Path
Near-end parameters			
ES	RS_N_ES	MS_N_ES	VC_N_ES
SES	RS_N_SES	MS_N_SES	VC_N_SES
BBE	RS_N_BBE	MS_N_BBE	VC_N_BBE
UAS	RS_N_UAS	MS_N_UAS	VC_N_UAS
FECC	—	MS_FECC	—
Far-end parameters			
ES	—	MS_F_ES	VC_F_ES
SES	—	MS_F_SES	VC_F_SES
BBE	—	MS_F_BBE	VC_F_BBE
UAS	—	MS_F_UAS	VC_F_UAS

SONET performance parameters

The following overview shows the available SONET performance parameters and their association to the monitoring points Section, Line and path (path termination and path monitoring at non-intrusive monitoring (NIM) points):

Parameter	Section	Line	Path
Near-end parameters			
CV	CV-S	CV-L	CV-P
ES	ES-S	ES-L	ES-P
SES	SES-S	SES-L	SES-P
UAS	–	UAS-L	UAS-P
FC	–	FC-L	FC-P
LOSS	LOSS-S	–	–
SEFS	SEFS-S	–	–
AISS	–	AISS-L	–
FECC	–	FECC-L	–
Far-end parameters			
CV	–	CV-LFE	CV-PFE
ES	–	ES-LFE	ES-PFE
SES	–	SES-LFE	SES-PFE
UAS	–	UAS-LFE	UAS-PFE
FC	–	FC-LFE	FC-PFE

□

Performance monitoring reports

Configuration options The following configuration options (the designations refer to the corresponding *WaveStar*® CIT windows) exist with regard to performance monitoring reports:

Option	Meaning
Time Period	This option specifies the monitoring interval for which performance information shall be retrieved from the NE. Possible values are 1 Day , 15 Min or Both .
Monitored Date	These two options specify the date and time of the monitoring interval for which performance information shall be retrieved from the NE. For the Monitored Date , the Current Date , Previous Date or Both can be selected.
Monitor Time	The Monitor Time is related to the selected Monitored Date . By selecting Current or Time(HH:MM) (indicating the starting time of the monitoring interval in the format hour-of-day:minute-of-hour), a single monitoring interval can be selected for being reported. By means of Range(HH:MM-HH:MM) , the starting time and end time of multiple 15-minutes intervals can be specified.
Monitor Level	This option can be used to suppress unnecessary “zero” output in performance monitoring reports. If registers which have a value of “0” are not wanted, then select 1-UP , otherwise select 0-UP .

Option	Meaning
Parameter selection	Which performance monitoring parameters are available to be included in performance monitoring reports depends on the interface standard (SDH/SONET) of the respective optical port and on the relevant signal structure. Please refer to: • “SDH Regenerator Section” (19-13) • “SDH Multiplex Section” (19-13) • “SDH path” (19-14) • “SONET Section” (19-15) • “SONET Line” (19-15) • “SONET path” (19-16) Please also refer to “Near-end performance parameters” (19-6) and “Far-end performance parameters” (19-8).

SDH Regenerator Section

The following are the parameters of the SDH Regenerator Section performance monitoring reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE. For further information on the validity flag, please refer to “Validity flag” (19-16).

Parameter	Description
RS_N_ES	Regenerator Section - Near-end Errored Seconds (ES)
RS_N_SES	Regenerator Section - Near-end Severely Errored Seconds (SES)
RS_N_BBE	Regenerator Section - Near-end Background Block Errors (BBE)
RS_N_UAS	Regenerator Section - Near-end Unavailable Seconds (UAS)

Please note that there is no far-end performance monitoring in the SDH Regenerator Section.

SDH Multiplex Section

The following are the parameters of the SDH Multiplex Section performance monitoring reports that are returned from the NE. In

addition to the value of each parameter, the time, date, and validity of the data is returned by the NE. For further information on the validity flag, please refer to “Validity flag” (19-16).

Parameter	Description
MS_N_ES	Multiplex Section - Near-end Errored Seconds (ES)
MS_N_SES	Multiplex Section - Near-end Severely Errored Seconds (SES)
MS_N_BBE	Multiplex Section - Near-end Background Block Errors (BBE)
MS_N_UAS	Multiplex Section - Near-end Unavailable Seconds (UAS)
MS_F_ES	Multiplex Section - Far-end Errored Seconds (ES)
MS_F_SES	Multiplex Section - Far-end Severely Errored Seconds (SES)
MS_F_BBE	Multiplex Section - Far-end Background Block Errors (BBE)
MS_F_UAS	Multiplex Section - Far-end Unavailable Seconds (UAS)

SDH path The following are the parameters of the SDH path performance monitoring reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to “Validity flag” (19-16).

Parameter	Description
VC_N_ES	SDH path - Near-end Errored Seconds (ES)
VC_N_SES	SDH path - Near-end Severely Errored Seconds (SES)
VC_N_BBE	SDH path - Near-end Background Block Errors (BBE)
VC_N_UAS	SDH path - Near-end Unavailable Seconds (UAS)

Parameter	Description
VC_F_ES	SDH path - Far-end Errored Seconds (ES)
VC_F_SES	SDH path - Far-end Severely Errored Seconds (SES)
VC_F_BBE	SDH path - Far-end Background Block Errors (BBE)
VC_F_UAS	SDH path - Far-end Unavailable Seconds (UAS)

SONET Section The following are the parameters of the SONET Section performance monitoring reports that are returned from the NE. All listed parameters are related to near-end performance monitoring. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter.

Parameter	Description
CVS	Code Violations (CV) - Section
ESS	Errored Seconds (ES) - Section
SESS	Severely Errored Seconds (SES) - Section
SEFS-S	Severely Errored Framing Seconds (SEFS) - Section
LOSS-S	Loss-of-Signal Seconds (LOSS) - Section

Please note that there is no far-end performance monitoring in the SONET Section.

SONET Line The following are the parameters of the SONET Line performance monitoring reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to “Validity flag” (19-16).

Parameter	Description
CVL	Code Violations (CV) - Line (near end)
ESL	Errored Seconds (ES) - Line (near end)
SESL	Severely Errored Seconds (SES) - Line (near end)

Parameter	Description
UASL	Unavailable Seconds (UAS) - Line (near end)
AISS-L	AIS Seconds (AISS) - Line (near end)
FC-L	Failure Count (FC) - Line (near end)
CV-LFE	Code Violations (CV) - Line, Far End
ES-LFE	Errored Seconds (ES) - Line, Far End
SES-LFE	Severely Errored Seconds (SES) - Line, Far End
UAS-LFE	Unavailable Seconds (UAS) - Line, Far End
FC-LFE	Failure Count (FC) - Line, Far End

SONET path The following are the parameters of the SONET path performance monitoring reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to “Validity flag” (19-16).

Parameter	Description
CVP	Code Violations (CV) - Path (near end)
ESP	Errored Seconds (ES) - Path (near end)
SESP	Severely Errored Seconds (SES) - Path (near end)
UASP	Unavailable Seconds (UAS) - Path (near end)
FC-P	Failure Count (FC) - Path (near end)
CV-PFE	Code Violations (CV) - Path, Far End
ES-PFE	Errored Seconds (ES) - Path, Far End
SES-PFE	Severely Errored Seconds (SES) - Path, Far End
UAS-PFE	Unavailable Seconds (UAS) - Path, Far End

Validity flag The validity flag shows the validity of the register whose value is reported. The validity flag is set to “1” if the corresponding value is valid. Otherwise, the validity flag is omitted.

The validity flag is omitted (the corresponding value is invalid) if:

- the elapsed time deviation is greater than 10 seconds, or
- the SES declaration threshold has been changed.



Impact of configuration changes on performance monitoring

Removal of monitoring points

When a performance monitoring point is removed from the system, the associated performance monitoring processing is stopped, and all associated bins (current and history) or logs are discarded.

Besides the explicit deletion of performance monitoring points via dedicated management commands performance monitoring points will implicitly be deleted as follows:

- If a circuit pack is deleted all monitoring points related to that circuit pack will be removed.
- If a 1+1 Multiplex Section Protection (MSP) is established, all Multiplex Section performance monitoring points and path performance monitoring points related to the protection port will be removed.
- If a 1+1 Line Protection (Linear APS) is established, all path performance monitoring points related to the protection port will be removed.

Interface standard of a port

The *LambdaUnite*[™] MSS system allows ports to be provisioned for operation according to the SDH or SONET standard.

Changing the interface standard of an optical port from SDH to SONET or vice versa has the following effects:

- The current bin counters are re-initialized.
- The currently provisioned SES declaration threshold remains unchanged.
- The recent bins are not affected.
- Unavailable periods are considered closed, the UAP logs are not reset.

Important! When the interface standard of an optical port is changed from SONET to SDH the value of the SES declaration threshold may be out of the allowed range for SDH.

Forward Error Correction (FEC)

The *LambdaUnite* MSS system supports in-service enabling or disabling of Forward Error Correction (FEC).

Enabling/disabling of in-band FEC

In-service enabling or disabling of in-band FEC has the following effects:

- When in-band FEC is enabled on a port with MS/Line performance monitoring enabled, then the FECC counter will be started.
- When in-band FEC is disabled on a port with MS/Line performance monitoring enabled, then the FECC counter will be reset to zero.

Changing the type of FEC

When, on a port with MS/Line performance monitoring enabled, the type of FEC is changed from in-band FEC to out-of-band FEC or vice versa, then the FECC counter continues counting.

Adaptive-rate tributary operation

The *LambdaUnite* MSS system supports the adaptive-rate tributary operation of optical ports. This means that the composition of the optical signal may vary dynamically up to the transport capacity of the optical port.

Performance monitoring is automatically adapted to the composition of the incoming signal.

XC320 equipment protection switching

All performance monitoring event processing as well as binning and reporting is performed on the active XC320 circuit pack.

On an XC320 circuit pack, performance monitoring data is stored in the current bin and one recent bin. Both XC320 circuit packs operate in a hot-standby mode with regard to performance monitoring. However, no transfer of the performance monitoring data is performed in case of an XC320 equipment protection switch. Thus, an XC320 equipment protection switch may result in loss of performance monitoring data, depending on the time the standby XC320 was plugged into the system.

Important! Prior to an (intentional) XC320 equipment protection switch the standby XC320 should have been present in the system for a full 24-hour binning period. Otherwise, performance monitoring data may be lost.

□



20 Software upgrade concepts

Overview

- Purpose** This section provides information on features relating to the NE Software Management, including
- *LambdaUnite*[™] MSS memory concept
 - Downloading new software
 - Activating new software

Related information For stepwise operating instructions on these items, please refer to the task oriented procedures part Chapter 10, “Software upgrade”) of this manual.

Contents	
NE memory concept	20-2
Software download	20-3

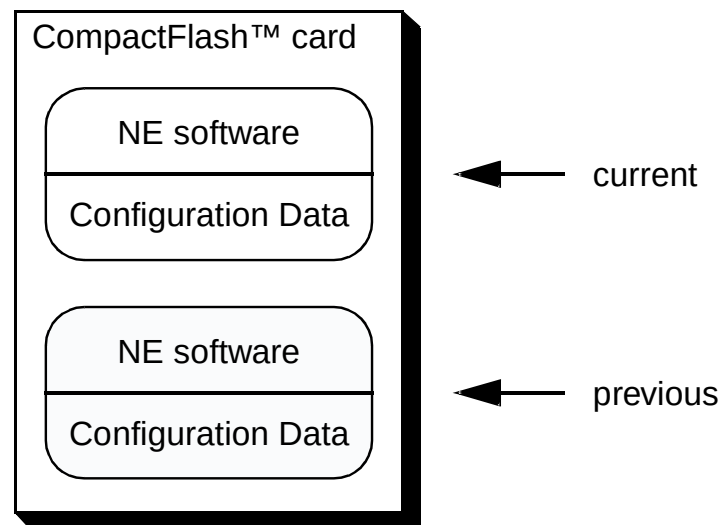


NE memory concept

Overview The *LambdaUnite*[™] MSS system is equipped with volatile working memory and non-volatile memory (NVM). *LambdaUnite* MSS systems make use of a *CompactFlash*[™] card as a non-volatile memory.

CompactFlash card The *CompactFlash* card is used to store the currently active and a previous version of the executable NE software and configuration data. The *CompactFlash* card is inserted into the CTL system controller. The “previous” store area is the one into which data can be downloaded using the SNMS network management system or the *WaveStar*[®] CIT. Activating (“installing”) a newly downloaded software version changes the current/previous assignment automatically.

The following figure illustrates the partitioning of the *CompactFlash* card.



Preparing a CompactFlash card When initially delivered, the compact card is empty. *WaveStar* CIT can be used to copy the initial software generic from the CD-ROM to the *CompactFlash* card .

□

Software download

Definition	Software download is the process of transferring a software generic from a remote entity to a target NE's memory. The remote entity may be a network management system or a CIT. The download process is responsible for establishing the association between the source of the software generic and the target NE and ensuring the integrity of the data during the transfer. The download procedure uses bulk transfer to move an uninterpreted binary file into an NE.
Types of software download	Depending on the state of the network element, there are two possible types of software download: • Initial software download • Software download for upgrade purposes. For each type, an individual procedure has to be applied. There are <i>WaveStar</i>® CIT screens to support the user initiated steps and to indicate progress during download, software application, and test.
Initial software download	Typically, when a software generic is installed for the first time, it is necessary for a craft person to be present on site to monitor the installation. The on-site installation is supported via removable storage media (<i>CompactFlash</i>™ card) associated with <i>WaveStar</i> CIT. The software is initially delivered to the customer on a CD-ROM. The <i>CompactFlash</i> card is initially empty. The software generic has to be copied from the CD-ROM to the empty <i>CompactFlash</i> card via <i>WaveStar</i> CIT. Afterwards, the <i>CompactFlash</i> card is inserted into the NE.
Software download for upgrade purposes	After a software generic is initially installed on-site, its future releases may be downloaded remotely from a centralized location supported by a configuration management application. Remote downloading of software generics not only minimizes dispatching of technicians, but also provides tighter coordination and synchronization among the activation of these software generics across multiple NEs.

Upgrading a software generic in the NE

- causes no disruption to customer services
- causes no disruption to operations support, such as performance monitoring and protection switching
- does not alter any of its existing option settings, e.g., performance monitoring parameters
- requires no re-entry of site-dependent data (e.g., provisioned parameters) into the service database of the NE.

Before accepting the loading of a software generic, the NE verifies a match between its type and the type specified in the software generic control information.

The download time for a software generic to the non-volatile memory (NVM) of the NE from a *WaveStar* CIT or a Management System connected indirectly via a LAN network is approx. 1 hour, via DCC approx. 2 hours.

After completion of the software download, there are now two versions of the software on the NE, the currently active version and the newly downloaded version which has replaced the former backup version.

After a software generic has successfully been loaded onto the NE, the NE waits for an activation (**Apply**) command.

□



21 Database backup concepts

Overview

Purpose This section provides information on features relating to NE database backup and restore.

Related information For stepwise operating instructions on these items, please refer to the task oriented procedures part Chapter 11, “Database backup”) of this manual.

Contents

Configuration backup and restoration

[21-2](#)



Configuration backup and restoration

Background To recover from loss of NE data because of human error, power failure, NE design flaws, software bugs etc, the system provides a backup and restoration capability.

Restore In the restoration process the backup data is copied back into the previous NVM. Then the NE reboots. The NE verifies the serial number of the database with the serial number in the NE's EEPROM. If they are identical the restoration database becomes the working database. All command processing is suspended during restoration.

Impact on service Backup and restoration impact the service as follows:

- The backup operation does not interfere with or interrupt the service.
- The restore operation in general impacts the service.

□



22 *WaveStar*[®] CIT Tutorial

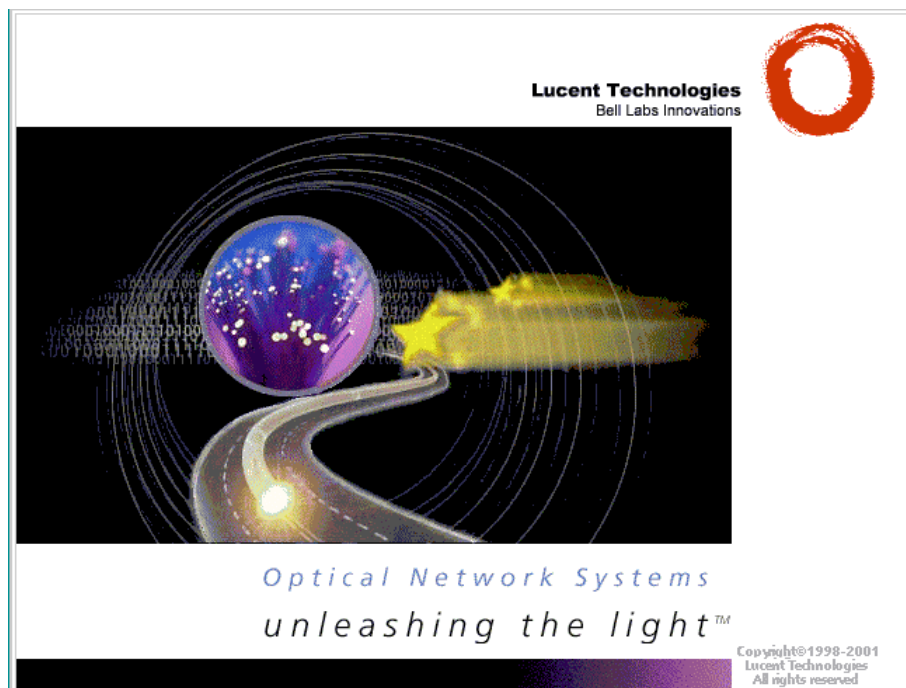
Overview

Purpose The purpose of this chapter is to describe the installation procedures of the *WaveStar* CIT application software on a PC and to give basic operating instructions.

This chapter provides information you should know before performing specific tasks, e.g.:

- how to log into and log out from the *WaveStar* CIT
- how to log into and log out from network elements
- the layout and the structure of the three different series of windows
 - *WaveStar* CIT main window and its menus and sub-menus
 - *WaveStar* CIT System View window and its menus and submenus
 - *WaveStar* CIT Cut-Through window and its menus
- the elements of the *WaveStar* CIT user interface
- the shelf display
- how to get help-information on items that are displayed on the *WaveStar* CIT main window
- how to display the system defaults for a particular component

- Menu structure overviews** Also, this chapter presents menu structure overviews of the *WaveStar* CIT application with references to the parts of this manual where the respective descriptions and tasks can be found.
- Intended audience** This subject is intended for personnel responsible for installation of the *WaveStar* CIT software on a PC, for administrators, and for first-time users of the *WaveStar* CIT application. Experienced users may benefit from the menu structure overviews.



Contents

Installation procedures	<u>22-4</u>
Installing the <i>WaveStar</i> CIT	<u>22-5</u>
Connecting the <i>WaveStar</i> CIT to the NE	<u>22-8</u>
<i>WaveStar</i> CIT login/logout procedure	<u>22-11</u>
General <i>WaveStar</i> CIT concept	<u>22-13</u>
<i>WaveStar</i> CIT main window	<u>22-14</u>
Elements of the <i>WaveStar</i> CIT user interface	<u>22-15</u>
Tool bar of the <i>WaveStar</i> CIT	<u>22-17</u>
Standard window components	<u>22-19</u>

Selection windows	22-24
General window handling	22-27
General pushbuttons	22-30
Basic operations	22-32
Network element selection and login	22-33
Overview of the menu structure	22-37
Logout from NE(s)	22-39
System view	22-41
Shelf view	22-42
The ring map	22-52
Overview of the shelf-view menu structure	22-54
Reports	22-61
View rolling events	22-62
Cut Through view	22-63
Entering the Cut Through view	22-64
Interactive – Execute TL1 single commands	22-67
Interactive – Manage a listbox file	22-69
Working with script files	22-70
Working with logs	22-72



Installation procedures

Overview

Purpose The purpose of this section is to describe the installation procedures of the *WaveStar*® CIT application software on a PC and to give basic operating instructions.

This chapter provides information you should know before performing specific tasks, e.g.:

- how to log into and log out from the *WaveStar* CIT
- how to log into and log out from network elements

Contents

Installing the <i>WaveStar</i> CIT	<u>22-5</u>
Connecting the <i>WaveStar</i> CIT to the NE	<u>22-8</u>
<i>WaveStar</i> CIT login/logout procedure	<u>22-11</u>
General <i>WaveStar</i> CIT concept	<u>22-13</u>



Installing the WaveStar® CIT

- Purpose** Use this procedure to:
- Install the *WaveStar* CIT software onto a new system.
 - Upgrade/change an existing *WaveStar* CIT to a new software version.

- Required equipment** The minimum requirements for a *WaveStar* CIT are a personal computer with
- Pentium® 266 MHz processor (Pentium® III 500 MHz or higher recommended) with 128 MB of RAM (256 MB of RAM or higher recommended)
 - Standard floppy-disk drive for 1.44 MB 3.5" floppy disks
 - 150 MB of free hard-disk drive space
 - CD-ROM drive (16X recommended)
 - PCMCIA (Personal Computer Manufacturer's Card Interface Adapter) slot type II
 - SVGA monitor set to 800x600 resolution or greater, with 256 colors (1024x768 recommended)
 - 10BaseT LAN interface built-in or supplied with a PCMCIA card, installed and working
 - Microsoft Windows® NT 4.0 operating system with Service Pack 5 or Microsoft Windows® 2000
 - Adobe Acrobat Reader for Windows (version 3.01 or later)
 - Removable hard-disk drive (optional; required only for system backup).

The performance of the user interface can be enhanced by using a higher performance personal computer.

- Before you begin** A user who has Windows NT / Windows 2000 System Administration privileges must install the software. That same user, then, becomes the *WaveStar* CIT System Administrator. The *WaveStar* CIT System

Administrator sets up the operating environment for other users. Some of these administration functions include:

- Assigning login IDs
- Assigning an initial password for each login ID
- Customizing the access privileges and security attributes for each login ID, and so forth.

The installation program cannot install system files or update shared files if they are in use by other programs. For this reason you should stop as many Windows® NT applications as possible, before starting with the installation procedure.

Installation Complete the following steps to install the WaveStar CIT software on your PC:

- 1 Insert the WaveStar CIT CD-ROM (ComCode: 109088708) into the appropriate drive of your PC.

Result:

Autorun will start the install process.

2	IF	THEN
	autorun does not start	manually start the program by clicking Start → Run , click on Browse , select the CD-ROM drive, and select setup.exe , click Open and click ok . Result: The WaveStar CIT CD Browser appears.
	autorun starts	no action is required. Result: The WaveStar CIT CD Browser appears.

- 3 Click on **continue**.

- 4 Choose the entry **CIT Software**.

-
- 5 Select the **WaveStar CIT** area on the right.
 - 6 Follow the on-screen instructions. Select **Full Install** when prompted.
 - 7 If there are 2 or more LAN cards on the PC, select the LAN card with the IP Address that corresponds to the OSI LAN, otherwise if there is only 1 LAN card, *WaveStar* CIT will select it automatically.
 - 8 If not yet available on your PC, install the **Acrobat Reader** by selecting the respective area below the entry **CIT Software**.
 - 9 The PC will have to be rebooted if the OSILLC driver is installed. This is installed on the initial *WaveStar* CIT installation. Subsequent upgrades do not require OSILLC driver installation.

END OF STEPS



Connecting the WaveStar® CIT to the NE

Overview The WaveStar CIT can be connected to a network element in four different ways:

- Direct LAN Access (point-to-point)
- LAN Access (network)
- Remote Access via DCC.

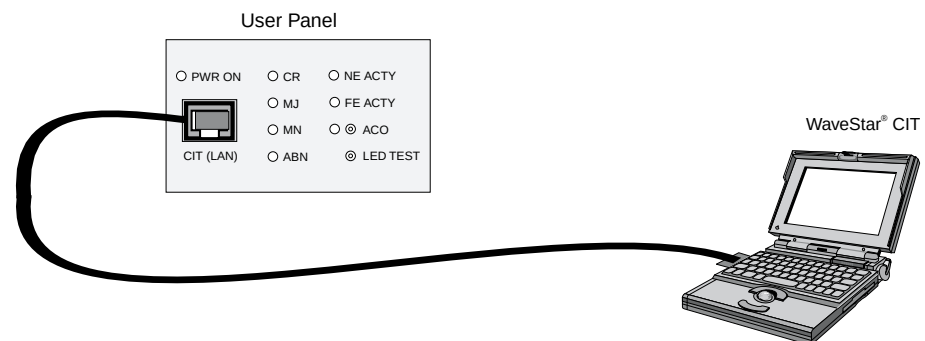
Direct LAN access (point-to-point)

The WaveStar CIT (LAN card) is connected to the *LambdaUnite*™ MSS via the “CIT” port of the user panel or through a backplane connector (LAN I/O Panel). An Ethernet LAN cable (10BaseT) with 4-wire RJ-45 connectors is used for this connection.

The usage of **shielded** 10BaseT LAN cables is only allowed if the applicable national safety requirements have been met by the user. Otherwise, there is a **risk of electrical shock and/or serious injury**.

For wiring details, refer to the *LambdaUnite* MSS Installation Manual.

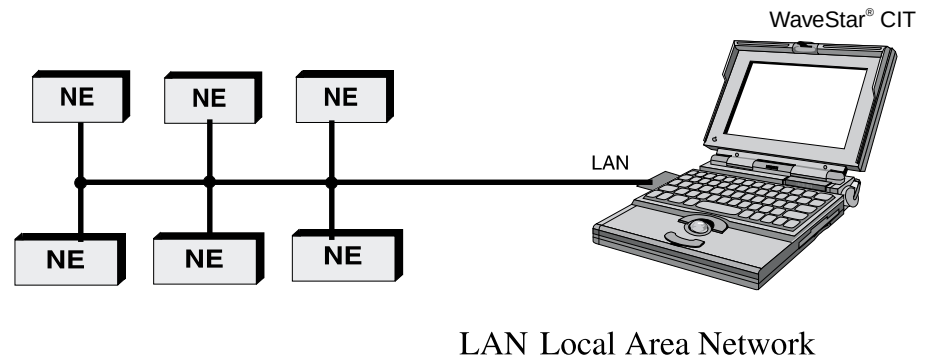
The following figure illustrates the Direct LAN Access (Point-to-Point).



WaveStar CIT LAN access (network)

WaveStar CIT access to more than one NE, e.g. within one site, can be done via a Local Area Network (LAN). The LAN is connected to the NEs by means of 10-BaseT Ethernet interfaces on 4-wire RJ-45 connectors.

The following figure illustrates the WaveStar CIT LAN Access (Network).

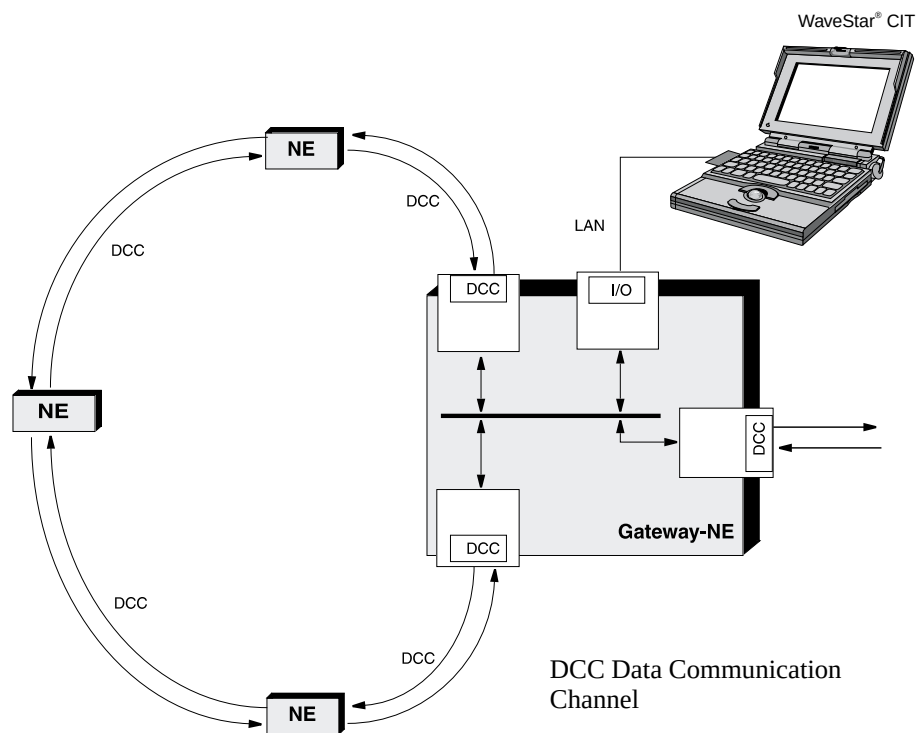


Important! The usage of *shielded* 10BaseT LAN cables is only allowed if the applicable national safety requirements have been met by the user. Otherwise, there is a *risk of electrical shock and/or serious injury*.

**WaveStar CIT access via
Data Communications
Channel (DCC)**

WaveStar CIT access to remote NEs can easily be done via the Data Communications Channel (DCC) which are part of the SDH aggregate or tributary signals. The CIT is connected via a point-to-point connection to one NE of the network (cf. "Direct Access"), which is then called the Gateway NE. All other NEs can be reached by the DCC. Thus, no additional management network is needed to connect the CIT to each individual NE.

The following figure shows an example of the access via the Data Communications Channel.



More Information Information on how to set up the Data Communications Network (DCN) are given in Chapter 14, “Management communication setup concepts” and “Configuring the data communication network (high level)” (3-6).

□

WaveStar® CIT login/logout procedure

Purpose Many procedures throughout this document require the user to log into and log out of the *WaveStar* CIT GUI. The following procedure describes how this is accomplished. This procedure requires the *WaveStar* CIT to already be loaded on the PC and the PC connected to an NE.

Login procedure Complete the following steps to log into the *WaveStar* CIT GUI:

- 1 Start the *WaveStar* CIT software by double clicking on the *WaveStar* CIT icon.
-

2	IF ... it is the first <i>WaveStar</i> CIT installation on the respective PC, a previous <i>WaveStar</i> CIT version has already been installed on the respective PC,	THEN ... log into <i>WaveStar</i> CIT with User Id: "LUC01" or "LUC02" and Password: "LUC+01" or "LUC+02". log into <i>WaveStar</i> CIT with User Id: "LUC01" or "LUC02" and the last used Password .
-

- 3 Click **OK** to connect. *WaveStar* CIT will be "initializing views" for about 3 minutes. Click **OK** and read the legal notice.
-

4	IF ... it is the first <i>WaveStar</i> CIT session, it is not the first <i>WaveStar</i> CIT session,	THEN ... proceed to Step 5. Stop! End of Task.
-

- 5 In the *WaveStar* CIT Main Window, choose the option **Administration → Data Communications...**
-

- 6 Make sure that the **Auto-Learn NSAP** box is not checked.
-

-
- 7 After initial login, it is recommended to change the passwords for the Super user logins immediately and to set up the logins for the other users.

Reference:

Please refer to “Administering user logins” (2-3).

.....
E N D O F S T E P S
.....

Logout from WaveStar CIT Complete the following steps to log out from *WaveStar CIT*:
.....

- 1 In the *WaveStar CIT* main window, click **File** → **Exit**.

Result:

If there are still connections to NEs established from this CIT session, an alert window appears which shows the currently established connections.

.....

2	IF	THEN
	you are sure you want to exit	click Yes in the alert window.
	you do not want to exit,	press the No pushbutton.

.....
E N D O F S T E P S
.....



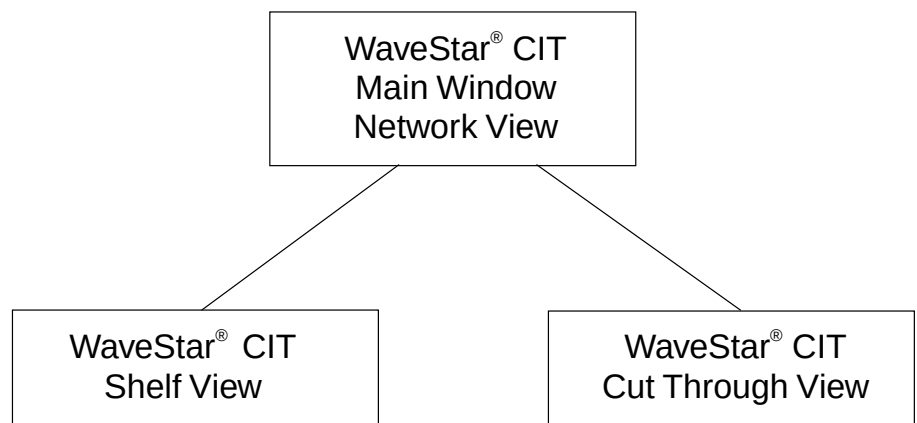
General WaveStar® CIT concept

Overview After login, *WaveStar* CIT comes up with the main window. This window allows you to perform general (NE independent) actions, e.g. administrative tasks, setting of preferences and options, etc. Furthermore, the main window serves as an entry screen for the log into the individual network element.

Interaction with network elements *WaveStar* CIT provides two possibilities to interact with a network element:

- *WaveStar* CIT System View: This is the shelf view of the network element.
- *WaveStar* CIT Cut-Through: here, you can execute TL1 commands on a one-at-a-time basis or in a series/script.

The following figure illustrates the general *WaveStar* CIT concept.



The structure of this chapter follows the *WaveStar* CIT concept.

□

WaveStar® CIT main window

Overview

- Purpose** This chapter provides information you should know before performing specific tasks, e.g.:
- how to log into and log out from network elements
 - the layout and the structure of the *WaveStar* CIT main window and its menus and sub-menus
 - the elements of the *WaveStar* CIT user interface
 - how to get help/information on items that are displayed on the *WaveStar* CIT main window
 - how to display the system defaults for a particular component.

Menu structure overviews Also, this chapter presents menu structure overviews of the *WaveStar* CIT application with references to the parts of this manual where the respective descriptions and tasks can be found.

Contents	
Elements of the <i>WaveStar</i> CIT user interface	22-15
Tool bar of the <i>WaveStar</i> CIT	22-17
Standard window components	22-19
Selection windows	22-24
General window handling	22-27
General pushbuttons	22-30
Basic operations	22-32
Network element selection and login	22-33
Overview of the menu structure	22-37
Logout from NE(s)	22-39

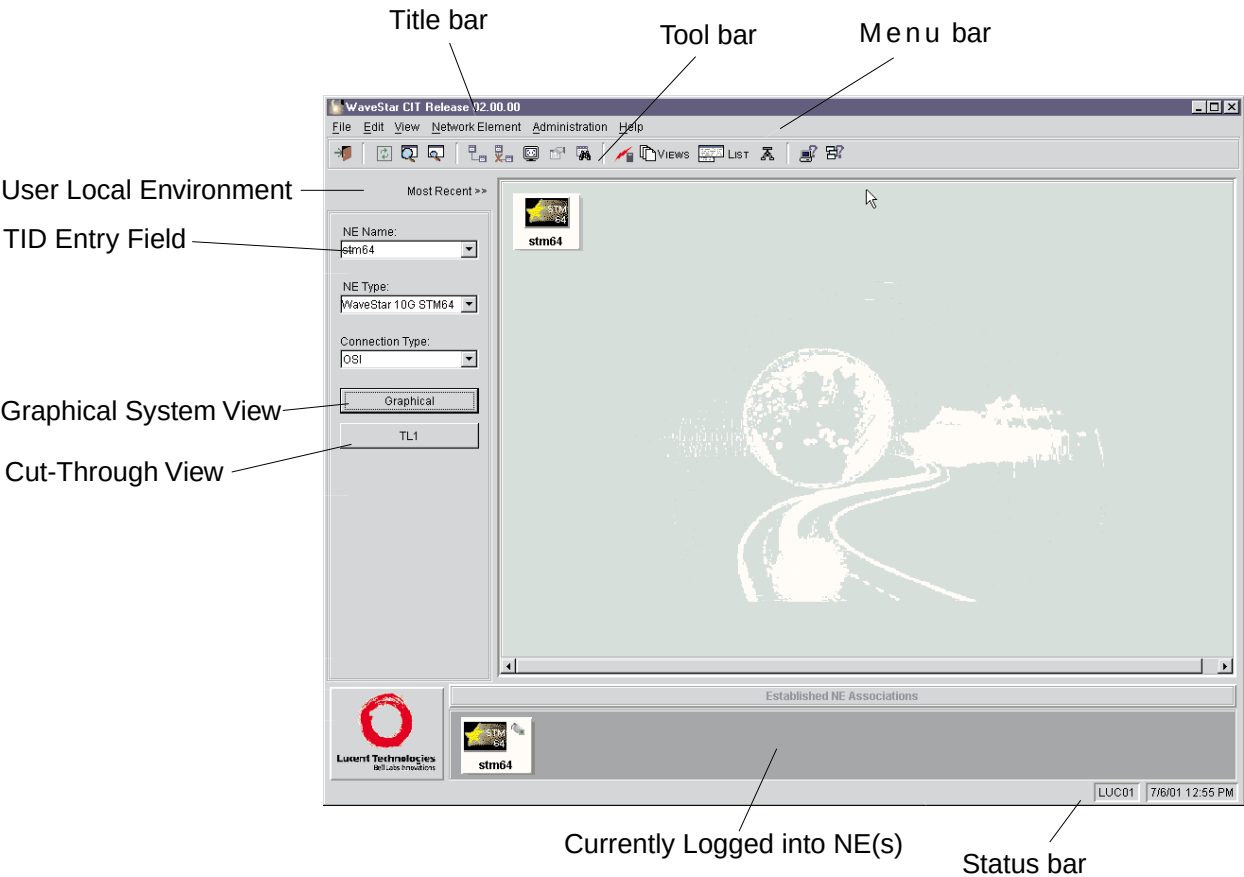


Elements of the WaveStar® CIT user interface

- Overview** The graphical user interface of *WaveStar* CIT consists of:
- The main window for accessing all functions of *WaveStar* CIT
 - *WaveStar* CIT System View window
 - *WaveStar* CIT Cut-Through window
 - Input and output windows for displaying and entering data
 - Notification windows that are displayed to inform you, for example, about the termination of a function or to have entries confirmed.

- Elements of the main window** The main window contains the following window bars:
- The title bar: shows the *WaveStar* CIT version.
 - The menu bar: contains the main menu of *WaveStar* CIT.
 - The status bar: displays information relevant in the current situation:
 - NE type, TID and, if available NE comment.
 - ID of currently logged in user
 - computer time settings, correlated to the local time
 - The tool bar: provides push-button access to common menu options.

The following figure illustrates the WaveStar CIT main window.



Tool bar of the WaveStar® CIT

Overview The tool bar: provides push-button access to common menu options. The WaveStar CIT applications software supports tool-tips.

CIT toolbar The following figure shows the toolbar of the WaveStar CIT application and its push-buttons.



Functions of the toolbar icons

To determine the meaning of a particular toolbar icon, place the cursor over that icon, hold for two seconds, and its name/function will be displayed.

The following table describes the push-buttons of the WaveStar CIT toolbar.

No.	Meaning	Equivalent Menu
1	Exit CIT	File/Exit
2	Refresh Directory	View/Refresh View
3	Large icon view	View/Large Icons
4	Small icon view	View/Small Icons
5	Connect to NE	Network Element/Connect to NE
6	Disconnect from NE	Network Element/Disconnect from NE
7	Cut-Through view	Network Element/Cut Through
8	NE Properties (not accessible)	Network Element/Properties
9	Find	Network Element/Find
10	Prepare PCMCIA	Administration/Prepare PCMCIA Disks
11	Administer Views	Administration/Administer Views...

No.	Meaning	Equivalent Menu
12	Address list	Administration/Address List...
13	SONET Directory Service	Administration/SDS Administration
14	CIT About	Help/About WaveStar CIT
15	NE support	Help/Supported NEs

User-defined toolbar settings

You can decide whether you want to have the tool bar displayed in the main window. Select the **View** → **Preferences** menu item. In the **Preferences** window select the **Network View** tab where in the **Misc.** group box you can either check or uncheck the **Hide Toolbar** check box.

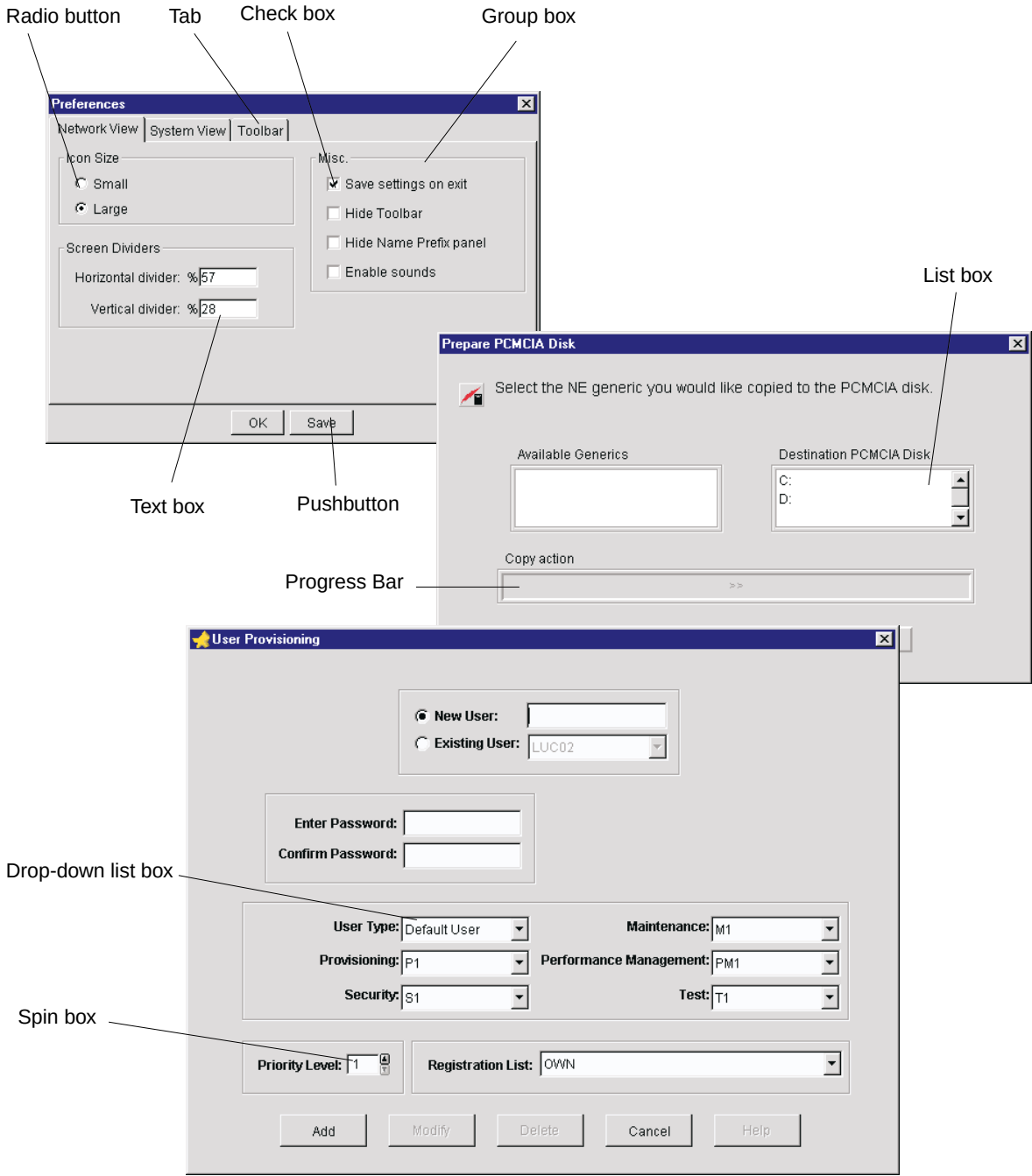
Moreover, the **Toolbar** tab in the **Preferences** window allows you to change the above described standard setting of the toolbar icons. Also, the toolbar can be re-arranged to another location on the screen by using the **ToolBar Location** group box.



Standard window components

Overview For the creation of input and output windows as well as the notification windows standard window components were used.

Diagram The following diagram illustrates the standard window components.

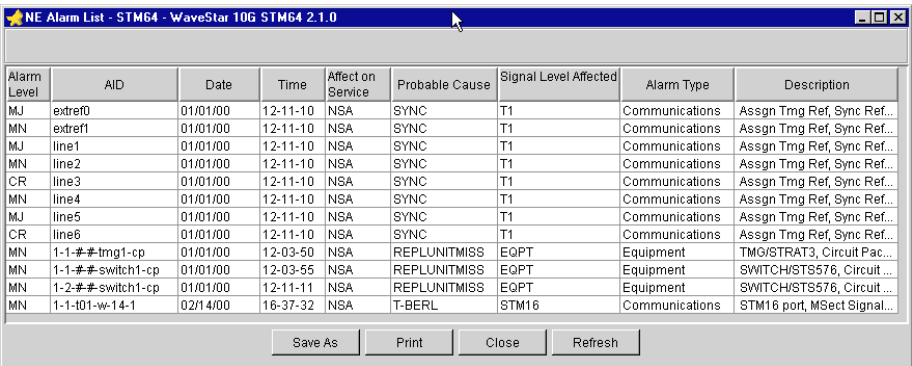


Functions of the window elements The functions of the window elements are as follows:

Window element	Function
Text box	A text box allows you to enter a text via the keyboard.
Information field	An information field is read-only. It only displays data.
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.
Radio button	A radio button functions as an on/off switch. If the radio button is pressed (on) the option next to it is selected. If it is not pressed (off), the option next to it has no meaning. Only one of the several radio buttons in a group box can be pressed at any one time.
Group box	A group box is used to indicate that a set of radio buttons or check buttons inside this box are logically related or to assign an additional title to the elements that are inside the group box.
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.
Pushbutton	The text of the pushbutton explains which function will be initiated when clicking on it. Pushbuttons like OK , Cancel and Apply are available in most of the windows. These general pushbuttons and their functions are explained below.
Check box	A check box functions as an on/off switch. If the check box is checked (on) the option next to it is selected. If it is not checked (off), the option next to it has no meaning. There is no limitation on how many check boxes in a group box can be pressed at the same time.
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.

Window element	Function
Tab	A window can contain several tabs. Clicking on a tab displays the corresponding contents in the window.
Progress Bar	A progress bar shows the percentage of completion of a lengthy operation, e.g. when loading software.
Table	The table element is often used for reports, alarm lists, etc. The table element provides you with several possibilities to configure the contained data according to your individual needs: • re-sizing of columns This is done by positioning the cursor on the right border of the column heading cell, pressing the left mouse button and dragging the cell border to the desired position. • re-arrangement of the columns This is done by positioning the cursor on the column heading cell, pressing the left mouse button and dragging the cell to the desired position. • sorting of the whole table depending on the selected column This is done by left-clicking on the respective column heading cell. The sort order depends on the column contents. For example, alarm descriptions will be sorted alphabetically (a...z), time and date will be sorted chronologically, alarm severity will be sorted in the order “critical”, “major”, “minor”, “not alarmed”.

Example: Table element: The following figure shows an example for the table element: The **NE Alarm List** window.



The screenshot shows a window titled "NE Alarm List - STM64 - WaveStar 10G STM64 2.1.0". It contains a table with the following data:

Alarm Level	AID	Date	Time	Affect on Service	Probable Cause	Signal Level Affected	Alarm Type	Description
MJ	extref0	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	extref1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MJ	line1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	line2	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
CR	line3	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	line4	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MJ	line5	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
CR	line6	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Ref...
MN	1-1-##-tmg1-cp	01/01/00	12-03-50	NSA	REPLUNITMISS	EQPT	Equipment	TMG/STRAT3, Circuit Pac...
MN	1-1-##-switch1-cp	01/01/00	12-03-55	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit ...
MN	1-2-##-switch1-cp	01/01/00	12-11-11	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit ...
MN	1-1-t01-w-14-1	02/14/00	16-37-32	NSA	T-BERL	STM16	Communications	STM16 port, MSect Signal...

At the bottom of the window are four buttons: "Save As", "Print", "Close", and "Refresh".



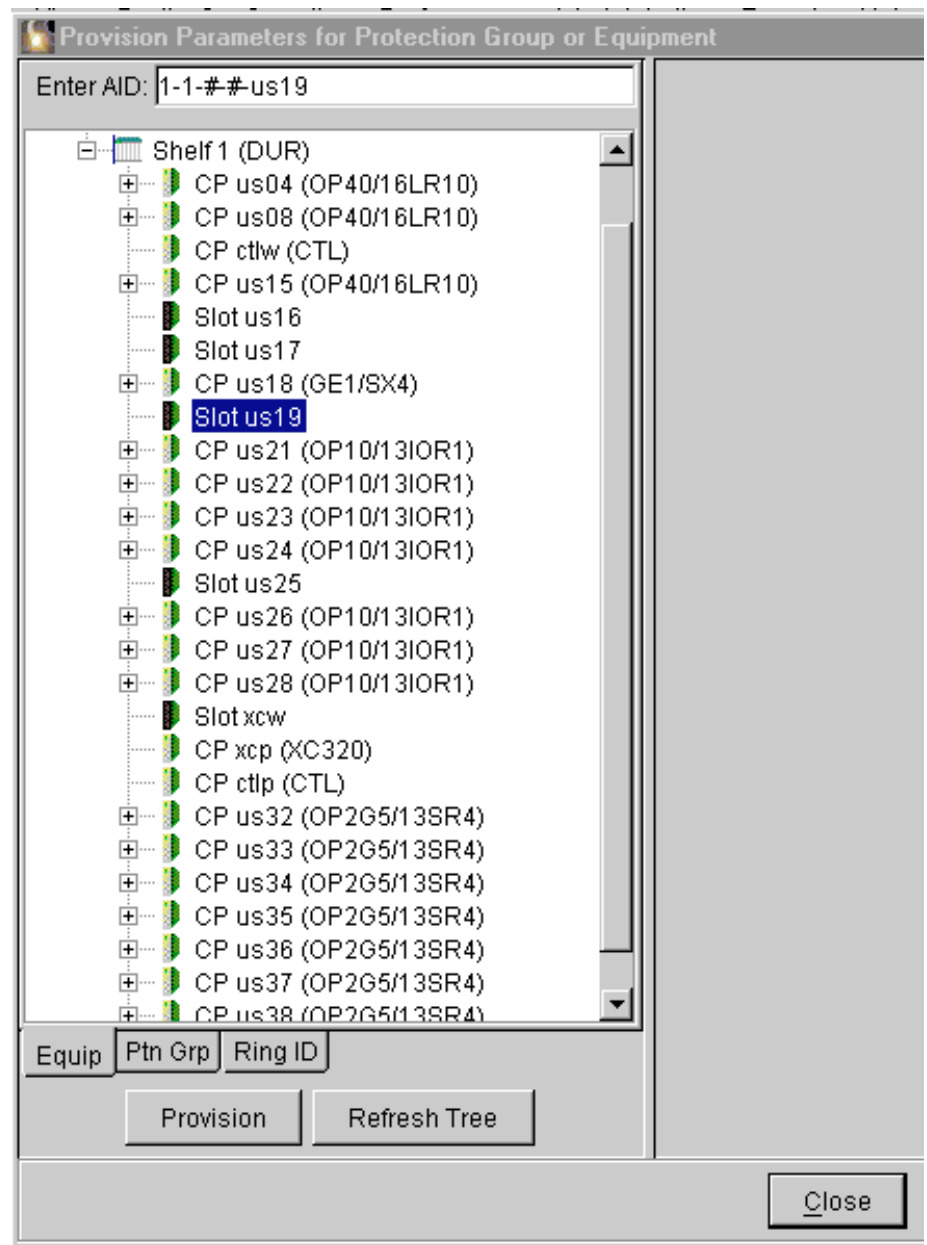
Selection windows

Overview The selection windows enable you to select any AID, or in the case of the Ring ID selection screen, any ring, defined for the system. Upon initial invocation, the user is presented with a hierarchical equipment view of the system appears. But there are also other selection views such as a protection group view which can be accessed through tabs on the screen.

Tabs The tabs appear in the following order:

- Equipment
- Protection Group
- Ring IDs.

Window layout The following figure shows an example of a selection window.



Specifying a component, a signal, etc.

There are two methods to specify/identify a particular component (bay, shelf, slot, circuit pack, port, etc.), signal, termination point, ring ID or protection group:

- by clicking through the directory tree
- by specifying the AID directly (for an overview of all applicable AIDs see “Overview of access identifiers” (15-8)).

Directory tree

You can make multiple selections browsing through the directory tree until finally selecting the desired item. The network element components are organised in a tree structure from the system level down to the tributaries. Components of a lower level become visible by clicking on the “+” in front of a higher-level component.

Enter AID directly

If you know the AID of the circuit pack and the signal identification - then you can enter it directly into the field labeled “Enter AID:”. And, as you make each selection the directory tree will highlight that entry.

Select or Provision button

It depends on the outer window type which selection in a selection window is valid and which is invalid. A valid selection can be recognized by means of the **Select** or **Provision** pushbutton at the bottom of the selection window. If a selection in the directory tree or in the **Enter AID** field is valid, the pushbutton is active and can be pressed. If a selection is invalid, the button is inactive.

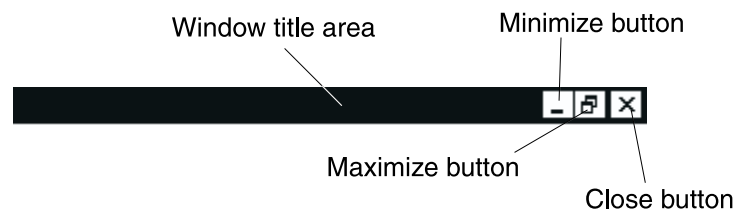


General window handling

Title bar Each input and output window and the main window of *WaveStar®* CIT contain a title bar consisting of

- the window title,
- the minimize pushbutton (in the following minimize button),
- the maximize pushbutton (in the following maximize button)
- and the close pushbutton (in the following close button).

The following figure illustrates the title bar.



Minimizing a window and opening a minimized window

To minimize a window and to open a minimized window proceed as follows:

IF

you want to minimize a window,

THEN

click with the left button of the mouse on the minimize button in the upper right corner of the window.

Result:

After minimizing a window, the window will appear on the WindowsNT task bar.

you want to open a minimized window,

click with the left button of the mouse on the minimized window on the task bar to open it again.

Maximizing a window

To maximize a window proceed as follows:

- 1 Click with the left button of the mouse on the maximize button in the upper right corner of the window.

Result:

After maximizing, the “square” in the maximize button becomes “two little squares”.

You cannot move or resize a maximized window.

-
- 2 Click with the left button of the mouse on the maximize button with the “two little squares” in the right corner of the window.

You may also double-click with the left button of the mouse on the window title area to maximize a window or to get the normal size of the window.

.....
E N D O F S T E P S
.....

Closing a window To close a window proceed as follows:

-
- 1 Click with the left button of the mouse on the close button in the upper right corner of the window to close the window.

Result:

Closing the main window will exit the *WaveStar* CIT application.

.....
E N D O F S T E P S
.....

Moving a window To move a window proceed as follows:

-
- 1 Press the left button of the mouse on the window title area.
 - 2 Keep the left button of the mouse pressed and move the window to the place you wish on the screen.
 - 3 Release the left button of the mouse to place the window.

.....
E N D O F S T E P S
.....

Resizing a window

To resize a window proceed as follows:

- 1 Move the mouse pointer to the border of the window.

Result:

The cursor changes from its default shape to a line with arrows.
The arrows indicate in which direction you can move the window border.

- 2 Press the left button of the mouse.

- 3 Drag the window border to the new size.

- 4 Release the left button of the mouse.

Result:

The window is now changed to the new size.

END OF STEPS



General pushbuttons

Overview In the following some general pushbuttons are explained. They are part of many windows of the WaveStar® CIT graphical user interface. Whenever they appear they have the same function and lead to the same reaction.

Description of general pushbuttons The following table describes the functions of the general pushbuttons.

Designation	Function
Apply	The Apply pushbutton allows you to commit changes in a dialog without closing the dialog. This control is useful in situations where a number of separate edit operations are to be invoked. It ensures that you do not have to keep invoking the edit window for each operation. An example is where you have to provision a number of cross connections separately. No changes are applied to a network element until the Apply or OK pushbutton has been selected.
Cancel	The Cancel pushbutton discards any changes to values in fields within an edit dialog and closes the dialog.
Close	The Close pushbutton closes an information-only window.
OK	The OK pushbutton commits any changes made within a window (if editable) and closes the window.
Refresh	If a window has been open for a while, the data displayed may no longer be up-to-date. The Refresh pushbutton allows you to obtain the most recent information.
Save As	Selecting the Save As pushbutton prompts you for a file name where WaveStar CIT shall store all data retrieved for the current window in ASCII format. The data stored includes visible data and data that is invisible on the screen such as data accessible via a scroll bar.

Designation	Function
Print	The Print pushbutton, e.g. in a report window, allows you to send the contents of the report, i.e. the data visible on the screen as well as data that is invisible such as data accessible via a scroll bar, to the printer.



Basic operations

Overview This section provides hints on several basic operations you can perform using the menus of the *WaveStar*® CIT main window:

- Setting preferences
- Requesting version information
- Viewing the list of supported NE types

Setting preferences The **View-Preferences** menu item provides several possibilities to configure the *WaveStar* CIT to your individual needs:

- **Tab Network View:**
 - specify the size of the icons which represent the network elements in the main window. If a large amount of NEs is to be shown, it is advantageous to choose **Small**.
 - re-configure the **Screen Dividers** between “User Local Environment” and SDS Listing (**Horizontal Divider**) field and the **Vertical Divider** in the main screen
 - some miscellaneous settings, e.g. hide toolbar, enable sounds.
- **Tab Toolbar:**

allows you to change the above described standard setting of the toolbar icons. Also, the toolbar can be re-arranged to another location on the screen by using the **ToolBar Location** group box.

The settings made in this window are retained for the respective user also after logging out.

Requesting version information To request the version information on *WaveStar* CIT select **Help About WaveStar CIT** in the main menu. The Release and Subrelease number is displayed.

Supported NE types The *WaveStar* CIT application software may function with different types of NEs (for example, *WaveStar* Bandwidth Manager, *WaveStar* 2.5G, *WaveStar* TDM 10G and so forth). The full list of supported NE types can be viewed from the *WaveStar* CIT view screen by selecting **Help Supported NE(s)**.

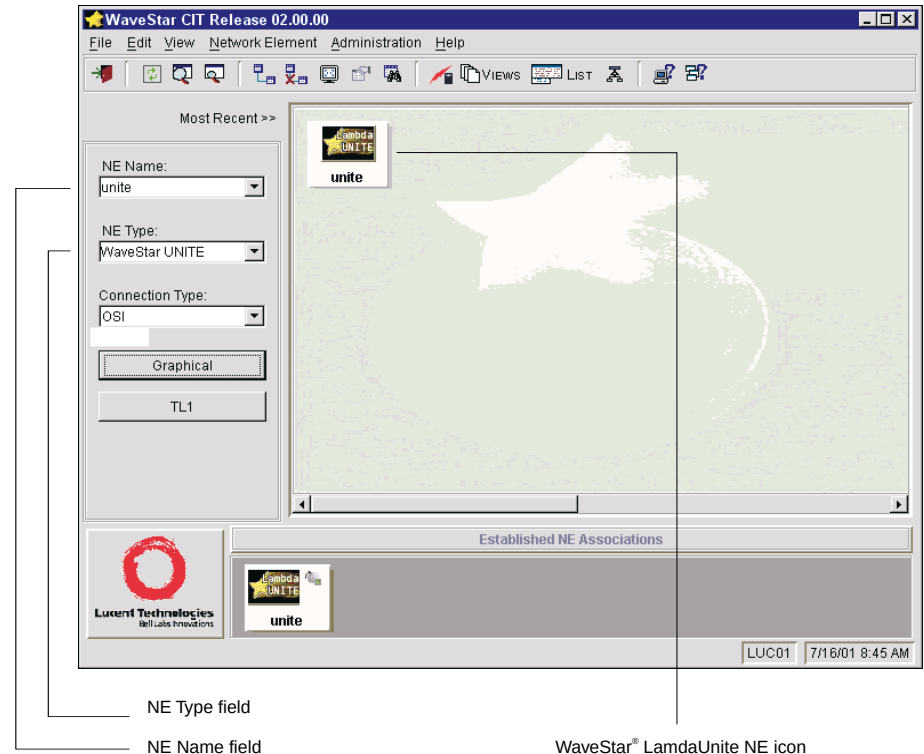


Network element selection and login

NE selection possibilities

Setting up an association to an NE is facilitated by the NE selection possibilities in the *WaveStar®* CIT main window. You can

- select the NE by specifying its NE Name
- select the NE via the “Graphical System View”.



Before you begin

A prerequisite for logging into a network element is to have *WaveStar* CIT connected physically to the desired network element for a local login. For a remote login, connect the *WaveStar* CIT to any network element that is part of the sub-network containing the remote NE.

When you log into an NE for the first time, you have to select the NE by specifying a NE Name. You can also use this method for other logins.

Important! If an initial load to the non-volatile memory (NVM) of a newly established network element has been performed, the NE comes up with a standard name or Target Identifier (TID). This name is LUCENT-UNITE-NE for all NEs. The first action that should be done

is to change the TID. To be able to work in a network properly, each NE has to be given its unique TID. Please refer to “Changing the NE name (TID)” (3-3) for changing the TID.

Logging into an NE In order to log into the NE, proceed as follows:

- 1 In the *WaveStar* CIT main window, enter the target identifier (TID) of the NE you wish to connect to in the **NE Name** box.

- 2 Select used **NE Type** and the preferred **Connection Type** and click **Graphical**.

Result:

The *WaveStar* CIT password is now being used for a login attempt to the NE.

- 3 If this password is accepted, no extra login window for the NE will appear. In this case, continue with Step 6.

- 4 Log in with your User Id and Password for the NE. For initial login after having the software installed the pre-installed Super-user logins “LUC01” and “LUC02” are used. The associated passwords are “UNITE+01” and “UNITE+02”.

- 5 Click **OK** to connect.

- 6 Click **OK** to the legal notice.

Result:

The **System View** window appears for the selected NE.

- 7 After initial login, it is recommended to change the passwords for the Super-user logins immediately and to set up the logins for the other users.

Reference:

Please refer to “Changing user passwords” (2-22) and
“Changing super user ids” (2-19).

END OF STEPS

**Selecting and displaying
an NE from the “Graphical
System View”**

If the *WaveStar* CIT has previously been used to display a system view for one or more NEs, then there exists a history of that event and the “User Local Environment” can be used to refer/select the previously displayed NEs.

- 1 In the connection type pull down menu, select **Most Recent**.

Result:

The previously displayed NEs are shown in the area on the right of the window.

- 2 Double-click on the NE icon to establish the connection to the respective NE.

END OF STEPS

Saving NE views

Besides the **Most Recent** view, you have the possibility to save each individual NE view, i.e. the icons shown in the area on the right of the window.

- 1 Select from the menu bar **Administration → Administer Views...** (alternatively press the right mouse button in the “User Local Environment” area and select **Save View As...**).

- 2 Specify a name for the new view.

Result:

This name is now shown in the “User Local Environment” area under the **Saved Views** directory and will be retained also when logging out from the *WaveStar* CIT.

END OF STEPS

Administer NE views The NE views can be administered by using the **Administration** menu in the menu bar.

IF	THEN
you want to add a NE view,	select from the menu bar: Administration → Administer Views... → Add (alternatively click on the icon Administer Views of the toolbar and then Add).
you want to modify a NE view,	select from the menu bar: Administration → Administer Views... → Modify .(alternatively click on the icon Administer Views of the toolbar and then Modify).
you want to delete a NE view,	select from the menu bar: Administration → Administer Views... → Delete .(alternatively click on the icon Administer Views of the toolbar and then Delete).

Editing the appearance of the icons The appearance of the NE icons in the area on the right of the window can be tailored to your individual needs.

IF	THEN
you want to change the display from large icons to small icons and vice versa,	select from the menu bar: View → Small Icons ; View → Large Icons .
you want to sort and arrange the icons by TID,	select from the menu bar: View → Arrange Icons → by NE Name .
you want to sort and arrange the icons by Type,	select from the menu bar: View → Arrange Icons → by Type .
you want to read the directory database and update the view,	select from the menu bar: View → Refresh OSI View .



Overview of the menu structure

The following table gives an overview where you can find the related description of the WaveStar® CIT main window menu structure.

Menu function	Submenu	refer to
File	Save Settings	“Network element selection and login” (22-33)
	Login as New User...	“Administering user logins” (2-3)
	Exit	“WaveStar CIT login/logout procedure” (22-11)
Edit	Copy Icon(s) to...	“Network element selection and login” (22-33)
View	Refresh OSI View	“Network element selection and login” (22-33)
	Large Icons	
	Small Icons	
	Arrange Icons	by TID
		by Type
	Preferences...	“Basic operations” (22-32)
Network Element	Graphical...	“Network element selection and login” (22-33)
	TL1...	“Entering the Cut Through view” (22-64)
	Disconnect from NE... (only accessible if connection to NE already established)	“Logout from NE(s)” (22-39)
	Disconnect from All NEs (only accessible if connection to NE already established)	
	Find...	“Network element selection and login” (22-33)
	Properties... (only accessible if connection to NE already established)	

Menu function	Submenu	refer to	
Administration	View CIT Administration...	“DCN protocols and services” (14-16) “NSAP address format” (14-19)	
	Change Password...	“Changing user passwords” (2-22)	
	Security	View User Logins...	“Displaying a list of all users logged into an NE” (2-36)
		User Provisioning...	“The WaveStar CIT User Provisioning window” (2-17)
		Change Superuser Login ID	“Changing super user ids on the WaveStar CIT” (2-20)
	Prepare PCMCIA Disks...		“Performing an initial software download using the CIT” (10-2)
	Data Communications...		“Configuring the data communication network (high level)” (3-6)
	Serial COM Selection		
	Address List...		“Administering the address list at the WaveStar CIT” (3-18)
	Administer Views...		“Network element selection and login” (22-33)
	Defaults...		
	SDS Administration...		
	(not accessible)		
Help	About WaveStar CIT...	“Basic operations” (22-32)	
	Help Contents, Index & Find...		
	(not accessible)		
	Supported NEs...	“Basic operations” (22-32)	
View Documents			
(not accessible)			



Logout from NE(s)

Procedure You have several possibilities to disconnect from an NE. Complete the following steps to disconnect from NE(s) using the WaveStar® CIT GUI:

- 1 Determine if you want to exit WaveStar CIT completely or if you want to disconnect from NE(s)
-

2	IF	THEN
	you want to exit WaveStar CIT completely,	in the WaveStar CIT Main window click File → Exit , then Yes in the confirmation window.
	you want to close all connections to all existing NEs,	in the WaveStar CIT Main window click Network Element → Disconnect from All NEs .
	you want to disconnect from single NE(s),	continue with Step 3.

3	If you want to disconnect from NE(s) in the	then
	System View for the NE	click File → NE Disconnect , then Yes in the confirmation window.
	WaveStar CIT Main window,	continue with Step 4.

- 4 Choose the menu option **Network Element** → **Disconnect from NE....**

Result:

The **NE Disconnect List** window appears.

- 5 Select the NE you want to disconnect from in the list.
-

6 Press the **Disconnect** pushbutton.

E N D O F S T E P S



System view

Overview

Purpose This section provides information about the layout and the structure of the WaveStar® CIT **System View** window and its menus and submenus.

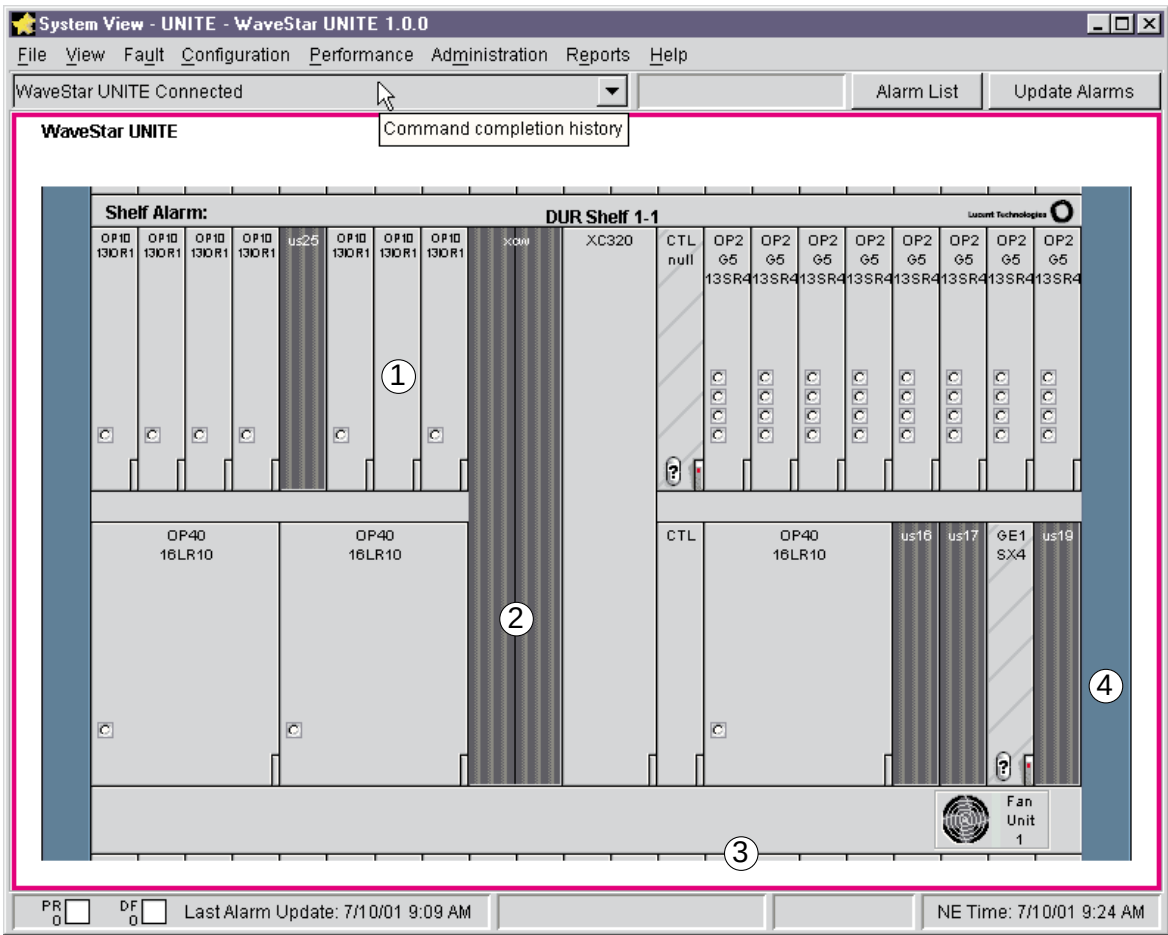
Contents

Shelf view	<u>22-42</u>
The ring map	<u>22-52</u>
Overview of the shelf-view menu structure	<u>22-54</u>
Reports	<u>22-61</u>
View rolling events	<u>22-62</u>



Shelf view

The shelf map The following figure illustrates the navigation through the graphical shelf view:



- ① View CP Details
mouse click right:

View Details
Provision Circuit Pack
Exchange Circuit Pack
Delete Circuit Pack
View Protection
Protection Switch
Refresh Circuit Pack
- ② View Slot Details
mouse click right:

View Details
Create New Circuit Pack
Delete Circuit Pack
Provision Slot
Refresh Slot
- ③ View Port Details
mouse click right:

View Details
Tributary Details
Provision Port #
View PM Port Parameters
Provision PM Parameters
View Protection
Protection Switch
View Cross Connections
Refresh Port #
- ④ View Shelf Details
mouse click right:

View Details
Provision Shelf
Refresh Shelf

The shelf map, a graphical representation of the selected shelf, displays the following:

- The top left corner displays the type of the shelf (Unite)
- Circuit pack slot positions are depicted
- Empty slots which have not been provisioned are depicted with a dark grey color
- Empty slots which have already been provisioned (or pre-provisioned) are depicted with a light grey color with dark grey diagonal stripes. The latch mechanism, which is located in the lower right-hand corner of the slot, is also depicted as being open.
- Equipped slots are shown with the label of the occupying circuit pack
- You can hold the cursor on a slot for 2 seconds to display a more detailed label (that is, Pack ctlw (CTL), Fan Unit 1, and so forth.)
- A double-click on an **equipped** slot brings up the **View Equipment Details** window for the individual circuit pack in this slot (e.g. for TMG/STRAT3 circuit pack, cf. “View Circuit Pack Details window” (22-46)).
- A double-click on an **unequipped** slot brings up the **View Equipment Details** window for this slot. This window shows which circuit packs are allowed for this individual slot and gives status information (cf. “View Slot Details window” (22-47)).
- A right-click on an **equipped** slot brings up the pop-up menu which provides several menu options shown in “View Circuit Pack Details window” (22-46), designation “1”.
- A right-click on an **unequipped** slot brings up the pop-up menu which provides several menu options shown in “The shelf map” (22-42), designation “2”.
- Each port unit has a light-emitting diode (LED) associated with each port. Each LED displays the alarm status (for example, green = no alarm, red = critical alarm, yellow = major alarm, cyan = minor alarm) for the associated port. A double-click on a port LED brings up the **View Equipment Details** window for this individual port (e.g. for Optical Port, cf. “View Port Details window” (22-50)).

- A right-click on a port LED brings up a pop-up menu which provides several menu options shown in “View Port Details window” (22-50), designation “3”.
- A double-click on the shelf area (outside the slot area) brings up the **View Equipment Details** window for the complete shelf (e.g. for the high-speed part, cf. “View Port Details window” (22-50)).
- A right-click on the shelf area (outside the slot area) brings up a pop-up menu which provides several menu options shown in “The shelf map” (22-42), designation “4”.

Alarm list The NE alarms can be displayed by pressing the **Alarm List** pushbutton.

Update alarms In order to retrieve the latest alarms from the NE, the **Update Alarms** pushbutton can be used.

Command list The most recently executed command is displayed on a command line near the top of the **System View** screen. Place your cursor on the drop-down arrow for this command line. To display a list of the last attempted commands, both those that were executed successfully and unsuccessfully, left-click on the “drop-down” arrow.

**View Circuit Pack Details
window**

The following figures illustrates a **View Circuit Pack Details** window.

The screenshot shows a window titled "View Equipment Details" with a yellow star icon and a close button. It has two tabs: "Pack Data" (selected) and "Status". The window is divided into three main sections: "Circuit Pack Information", "Equipment Details", and "Alarms".

Circuit Pack Information

- Circuit Pack AID: 1-1-#-#-us08
- Circuit Pack Type: OP40/16LR10

Equipment Details

- Apparatus Code: -
- Series Number: -
- CLEI Code: -
- Equipment Carrier Code: -
- Serial Number: -

Alarms

- Alarm Level: Info
- Equipment Alarm Profile: DEFAULT

At the bottom, there are three buttons: "Save As", "Refresh", and "Close".



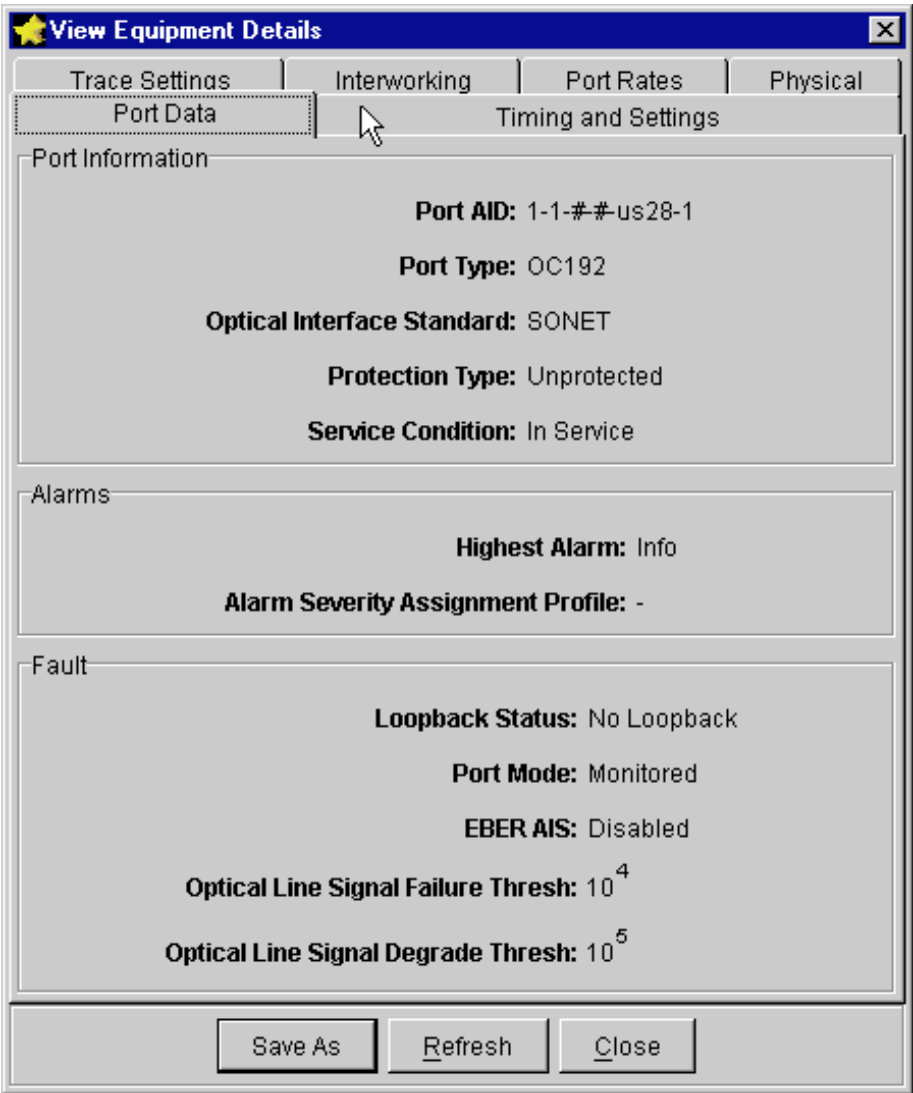
View Slot Details window The following figure illustrates the **View Slot Details** window.

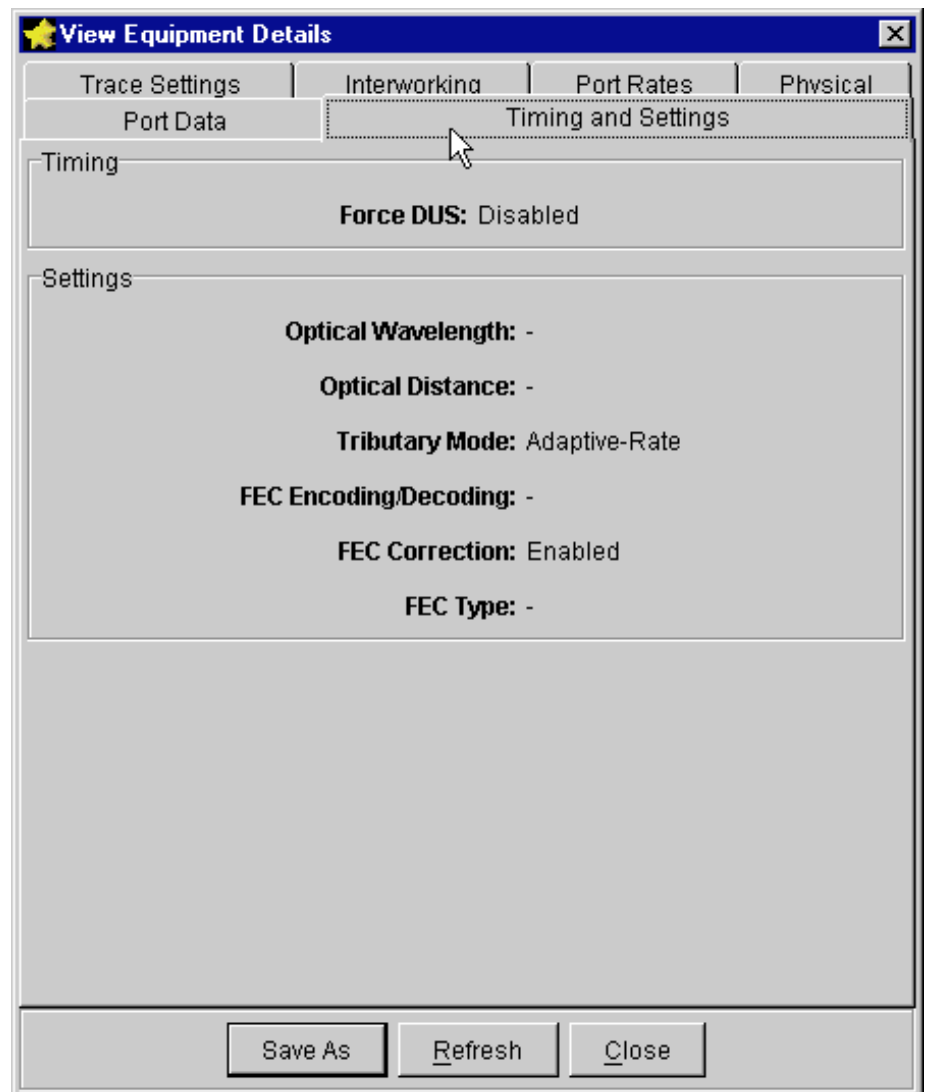
The screenshot shows a window titled "View Equipment Details" with a yellow star icon and a close button. The window is divided into four main sections: "Slot Information", "Equipment", "Status", and "Equipment Details".

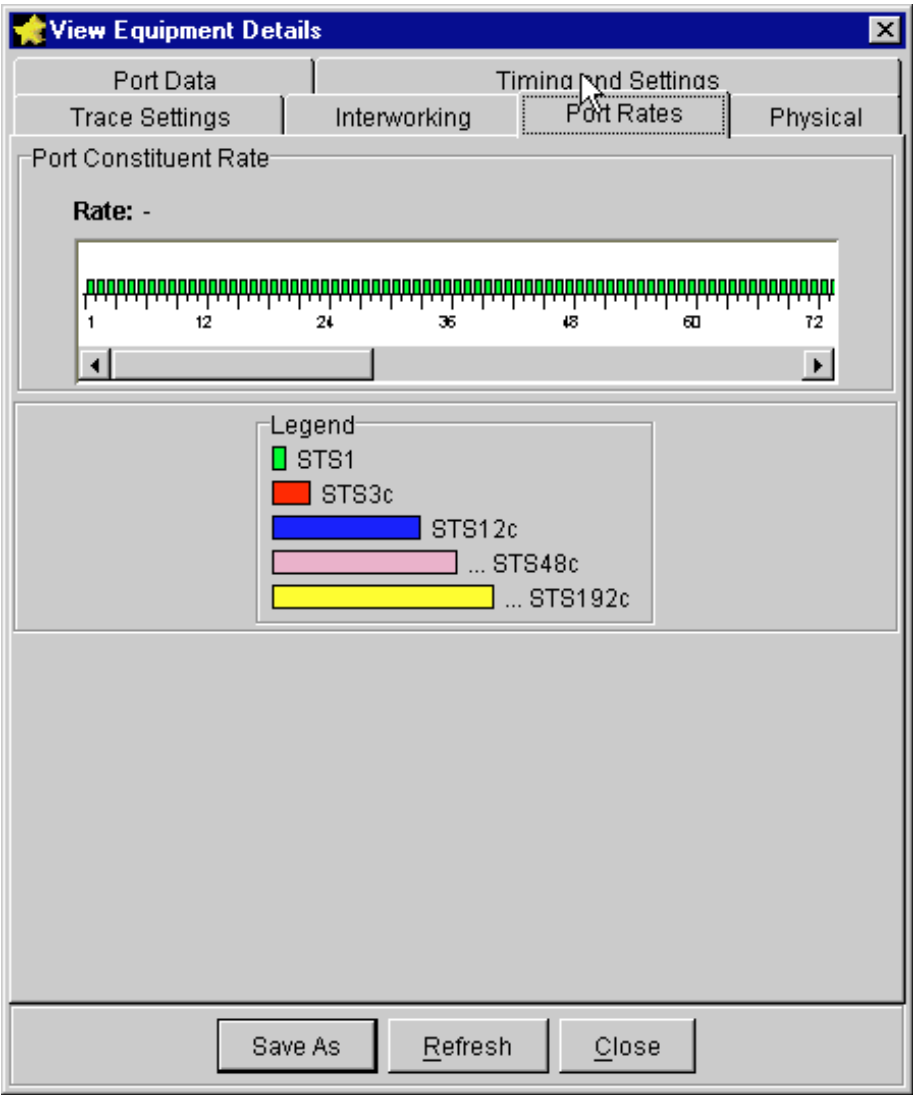
- Slot Information:** Displays "Slot AID: 1-1-##us25".
- Equipment:** Displays "Acceptable Pack Types:" with a list box containing "OP2G5/138R4" and "OP10/131OR1". Below this, it shows "Equipment ASAP Profile: DEFAULT".
- Status:** Displays "Alarm Level: Info" and "Slot Holder Status: Empty".
- Equipment Details:** Displays several fields, all with a value of "-":
 - Apparatus Code: -
 - Series Number: -
 - CLEI Code: -
 - Equipment Carrier Code: -
 - Serial Number: -

At the bottom of the window, there are three buttons: "Save As", "Refresh", and "Close".

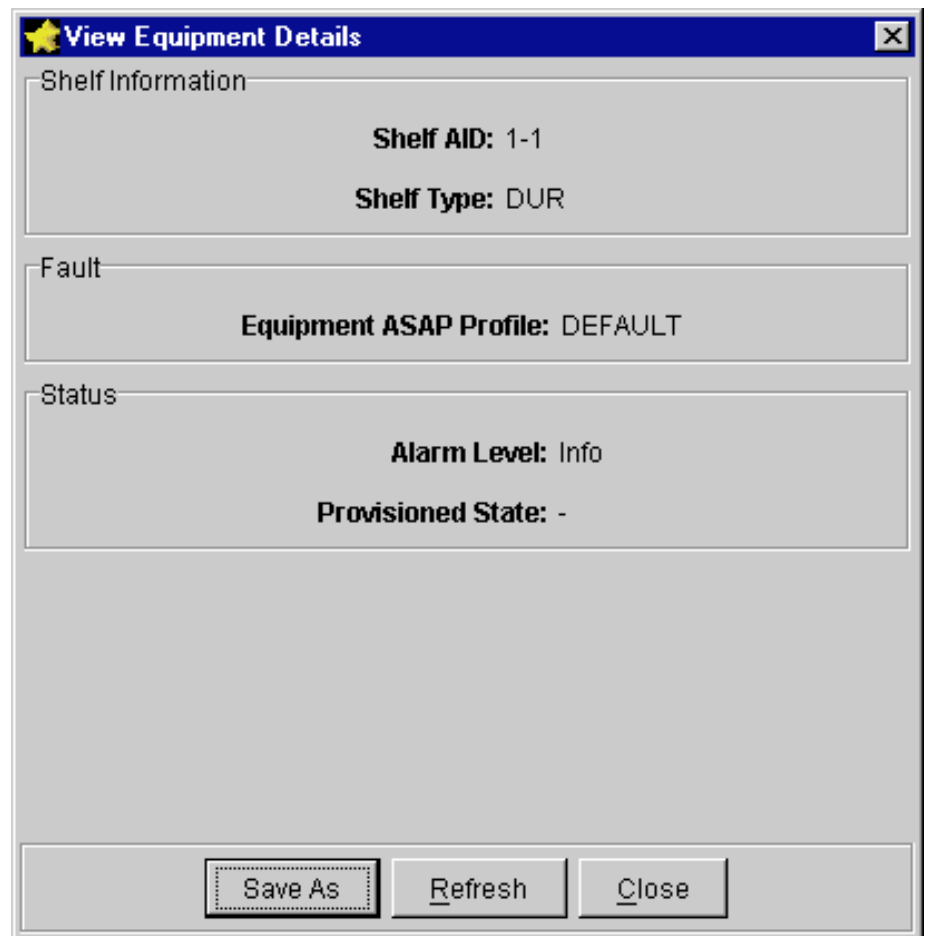
View Port Details window The following figures illustrate the **View Port Details** window.







View Shelf Details window The following figure illustrates the **View Shelf Details** window.



□

The ring map

Overview For MS-SPRing protected rings, WaveStar® CIT provides textual and graphical information on the ring configuration, the so-called ring map. Here, all the nodes in a selected ring are displayed.

How to get there In order to view a certain ring map, use the menu **View → Rings → Ring Map....** The **View Ring Map** window appears. The windows type explorer allows you to select a configured MS-SPRing. This can be done either via the **PTN Grp** (Protection Group) tab which shows the established MS-SPRing protection groups or via the **Ring ID** tab which identifies the rings by use of their 15 character ring identification.

Contents of the ring map After pressing the **Select** pushbutton, the ring map is shown in table format in the right window area and contains the following columns:

Column	Description/Behavior
Node NE Name	Up to 20 character Target Identifier (TID) of this Ring Node NE
Node Port	Port AID on this node. If this is an end node of an open ring, the field is left blank.
Node Port Direction	Values of E(ast) or W(est).
Node Neighbor NE Name	NE Name of the Neighbor NE. If this is an end node of an open ring, the field is left blank. Otherwise, up to 20 ASCII characters can be displayed.
Neighbor Port	Port AID on the Neighbor NE. If this is an end node of an open ring, the field is left blank.
Neighbor Port Direction	Values of E(ast) or W(est).
Node NE Title	First part of the NSAP Address for this Ring Node NE.
Node ID	Ring address of this Ring Node NE. May take the integer values 0 through 15, inclusive.

Graphical view The graphical view of the ring map is invoked by the **Display Ring Map Graph** pushbutton.

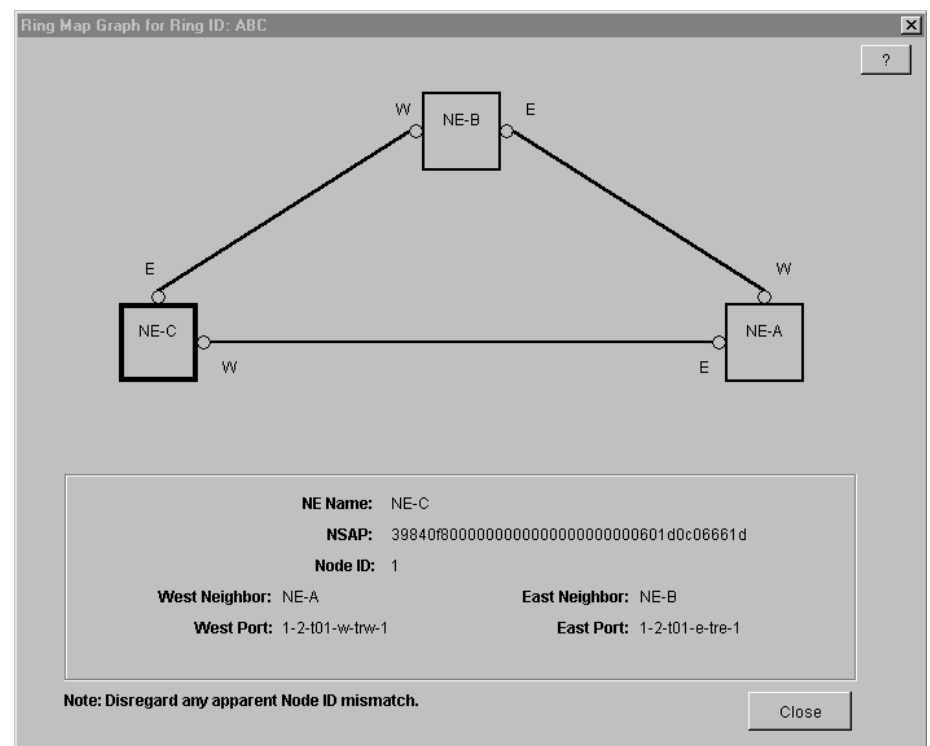
The individual NEs are shown as boxes with the NE name in them. The bottom part of the window shows the data of the currently selected NE. The currently selected NE is displayed as a bold box. You can select an NE by clicking on the respective NE box.

The data displayed at the bottom of the window for the selected NE are:

- NE Name
- NSAP Address of the NE
- Node ID
- Names of west and east neighbor NEs
- West and East NE Ports involved in the MS-SPRing

Graphical ring map display

The figure below is an example of how a ring map is graphically depicted.



Overview of the shelf-view menu structure

Menu structure overview The next figure gives an overview of the WaveStar® CIT system view or shelf view menu structure (after logging into a LambdaUnite™ MSS network element).

The following table gives an overview where you can find the related description of the WaveStar CIT system view or shelf view menu structure (after logging into a LambdaUnite MSS network element).

Menu function	Submenu	please refer to
File	Enable TL1 Logging ...	“Working with logs” (22-72)
	Disable TL1 Logging ...	
	Set/Change TL1 Logging File	
	NE Disconnect	“WaveStar CIT login/logout procedure” (22-11)

Menu function	Submenu	please refer to
View	Preferences	“Shelf view” (22-42)
	View Equipment Details...	
	View Rolling Events	“View rolling events” (22-62)
	Rings	“The ring map” (22-52)
	Protection...	“Protection mechanisms” (18-12)
	View Alarms	Chapter 5, “Alarm management”
	View Alarm Severity Assignment Profile...	
	View Alarm Configuration...	
	Cross Connections...	“Parameters of the window “View Cross Connections”” (7-5)
	Loopback...	Chapter 5, “Alarm management”
	DCC Terminations...	Chapter 14, “Management communication setup concepts”
	Misc. Discretes...	(not applicable for this release)
	Timing/Sync...	“Parameters of the “Synchronization Characteristics” window” (6-5)
	Software Generic...	Chapter 20, “Software upgrade concepts”
	NE Data...	Chapter 21, “Database backup concepts”
	Refresh Equipment...	“Shelf view” (22-42)
	Refresh System View...	

Menu function	Submenu	please refer to
Fault	NE Alarm List...	Chapter 5, "Alarm management"
	View Alarm Severity Assignment Profile	
	NE Alarm Log...	
	Protection Switch...	AMTCG (Alarm Messages and Trouble Clearing Guide)
	Enter/Exit Maintenance Condition...	Chapter 15, "Equipment provisioning concepts"
	Enter Maintenance Condition...	Chapter 5, "Alarm management"
	Exit Maintenance Condition...	
	Test	Chapter 5, "Alarm management"
	LED...	
	Analysis	AMTCG (Alarm Messages and Trouble Clearing Guide)
	Facility Loopback...	
	Facility Failure States...	
	Equipment Failure States...	
	View Current Optical Trib. Maintenance Signal...	
	View Current DS3 Maintenance Signal...	
	View Current VCG Tributary Maintenance Signal...	
	View Current VCG Tributary delays within VC group...	
Reset	Slot...	
	Controller Group... (not accessible)	
	System...	AMTCG (Alarm Messages and Trouble Clearing Guide)
Timing/Sync Protection Switch	Clock Mode Switch...	
	Switch Timing Reference Switch...	Chapter 17, "Timing provisioning concepts"
	Output Timing Reference Switch...	

Menu function		Submenu	please refer to
Configuration	Provision...		“WaveStar CIT methods to perform provisioning” (15-3)
	Create New	Circuit Pack...	“Provisioning of new components” (15-5)
		Protection Group...	
	Exchange Circuit Pack...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	(not accessible)		
	Delete...		“Provisioning of new components” (15-5)
	Misc. Discretes...		(not applicable for this release)
	DCC Terminations...		“Configuring data communication channels” (3-36)
	Cross-Connection...		“Cross-connection management” (18-2)
	Timing/Sync		Chapter 17, “Timing provisioning concepts”
	Alarms	Alarm Severity Assignment Profile...	Chapter 5, “Alarm management”
		Create NonReporting ASAPs...	
		Set NonReporting ASAPs...	
Software		Alarm Configuration...	
	Remote Backup...		Chapter 21, “Database backup concepts”
	Remote Restore...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	(not accessible)		
	Copy NVM...		
	(not accessible)		
	Download Software...		
	Activate Software...		Chapter 20, “Software upgrade concepts”
	FTP Browser...		

Menu function		Submenu	please refer to
Performance	View TCA Profile	SONET Section Line...	
		SDH Regenerator-Multiplex...	
		SDH HOVC Path...	
	Provision TCA Profile	Physical...	
		SONET Section Line...	
		(not accessible)	
		SONET Path...	
		(not accessible)	
		DS3...	
		(not accessible)	
		SDH Regenerator-Multiplex...	
		SDH HOVC Path...	
	Reports	SDH Regenerator Section...	
		SDH Multiplex Section...	
		SDH Path...	
		SDH UAT...	
		(not accessible)	
	Initialize Registers...		
	View PM Ports...		
	Provision Ports...		

Menu function	Submenu	please refer to
Administration	Change Password...	“Changing user passwords” (2-22)
	Change Notifications...	“Modifying a user’s own notification list” (2-28)
	Security	
	View User Logins...	“Displaying login information for an NE” (2-38)
	View Logged-In Users...	“Displaying a list of all users logged into an NE” (2-36)
	Disable User Login...	“Administering user logins” (2-3)
	Enable User Login...	
	Logout NE User...	“Logging out NE users” (2-15)
	User Provisioning...	“Administering user logins” (2-3)
	Security Provisioning...	“Provision global security parameters” (2-33)
	View NE Administration...	Chapter 3, “Management communication setup”
	View MAC Addresses...	“NSAP address fields” (14-20)
	Set TID...	“Changing the NE name (TID)” (3-3)
	Data Communications...	“Configuring the data communication network (high level)” (3-6)
	OSI Routing Map...	“OSI routing map and OSI neighbor map” (14-5)
	OSI Neighbor Map...	

Menu function		Submenu	please refer to
Reports	Equipment Lists	Pack/Backplane...	“Reports” (22-61)
		Shelf...	
		Pack...	
		Port...	
		VCG...	
	Status Lists	Trib...	
		Shelf...	
		Pack...	
		Port...	
		Trib...	
	Cross-Connection List...		
	NE Alarm List...		
	NE ALarm Log...		
	NE Protection Switch Activity Log...		
	(not accessible)		
	BLSR Protection Switch List...		
	NE User Log...		
	(not accessible)		
	NE Security Log...		
	NE Notification Log...		
	(not accessible)		
Help	About This Network Element...		“Basic operations” (22-32)
	Help		
	Library		
	Description		
	Support		



Reports

Overview WaveStar® CIT allows you to generate reports of the NE equipment configuration, switched cross-connections, alarm lists, etc. via the **Reports** menu item.

Report formats The reports are formatted as tables and can be saved to a specified file (ASCII format) and/or can be sent to a printer as well.

The following reports are provided on demand:

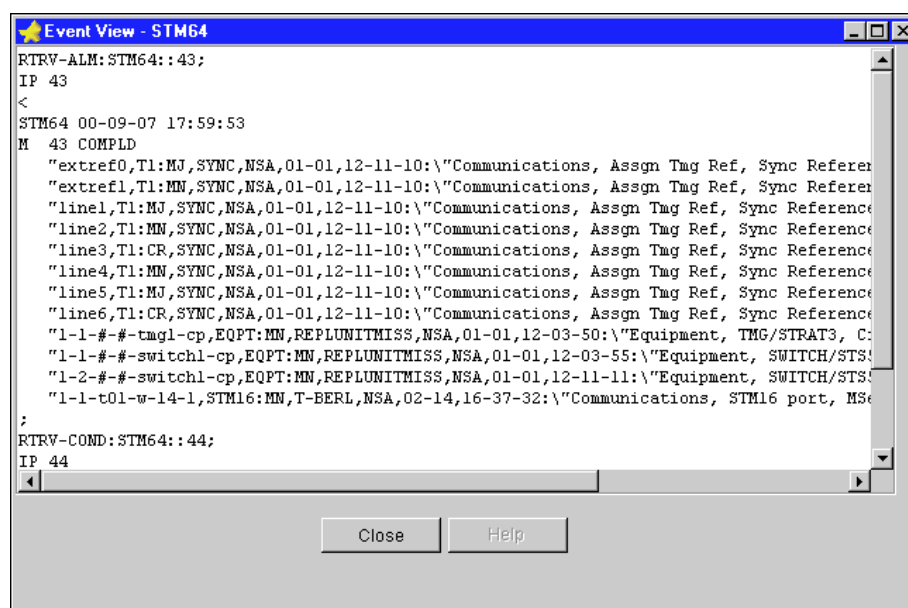
- Equipment lists for shelves, circuit packs or ports or tributaries
- Status lists for shelves, circuit packs, ports or tributaries
- Cross-connection list
- NE alarm list
- NE alarm log
- NE protection switch activity log
- MS-SPRing protection switch list

□

View rolling events

Overview There are some events (e.g. protection switch) which do not generate an alarm. Therefore it may be difficult for a user to determine whether such events occur. The “View rolling events” screen is intended to fill that void. The user can invoke it and leave it open, to see at an instant the latest received autonomous event notification.

The Event View window The **Event View** window can be invoked via **View → View Rolling Events** from the NE **Shelf View**.



Syntax The syntax of the events shown in this window is the TL1 syntax. For details about TL1, please refer to the *LambdaUnite™* MSS TL1 Reference Manual.

Log length The log is max. 256 lines long. As additional autonomous notifications are received in excess of 256, they are added to the screen at the bottom and the oldest entry (i.e., at the top) is removed.



Cut Through view

Overview

Purpose This section provides information about the layout and the structure of the Cut Through view window and its menus.

**Usage of the WaveStar®
CIT Cut Through window**

As an alternative to using the graphical-user-interface based System View, the *LambdaUnite™* MSS provides a Cut-Through to TL1 capability. With Cut-Through you can execute single TL1 commands or commands in a series/script.

Important! While in System View, the user is alerted with a warning message to inform them that if they follow through with their command it could be service impacting. As a contrast, Cut-Through mode does not provide any warning message and thus the user does not get a second opportunity to review/consider the consequences of their command.

TL1 commands For the detailed descriptions of each of the TL1 commands, please refer to the *LambdaUnite* MSS **TL1 Reference Manual**

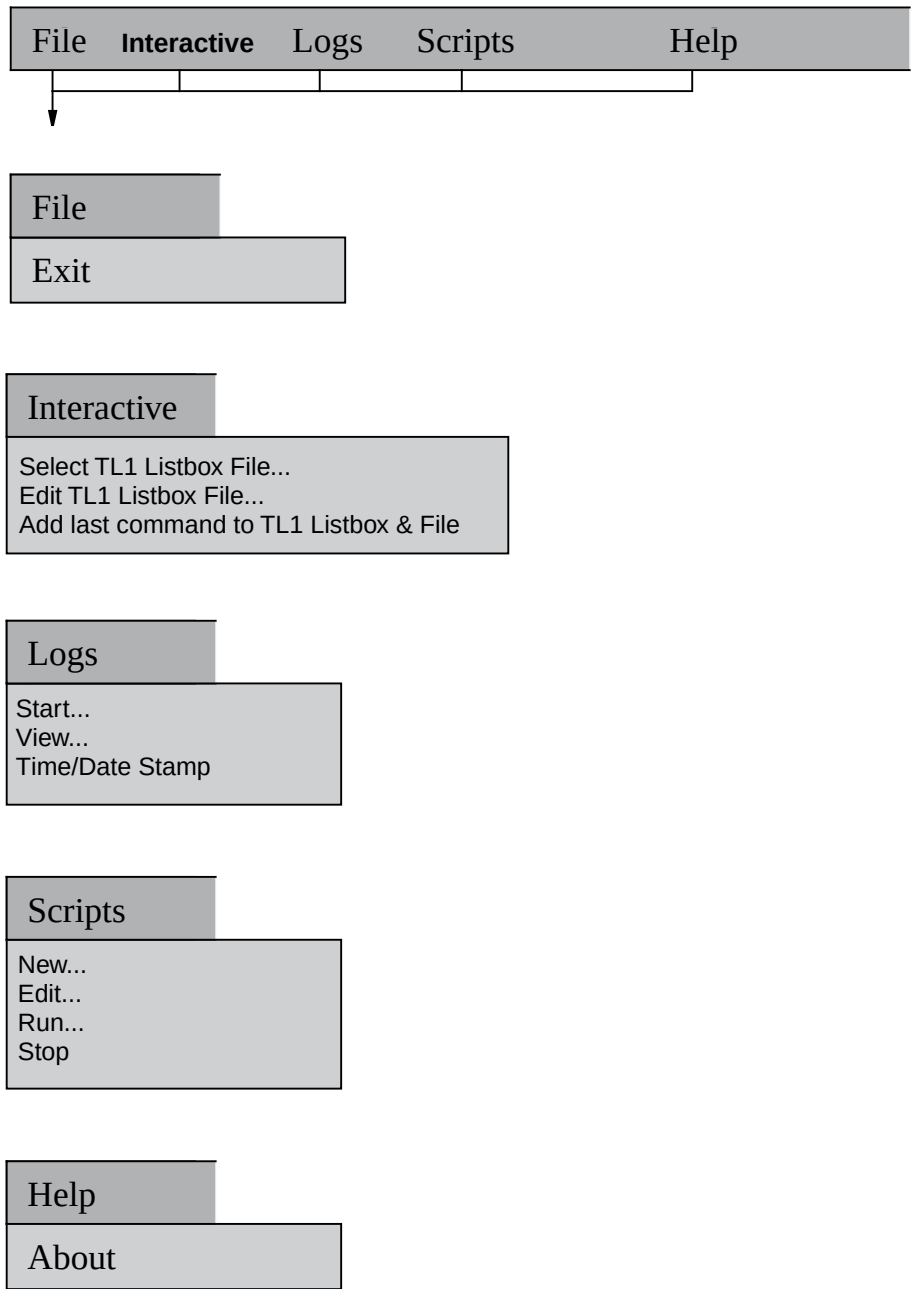
Contents

Entering the Cut Through view	22-64
Interactive – Execute TL1 single commands	22-67
Interactive – Manage a listbox file	22-69
Working with script files	22-70
Working with logs	22-72



Entering the Cut Through view

The following figure is a functional illustration of the **Cut Through** view menus.



Legend:

Interactive	see “Interactive – Manage a listbox file” (22-69)
Logs	see “Working with logs” (22-72)
Scripts	see “Working with script files” (22-70)
Help	see “Basic operations” (22-32)

Procedure For entering the Cut-Through view, proceed as follows:

- 1 In the WaveStar® CIT main window, enter the **NE Name** and select the **NE Type** and **Connection Type** of the NE for which you wish to establish a Cut-Through session.

- 2 Select (left-click) the **TL1** option.

Result:

The **Connection Type Selection** window appears.

You can select the following modes:

- **TL1PeerComm (TL1 Command Response Only):** by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.
- **TL1 Maintenance (TL1 Alarms, EventsCommand Responses):** by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.
- **TL1MemoryAdministration (TL1 Database Changes and Command):** by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.
- **TL1test (TL1 Test and Command):** by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.

- 3 Left-click on the **OK** button.

Result:

The **Select Cut-Through Execution Mode** window appears.

You can select the following modes:

- **Filter TL1 Commands/Replies:** by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.
- **Raw TL1 Commands:** In raw mode, any command entered will not be in any way modified or verified by the CIT application prior to being sent.

4 Click **OK**.

Result:

The **Cut Through** window appears.

5 As an alternative, the Cut-Through window can be accessed via the menu bar. Select **Network Element** → **TL1....** In the **NE Selection** window, select the TID of the NE for which you wish to establish a Cut-Through session.

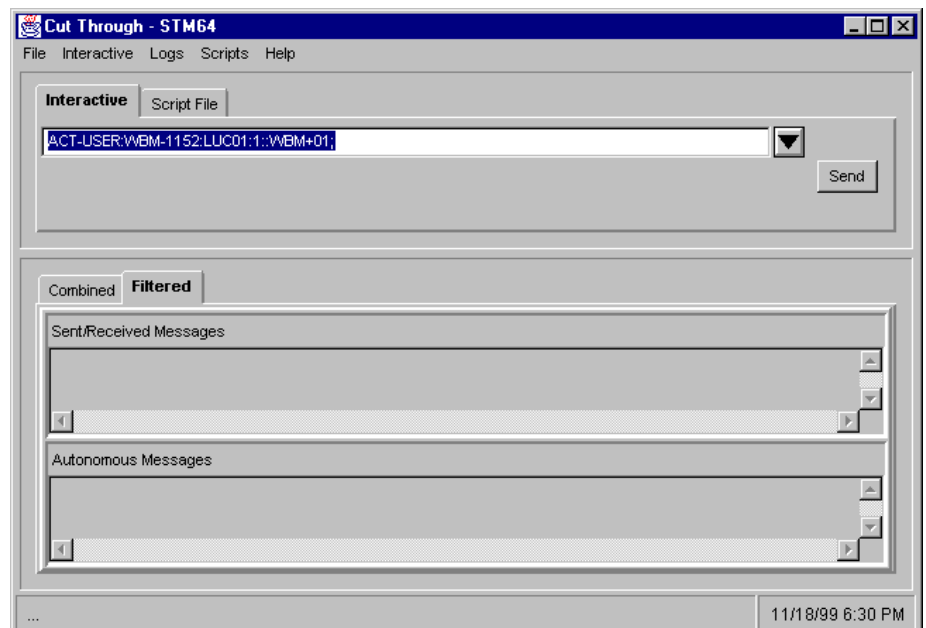
END OF STEPS



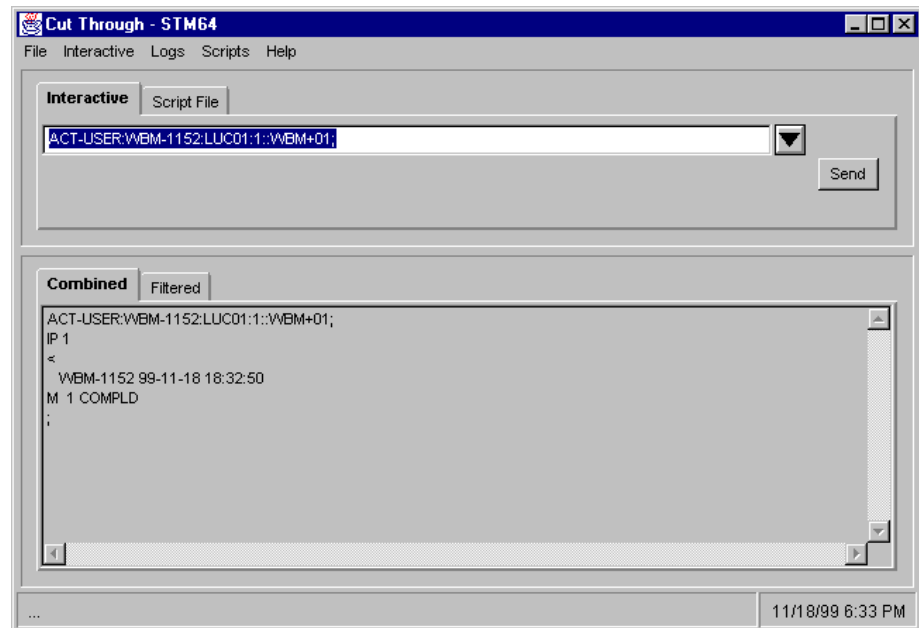
Interactive – Execute TL1 single commands

Two methods You can execute single TL1 commands on an interactive basis. There are two methods:

- If you know the exact TL1 command, enter the command on the command line
- If you do not know the exact command, left-click on the drop-down arrow, which is located at the end of the command line. A drop-down list appears, called the TL1 listbox file (for default location and editing of the listbox file, please refer to “Interactive – Manage a listbox file” (22-69)):
 - Scroll down the list until you see the command that you want to send to the NE or a command that is similar and which can be easily changed in the command line.
 - Left-click on the command to select/place it on the command line.
 - Left-click on the Send button. Your display should look similar to the following figure.



As desired, you can view the system response in a combined format, which is shown in the figure below, or a filtered format. Alternatively, if **Raw TL1 Commands** has been chosen in the **Select Cut-Through Execution Mode** window, the system response is shown in raw mode.



Combined format The combined format displays commands in the order they are sent along with the received replies. Due to delays a command and its received reply may be separated by other commands and replies from other commands. This is especially true when sending commands from a script file where the commands are separated by a small delay interval.

Filtered format The filtered format separates autonomous messages from the sent commands and their received replies. A sent command will not be displayed until its corresponding reply is received. Demarcation banners are added to help distinguish between sent/received messages.



Interactive – Manage a listbox file

Overview WaveStar® CIT allows you to create and modify the TL1 listbox files which can be used for easier access to the appropriate TL1 commands in the interactive operating mode of the Cut Through interface.

Options From the interactive menu, you can choose the following options:

- **Select TL1 Listbox File...** that already exists on the PC hard-disk drive.
The text contained within the newly selected file will replace the previous text displayed in the interactive TL1 box when the drop-down arrow is clicked.
- **Edit TL1 Listbox File...** opens up the Wordpad application. The Wordpad application will open the file selected from the item above, or will default to the originally displayed TL1 list box found in the default file of [drive:]Program Files\Lucent Technologies\WaveStar CIT\bin\tl1-listbox.txt. You can also manually overwrite the tl1-listbox.txt file outside of the CIT application so that it becomes the new default.
- **Add last TL1 command to TL1 Listbox & File.** No NE operations are performed in this step.
The last command sent from the interactive command line will be added to the interactive TL1 listbox.

□

Working with script files

Overview If several network elements have to be provisioned in the same way, it is advantageous to create a script file containing all the TL1 commands required for that provisioning. This script file can then be run on several NEs.

Executing a script file You can execute a script by selecting **Scripts** → **Run...** from the menu bar.

In the **Run TL1 Script File** window, an existing script file can be selected by using the **Browse** button. The script file(s) exist(s) on the PC hard disk. The **Browse** button is simply the means to move up and down the directory structure in order to locate the desired script file.

When beginning to execute a script file, you are prompted once to select one of the following execution modes:

- Pause and Prompt each command
- Stop on deny from NE
- Send all commands.

**Editing a script file /
Creating a new script file**

When editing a script file (**Scripts - Edit**) or creating a new script file (**Scripts - New**) the following should be observed:

- A script file can contain any number of lines of ASCII text.
- Any line not containing a valid command will be displayed in an Invalid TL1 message box.
- Lines beginning with forward-slash forward-slash “//” are ignored.
- A script file may be edited from the script menu, and a script may be stopped at any time by selecting **Stop** from the script menu.

- A log file can be created (automatically) for each script file by inserting **#logfile=on** on any single line. This can be inserted/turned-on at any time during the script file and can be turned on multiple times. Each time that a new **#logfile=on** command is executed, the previous logfile is closed. The generated log file will have a unique name consisting of the current time/date-stamp plus the name of the current script file.
- Between the individual commands, pauses can be inserted (e.g. **#delay=5000** indicates a pause of 5 seconds).



Working with logs

Overview WaveStar® CIT can create log files for all TL1 commands that have been sent/received.

Start logging To create a log file, proceed as follows:

- 1 From the menu bar, select **Logs** → **Start**, and you are prompted to:
 1. Enter the name for a new log file (for example, [drive:]\Program Files\Lucent Technologies\WaveStar CIT\bin\new-log-file), or
 2. Enter the full path name of an existing log file
-

- 2 Start the TL1 logging process by left-clicking on the **OK** button.

Result:

All TL1 commands sent/received are now logged in a filtered format.

END OF STEPS

Stop logging To stop logging TL1 commands, proceed as follows:

- 1 Select **Stop**.

Result:

Once TL1 logging is started, the next time that menu bar item **Logs** is selected, the start menu item will toggle to stop.

- 2 Close the user's log file.

END OF STEPS

View log file To view the log file, proceed as follows:

- 1 From the menu bar, select **Logs → View**.

Result:

You are prompted to enter the name of an existing log file that you wish to view.

- 2 Enter the name of the log file that you wish to view.

Result:

The selected log file is displayed using Wordpad. You can view and/or print the log file.

END OF STEPS

**Activating/deactivating
time and data stamp**

To activate or deactivate the time and data stamp, proceed as follows:

- 1 From the menu bar, select menu item **Logs-Time/Date Stamp** to toggle (on/off) the time and date stamp.

Result:

The time and date stamp, when on, is listed at the beginning of the command head for both the filtered view and the log file.

END OF STEPS





Glossary

μ
Microns

NUMERICS

0x1 Line Operation

0x1 means unprotected operation. The connection between network elements has one bidirectional line (no protection line).

1+1 Line Protection

A protection architecture in which the transmitting equipment transmits a valid signal on both the working and protection lines. The receiving equipment monitors both lines. Based on performance criteria and OS control, the receiving equipment chooses one line as the active line and designates the other as the standby line.

1xN Equipment Protection

1xN protection pertains to N number of circuit pack/port units protected by one circuit pack or port unit. When a protection switch occurs, the working signals are routed from the failed pack to the protection pack. When the fault clears, the signals revert to the working port unit.

12NC (12-digit Numerical Code)

Used to uniquely identify an item or product. The first ten digits uniquely identify an item. The eleventh digit is used to specify the particular variant of an item. The twelfth digit is used for the revision issue. Items with the first eleven digits the same, are functionally equal and may be exchanged.

A ABN

Abnormal (condition)

ABS (Absent)

Used to indicate that a given circuit pack is not installed.

AC

Alternating Current

ACO (Alarm Cut-Off)

A button on the user panel used to silence audible alarms.

ACT (Active)

Used to indicate that a circuit pack or module is in-service and currently providing service functions.

Adaptive-rate tributary operation of a port (Pipe mode)

Mode of operation of a port in which tributaries are *not* explicitly provisioned for the expected signal rates. The signal rates are automatically identified.

ADM (Add/Drop Multiplexer)

The term for a synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

AEL

Accessible Emission Limits

Agent

Performs operations on managed objects and issues events on behalf of these managed objects. All SDH managed objects will support at least an agent. Control of distant agents is possible via local “Managers”.

AGNE

Alarm Gateway Network Element

AID (Access Identifier)

A technical specification for explicitly naming entities (both physical and logical) of an NE using a grammar comprised of ASCII text, keywords, and grammar rules.

AIS (Alarm Indication Signal)

A code transmitted downstream in a digital network that indicates that an upstream failure has been detected and alarmed if the upstream alarm has not been suppressed.

AIMS

Acknowledged Information Transfer Service: Confirmed mode of operation of the LAPD protocol.

Alarm

Visible or audible signal indicating that an equipment failure or significant event/condition has occurred.

Alarm Correlation

The search for a directly-reported alarm that can account for a given symptomatic condition.

Alarm Severity

An attribute defining the priority of the alarm message. The way alarms are processed depends on the severity.

Alarm Suppression

Selective removal of alarm messages from being forwarded to the GUI or to network management layer OSs.

Alarm Throttling

A feature that automatically or manually suppresses autonomous messages that are not priority alarms.

Aligning

Indicating the head of a virtual container by means of a pointer, for example, creating an Administrative Unit (AU) or a Tributary Unit (TU).

AMI (Alternate Mark Inversion)

A line code that employs a ternary signal to convert binary digits, in which successive binary ones are represented by signal elements that are normally of alternative positive and negative polarity but equal in amplitude and in which binary zeros are represented by signal elements that have zero amplitude.

Anomaly

A difference between the actual and desired operation of a function.

ANSI

American National Standards Institute

APD

Avalanche Photo Diode

APS (Automatic Protection Switch)

A protection switch that occurs automatically in response to an automatically detected fault condition.

ASCII (American Standard Code for Information Interchange)

A standard 7-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

ASN.1

Abstract Syntax Notation 1

Assembly

Gathering together of payload data with overhead and pointer information (an indication of the direction of the signal).

Association

A logical connection between manager and agent through which management information can be exchanged.

Asynchronous

The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

ATM (Asynchronous Transfer Mode)

A high-speed transmission technology characterized by high bandwidth and low delay. It utilizes a packet switching and multiplexing technique which allocates bandwidth on demand.

Attribute

Alarm indication level: critical, major, minor, or no alarm.

AU (Administrative Unit)

Carrier for TUs.

AU PTR (Administrative Unit Pointer)

Indicates the phase alignment of the VC-N with respect to the STM-N frame. The pointer position is fixed with respect to the STM-N frame.

AUG

Administrative Unit Group

AUTO (Automatic)

One possible state of a port or slot. When a port is in the AUTO state and a good signal is detected, the port automatically enters the IS (in-service) state. When a slot is in the AUTO state and a circuit pack is detected, the slot automatically enters the EQ (equipped) state.

Autolock

Action taken by the system in the event of circuit pack failure/trouble. System switches to protection and prevents a return to the working circuit pack even if the trouble clears. Multiple protection switches on a circuit pack during a short period of time cause the system to autolock the pack.

Autonomous Message

A message transmitted from the controlled Network Element to the *Navis*[™] OEMS which was not a response to an *Navis* OEMS originated command.

AVAIL

Available

B Bandwidth

The difference in Hz between the highest and lowest frequencies in a transmission channel. The data rate that can be carried by a given communications circuit.

Baud Rate

Transmission rate of data (bits per second) on a network link.

BER (Bit Error Rate)

The ratio of error bits received to the total number of bits transmitted.

Bidirectional Line

A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bidirectional Ring

A ring in which both directions of traffic between any two nodes travel through the same network elements (although in opposite directions).

Bidirectional Switch

Protection switching performed in both the transmit and receive directions.

BIP-N (Bit Interleaved Parity-N)

A method of error monitoring over a specified number of bits (BIP-3 or BIP-8).

Bit

The smallest unit of information in a computer, with a value of either 0 or 1.

Bit Error Rate Threshold

The point at which an alarm is issued for bit errors.

BLD OUT LG

Build-Out Lightguide

Bridge Cross-Connection

The setting up of a cross-connection leg with the same input tributary as that of an existing cross-connection leg. Thus, forming a 1:2 bridge from an input tributary to two output tributaries.

Broadband Communications

Voice, data, and/or video communications at greater than 2 Mbit/s rates.

Broadband Service Transport

STM-1 concatenation transport over the *LambdaUnite*[™] MSS for ATM applications.

Byte

Refers to a group of eight consecutive binary digits.

C C

Container

CC (Clear Channel)

A digital circuit where no framing or control bits are required, thus making the full bandwidth available for communications.

CC (Cross-Connection)

Path-level connections between input and output tributaries or specific ports within a single NE. Cross-connections are made in a consistent way even though there are various types of ports and various types of port protection. Cross-Connections are re-configurable interconnections between tributaries of transmission interfaces.

Cell Relay

Fixed-length cells. For example, ATM with 53 octets.

CEPT

Conférence Européenne des Administrations des Postes et des Télécommunications

Channel

A sub-unit of transmission capacity within a defined higher level of transmission capacity.

Circuit

A set of transmission channels through one or more network elements that provides transmission of signals between two points, to support a single communications path.

CIT or WaveStar® CIT (Craft Interface Terminal)

The user interface terminal used by craft personnel to communicate with a network element.

CL

Clear

CLEI

Common Language Equipment Identifier

Client

Computer in a computer network that generally offers a user interface to a server.

CLLI

Common Language Location Identifier

Closed Ring Network

A network formed of a ring-shaped configuration of network elements. Each network element connects to two others, one on each side.

CM (Configuration Management)

Subsystem that configures the network and processes messages from the network.

CMI

Coded Mark Inversion

CMIP

Common Management Information Protocol. OSI standard protocol for OAM&P information exchange.

CMISE

Common Management Information Service Element

CO (Central Office)

A building where common carriers terminate customer circuits.

Co-Resident

A hardware configuration where two applications can be active at the same time independently on the same hardware and software platform without interfering with each others functioning.

Collocated

System elements that are located in the same location.

Command Group

An administrator-defined group that defines commands to which a user has access.

Concatenation

A procedure whereby multiple virtual containers are associated one with each other resulting in a combined capacity that can be used as a single container across which bit sequence integrity is maintained.

Correlation

A process where related hard failure alarms are identified.

CP

Circuit Pack

CPE

Customer Premises Equipment

CPU

Central Processing Unit

CR (Critical (alarm))

Alarm that indicates a severe, service-affecting condition.

CRC

Cyclical Redundancy Check

Cross-Connect Map

Connection map for an SDH Network Element; contains information about how signals are connected between high speed time slots and low speed tributaries.

Crosstalk

An unwanted signal introduced into one transmission line from another.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

CTIP

Customer Training and Information Products

CTS

Customer Technical Support within Lucent Technologies

Current Value

The value currently assigned to a provisionable parameter.

D DACS/DCS

Digital Access Cross-Connect System

Data

A collection of system parameters and their associated values.

Database Administrator

A user who administers the database of the application.

dB

Decibels

DC

Direct Current

DCC (Data Communications Channel)

The embedded overhead communications channel in the synchronous line, used for end-to-end communications and maintenance. The DCC carries alarm, control, and status information between network elements in a synchronous network.

DCE (Data Communications Equipment)

The equipment that provides signal conversion and coding between the data terminating equipment (DTE) and the line. The DCE may be separate equipment or an integral part of the DTE or of intermediate equipment. A DCE may perform other functions usually performed at the network end of the line.

DCF

Data Communications Function; Dispersion Compensation Fiber

DCM (Dispersion Compensation Module)

A device used to compensate the dispersion, the pulse spreading properties of an optical fiber. DCMs are necessary for very-long-haul applications and high bit rates.

DCN

Data Communications Network

Default

An operation or value that the system or application assumes, unless a user makes an explicit choice.

Default Provisioning

The parameter values that are pre-programmed as shipped from the factory.

Defect

A limited interruption of the ability of an item to perform a required function. It may or may not lead to maintenance action depending on the results of additional analysis.

Demultiplexing

A process applied to a multiplexed signal for recovering signals combined within it and for restoring the distinct individual channels of these signals.

DEMUX (Demultiplexer)

A device that splits a combined signal into individual signals at the receiver end of transmission.

Deprovisioning

The inverse order of provisioning. To manually remove/delete a parameter that has (or parameters that have) previously been provisioned.

Digital Link

A transmission span such as a point-to-point 2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3 or VC4 link between controlled network elements.

Digital Multiplexer

Equipment that combines by time-division multiplexing several digital signals into a single composite digital signal.

Digital Section

A transmission span such as an STM-N signal. A digital section may contain multiple digital channels.

Disassembly

Splitting up a signal into its constituents as payload data and overhead (an indication of the direction of a signal).

Dispersion

Time-broadening of a transmitted light pulse.

Dispersion Shifted Optical Fiber

1330/1550 nm minimum dispersion wavelength.

Divergence

When there is unequal amplification of incoming wavelengths, the result is a power divergence between wavelengths.

DNI (Dual Node Ring Interworking)

A topology in which two rings are interconnected at two nodes on each ring and operate so that inter-ring traffic is not lost in the event of a node or link failure at an interconnecting point.

Doping

The addition of impurities to a substance in order to attain desired properties.

Downstream

At or towards the destination of the considered transmission stream, for example, looking in the same direction of transmission.

DPLL

Digital Phase Locked Loop

DRAM

Dynamic Random Access Memory

Drop and Continue

A circuit configuration that provides redundant signal appearances at the outputs of two network elements in a ring. Can be used for Dual Node Ring Interworking (DNI) and for video distribution applications.

Drop-Down Menu

A menu that is displayed from a menu bar.

DSNE (Directory Service Network Element)

A designated Network Element that is responsible for administering a database that maps Network Elements names (node names) to addresses (node Id). There can be one DSNE per (sub)network.

DTE (Data Terminating Equipment)

The equipment that originates data for transmission and accepts transmitted data.

DTMF

Dual Tone Multifrequency

DUR

Dual Unit Row (subrack)

DUS

Do not Use for Synchronization

DWDM (Dense Wavelength Division Multiplexing)

Transmitting two or more signals of different wavelengths simultaneously over a single fiber.

E EBER (Excessive Bit Error Rate)

The calculated average bit error rate over a data stream.

ECC

Embedded Control Channel

EEPROM

Electrically Erasable and Programmable Read-Only Memory

EIA (Electronic Industries Association)

A trade association of the electronic industry that establishes electrical and functional standards.

EM (Event Management)

Subsystem of *Navis* OEMS that processes and logs event reports of the network.

EMC (Electromagnetic Compatibility)

A measure of equipment tolerance to external electromagnetic fields.

EMI (Electromagnetic Interference)

High-energy, electrically induced magnetic fields that cause data corruption in cables passing through the fields.

EMS

Element Management System

Entity

A specific piece of hardware (usually a circuit pack, slot, or module) that has been assigned a name recognized by the system.

Entity Identifier

The name used by the system to refer to a circuit pack, memory device, or communications link.

EPROM

Erasable Programmable Read-Only Memory

EQ (Equipped)

Status of a circuit pack or interface module that is in the system database and physically in the frame, but not yet provisioned.

ES (Errored Seconds)

A performance monitoring parameter. ES “type A” is a second with exactly one error; ES “type B” is a second with more than one and less than the number of errors in a severely errored second for the given signal. ES by itself means the sum of the type A and type B ESs.

ESD

Electrostatic Discharge

ESP

Electrostatic Protection

Establish

A user initiated command, at the *LambdaUnite* CIT, to create an entity and its associated attributes in the absence of certain hardware.

ETSI

European Telecommunications Standards Institute

Event

A significant change. Events in controlled Network Elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs in a controlled Network Element, the controlled Network Element will generate an alarm or status message and send it to the management system.

Event Driven

A required characteristic of network element software system: NEs are reactive systems, primarily viewed as systems that wait for and then handle events. Events are provided by the external interface packages, the hardware resource packages, and also by the software itself.

Externally Timed

An operating condition of a clock in which it is locked to an external reference and is using time constants that are altered to quickly bring the local oscillator's frequency into approximate agreement with the synchronization reference frequency.

Extra traffic

Unprotected traffic that is carried over protection channels when their capacity is not used for the protection of working traffic.

F Fault

Term used when a circuit pack has a hard (not temporary) fault and cannot perform its normal function.

Fault Management

Collecting, processing, and forwarding of autonomous messages from network elements.

FCC

Federal Communications Commission

FDA/CDRH

The Food and Drug Administration's Center for Devices and Radiological Health.

FDI (Fiber Distributed Data Interface)

Fiber interface that connects computers and distributes data among them.

FE (Far End)

Any other network element in a maintenance subnetwork other than the one the user is at or working on. Also called remote.

FEBE (Far-End Block Error)

An indication returned to the transmitting node that an errored block has been detected at the receiving node. A block is a specified grouping of bits.

FEC (Forward Error Correction)

An error correction technique in which redundant bits are added to the payload signal enabling the receiving station to detect and correct bit errors that unavoidably occur when an optical line signal is transmitted over longer distances over an optical fiber. FEC is used to increase the transmission span length.

FEPRM (Flash EPROM)

A technology that combines the non-volatility of EPROM with the in-circuit re-programmability of EEPROM.

FERF (Far-End Receive Failure)

An indication returned to a transmitting Network Element that the receiving Network Element

has detected an incoming section failure. Also known as RDI.

FIT (Failures in Time)

Circuit pack failure rates per 10^9 hours as calculated using the method described in Reliability Prediction Procedure for Electronic Equipment, BellCore Method I, Issue 6, December 1997.

Fixed-rate tributary operation of a port

Mode of operation of a port in which tributaries are provisioned for the expected signal rates. This provisioning information is used for cross-connection rate validation and for alarm handling (for example “Loss of Pointer”).

Folded Rings

Folded (collapsed) rings are rings without fiber diversity. The terminology derives from the image of folding a ring into a linear segment.

Forced

Term used when a circuit pack (either working or protection) has been locked into a service-providing state by user command.

FR (Frame Relay)

A form of packet switching that relies on high-quality phone lines to minimize errors. It is very good at handling high-speed, bursty data over wide area networks. The frames are variable lengths and error checking is done at the end points.

Frame

The smallest block of digital data being transmitted.

Framework

An assembly of equipment units capable of housing shelves, such as a bay framework.

Free Running

An operating condition of a clock in which its local oscillator is not locked to an internal synchronization reference and is using no storage techniques to sustain its accuracy.

G GB
Gigabytes

Gbit/s
Gigabits per second

GHz
Gigahertz

Global Wait to Restore Time

Corresponds to the time to wait before switching back to the timing reference. It occurs after a timing link failure has cleared. This time applies for all timing sources in a system hence the name global. This can be between 0 and 60 minutes, in increments of one minute.

GNE (Gateway Network Element)

A network element that passes information between other network elements and management systems through a data communication network.

Grooming

In telecommunications, the process of separating and segregating channels, as by combing, such that the broadest channel possible can be assembled and sent across the longest practical link. The aim is to minimize de-multiplexing traffic and reshuffling it electrically.

H Hard Failure

An unrecoverable non-symptomatic (primary) failure that causes signal impairment or interferes with critical network functions, such as DCC operation.

HDB3 (High Density Bipolar 3 Code)

Line code for 2 Mbit/s transmission systems.

HDLC (High Level Data Link Control)

OSI reference model datalink layer protocol.

HMI

Human Machine Interface

HML (Human Machine Language)

A standard language developed by the ITU for describing the interaction between humans and dumb terminals.

HO

High Order

Holdover

An operating condition of a clock in which its local oscillator is not locked to an external reference but is using storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronization reference.

Hot Standby

A circuit pack ready for fast, automatic placement into operation to replace an active circuit pack. It has the same signal as the service going through it, so that choice is all that is required.

HPA (Higher Order Path Adaptation)

Function that adapts a lower order Virtual Container to a higher order Virtual Container by

processing the Tributary Unit pointer which indicates the phase of the lower order Virtual Container Path Overhead relative to the higher order Virtual Container Path Overhead and assembling/disassembling the complete higher order Virtual Container.

HPC (Higher Order Path Connection)

Function that provides for flexible assignment of higher order Virtual Containers within an STM-N signal.

HPT (Higher Order Path Termination)

Function that terminates a higher order path by generating and adding the appropriate Virtual Container Path Overhead to the relevant container at the path source and removing the Virtual Container Path Overhead and reading it at the path sink.

HS

High Speed

HW

Hardware

Hz

Hertz

I I/O

Input/Output

IAO LAN

Intraoffice Local Area Network

ID

Identifier

IEC

International Electro-Technical Commission

IEEE

Institute of Electrical and Electronics Engineers

IMF

Infant Mortality Factor

Insert

To physically insert a circuit pack into a slot, thus causing a system initiated restore of an entity into service and/or creation of an entity and associated attributes.

Interface Capacity

The total number of STM-1 equivalents (bidirectional) tributaries in all transmission interfaces with which a given transmission interface shelf can be equipped at one time. The interface capacity varies with equipage.

Intermediate System (IS)

A system which routes/relays management information. An SDH Network Element may be a combined intermediate and end system.

IS (In-Service)

A memory administrative state for ports. IS refers to a port that is fully monitored and alarmed.

IS-IS Routing

The Network Elements in a management network, route packets (data) between each other using an IS-IS level protocol. The size of a network running IS-IS Level 1 is limited, and therefore certain mechanisms are employed to facilitate the management of larger networks.

For STATIC ROUTING, the capability exists for disabling the protocol over the LAN connections, effectively causing the management network to be partitioned into separate IS-IS Level 1 areas. In order for the network management system to communicate with a specific Network Element in one of these areas, the network management system must identify through which so-called Gateway Network Element this specific Network Element is connected to the LAN. All packets to this specific Network Element are routed directly to the Gateway Network Element by the network management system, before being re-routed (if necessary) within the Level 1 area.

For DYNAMIC ROUTING an IS-IS Level 2 routing protocol is used allowing a number of Level 1 areas to interwork. The Network Elements which connect an IS-IS area to another area are set to run the IS-IS Level 2 protocol within the Network Element and on the connection between other Network Elements. Packets can now be routed between IS-IS areas and the network management system does not have to identify the Gateway Network Elements.

ISDN

Integrated Services Digital Network

ITM

Integrated Transport Management

ITM-NM

Integrated Transport Management Network Module

ITU

International Telecommunications Union

ITU-T

International Telecommunications Union — Telecommunication standardization sector. Formerly known as CCITT: Comité Consultatif International Télégraphique & Téléphonique; International

J Jitter

Short term variations of amplitude and frequency components of a digital signal from their ideal position in time.

K kbit/s

Kilobits per second

L *LambdaUnite* OLS 1.6T (400G/800G)

LambdaUnite Optical Line System 1.6 Terabit/s (400Gbit/s/800Gbit/s)

LAN (Local Area Network)

A communications network that covers a limited geographic area, is privately owned and user administered, is mostly used for internal transfer of information within a business, is normally contained within a single building or adjacent group of buildings, and transmits data at a very rapid speed.

LAPD (Link Access Procedure D-bytes)

Protocol used on Data Link Layer (OSI layer two) according to ITU-T Q.921.

LBC

Laser Bias Current

LBFC

Laser Backface Currents

LBO (Lightguide Build-Out)

An attenuating (signal-reducing) element used to keep an optical output signal strength within desired limits.

LCN

Local Communications Network

LCS

Local Customer Support

LED

Light-Emitting Diode

LH

Long Haul

Line

A transmission medium, together with the associated equipment, required to provide the means of transporting information between two consecutive network elements. One network element originates the line signal; the other terminates it.

Line Protection

The optical interfaces can be protected by line protection. Line protection switching protects against failures of line facilities, including the interfaces at both ends of a line, the optical fibers, and any equipment between the two ends. Line protection includes protection of equipment failures.

Line Timing

Refers to a network element that derives its timing from an incoming STM-N signal.

Link

The mapping between in-ports and out-ports. It specifies how components are connected to one another.

LL

Lucent Learning (former CTIP)

LO

Low Order

Location

An identifier for a specific circuit pack, interface module, interface port, or communications link.

Lockout of Protection

The *LambdaUnite* CIT command that prevents the system from switching traffic to the protection line from a working line. If the protection line is active when a “Lockout of Protection” is entered – this command causes the working line to be selected. The protection line is then locked from any Automatic, Manual, or Forced protection switches.

Lockout State

The Lockout State shall be defined for each working or protection circuit pack. The two permitted states are: None – meaning no lockout is set for the circuit pack, set meaning the circuit pack has been locked out. The values (None & Set) shall be taken independently for each working or protection circuit pack.

LOF (Loss of Frame)

A failure to synchronize an incoming signal.

LOM

Loss Of Multiframe

Loop Timing

A special case of line timing. It applies to network elements that have only one OC-N/STM-N interface. For example, terminating nodes in a linear network are loop timed.

Loopback

Type of diagnostic test used to compare an original transmitted signal with the resulting received signal. A loopback is established when the received optical or electrical external transmission signal is sent from a port or tributary input directly back toward the output.

LOP (Loss of Pointer)

A failure to extract good data from a signal payload.

LOS (Loss of Signal)

The complete absence of an incoming signal.

Loss Budget

Loss (in dB) of optical power due to the span transmission medium (includes fiber loss and splice losses).

LPA (Lower order Path Adaptation)

Function that adapts a PDH signal to a synchronous network by mapping the signal into or de-mapping the signal out of a synchronous container.

LPC (Lower Order Path Connection)

Function that provides for flexible assignment of lower order VCs in a higher order VC.

LPT (Lower Order Path Termination)

Function that terminates a lower order path by generating and adding the appropriate VC POH to the relevant container at the path source and removing the VC POH and reading it at the path sink.

LS

Low Speed

LTE

Line Terminating Equipment

M μm

Micrometer

MAF

Management Application Function

Maintenance Condition

An equipment state in which some normal service functions are suspended, either because of a problem or to perform special functions (copy memory) that can not be performed while normal service is being provided.

Management Connection

Identifies the type of routing used (STATIC or DYNAMIC), and if STATIC is selected allows the gateway network element to be identified.

Manager

Capable of issuing network management operations and receiving events. The manager communicates with the agent in the controlled network element.

Manual Switch State

A protection group shall enter the Manual Switch State upon the initiation and successful completion of the Manual Switch command. The protection group leaves the Manual Switch state by means of the Clear or Forced Switch commands. While in the Manual Switch state the system may switch the active unit automatically if required for protection switching.

Mapping

The logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices or addresses on another network.

MB

Megabytes

Mbit/s

Megabits per second

MCF (Message Communications Function)

Function that provides facilities for the transport and routing of Telecommunications Management Network messages to and from the Network Manager.

MD (Mediation Device)

Allows for exchange of management information between Operations System and Network Elements.

MDI

Miscellaneous Discrete Input

MDO

Miscellaneous Discrete Output

MEC (Manufacturer Executable Code)

Network Element system software in binary format that after being downloaded to one of the stores can be executed by the system controller of the network element.

MEM

Memory

Mid-Span Meet

The capability to interface between two lightwave network elements of different vendors. This applies to high-speed optical interfaces.

MIPS

Millions of Instructions Per Second

Miscellaneous Discrete Interface

Allows an operations system to control and monitor equipment collocated within a set of input and output contact closures.

MJ (Major (alarm))

Indicates a service-affecting failure, main or unit controller failure, or power supply failure.

MMF

Multi-Mode Fiber

MMI

Man-Machine Interface

MML

Human-Machine Language

MN (Minor (alarm))

Indicates a non-service-affecting failure of equipment or facility.

MO

Managed Object

MS

Multiplexer Section

ms

Millisecond

MS-SPRING (Multiplexer Section Shared Protection Ring)

A protection method used in Add-Drop Multiplexer Network Elements.

MSOH (Multiplexer Section OverHead)

Part of the Section Overhead. Is accessible only at line terminals and multiplexers.

MSP (Multiplexer Section Protection)

Provides capability for switching a signal from a working to a protection section.

MST (Multiplexer Section Termination)

Function that generates the Multiplexer Section OverHead in the transmit direction and terminates the part of the Multiplexer Section overhead that is acceptable in the receive direction.

MTBF

Mean Time Between Failures

MTBMA

Mean Time Between Maintenance Activities

MTIE

Maximum Time Interval Error

MTPI

Multiplexer Timing Physical Interface

MTS (Multiplexer Timing Source)

Function that provides timing reference to the relevant component parts of the multiplex equipment and represents the SDH Network Element clock.

MTTR

Mean Time To Repair

Multiplexer

A device (circuit pack) that combines two or more transmission signals into a combined signal on a shared medium.

Multiplexing

A procedure by which multiple lower order path layer signals are adapted into a higher order path, or the multiple higher order path layer signals are adapted into a multiplex section.

N NA

Not Applicable

NE (Network Element)

A node in a telecommunication network that supports network transport services and is directly manageable by a management system.

NEBS

Network Equipment-Building System

nm

Nanometer (10^{-9} meters)

NMON (Not Monitored)

A provisioning state for equipment that is not monitored or alarmed.

No Request State

This is the routine-operation quiet state in which no external command activities are occurring.

Node

A network element in a ring or, more generally, in any type of network. In a network element supporting interfaces to more than one ring, node refers to an interface that is in a particular ring. Node is also defined as all equipment that is controlled by one system controller. A node is not always directly manageable by a management system.

Non-Revertive Switching

In non-revertive switching, an active and stand-by line exist on the network. When a protection switch occurs, the standby line is selected to support traffic, thereby becoming the active line. The original active line then becomes the stand-by line. This status remains in effect even when the fault clears. That is, there is no automatic switch back to the original status.

Non-Synchronous

The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

NORM

Normal

NPI

Null Pointer Indication

NPPA (Non-Preemptible Protection Access)

Non-preemptible protection access increases the available span capacity for traffic which does not require protection by a ring, but which cannot be preempted.

NRZ

Nonreturn to Zero

NSA

Non-Service Affecting

NSAP Address (Network Service Access Point Address)

Network Service Access Point Address (used in the OSI network layer 3). An automatically assigned number that uniquely identifies a Network Element for the purposes of routing DCC messages.

NVM (Non-Volatile Memory)

Memory that retains its stored data after power has been removed. An example of NVM would be a hard disk.

O O&M

Operation and Maintenance

OA

Optical Amplifier

OAM&P

Operations, Administration, Maintenance, and Provisioning

OC, OC-n

Optical Carrier

OC-12

Optical Carrier, Level 12 Signal (622.08 Mbit/s)

OC-192

Optical Carrier, Level 192 (9953.28 Mbit/s) (10 Gbit/s)

OC-3

Optical Carrier, Level 3 Signal (155 Mbit/s)

OC-48

Optical Carrier, Level 48 (2488.32 Mbit/s) (2.5 Gbit/s)

OC-768

Optical Carrier, Level 768 (39813.12 Mbit/s) (40 Gbit/s)

OI (Operations Interworking)

The capability to access, operate, provision, and administer remote systems through craft interface access from any site in an SDH network or from a centralized operations system.

OLS

Optical Line System

ONMS

Optical Network Management System

OOF

Out-of-Frame

OOS (Out-of-Service)

The circuit pack is not providing its normal service function (removed from either the working or protection state) either because of a system problem or because the pack has been removed from service.

Open Ring Network

A network formed of a linear chain-shaped configuration of network elements. Each network element connects to two others, one on each side, except for two network elements at the ends which are connected on only one side. A closed ring can be formed by adding a connection between the two end nodes.

Operations Interface

Any interface providing you with information on the system behavior or control. These include the equipment LEDs, user panel, *LambdaUnite* CIT, office alarms, and all telemetry interfaces.

Operator

A user of the system with operator-level user privileges.

Optical Channel

A STM-N wavelength within an optical line signal. Multiple channels, differing by 1.5 μm in wavelength, are multiplexed into one signal.

Optical Line Signal

A multiplexed optical signal containing multiple wavelengths or channels.

Original Value Provisioning

Preprogramming of a system's original values at the factory. These values can be overridden using local or remote provisioning.

OS (Operations System)

A central computer-based system used to provide operations, administration, and maintenance functions.

OSF

Open Software Foundation; Operations System Function

OSI (Open Systems Interconnection)

Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Outage

A disruption of service that lasts for more than 1 second.

OW (Orderwire)

A dedicated voice-grade line for communications between maintenance and repair personnel.

P Parameter

A variable that is given a value for a specified application. A constant, variable, or expression that is used to pass values between components.

Parity Check

Tests whether the number of ones (or zeros) in an array of binary bits is odd or even; used to determine that the received signal is the same as the transmitted signal.

Pass-Through

Paths that are cross-connected directly across an intermediate node in a network.

Path

A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Terminating Equipment

Network elements in which the path overhead is terminated.

PCB

Printed Circuit Board

PCM

Pulse Code Modulation

PDH

Plesiochronous Digital Hierarchy

PI

Physical Interface

Pipe mode (Adaptive-rate tributary operation of a port)

Mode of operation of a port in which tributaries are *not* explicitly provisioned for the expected signal rates. The signal rates are automatically identified.

Platform

A family of equipment and software configurations designed to support a particular application.

Plesiochronous Network

A network that contains multiple subnetworks, each internally synchronous and all operating at the same nominal frequency, but whose timing may be slightly different at any particular instant.

PM (Performance Monitoring)

Measures the quality of service and identifies degrading or marginally operating systems (before an alarm would be generated).

PMD (Polarization Mode Dispersion)

Output pulse broadening due to random coupling of the two polarization modes in an optical fiber.

POH (Path Overhead)

Informational bytes assigned to, and transported with the payload until the payload is de-multiplexed. It provides for integrity of communication between the point of assembly of a virtual container and its point of disassembly.

Pointer

An indicator whose value defines the frame offset of a virtual container with respect to the frame reference of the transport entity on which it is supported.

POP

Point of Presence

Port (also called Line)

The physical interface, consisting of both an input and output, where an electrical or optical transmission interface is connected to the system and may be used to carry traffic between network elements. The words “port” and “line” may often be used synonymously. “Port” emphasizes the physical interface, and “line” emphasizes the interconnection. Either may be used to identify the signal being carried.

Port State Provisioning

A feature that allows a user to suppress alarm reporting and performance monitoring during provisioning by supporting multiple states (automatic, in-service, and not monitored) for low-speed ports.

POTS

Plain Old Telephone Service

PP

Pointer Processing

PRC (Primary Reference Clock)

The main timing clock reference in SDH equipment.

Preprovisioning

The process by which the user specifies parameter values for an entity in advance of some of the equipment being present. These parameters are maintained only in NVM. These modifications are initiated locally or remotely by either *LambdaUnite* CIT or *Navis* OEMS. Preprovisioning provides for the decoupling of manual intervention tasks (for example, install circuit packs) from those tasks associated with configuring the node to provide services (for example, specifying the entities to be cross-connected).

PRI

Primary

Proactive Maintenance

Refers to the process of detecting degrading conditions not severe enough to initiate protection switching or alarming, but indicative of an impending signal fail or signal degrade defect.

Protection Access

To provision traffic to be carried by protection tributaries when the port tributaries are not being used to carry the protected working traffic.

Protection Group Configuration

The members of a group and their roles, for example, working protection, line number, etc.

Protection Path

One of two signals entering a path selector used for path protection switching or dual ring interworking. The other is the working path. The designations working and protection are provisioned by the user, whereas the terms active path and standby path indicate the current protection state.

Protection State

When the working unit is currently considered active by the system and that it is carrying traffic. The “active unit state” specifically refers to the receive direction of operation — since protection switching is unidirectional.

PROTN (Protection)

Extra capacity (channels, circuit packs) in transmission equipment that is not intended to be used for service, but rather to serve as backup against equipment failures.

PROV (Provisioned)

Indicating that a circuit pack is ready to perform its intended function. A provisioned circuit pack can be active (ACT), in-service (IS), standby (STBY), provisioned out-of-service (POS), or out-of-service (OOS).

PSDN

Public Switched Data Network

PSTN

Public Switched Telephone Network

PTE

Path Terminating Equipment

PTR

Pointer

PWR

Power

PWR ON

Power On

Q Q-LAN

Thin Ethernet LAN which connects the manager to Gateway Network Elements so that management information between Network Elements and management systems can be exchanged.

QL (Quality Level)

The quality of the timing signal(s) provided to synchronize a Network Element. In case of optical line timing the level can be provided by the Synchronization Status Message (S-1 byte). If the System and Output Timing Quality Level mode is “Enabled”, and if the signal selected for the Station Clock Output has a quality level below the Acceptance Quality Level, the Network Element “squelsches” the Station Clock Output Signal, which means that no signal is forwarded at all.

QOS

Quality of Service

R RAM

Random Access Memory

RDI (Remote Defect Indication)

An indication returned to a transmitting terminal that the receiving terminal has detected an incoming section failure. [Previously called far-end-receive failure (FERF).]

Reactive Maintenance

Refers to detecting defects/failures and clearing them.

Receive-Direction

The direction towards the Network Element.

Regeneration

The process of reconstructing a digital signal to eliminate the effects of noise and distortion.

Regenerator Loop

Loop in a Network Element between the Station Clock Output(s) and one or both Station Clock Inputs, which can be used to de-jitterize the selected timing reference in network applications.

Regenerator Section Termination (RST)

Function that generates the Regenerator Section Overhead (RSOH) in the transmit direction and terminates the RSOH in the receive direction.

Reliability

The ability of a software system performing its required functions under stated conditions for a stated period of time. The probability for an equipment to fulfill its function. Some of the ways in which reliability is measured are: MTBF (Mean Time Between Failures) expressed in hours; Availability = $(MTBF)/(MTBF+MTTR)(\%)$ [where MTTR = mean time to restore]; outage in minutes per year; failures per hour; percentage of failures per 1,000 hours.

Remote Network Element

Any Network Element that is connected to the referenced Network Element through either an electrical or optical link. It may be the adjacent node on a ring, or N nodes away from the reference. It also may be at the same physical location but is usually at another (remote) site.

Restore Timer

Counts down the time (in minutes) during which the switch waits to let the worker line recover before switching back to it. This option can be set to prevent the protection switch continually switching if a line has a continual transient fault.

Revertive

A protection switching mode in which, after a protection switch occurs, the equipment returns to the nominal configuration (that is, the working equipment is active, and the protection equipment is standby) after any failure conditions that caused a protection switch to occur, clear, or after any external switch commands are reset. (See “Non-Revertive”.)

Revertive Switching

In revertive switching, there is a working and protection high-speed line, circuit pack, etc. When a protection switch occurs, the protection line, circuit pack, etc. is selected. When the fault clears, service “reverts” to the working line.

Ring

A configuration of nodes comprised of network elements connected in a circular fashion. Under normal conditions, each node is interconnected with its neighbor and includes capacity for transmission in either direction between adjacent nodes. Path switched rings use a head-end bridge and tail-end switch. Line switched rings actively reroute traffic over the protection capacity.

Route

A series of contiguous digital sections.

Router

An interface between two networks. While routers are like bridges, they work differently. Routers provide more functionality than bridges. For example, they can find the best route between any two networks, even if there are several different networks in between. Routers also provide network management capabilities such as load balancing, partitioning of the network, and trouble-shooting.

RSOH

Regenerator Section OverHead; part of SOH

RST

Regenerator Section Termination

RT

Remote Terminal

RTRV

Retrieve

RZ (Return to Zero)

A code form having two information states (termed zero and one) and having a third state or an at-rest condition to which the signal returns during each period.

S SA

Service Affecting

SA

Section Adaptation

SD

Signal Degrade

SDH (Synchronous Digital Hierarchy)

A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

SDS

Standard Directory Service based on ANSI recommendation T1.245

SEC

Secondary

SEC

SDH Equipment Clock

Section

The portion of a transmission facility, including terminating points, between a terminal network element and a line-terminating network element, or two line-terminating network elements.

Section Adaptation

Function that processes the AU-pointer to indicate the phase of the VC-3/4 POH relative to the STM-N SOH and assembles/disassembles the complete STM-N frame.

Self-Healing

A network's ability to automatically recover from the failure of one or more of its components.

SEMF (Synchronous Equipment Management Function)

Function that converts performance data and implementation specific hardware alarms into object-oriented messages for transmission over the DCC and/or Q-interface. It also converts object-oriented messages related to other management functions for passing across the S reference points.

Server

Computer in a computer network that performs dedicated main tasks which generally require sufficient performance.

Service

The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

SES (Severely Errored Seconds)

This performance monitoring parameter is a second in which a signal failure occurs, or more than a preset amount of coding violations (dependent on the type of signal) occurs.

SH

Short Haul

Single-Ended Operations

Provides operations support from a single location to remote Network Elements in the same SDH subnetwork. With this capability you can perform operations, administration, maintenance, and provisioning on a centralized basis. The remote Network Elements can be those that are specified for the current release.

Site Address

The unique address for a Network Element.

Slot

A physical position in a shelf designed for holding a circuit pack and connecting it to the backplane. This term is also used loosely to refer to the collection of ports or tributaries connected to a physical circuit pack placed in a slot.

SM or SMF (Single-Mode Fiber)

A low-loss, long-span optical fiber typically operating at either 1310 nm, 1550 nm, or both.

SMN

SDH Management Network

SNC/I

SubNetwork Connection (protection) / Inherent monitoring

SNC/N

SubNetwork Connection (protection) / Non-Intrusive Monitoring

SNR (Signal-to-Noise Ratio)

The relative strength of signal compared to noise.

Software Backup

The process of saving an image of the current network element's databases, which are contained in its NVM, to a remote location. The remote location could be the *LambdaUnite* CIT or *Navis* OEMS.

Software Download

The process of transferring a generic (full or partial) or provisioned database from a remote entity to the target network element's memory. The remote entity may be the *LambdaUnite* CIT or *Navis* OEMS. The download procedure uses bulk transfer to move an un-interpreted binary file into the network element.

Software ID

Number that provides the software version information for the system.

SOH (Section Overhead)

Capacity added to either an AU-4 or assembly of AU-3s to create an STM-1. Contains always STM-1 framing and optionally maintenance and operational functions. SOH can be subdivided in MSOH (multiplex section overhead) and RSOH (regenerator section overhead).

SONET (Synchronous Optical Network)

The North American standard for the rates and formats that defines optical signals and their constituents.

Span

An uninterrupted bidirectional fiber section between two network elements.

Span Growth

A type of growth in which one wavelength is added to all lines before the next wavelength is added.

SPE

Synchronous Payload Envelope

SPF (Single point of failure)

A single failure in the OSI-network (DCC, LAN or node), that causes isolation of more than one node in the OSI-network. The use of IS-IS areas, without obeying all rules & guidelines, increases the risk of a single point of failure in the network.

SPI

SDH Physical Interface

Squelch Map

This map contains information for each cross-connection in a ring and indicates the source and destination nodes for the low-speed circuit that is part of the cross-connection. This information is used to prevent traffic misconnection in rings with isolated nodes or segments.

SSM

Synchronization Status Marker

SSU_L

Synchronization Supply Unit — Local

SSU_T

Synchronization Supply Unit — Transit

Standby Path

One of two signals entering a constituent path selector, the standby path is the path not currently being selected.

State

The state of a circuit pack indicates whether it is defective or normal (ready for normal use).

Station Clock Input

An external clock may be connected to a Station Clock Input.

Status

The indication of a short-term change in the system.

STBY (Standby)

The circuit pack is in service but is not providing service functions. It is ready to be used to replace a similar circuit pack either by protection or by duplex switching.

STM

Synchronous Transport Module (SDH)

STM-N (Synchronous Transport Module, Level N)

A building block information structure that supports SDH section layer connections, where N represents a multiple of 155.52 Mbit/s. Normally N = 1, 4, 16, 64 or 256.

Stream (Line; aggregate)

A synchronous high rate connection between multiplexers, typically 10 or 40 Gbit/s.

STS

Synchronous Transport Signal (SONET)

Subnetwork

A group of interconnected/interrelated Network Elements. The most common connotation is a synchronous network in which the Network Elements have data communications channel (DCC) connectivity.

Supervisor

A user of the application with supervisor user privileges.

Suppression

A process where service-affecting alarms that have been identified as an “effect” are not displayed to a user.

SYNC

Synchronizer

Synchronization Messaging

Synchronization messaging is used to communicate the quality of network timing, internal timing status, and timing states throughout a subnetwork.

Synchronous

The essential characteristic of time scales or signals such that their corresponding significant instances occur at precisely the same average rate, generally traceable to a single Stratum 1 source.

Synchronous Network

The synchronization of transmission systems with synchronous payloads to a master (network) clock that can be traced to a reference clock.

Synchronous Payload

Payloads that can be derived from a network transmission signal by removing integral numbers of bits from every frame. Therefore, no variable bit-stuffing rate adjustments are required to fit the payload in the transmission signal.

SYSCTL

System Controller circuit pack

System Administrator

A user of the computer system on which the system's OS software application can be installed.

T TARP

Target Identifiers Address Resolution Protocol

TBD

To Be Determined

TCA (Threshold-Crossing Alert)

A message type sent from a Network Element that indicates that a certain performance monitoring parameter has exceeded a specified threshold.

TDM (Time Division Multiplexing)

A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a portion of each signal one after another.

TEN

Telecommunications Management Network

Through (or Continue) Cross-Connection

A cross-connection within a ring, where the input and output tributaries have the same tributary number but are in lines opposite each other.

Through Timing

Refers to a network element that derives its transmit timing in the east direction from a received line signal in the east direction and its transmit timing in the west direction from a received line signal in the west direction.

THz

Terahertz (10^{12} Hz)

TID (Target Identifier)

A provisionable parameter that is used to identify a particular Network Element within a network. It is a character string of up to 20 characters where the characters are letters, digits, or hyphens (-).

TL1 (Transaction Language One)

A subset of ITU's human-machine language.

TM (Terminal Multiplexer)

An Add/Drop Multiplexer with only one stream interface.

Transmit-Direction

The direction outwards from the Network Element.

Tributary

A signal of a specific rate (2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3, VC4, STM-1 or STM-4) that may be added to or dropped from a line signal.

Tributary

A path-level unit of bandwidth within a port, or the constituent signal(s) being carried in this unit of bandwidth, for example, an STM-1 tributary within an STM-N port.

Tributary Unit Pointer

Indicates the phase alignment of the VC with respect to the TU in which it resides. The pointer position is fixed with respect to the TU frame.

True Wave[™] Optical Fiber

Lucent Technologies' fiber generally called non-zero dispersion-shift fiber, with a controlled amount of chromatic dispersion designed for amplified systems in the 1550/1310 nm range.

TRY

Technical Requirement

TSA (Time Slot Assignment)

A capability that allows any tributary in a ring to be cross-connected to any tributary in any lower-rate, non-ring interface or to the same-numbered tributary in the opposite side of the ring.

TSI (Time Slot Interchange)

The ability of the user to assign cross-connections between any tributaries of any lines within a Network Element. Three types of TSI can be defined: Hairpin TSI, Interring TSI (between rings), and intra-ring TSI (within rings).

TSO

Technical Support Organization

TTP

Trail Termination Point

TU (Tributary Unit)

An information structure which provides adaptation between the lower order path layer and the higher path layer. Consists of a VC-n plus a tributary unit pointer (TU PTR).

TUG

Tributary Unit Group

Two-Way Point-to-Point Cross-Connection

A two-legged interconnection, that supports two-way transmission, between two and only two tributaries.

Two-Way Roll

The operation which moves a two-way cross-connection between tributary i and tributary j to a two-way cross-connection between the same tributary i and a new tributary k with a single user command.

U UAS (Unavailable Seconds)

In performance monitoring, the count of seconds in which a signal is declared failed or in which 10 consecutively severely errored seconds (SES) occurred, until the time when 10 consecutive non-SES occur.

UITS (Unacknowledged Information Transfer Service)

Unconfirmed mode of LAPD operation.

UNEQ

Path Unequipped

Upstream

At or towards the source of the considered transmission stream, for example, looking in the opposite direction of transmission.

User Privilege

Permissions a user must perform on the computer system on which the system software runs.

UTC (Universal Time Coordinated)

A time-zone independent indication of an event. The local time can be calculated from the Universal Coordinated Time.

V V

Volts

VAC

Volts Alternating Current

Value

A number, text string, or other menu selection associated with a parameter.

Variable

An item of data named by an identifier. Each variable has a type, such as int or Object, and a scope.

VC (Virtual Container)

Container with path overhead.

VDC

Volts Direct Current

VF

Voice frequency

Virtual

Refers to artificial objects created by a computer to help the system control shared resources.

Virtual Circuit

A logical connection through a data communication (for example, X.25) network.

Voice Frequency (VF) Circuit

A 64 kilobit per second digitized signal.

Volatile Memory

Type of memory that is lost if electrical power is interrupted.

W WAD

Wavelength Add/Drop

WAN (Wide Area Network)

A communication network that uses common-carrier provided lines and covers an extended geographical area.

Wander

Long term variations of amplitude frequency components (below 10 Hz) of a digital signal from their ideal position in time possibly resulting in buffer problems at a receiver.

Wavelength Interchange

The ability to change the wavelength associated with an STM-N signal into another wavelength.

WDCS

Wideband Digital Cross-Connect System

WDM (Wavelength Division Multiplexing)

A means of increasing the information-carrying capacity of an optical fiber by simultaneously transmitting signals at different wavelengths.

Wideband Communications

Voice, data, and/or video communication at digital rates from 64 kbit/s to 2 Mbit/s.

Working

Label attached to a physical entity. In case of revertive switching the working line or unit is the entity that is carrying service under normal operation. In case of nonrevertive switching the label has no particular meaning.

Working State

The working unit is currently considered active by the system and that it is carrying traffic.

WRT (Wait to Restore Time)

Corresponds to the time to wait before switching back after a failure has cleared, in a revertive protection scheme. This can be between 0 and 15 minutes, in increments of one minute.

WS

Work Station

WTR (Wait to Restore)

Applies to revertive switching operation. The protection group enters the WTR state when all Equipment Fail (EF) conditions are cleared, but the system has not yet reverted back to its working line. The protection group remains in the WTR state until the Wait-to-Restore timer completes the WTR time interval.

X X.25

An ITU standard defining the connection between a terminal and a public packet-switched network

X.25 Interface/Protocol

The ITU packet-switched interface standard for terminal access that specifies three protocol layers: physical, link, and packet for connection to a packet-switched data network.

XC

Cross Connect

Z Zero Code Suppression

A technique used to reduce the number of consecutive zeros in a line-coded signal (B3ZS, B8ZS).



Index

Symbols

(Multiplex Section Shared
Protection Ring
(MS-SPRing), [15-5](#)

Numerics

1-way cross-connection,
[7-18](#) [18-4](#)

2-way cross-connection,
[7-18](#) [18-4](#)

- A** ABN LED, [16-39](#)
- Abnormal conditions,
[16-39](#)
- Access identifier, [15-8](#)
- Access identifier (AID)
 Overview of AIDs, [15-9](#)
- Access Identifiers (AID),
[18-7](#)
- Access privileges, [13-6](#)
- Access privileges; User
 access privileges, [13-2](#)
- Acknowledged Information
Transfer Service (AITS),
[14-29](#)
- ACO
 button, [16-40](#)
- ACO button, [16-40](#)

ACO LED, [16-39](#)

Activity LED, [16-44](#)

Adaptive-rate tributary
operation, [19-6](#) [19-19](#)

Adjacencies, [14-35](#)

ADM-16/1, [14-26](#)

Affect-on-service attribute,
[16-23](#)

AFI Authority and Format
Identifier, [14-20](#)

AID, [15-8](#)

Alarm, [16-3](#)

Alarm acknowledgment,
[16-40](#)

Alarm category, [5-8](#)

Alarm cut-off, [16-40](#)

Alarm format, [16-10](#) [16-12](#)

Alarm history, [5-9](#) [5-9](#)

Alarm indicators, [16-19](#)

Alarm LEDs, [16-39](#)

Alarm level, [5-5](#)

Alarm list, [5-3](#)

Alarm log, [5-9](#) [13-10](#)
[13-12](#) [13-12](#)

Alarm notification, [5-41](#)
[16-3](#) [16-22](#)

Alarm notifications
(ALARMS), [13-8](#)

Alarm presentation formats,
[16-9](#)

Alarm severities, [16-40](#)

 SDH format, [16-10](#)
 [16-12](#)

 SONET format, [16-10](#)
 [16-12](#)

Alarm severity, [16-22](#)

Alarm severity assignment
profile, [16-9](#) [16-12](#)

Alarm severity assignment
profile (ASAP), [4-7](#) [4-9](#)
[4-28](#) [5-15](#) [5-18](#) [5-21](#)
[5-26](#) [5-31](#) [5-36](#)

Alarm Severity Assignment
Profile (ASAP), [7-38](#)
[7-48](#) [15-13](#) [15-14](#) [16-25](#)

Alarm severity assignment
profile (ASAP)
 ASAP types, [16-26](#)

Automatic Protection
Switch, [16-27](#)

Basic ASAP variants,
[16-25](#)

BLSR/MS SPRing
Protection Switch,
[16-27](#)

DCN, [16-28](#)

- Default ASAP, [16-26](#)
 - Equipment with
 - SA/NSA, [16-29](#)
 - Equipment without
 - SA/NSA, [16-28](#)
 - Ethernet, [16-30](#)
 - MSA/NIM, [16-30](#)
 - Path Protection
 - SNCP_UPSR, [16-30](#)
 - Path terminating SDH, [16-31](#)
 - Port, [16-31](#)
 - System Timing, [16-32](#)
 - Alarm signalling, [16-17](#)
 - Alarm status, [4-49](#) [7-34](#) [7-37](#)
 - Alarm status display, [5-3](#) [5-8](#) [16-19](#)
 - Alarm test, [16-42](#)
 - Alarm type
 - See: Alarm category
 - Anomaly, [16-3](#)
 - Antistatic covers, [1-24](#)
 - Area address, [3-6](#) [3-13](#) [3-13](#) [3-28](#) [3-32](#) [3-47](#) [14-20](#) [14-22](#) [14-32](#)
 - Area identifier, [14-6](#) [14-20](#)
 - ASAP
 - See: Alarm severity assignment profile
 - ASAP Alarm Severity Assignment Profile, [15-14](#) [16-25](#)
 - ASAP name, [5-18](#) [16-32](#)
 - Authority and Format Identifier (AFI), [14-20](#)
 - Authorization level, [13-2](#) [13-6](#)
 - Auto-Learn NSAP function, [3-12](#)
 - Automatic Protection Switch, [15-5](#)
 - Automatic Protection Switch (APS), [18-18](#)
 - Automatic Protection Switching (APS), [7-34](#) [7-46](#) [7-56](#) [8-2](#) [18-12](#)
 - Autonomous alarm forwarding, [5-41](#) [16-22](#)
 - Autoprovisioning, [15-2](#)
-
- B**
- B1 byte, [19-4](#)
 - B2 bytes, [19-4](#)
 - B3 byte, [19-4](#)
 - Barred-hand symbol, [1-18](#)
 - BCH-2 algorithm, [16-36](#)
 - Bell symbol, [16-19](#)
 - Bidirectional cross-connection, [18-4](#)
 - Bidirectional Line Switched Ring, [15-5](#)
 - Bidirectional Line Switched Ring (BLSR), [18-12](#)
 - Bidirectional Line Switched Rings (BLSR), [18-20](#)
 - Bidirectional Line-Switched Ring (BLSR), [7-37](#) [7-49](#) [7-56](#) [8-4](#)
 - Bidirectional Sub-Network Connection Protection (SNCP), [18-4](#)
 - BIP
 - See: Bit-interleaved parity
-
- C**
- Central office alarm facility, [16-49](#)
 - Change your password, [2-20](#) [2-23](#) [2-25](#)
 - Characters allowed in a password, [13-5](#)
 - Characters allowed in a TID, [3-3](#) [3-24](#) [14-37](#)
 - Characters allowed in a user login, [13-5](#)
 - Circuit pack alarm indicator, [16-19](#)
 - Circuit pack provisioning, [15-5](#) [15-14](#)
 - Circuit pack status indications; Status indications, [16-45](#) [16-45](#)
 - circuit packs, [15-7](#)
 - CIT connector, [16-40](#)
 - Clear validation time, [16-3](#)
 - Climatic conditions, [1-25](#)
 - CLNP PDU lifetime, [3-6](#) [3-28](#) [3-32](#)
 - Clock protection, [6-13](#) [6-15](#)
 - Code violations, [19-4](#) [19-4](#) [19-6](#) [19-8](#)
 - Color scheme, [16-20](#)

CompactFlash™ card, [20-2](#)

Compound AID, [15-9](#)

Configure DCC terminations, [3-41](#)

Connection types, [18-3](#)

Connectionless Network Protocol (CLNP), [14-3](#) [14-35](#)

Connectionless Network Service (CLNS), [14-35](#)

Connector types, [1-14](#)

Consequent actions, [16-3](#)

Conventions, [xix](#)

Correlated fault cause, [16-3](#)

Correlation, [16-3](#)

Cost of a route, [14-30](#)

Create new components, [15-5](#)

Creating new cross-connections, [18-7](#)

Critical alarm, [16-39](#)

Cross-connection, [7-3](#) [7-8](#)

 Bidirectional, [18-3](#)

 Broadcast, [18-3](#)

 Unidirectional, [18-3](#)

Cross-connection level, [18-5](#)

Cross-connection wizard, [7-16](#) [7-21](#) [7-23](#) [7-26](#) [7-29](#) [7-52](#) [18-6](#)

customer comment form; commenting, [xxii](#)

D Danger classification, [1-4](#)

Data communication channel (DCC), [7-51](#)

Data Communication Channel (DCC), [14-2](#) [14-2](#) [14-24](#)

Data Communication Network (DCN), [3-6](#) [14-2](#) [14-24](#)

Database changes (DBCHG), [13-8](#)

DCC channels, [3-39](#)

DCC controller, [14-3](#) [14-5](#) [14-23](#) [14-24](#)

DCC protection switching, [14-26](#)

DCC provisioned state, [14-26](#)

DCC termination, [14-24](#)

DCC-M Multiplex Section Data Communication Channel, [14-24](#) [14-26](#)

DCC-R Regenerator Section Data Communication Channel, [14-24](#)

Default ASAP, [5-26](#)

Default user, [13-7](#)

Defect, [16-3](#)

DFI DSP Format Identifier, [14-20](#)

Disabling of DCCs, [14-28](#)

Document conventions, [xix](#)

documentation

 numbers, [xx](#)

 set; manuals, [xx](#)

Domain Specific Part (DSP), [14-20](#)

Download of configuration data, [4-2](#)

DSP Format Identifier (DFI), [14-20](#)

E Electrostatic discharge, [1-18](#) [1-24](#) [1-26](#) [1-32](#) [1-37](#)

Electrostatic protection, [1-18](#)

Enabling of DCCs, [14-28](#)

End System (ES), [14-3](#)

End System Configuration Timer (ESCT), [3-13](#) [14-4](#)

Enter/Exit Maintenance Condition, [3-3](#) [3-3](#)

Equipment protection, [4-49](#) [15-18](#)

 Cross-connection and timing generator circuit pack, [15-18](#)

 Power supply, [15-18](#)

Equipment provisioning, [15-2](#)

Errored seconds, [19-6](#) [19-8](#)

ES-Hellos (ESHs), [3-13](#) [14-4](#)

ES-IS protocol, [14-3](#) [14-35](#)

ESD

 See: Electrostatic discharge

ESP

 See: Electrostatic protection

ESP bonding point, [1-18](#)

Ethernet, [14-3](#)

External timing input port, [6-3](#) [6-6](#) [6-27](#) [6-29](#)

External timing output port, [6-3](#) [6-7](#) [6-19](#) [6-23](#)

F Failure, [16-3](#)
 Far-end performance parameters, [19-8](#)
 Fault, [16-3](#)
 Fault LED, [16-44](#)
 Fault management, [4-28](#)
 Fault management process, [16-3](#)
 FDA/CDRH laser classification, [1-12](#) [1-16](#)
 FDA/CDRH Regulations, [1-15](#)
 FE ACTY LED, [16-39](#)
 FEC
 See: Forward Error Correction
 File Transfer, Access and Management (FTAM), [14-17](#)
 Flash disk, [20-2](#)
 Forced switch, [4-50](#) [7-36](#) [7-38](#) [7-41](#)
 Forced Switch, [7-56](#)
 Forced switch, [8-2](#) [8-5](#) [8-6](#) [18-17](#)
 Forced switch to holdover mode, [6-37](#)
 Forward error correction (FEC), [4-22](#)
 Forward Error Correction (FEC), [5-31](#) [5-36](#) [16-35](#) [19-18](#)
 Free running mode, [17-2](#)
 Functional category, [13-6](#)

G Gateway network element (GNE), [14-2](#)
 General user, [13-7](#)
 Gigabit Ethernet, [15-16](#)
 GNE Gateway network element, [14-2](#)
 Graphical user interface
 Elements of the ~, [22-15](#)

H Handling windows, [22-27](#)
 Hazard level, [1-17](#)
 Hierarchical routing, [14-6](#)
 History alarms, [5-9](#)
 History logs, [13-10](#) [13-12](#)
 Holdover mode, [6-33](#) [6-37](#) [17-2](#) [17-6](#)

I
 IDI Initial Domain Identifier, [14-20](#)
 IEC laser classification, [1-12](#) [1-16](#)
 IEC Requirements, [1-15](#)
 IEEE 802.3 MAC address, [3-18](#) [14-20](#)
 IEEE 8023 MAC address, [14-33](#)
 In-band FEC, [5-31](#) [5-31](#) [5-36](#) [5-36](#) [16-35](#) [19-18](#)
 Initial Domain Identifier (IDI), [14-20](#)
 Initial Domain Part (IDP), [14-20](#)
 Initial provisioning, [4-3](#)

Initial software download, [20-3](#)
 Initialization, [16-45](#)
 Insertion and removal facilities, [1-18](#)
 Insertion of circuit packs, [16-45](#)
 Intermediate System (IS), [3-6](#) [3-28](#) [14-3](#)
 Intermediate System Configuration Timer (ISCT), [14-4](#)
 Interworking, [18-5](#)
 Intraoffice LAN (IAO-LAN), [3-6](#) [3-28](#) [3-29](#)
 Invisible laser radiation, [1-29](#) [1-31](#) [1-36](#)
 IS routing capability, [3-34](#)
 IS-Hellos (ISHs), [14-4](#)
 IS-IS area-divided DCN, [14-8](#)
 IS-IS protocol, [14-3](#) [14-4](#) [14-35](#)
 ISO-DCC NSAP address format, [3-26](#) [14-20](#) [14-20](#)
 ISO-OSI network protocols, [14-3](#)

K K1/K2 byte protocol, [7-35](#)

L L1-LSP, [14-4](#)
 L2-LSP, [14-4](#)
LambdaUnite™ CIT NE Alarm Log, [5-9](#)
 LAN connectors, [14-31](#)
 LAN I/O-Panel, [14-31](#)

LAN Router Priority, [3-32](#)
 LAPD channels, [14-24](#)
 LAPD protocol, [14-3](#)
 Laser classes, [1-12](#)
 Laser safety instructions, [1-12](#)
 Laser warning labels, [1-26](#)
[1-31](#)
 LCN Local Communication Network, [14-2](#)
 LDB entry timer, [3-17](#)
[14-36](#)
 LDB flush timer, [3-17](#)
[14-36](#)
 LDB Loop detection buffer, [3-15](#) [14-36](#)
 LED TEST button, [5-14](#)
[16-40](#) [16-41](#)
 Level-1 Intermediate System, [14-6](#)
 level-2 Intermediate System, [14-6](#)
 Level-2 subdomain, [14-6](#)
 Line DCC, [14-24](#)
 Line timing, [6-12](#)
 Link Metric, [3-32](#)
 Link State Protocol Data Unit (LSP), [14-4](#)
 List of current alarms, [5-3](#)
[5-5](#) [16-20](#)
 List of history alarms, [5-9](#)
 Local Communication Network (LCN), [14-2](#)
 Locked mode, [17-2](#)
 Lockout of protection, [7-35](#) [7-38](#) [7-41](#) [8-2](#) [8-5](#)
[8-6](#)

Logging Out NE User, [2-15](#)
 Login, [13-2](#)
 Network element, [22-33](#)
 Loop detection buffer (LDB), [14-36](#)
 LSP database, [14-5](#)

M Maintenance user, [13-7](#)
 Maintenance-oriented performance monitoring, [19-2](#)
 Major alarm, [16-39](#)
 Management interfaces for alarm signalling, [16-17](#)
 Manual switch, [4-50](#) [7-36](#)
 [7-38](#) [7-41](#) [8-2](#) [8-5](#) [8-7](#)
 [18-17](#)
 Master timing generator, [17-2](#)
 Media access protocols, [14-3](#)
 Menu bar, [22-15](#)
 Menu structure overview, [22-37](#) [22-54](#)
 Minor alarm, [16-39](#)
 Modifying User ID Lockout parameters, [2-28](#)
 [2-30](#) [2-33](#) [2-45](#)
 MS-SPRing Multiplex Section - Shared Protection Ring, [14-26](#)
 MS-SPRing protection group, [14-26](#)
 Multibit FEC, [16-35](#)
 Multiplex Section - Shared Protection Ring (MS-SPRing), [14-26](#)

Multiplex Section Data Communication Channel (DCC-M), [14-24](#) [14-26](#)
 Multiplex Section Protection (MSP), [7-34](#)
[7-46](#) [7-56](#) [8-2](#) [15-5](#)
[18-12](#) [18-18](#)
 Multiplex Section Shared Protection Ring (MS-SPRing), [7-37](#) [7-49](#)
[7-56](#) [8-4](#) [18-12](#)
 2-fiber MS-SPRing, [18-20](#)

N Name/Address List, [3-18](#)
 [14-32](#)
 NE ACTY LED, [16-39](#)
 NE alarm list, [5-3](#)
 NE alarm list; Alarm list, [16-20](#)
 NE alarm log, [5-9](#)
 NE configuration data, [20-2](#)
 NE name, [3-18](#) [3-28](#) [14-3](#)
 [14-37](#)
 NE selection and login, [22-33](#)
 NE software, [20-2](#)
 NE User, [2-15](#)
 Near-end performance parameters, [19-6](#)
 Network Entity Title (NET), [3-47](#) [3-47](#) [14-22](#)
 Network Service Access Point (NSAP), [14-19](#)
 Network Service Access Point (NSAP); NSAP address, [3-28](#) [14-3](#)
 Nominal voltage, [1-29](#)

Non-reporting ASAP, [5-21](#),
[5-26](#) [16-33](#)

Non-revertive mode, [7-55](#)
[15-18](#) [18-19](#)

Non-volatile memory
(NVM), [4-1](#)

Nonvolatile memory
(NVM), [20-2](#)

Notification log, [13-10](#)

Notification registration
list, [13-12](#)

NSAP address, [3-12](#) [3-23](#)
[3-28](#) [3-32](#) [3-34](#) [14-19](#)
[14-32](#)

NSAP address format,
[3-26](#) [14-20](#) [14-20](#)

NSAP Network Service
Access Point, [14-19](#)

NVM Nonvolatile memory,
[20-2](#)

O Office alarm interfaces,
[16-48](#)

Operator identifier, [14-20](#)

Optical Channel, [16-35](#)

Optical circuit pack
specifications, [1-14](#)

Optical interfaces, [18-4](#)

Optical port provisioning,
[15-15](#)

Optical signal-to-noise
ratio (OSNR), [16-35](#)

Organization identifier
(ORG), [14-20](#)

OSI Neighbor Map, [14-5](#)

OSI network protocol, [14-3](#)

OSI protocol stack, [14-16](#)
[14-24](#)

OSI Routing Map, [14-5](#)

OSI-DCN, [14-2](#)

OSNR
See: Optical
signal-to-noise ratio

Out-of-band FEC, [5-31](#)
[5-31](#) [5-36](#) [5-36](#) [16-35](#)
[19-18](#)

Output mode, [18-5](#)

Output timing reference,
[6-17](#)

P Packaging, [1-24](#)

Password, [2-17](#) [2-18](#) [13-2](#)
[13-5](#)

Path protection, [18-12](#)

PDP
See: Power Distribution
Panel

Performance monitoring,
[19-1](#)

Performance monitoring
points, [19-6](#)

Persistency check, [16-3](#)

Point-to-point
cross-connection, [7-18](#)
[18-4](#)

Point-to-point LAN bridge
promiscuous mode, [15-17](#)

Port monitoring mode,
[16-34](#)

Port unit LED, [16-19](#)

port units, [15-7](#)

Power Distribution Panel
(PDP), [1-29](#) [1-31](#) [1-36](#)

Powering-up, [16-45](#)

Preconditions for disabling
a DCC, [3-39](#)

Preconditions for enabling
a DCC, [3-39](#)

Priority level, [2-5](#) [13-7](#)

Privileged user, [13-7](#)

Protection configurations,
[18-24](#)

Protection group, [7-32](#)
[7-37](#) [7-56](#) [15-5](#)

Protection group
provsioning, [15-5](#)

Protection mechanisms,
[18-12](#)

Protection section, [18-18](#)

Protection switch activity
log, [13-10](#) [13-12](#) [13-12](#)

Protection switching
changes (PSCHG), [13-8](#)

protection, timing, [17-4](#)

Protocol stacks, [14-17](#)

provisioning, timing, [17-5](#)

Pushbutton, [22-30](#)

PWR ON LED, [16-39](#)
[16-41](#)

Q Q-LAN, [14-2](#)

Quality-of-service-oriented
performance monitoring,
[19-2](#)

R Rack alarm facility, [16-48](#)

Rack alarm interface, [16-48](#)

Raise validation time, [16-3](#)

RD Routing Domain, [14-20](#)

RDI
See: Remote Defect
Indication

Reed-Solomon code, [16-36](#)

reference signals, [17-4](#)

Refresh button, [5-8](#)

Regenerator Section Data
Communication Channel
(DCC-R), [14-24](#)

Registration list, [13-7](#)

REI
See: Remote Error
Indication

Remote Defect Indication,
[19-8](#)

Remote Error Indication,
[19-8](#)

Remote Error Indication
(REI), [19-4](#) [19-4](#)

Remote Failure Indication,
[19-8](#)

Reports only (user), [13-7](#)

Reserved portion of the
NSAP, [14-20](#)

Revertive mode, [7-55](#) [17-9](#)

RFI
See: Remote Failure
Indication

Ring map, [8-4](#)

Ring-to-ring UPSR/SNCP,
[18-15](#)

Rolling a cross-connection,
[7-23](#)

Routing Domain (RD),
[14-20](#)

Routing Information Base
(RIB), [14-4](#)

Routing metric, [14-30](#)

Routing table, [14-33](#)

Routing tables, [14-5](#)

RS(255,239), [16-36](#)

S Safety of laser products,
[1-15](#) [1-15](#)

SDH management network,
[14-2](#)

SDH performance
monitoring, [19-4](#) [19-4](#)

SDH performance
parameters, [19-10](#)

SDH tributary AIDs, [5-10](#)

SDH tributary numbering
format, [16-14](#)

Section DCC, [14-24](#)

Security administrator, [13-3](#)

Security database, [13-2](#)
[13-3](#)

Selector, [14-20](#)

Self healing rings, [18-21](#)

Self-test, [16-45](#)

SES threshold, [19-9](#)

Severely errored seconds,
[19-6](#) [19-8](#)

Shelf, [4-7](#) [15-6](#)

Shelf layout, [15-6](#)

Shelf provisioning, [15-13](#)

Shortest path first
algorithm, [14-4](#) [14-6](#)
[14-30](#)

Signal Degrade, [7-36](#) [7-36](#)
[7-41](#)

Signal Fail, [7-36](#) [7-36](#)
[7-41](#)

Single-ring UPSR/SNCP,
[18-14](#)

Slave timing generator,
[17-2](#)

Slot provisioning, [15-14](#)

Software download, [14-17](#)
[16-45](#) [20-3](#)

SONET performance
monitoring, [19-4](#) [19-4](#)

SONET performance
parameters, [19-11](#)

SONET tributary
numbering format, [16-14](#)

Standards Compliance,
[1-15](#)

State changes, [16-22](#)

State changes (STCHG),
[13-8](#)

Static routing table, [14-33](#)

Static routing table;
Routing table, [3-3](#) [3-6](#)
[3-18](#) [3-18](#) [14-32](#)

Station alarm interface,
[16-49](#)

Status bar, [22-15](#)

Status indications, [16-45](#)

Strong FEC, [16-35](#)

Sub-Network Connection
Protection, [7-18](#)

Sub-Network Connection
Protection (SNCP), [7-3](#)
[7-8](#) [7-40](#) [7-52](#) [8-6](#)
[18-12](#) [18-13](#)

Subsystem, [16-8](#)

Super user, [13-6](#) [13-7](#)

Switch circuit pack, [4-50](#)

Switch request, [4-49](#) [7-35](#)

Switch request state, [7-35](#)
[7-38](#) [7-41](#)

Switching an MSP, [8-2](#)

Switching APS, [8-2](#)

Synchronization Status
Marker (SSM), [6-9](#) [17-5](#)

System, [4-4](#)
System controller, [20-2](#)
System identifier, [14-20](#)
System reset, [3-3](#)
System timing, [6-3](#) [6-15](#)
[6-15](#) [6-34](#)
System timing reference,
[6-15](#) [6-17](#)

T Target identifier (TID), [3-3](#)
[3-28](#) [14-3](#) [14-32](#) [14-37](#)
Target Identifier (TID),
[18-10](#)
TARP Data Cache (TDC),
[14-33](#) [14-35](#)
TARP manual adjacencies;
Manual adjacencies, [3-47](#)
[14-35](#)
TARP originator
functionality, [3-17](#) [14-33](#)
TARP PDU lifetime, [14-33](#)
TARP PDU types, [14-33](#)
TARP propagation
functionality, [3-44](#)
TARP responder
functionality, [3-44](#) [14-33](#)
TID Address Resolution
Protocol (TARP), [14-20](#)
[14-32](#) [14-33](#)
TID to NSAP address
translation; Name to
address translation, [14-32](#)
TID/NSAP address pair,
[3-23](#)
timing, [17-5](#)
Timing circuit pack, [4-50](#)
Timing configuration, [6-3](#)
[17-3](#)

Timing generator, [6-33](#)
[17-2](#)
Timing input format, [6-6](#)
Timing marker, [17-5](#)
Timing modes, [17-2](#)
Timing protection, [17-8](#)
Timing provisioning, [17-1](#)
Timing quality, [17-4](#)
Timing reference, [6-3](#)
[6-12](#) [6-39](#)
Timing reference protection
switching, [17-8](#)
Timing references, [6-31](#)
Title bar, [22-15](#)
Tool bar, [22-15](#)
Transmission interfaces,
[18-4](#)
Tributary numbering
format, [16-14](#)
Tributary provisioning,
[15-15](#)

U Unacknowledged
Information Transfer
Service (UITs), [14-29](#)
Unavailability period
(UAP), [19-6](#) [19-8](#)
Undivided DCN, [14-8](#)
Unidirectional Path
Switched Ring (UPSR),
[18-4](#) [18-12](#)
Unidirectional
cross-connection, [18-4](#)
Unidirectional Path
Switched Rings (UPSR),
[18-13](#)

Unidirectional
Path-Switched Ring
(UPSR), [7-3](#) [7-8](#) [7-40](#)
[8-6](#)
Unidirectional MSP, [7-34](#)
Update Alarms button, [5-8](#)
[16-19](#)
Updating the alarm list, [5-8](#)
User interface
Elements of the ~,
[22-15](#)
User log, [13-10](#)
User login, [2-1](#) [2-3](#) [2-17](#)
[2-18](#) [13-4](#) [13-5](#)
User panel, [5-14](#)
User panel alarm LEDs,
[16-40](#)
User privilege code, [13-6](#)
User privilege codes, [2-5](#)
User provisioning, [2-15](#)
[2-17](#) [2-18](#)
User type, [2-5](#)
User types, [13-7](#)
User types; Predefined user
types, [13-7](#)
User-Network Side MSect
Failure, [3-36](#)
User-Network Side RSect
Failure, [3-36](#)

V Validation, [16-3](#)
View DCC terminations,
[3-39](#)
Virtual Concatenation,
[15-16](#)

W Wait-to-restore time
 (WTR), [6-15](#) [7-38](#) [7-41](#)
 [17-9](#)

WaveStar[®] CIT NE Alarm
List, [5-3](#)

WaveStar CITNE Alarm
List, [5-5](#)

Window handling, [22-27](#)

Working port, [3-40](#)

Working section, [18-18](#)

