



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

Release 2.1

User Operations Guide

365-374-070
CC109192542
Issue a
April 2002



Copyright © 2002 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.

Lucent Learning WO +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:

ANSI is a registered trademark of American National Standards Institute, Inc.

CompactFlash is a trademark of SanDisk Corporation

LambdaUnite is a trademark of Lucent Technologies.

Navis is a trademark of Lucent Technologies.

SanDisk is a registered trademark of SanDisk Corporation

WaveStar is a registered trademark of Lucent Technologies.

Windows is a registered trademark of Microsoft Corporation

Ordering information

The order number of this document is 365-374-070 (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.



Contents

About this information product

<u>Purpose</u>	<u>xxi</u>
<u>Reason for reissue</u>	<u>xxi</u>
<u>Safety labels</u>	<u>xxi</u>
<u>Conventions used</u>	<u>xxiii</u>
<u>Related documentation</u>	<u>xxv</u>
<u>Related training</u>	<u>xxvi</u>
<u>Documented feature set</u>	<u>xxvii</u>
<u>How to comment</u>	<u>xxvii</u>

1 Safety

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

Optical circuit pack specifications	1-14
Laser product classification	1-16
Electrostatic discharge	1-20
Safety requirements in specific deployment phases	
Overview	1-22
Transportation	1-23
Storage	1-26
Installation	1-28
Taking into operation	1-31
Operation and maintenance	1-33
Taking out of operation	1-39

2 Security administration

Overview	2-1
Administering user logins	
Overview	2-3
Creating a user login	2-5
Modifying a user login	2-10
Deleting a user login	2-12
Disabling user logins	2-13
Enabling user logins	2-15
Logging out NE users	2-17
Supporting information for “Administering user logins”	2-19
Changing super user IDs	
Overview	2-22

Changing super user IDs on the WaveStar® CIT	2-23

Changing user passwords

Overview	2-25

Changing the user password on the WaveStar® CIT	2-26

Changing the user password on the NE	2-28

Modifying user security parameters

Overview	2-30

Modifying a user's own notification list	2-31

Modifying user security parameters by admin	2-33

Provision global security parameters	2-35

Retrieving security information

Overview	2-37

Displaying a list of all users logged into an NE	2-38

Displaying login information for an NE	2-40

Retrieve system wide security parameters	2-42

Retrieve security info of own user	2-44

Retrieve security info of other users	2-46

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	3-11

Supporting information for “Configuring the basic DCN parameters for the WaveStar® CIT”	3-14

Configuring the LDB timers for the WaveStar® CIT	3-16

<u>Supporting information for “Configuring the LDB timers for the WaveStar® CIT”</u>	<u>3-18</u>
<u>Administering the address list at the WaveStar® CIT</u>	<u>3-19</u>
<u>Supporting information for “Administering the address list at the WaveStar® CIT”</u>	<u>3-23</u>
<u>Configuring the basic DCN parameters for an NE</u>	<u>3-28</u>
<u>Supporting information on the “LAN Management” tab</u>	<u>3-35</u>
<u>Supporting information on the “Network Layer” tab</u>	<u>3-37</u>
<u>Configuring a NE as T-TD Gateway</u>	<u>3-39</u>
<u>Supporting information on the “TCP/IP Gateway” tab</u>	<u>3-44</u>
<u>Configuring an NE as FTAM-FTP Gateway</u>	<u>3-47</u>
<u>Provisioning OSI nodes</u>	<u>3-50</u>
<u>Supporting information on the “OSI Nodes” tab</u>	<u>3-54</u>
<u>Configuring data communication channels</u>	<u>3-57</u>
<u>Supporting information for “Configuring data communication channels”</u>	<u>3-60</u>
<u>Supporting information on the “View DCC Terminations” window</u>	<u>3-61</u>
<u>Supporting information on the “Configure DCC Terminations” window</u>	<u>3-63</u>
<u>Configuring the TARP parameters for an NE</u>	<u>3-65</u>
<u>Supporting information on the “TARP” tab of the “Data Communications” window</u>	<u>3-68</u>
<u>Assigning TARP manual adjacencies</u>	<u>3-69</u>
<u>Supporting information on the “TARP Manual Adj.” tab of the “Data Communications” window</u>	<u>3-73</u>
<u>Viewing MAC Addresses</u>	<u>3-74</u>

4 Equipment provisioning

<u>Overview</u>	<u>4-1</u>
<u>Initial equipment provisioning – overview procedure</u>	<u>4-4</u>
<u>Configuring the basic system parameters</u>	<u>4-5</u>
<u>Viewing equipment details of the system</u>	<u>4-10</u>
<u>Equipment details of the system</u>	<u>4-12</u>
<u>Configuring the shelf</u>	<u>4-14</u>
<u>Viewing equipment details of the backplane</u>	<u>4-16</u>
<u>Equipment details of the backplane</u>	<u>4-18</u>
<u>Viewing equipment details of the CI-CTL</u>	<u>4-20</u>
<u>Equipment details of the CI-CTL</u>	<u>4-22</u>
<u>Viewing equipment details of the user panel</u>	<u>4-24</u>
<u>Equipment details of the user panel</u>	<u>4-26</u>
<u>Viewing equipment details of a Timing Interface</u>	<u>4-28</u>
<u>Equipment details of a Timing Interface</u>	<u>4-30</u>
<u>Viewing equipment details of a Power Interface</u>	<u>4-32</u>
<u>Equipment details of a Power Interface</u>	<u>4-34</u>
<u>Viewing equipment details of the fan unit</u>	<u>4-36</u>
<u>Equipment details of the fan unit</u>	<u>4-38</u>
<u>Provisioning a slot</u>	<u>4-39</u>
<u>Preprovisioning a circuit pack</u>	<u>4-42</u>
<u>Provisioning a circuit pack</u>	<u>4-44</u>
<u>Reassigning a circuit pack</u>	<u>4-46</u>
<u>Configuring an optical SDH/SONET port</u>	<u>4-49</u>

<u>Configuring an optical SDH/SONET port</u>	<u>4-52</u>
<u>Viewing equipment details of an optical SDH/SONET port</u>	<u>4-72</u>
<u>Equipment details of an optical SDH/SONET port</u>	<u>4-74</u>
<u>Configuring an Ethernet port</u>	<u>4-81</u>
<u>Ethernet port parameters”</u>	<u>4-86</u>
<u>Configuring a VCG port</u>	<u>4-88</u>
<u>VCG port parameters</u>	<u>4-91</u>
<u>Configuring a tributary</u>	<u>4-92</u>
<u>Removing equipment from the system</u>	<u>4-94</u>
<u>Viewing an equipment protection group</u>	<u>4-96</u>
<u>Parameters for a 1+1 equipment protection</u>	<u>4-98</u>
<u>Protection Switch (1+1 Equipment)</u>	<u>4-99</u>
<u>Switching a 1+1 equipment protection</u>	<u>4-100</u>
<u>Retrieving an equipment list</u>	<u>4-102</u>
<u>Equipment list of a circuit pack/backplane</u>	<u>4-107</u>
<u>Equipment list of the shelf</u>	<u>4-108</u>
<u>Equipment list of a port</u>	<u>4-109</u>
<u>Equipment list of a virtual concatenation group (VCG)</u>	<u>4-111</u>
<u>Equipment list of a tributary</u>	<u>4-113</u>
<u>Equipment list of the Miscellaneous Discretes</u>	<u>4-114</u>
<u>Configuring Miscellaneous Discrete Outputs</u>	<u>4-115</u>
<u>Activating or deactivating Miscellaneous Discrete Outputs manually</u>	<u>4-117</u>
<u>Replacing an XC320 circuit pack by an XC320/A circuit pack</u>	<u>4-119</u>

5 Alarm management

Overview	5-1
Setting the view preferences	5-3
Retrieving the WaveStar® CIT NE Alarm List	5-6
The WaveStar® CIT NE Alarm List	5-8
Retrieving the WaveStar® CIT NE Alarm Log	5-12
The WaveStar® CIT NE Alarm Log	5-14
Identifying SDH tributaries in alarm messages	5-19
Performing an LED test	5-23
Retrieving Alarm Severity Assignment Profile (ASAP) information	5-24
Creating a new Alarm Severity Assignment Profile (ASAP)	5-27
Creating non-reporting Alarm Severity Assignment Profiles (ASAPs)	5-29
Modifying an existing Alarm Severity Assignment Profile (ASAP)	5-31
Deleting an Alarm Severity Assignment Profile (ASAP)	5-34
Assigning the same Alarm Severity Assignment Profile (ASAP) to all equipment components of a particular type	5-36
Setting the port monitoring mode	5-39
Configuring fault management parameters of an SDH/SONET port	5-41
Enabling or disabling autonomous alarm forwarding	5-46
Configuring Miscellaneous Discrete Inputs	5-48

6 Timing provisioning

Overview	6-1
Viewing the timing configuration	6-3
Synchronisation characteristics – External timing input ports	6-5

Synchronisation characteristics – External timing output ports	6-7
Synchronisation characteristics – Line timing references	6-13
Synchronisation characteristics – External timing references	6-15
Synchronisation characteristics – System timing	6-17
Configuring the external timing output ports (SDH mode)	6-20
Configuring the external timing output ports (SONET mode)	6-25
Configuring the external timing input ports (SDH mode)	6-29
Configuring the external timing input ports (SONET mode)	6-31
Configuring the line timing references	6-33
Configuring the external timing references	6-36
Configuring the system timing	6-39
Switching between different clock modes	6-42
Switching to another timing reference for system timing	6-44
Switching to another timing reference for the external timing output ports	6-47

7 Traffic provisioning

Overview	7-1
Viewing existing cross-connections	7-4
Parameters of the window “View Cross Connections”	7-6
Retrieve Cross-connection Lists	7-10
Supporting information on the “Cross Connection List”	7-12
Substructuring of input and output signals	7-14
Creating a new cross-connection	7-18
Modifying a cross-connection	7-23
Rolling a cross-connection	7-25

<u>Bridging a cross-connection</u>	<u>7-28</u>
<u>Deleting a cross-connection</u>	<u>7-31</u>
<u>Viewing an existing protection group</u>	<u>7-34</u>
<u>Parameters of the window “View Protection” for a 1+1 MSP or APS</u>	<u>7-35</u>
<u>Parameters of the window “View Protection” for a 2-Fiber MS-SPRing or 2-fiber BLSR</u>	<u>7-39</u>
<u>Parameters of the window “View Protection” for a 4-Fiber MS-SPRing or 4-fiber BLSR</u>	<u>7-42</u>
<u>Parameters of the window “View Protection” for SNCP and UPSR</u>	<u>7-46</u>
<u>Parameters of the window “View Protection” for a one way path protection</u>	<u>7-48</u>
<u>Creating a cross-connection in a 2- or 4-fiber MS-SPRing/BLSR network environment</u>	<u>7-50</u>
<u>Creating a new 1+1 MSP or 1+1 APS (NE level)</u>	<u>7-54</u>
<u>Creating a new 2-fiber MS-SPRing or 2-fiber BLSR (NE level)</u>	<u>7-57</u>
<u>Creating a new 4-fiber MS-SPRing or 4-fiber BLSR (NE level)</u>	<u>7-60</u>
<u>Creating an SNCP or UPSR (NE level)</u>	<u>7-63</u>
<u>Creating an unidirectional path protection</u>	<u>7-67</u>
<u>Provisioning path protection parameters</u>	<u>7-71</u>
<u>Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings</u>	<u>7-73</u>
<u>Creating an unidirectional DNI/DRI between two protected rings.</u>	<u>7-77</u>
<u>Creating a bidirectional DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR protected ring</u>	<u>7-86</u>
<u>Creating a bidirectional ring-to-ring SNCP</u>	<u>7-90</u>
<u>Deleting a protection group</u>	<u>7-93</u>
<u>Configuring VCG tributaries</u>	<u>7-95</u>

Retrieving VCG/VCG tributary information	7-97
VCG tributary details	7-99
VCG Port Details	7-105
Retrieving current VCG delay	7-109
Parameters of the window “View VCG Delay”	7-111
Retrieving current VCG tributary maintenance signal	7-113
Parameters of the window “View Current VCG Trib. Maintenance Signal”	7-115

8 Traffic maintenance

Overview	8-1
Switching an MSP or APS	8-3
Supporting information on the “Switching an MSP or APS”	8-5
Switching a 2-fiber MS-SPRing or 2-fiber BLSR	8-7
Supporting information on the “Switching a 2-fiber MS-SPRing or 2-fiber BLSR”	8-9
Switching a 4-fiber MS-SPRing or 4-fiber BLSR	8-11
Supporting information on the “Switching a 4-fiber MS-SPRing or 4-fiber BLSR”	8-13
Switching a DNI, UPSR or SNCP	8-15
Switching a path protection	8-17
Clearing a protection switch request	8-19
Retrieve protection switch reports	8-21
Supporting information on the “BLSR Protection Switch List”	8-22
Supporting information on the “NE Protection Switch Activity Log”	8-23
Retrieving current optical tributary maintenance signal	8-24

	<u>Supporting information on the “View Current Optical Trib. Maintenance Signal”</u>	<u>8-26</u>
	<u>Performing facility loopbacks</u>	<u>8-27</u>
	<u>Releasing a facility loopback</u>	<u>8-30</u>
9	Performance monitoring	
	<u>Overview</u>	<u>9-1</u>
	<u>Enabling or disabling performance monitoring data collection</u>	<u>9-2</u>
	<u>Retrieving performance monitoring settings for individual ports or tributaries</u>	<u>9-5</u>
	<u>Retrieving performance monitoring reports</u>	<u>9-11</u>
10	Software upgrade	
	<u>Overview</u>	<u>10-1</u>
	<u>Performing an initial software download using the CIT</u>	<u>10-2</u>
	<u>Performing a software download for upgrade purposes using the WaveStar® CIT</u>	<u>10-7</u>
	<u>Activating an NE software generic</u>	<u>10-12</u>
	<u>Retrieving NE software generic information</u>	<u>10-14</u>
	<u>Supporting information for “Retrieving NE software generic information”</u>	<u>10-15</u>
11	Database backup	
	<u>Overview</u>	<u>11-1</u>
	<u>Limiting the number of saved backups</u>	<u>11-2</u>
	<u>Manually backup database to the WaveStar® CIT</u>	<u>11-3</u>
	<u>Retrieving NE database information</u>	<u>11-6</u>
	<u>Supporting information for NSAPRetrieving NE database information</u>	<u>11-7</u>

Restoring a database to a network element	11-9

12 Periodic activities

Overview	12-1

Replacing the air filter	12-2

13 Security and administration concepts

Overview	13-1

Security management

Overview	13-2

Security management concept	13-3

User administration

Overview	13-4

User administration concept	13-5

User login and password	13-7

User provisioning	13-10

History logs

Overview	13-19

NE alarm log	13-20

NE protection switch activity log	13-21

14 Management communication setup concepts

Overview	14-1

Basic DCN principles	14-2

DCN configurations	14-6

DCN configuration guidelines	14-14

Partition repair guidelines	14-15
DCN protocols and services	14-19
NSAP address format	14-24
Data communication channels	14-29
LAN access	14-36
Name-to-address translation	14-37
NE name administration	14-41
System provisioning	14-42

15 Equipment provisioning concepts

Overview	15-1
Equipment provisioning and autoprovisioning	15-2
WaveStar[®] CIT methods to perform provisioning	15-4
Provisioning of new components	15-6
Shelf configuration	15-7
Overview of access identifiers	15-9
Shelf provisioning	15-15
Slot provisioning	15-16
Circuit pack provisioning	15-17
Port and tributary provisioning	15-18
XC320 equipment protection	15-19

16 Alarm management concepts

Overview	16-1
<i>LambdaUnite[™]</i> MSS fault management	
Overview	16-3

<u>Basic fault management concepts</u>	<u>16-4</u>
<u><i>LambdaUnite</i>[™] MSS fault management principle</u>	<u>16-7</u>
<i>WaveStar</i>[®] CIT alarm presentation formats	
<u>Overview</u>	<u>16-10</u>
<u>Alarm severities</u>	<u>16-11</u>
<u>Alarm format preferences</u>	<u>16-13</u>
Signalling of alarms	
<u>Overview</u>	<u>16-18</u>
<u><i>WaveStar</i>[®] CIT visual alarm indicators</u>	<u>16-20</u>
<u>NE local indications</u>	<u>16-22</u>
<u>Impact of state changes on the signalling of alarms</u>	<u>16-23</u>
Alarm provisioning	
<u>Overview</u>	<u>16-25</u>
<u>Alarm Severity Assignment Profiles</u>	<u>16-26</u>
<u>Port monitoring mode</u>	<u>16-36</u>
<u>Forward error correction</u>	<u>16-37</u>
Operations interfaces	
<u>Overview</u>	<u>16-40</u>
<u>The <i>LambdaUnite</i>[™] MSS user panel</u>	<u>16-41</u>
<u>ACO interaction with an alarm test</u>	<u>16-44</u>
<u>Circuit pack status indicators</u>	<u>16-46</u>
<u>Fan unit status indicators</u>	<u>16-49</u>
<u>Office alarm interfaces</u>	<u>16-50</u>
<u>Miscellaneous Discretes</u>	<u>16-52</u>

17 Timing provisioning concepts

Overview	17-1
Timing generator	17-3
Timing configuration	17-4
Timing quality	17-5
Timing protection	17-9
Timing with facility loopbacks	17-11
Timing slaved to MSP/APS groups	17-12
4-fiber MS-SPRing/BLSR protection switching	17-13

18 Traffic provisioning concepts

Overview	18-1
Cross-connection management	18-2
Cross-connection wizard	18-7
Protection mechanisms	18-13
Path Protection	18-14
Line Protection	18-19
Ring Protection	18-21
Dual Node Ring Interworking (DNI)/Dual Ring Interworking (DRI) for MS-SPRing or BLSR	18-29
DNI/DRI SNCP or UPSR	18-35
DNI/DRI between MS-SPRing and SNCP or BLSR and UPSR	18-36
Gigabit Ethernet Interface	18-43
Facility loopback	18-49
Protection configurations	18-52

19 Performance monitoring concepts

Overview	19-1
Introduction	19-2
The performance monitoring process	19-5
Performance measurements	19-6
Performance monitoring reports	19-14
Impact of configuration changes on performance monitoring	19-20

20 Software upgrade concepts

Overview	20-1
NE memory concept	20-2
Software download	20-3
Software download for upgrade purposes	20-4

21 Database backup concepts

Overview	21-1
Configuration backup and restoration	21-2
Backup database	21-3
Restore database	21-6

22 WaveStar® CIT Tutorial

Overview	22-1
Basic WaveStar® CIT procedures	
Overview	22-5
Installing the WaveStar® CIT	22-6

<u>WaveStar® CIT login/logout procedure</u>	<u>22-9</u>
Connecting/disconnecting the WaveStar® CIT to/from the NE	
<u>Overview</u>	<u>22-11</u>
<u>Concepts for connecting the WaveStar® CIT to the NE</u>	<u>22-12</u>
<u>Network element selection and login</u>	<u>22-16</u>
<u>Logout from NE(s)</u>	<u>22-27</u>
WaveStar® CIT main window	
<u>Overview</u>	<u>22-29</u>
<u>Elements of the WaveStar® CIT user interface</u>	<u>22-30</u>
<u>Tool bar of the WaveStar® CIT</u>	<u>22-32</u>
<u>NE connection types menu</u>	<u>22-34</u>
<u>Standard window components</u>	<u>22-36</u>
<u>Selection windows</u>	<u>22-41</u>
<u>General window handling</u>	<u>22-45</u>
<u>General pushbuttons</u>	<u>22-48</u>
<u>Basic operations</u>	<u>22-50</u>
<u>Administering NE views</u>	<u>22-51</u>
<u>Overview of the menu structure</u>	<u>22-55</u>
System view	
<u>Overview</u>	<u>22-57</u>
<u>Shelf view</u>	<u>22-58</u>
<u>The ring map</u>	<u>22-68</u>
<u>Graphical view of the ring map</u>	<u>22-70</u>
<u>Overview of the shelf-view menu structure</u>	<u>22-72</u>
<u>Reports and log files</u>	<u>22-80</u>

[View rolling events](#) [22-81](#)

Cut Through view

[Overview](#) [22-82](#)

[Entering the Cut Through view](#) [22-83](#)

[Interactive – Execute TL1 single commands](#) [22-85](#)

[Interactive – Manage a listbox file](#) [22-87](#)

[Working with script files](#) [22-88](#)

[Working with logs](#) [22-90](#)

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 <i>LambdaUnite™</i> MSS.
Reason for reissue	This is the initial version of this guide for <i>LambdaUnite</i> MSS Release 2.1.
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.



Example of a warning about laser radiation.



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.
- **Navis® Optical EMS Provisioning Guide (Application *LambdaUnite* MSS)**

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

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

Document title	Document code A4-format	Document code UL-format
<i>LambdaUnite</i> MSS Applications and Planning Guide	109192484 (365-374-067)	109192534 (365-374-068)
<i>LambdaUnite</i> MSS User Operations Guide	109192492 (365-374-069)	109192542 (365-374-070)
<i>LambdaUnite</i> MSS Alarm Messages and Trouble Clearing Guide	109192468 (365-374-071)	109192476 (365-374-072)
<i>LambdaUnite</i> MSS Installation Guide	109192500 (365-374-073)	109192567 (365-374-074)
<i>LambdaUnite</i> MSS Operations System Engineering Guide (TL1 Reference Manual)	109192518 (365-374-075)	109192583 (365-374-076)
<i>Navis Optical EMS Provisioning Guide</i> (Application <i>LambdaUnite</i> MSS)	109192443 (365-374-077)	109192450 (365-374-078)
<i>LambdaUnite</i> MSS Safety Guide	109192617 (365-374-079)	109192625 (365-374-080)
CD-ROM Documentation <i>LambdaUnite</i> MSS (all manuals on one CD-ROM)	109192526 (365-374-081)	

Related training For detailed information about the training courses that are related to the *LambdaUnite* MultiService Switch (MSS) please refer to the *LambdaUnite* MSS Applications and Planning Guide, chapter 8 ***Product support - Training courses.***

Documented feature set This manual describes *LambdaUnite* MSS release 2.1. 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 To comment on this information product online, go to <http://www.lucent-info.com/comments> or email your comments to ctiphotline@lucent.com (<mailto:ctiphotline@lucent.com>).

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

You can also send or fax comments about this document to:

Lucent Technologies Network Systems GmbH

Lucent Learning WO

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

<u>General notes on safety</u>	<u>1-3</u>
<u>Structure of safety instructions</u>	<u>1-4</u>
<u>Basic safety aspects</u>	<u>1-6</u>
<u>Specific safety areas</u>	<u>1-10</u>
<u>Laser safety</u>	<u>1-11</u>
<u>Optical circuit pack specifications</u>	<u>1-14</u>
<u>Laser product classification</u>	<u>1-16</u>
<u>Electrostatic discharge</u>	<u>1-20</u>
<u>Safety requirements in specific deployment phases</u>	<u>1-22</u>
<u>Transportation</u>	<u>1-23</u>
<u>Storage</u>	<u>1-26</u>
<u>Installation</u>	<u>1-28</u>
<u>Taking into operation</u>	<u>1-31</u>
<u>Operation and maintenance</u>	<u>1-33</u>
<u>Taking out of operation</u>	<u>1-39</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.

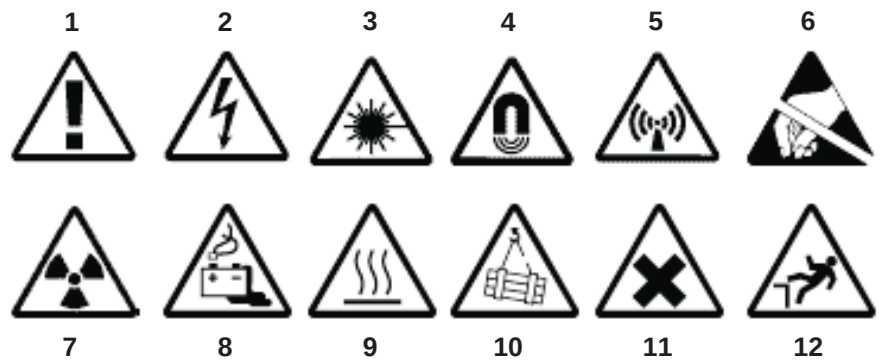
Danger classification There are three classes of safety instructions: “DANGER”, “WARNING” and “CAUTION”. Which class is relevant depends on the consequences of ignoring the safety instruction:

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	1-11
Optical circuit pack specifications	1-14
Laser product classification	1-16
Electrostatic discharge	1-20



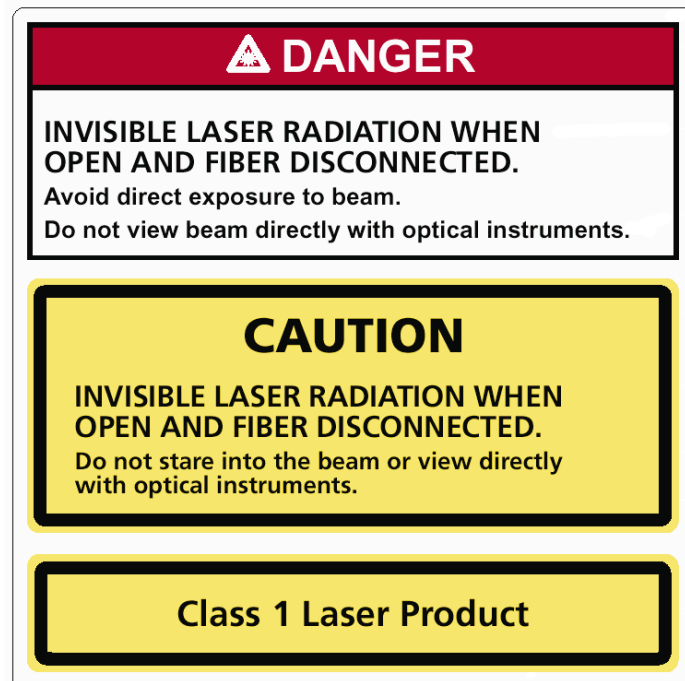
Laser safety

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" \(1-16\)](#).

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.

Release 1.0, Release 2.0





Release 2.1



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” \(1-16\)](#).

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. Please refer to the *LambdaUnite MSS Applications and Planning Guide* for more detailed technical specifications.

Circuit pack	Wavelength [nm]	Fiber type ¹ (core/cladding diameter [μm])	Maximum output power [mW / dBm]	Laser class ² (IEC / FDA)
155-Mbit/s optical circuit packs				
OP155M/1.3IR16 (KFA18)	1310	SM (9/125)	0.15 / -8	1 / I
622-Mbit/s optical circuit packs				
OP622/1.3IR16 (KFA17)	1310	SM (9/125)	0.15 / -8	1 / I
2.5-Gbit/s optical circuit packs				
OP2G5/1.3IOR4 (KFA12)	1310	SM (9/125)	0.5 / -3	1 / I
OP2G5/1.3LR4 (KFA203)	1310	SM (9/125)	1.6 / +2	1 / I
OP2G5/1.5LR4 (KFA204)	1550	SM (9/125)	1.6 / +2	1 / I
OP2G5-1...32PWDM (KFA20) with OM2G5/921PWDM ... 959PWDM (OM2G5A921 ... OM2G5A959)	1560.61 ... 1530.33	SM (9/125)	1 / 0	1 / I
10-Gbit/s optical circuit packs				
OP10/1.3IOR1 (KFA7)	1310	SM (9/125)	0.8 / -1	1 / I
OP10/1.5IR1 (KFA14)	1550	SM (9/125)	1.6 / +2	1 / I
OP10/1.5LR1 (KFA6) ³	1550	SM (9/125)	20 / +13	1M / IIb
OP10/01...80/800G (KFA9, KFA81 ... 159)	1530.72 ... 1562.23	SM (9/125)	0.41 / -3.8	1 / I
OP10/9285XT...8650XT (KFA210 ... KFA482)	1554.537 ... 1607.466	SM (9/125)	0.63 / -2	1 / I
40-Gbit/s optical circuit packs				
OP40/1.3IOR1 (KFA202)	1311	SM (9/125)	5 / +7	1M / IIb
OP40/9280XT ... 8650XT (KFA290 ... 353)	1554.940 ... 1607.466	SM (9/125)	0.5 / -3	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.

3. The OP10/1.5LR1 circuit packs delivered with *LambdaUnite* MSS Releases 1.0 or 2.0 are classified as Class 3A laser products in accordance with the IEC classification (cf. [“Laser product classification” \(1-16\)](#)).

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” \(1-17\)](#)):

- 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. The IEC 60825 standard 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” \(1-17\)](#)):

- Class 1,
- Class 1M,
- Class 3R,
- 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 60825-1 Ed. 1.2 (2001) standard. The precise power limits depend on the mode field diameter and the numerical aperture (NA) of the laser source.

Laser class	Wavelength	Max. output power of laser radiation	
1	1310 nm	15.6 mW	+11.93 dBm
	1550 nm	10 mW	+10 dBm
1M	1310 nm	50.84 mW	+17.06 dBm
	1550 nm	121.20 mW	+20.84 dBm
3R	1310 nm	86 mW	+18.92 dBm
	1550 nm	— ¹	
3B	1310 nm	500 mW	+27 dBm
	1550 nm	500 mW	+27 dBm
4	1310 nm	> 500 mW	> +27 dBm
	1550 nm	> 500 mW	> +27 dBm

Notes:

1. Class 3R only exists if the maximum power is within five times the Accessible Emission Limit (AEL) of Class 1.

In earlier editions of the IEC 60825 standard the following laser classes and corresponding power limits were defined for wavelengths of 1310 nm and 1550 nm.

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
4	1310 nm	> 500 mW	> +27 dBm
	1550 nm	> 500 mW	> +27 dBm

Notes:

1. Corresponding laser warning labels can still be found on equipment manufactured before publication of the IEC 60825-1 Ed. 1.2 (2001) standard.

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 1M or FDA/CDRH Class I or Class 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” \(1-23\)](#)
- [“Storage” \(1-26\)](#)
- [“Installation” \(1-28\)](#)
- [“Taking into operation” \(1-31\)](#)
- [“Operation and maintenance” \(1-33\)](#)
- [“Taking out of operation” \(1-39\)](#)



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 antistatic packaging if possible.

Climatic conditions



CAUTION

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

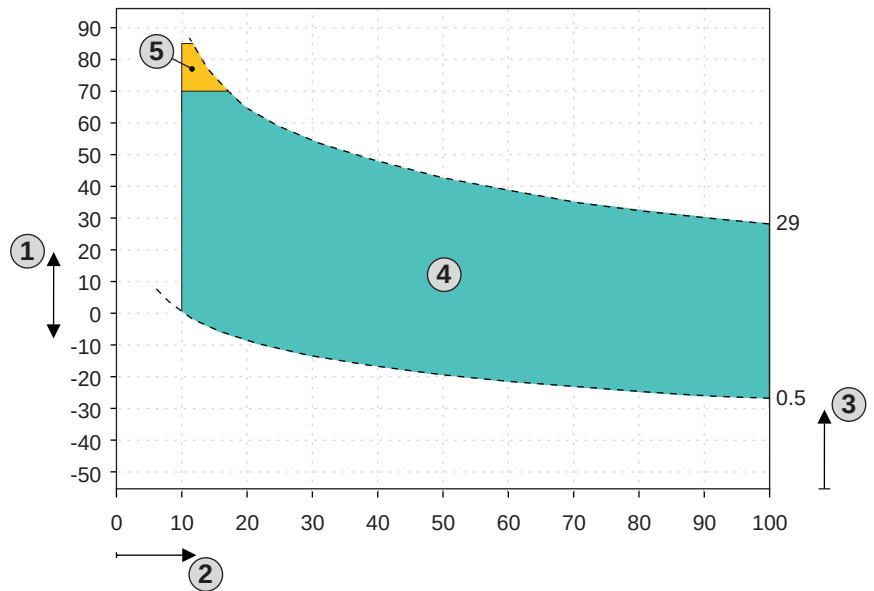
Ensure that the climatic limits for transportation and storage of LambdaUnite™ MSS equipment are complied with during transportation; please refer to [“Climatic limits for transportation and storage” \(1-24\)](#).

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: up to +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 in degrees Celsius [°C] or degrees Fahrenheit [°F]
- 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 antistatic packaging if possible. Always observe the ESD instructions (cf. [“Electrostatic discharge” \(1-20\)](#)).

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 antistatic 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” \(1-24\)](#).



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” \(1-20\)](#)).

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



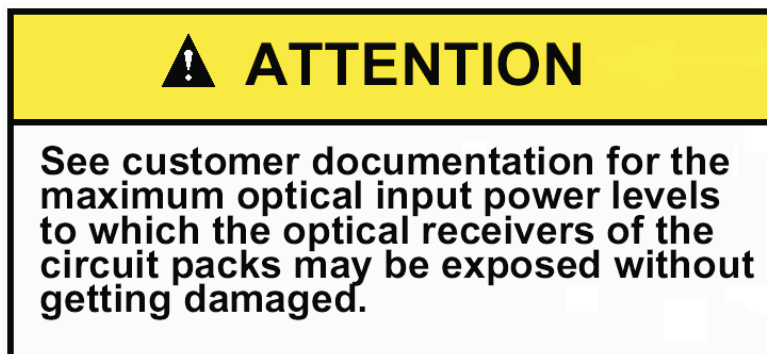
CAUTION

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.

The following label is affixed on the *LambdaUnite* MSS subrack:



Receiver sensitivities

You can find the receiver sensitivities in the *LambdaUnite MSS Applications and Planning Guide* (Technical specifications).



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” \(1-20\)](#)).

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



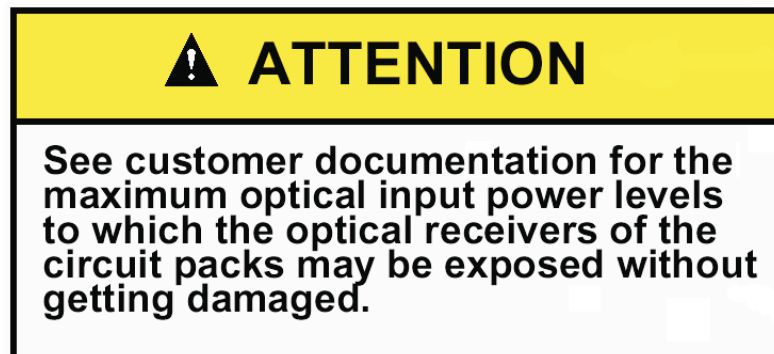
CAUTION

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.

The following label is affixed on the *LambdaUnite* MSS subrack:



Receiver sensitivities

You can find the receiver sensitivities in the *LambdaUnite MSS Applications and Planning Guide* (Technical specifications).

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.

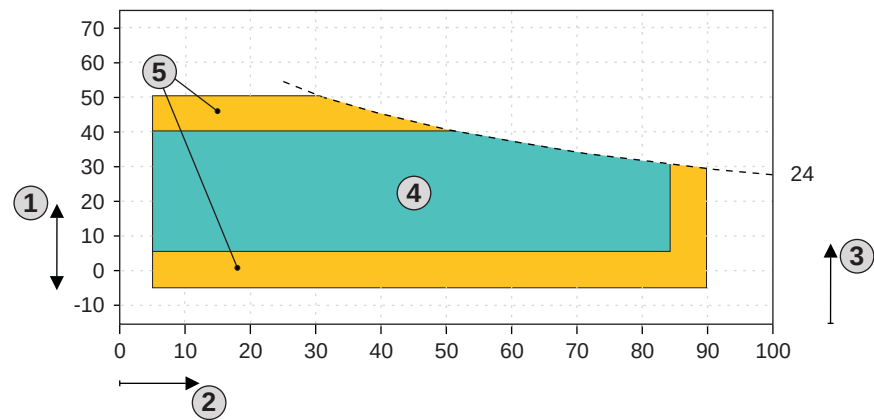
Ensure that the [“Climatic limits for the operation of LambdaUnite MSS equipment” \(1-37\)](#) are complied with during operation.

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: –5 °C to +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 in degrees Celsius [°C] or degrees Fahrenheit [°F]
- 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” \(1-20\)](#)).

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	2-3
Creating a user login	2-5
Modifying a user login	2-10
Deleting a user login	2-12
Disabling user logins	2-13
Enabling user logins	2-15
Logging out NE users	2-17
Supporting information for “Administering user logins”	2-19
Changing super user IDs	2-22
Changing super user IDs on the WaveStar® CIT	2-23
Changing user passwords	2-25
Changing the user password on the WaveStar CIT	2-26
Changing the user password on the NE	2-28
Modifying user security parameters	2-30

Modifying a user's own notification list	2-31
Modifying user security parameters by admin	2-33
Provision global security parameters	2-35
Retrieving security information	2-37
Displaying a list of all users logged into an NE	2-38
Displaying login information for an NE	2-40
Retrieve system wide security parameters	2-42
Retrieve security info of own user	2-44
Retrieve security info of other users	2-46



Administering user logins

Overview

Purpose User administration basically consists of:

- [“Creating a user login” \(2-5\)](#),
- [“Modifying a user login” \(2-10\)](#),
- [“Deleting a user login” \(2-12\)](#),
- [“Disabling user logins” \(2-13\)](#),
- [“Enabling user logins” \(2-15\)](#).
- [“Logging out NE users” \(2-17\)](#)

It is suggested to use [“User administration” \(13-4\)](#) 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” \(13-4\)](#).
- [“Retrieving security information” \(2-37\)](#)
- [Chapter 22, “WaveStar CIT Tutorial”](#)

Contents

Creating a user login	2-5
Modifying a user login	2-10
Deleting a user login	2-12
Disabling user logins	2-13
Enabling user logins	2-15
Logging out NE users	2-17

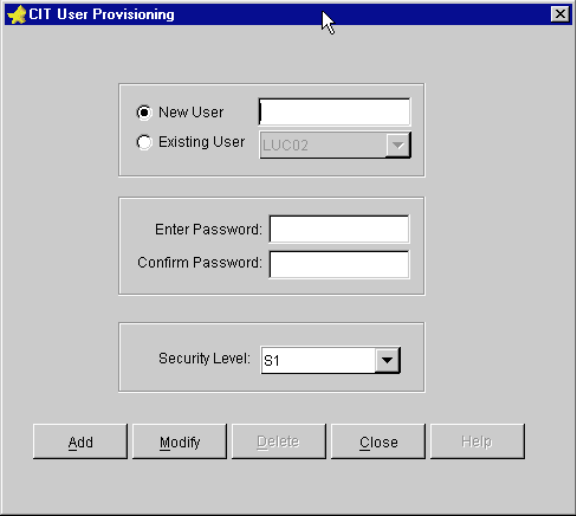
Supporting information for “Administering user logins”	2-19

Creating a user login

When to use Use this procedure to create a user login.

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. It includes fields for creating a new user or selecting an existing one (LUC01), setting a password and confirming it, and configuring user class (MEMADMIN or Other), password aging interval (90 days), and inactivity timeout (30 minutes). There are also dropdown menus for User Type (Other), Maintenance, Provisioning, Performance Management, Security (S1), and Test (No Authorization). A Notification List dropdown is set to OWN. Action buttons at the bottom include Add, Modify, Delete, Cancel, and 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.

Before you begin

The starting point for the following procedure is according to [“User administration” \(13-4\)](#). The procedure itself is limited to the necessary steps to create a new 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! 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” \(13-7\)](#) .

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

Reference:

Please refer to [“User class” \(13-16\)](#) .

- 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” \(13-8\)](#) .

- 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” (13-17) .
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” (13-16) .
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.
-

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** if you don’t want to add a new user.

END OF STEPS



Modifying a user login

Before you begin The starting point for the following procedure is according to [“User administration” \(13-4\)](#). The procedure itself is limited to the necessary steps to modify an existing user login using [“The NE User Provisioning window” \(2-6\)](#).

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

When to use Use this procedure to delete a user login. Please note that superusers can not be deleted.

Before you begin The starting point for the following procedure is according to [“User administration” \(13-4\)](#). 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.

Result:

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

You may now:

1. Click **Yes** to delete the user login, or
2. Click **No** to close the confirmation window without deleting the user login.

Notice that on other WaveStar CITs 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 ...	THEN
you want to disable all user logins,	select the radio button Disable all the user logins .
you want to disable a single user login,	select a user login and select the radio button Disable only the selected user login .

Important! Be sure that you do not disabled all the users, 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.

When a user is logged into an other *WaveStar* CIT using a disabled user login, he will be disconnected.

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 ...	THEN ...
you want to enable all user logins,	select the radio button Enable all the user logins .
you want to enable a single user login,	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.

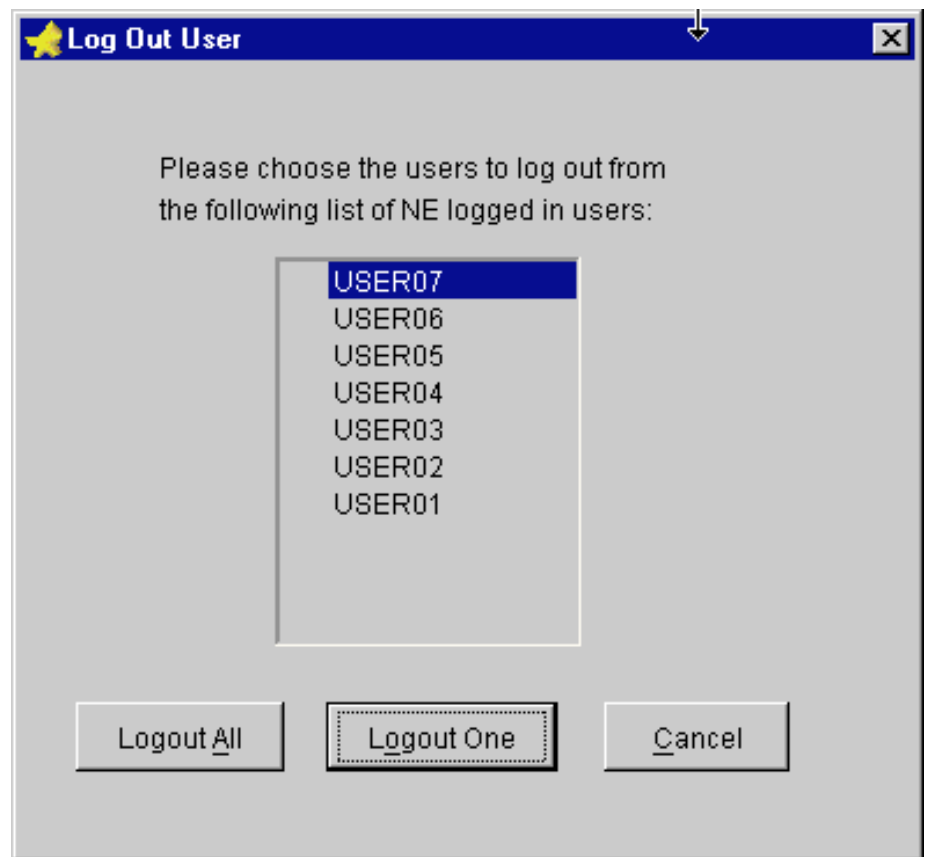
END OF STEPS



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 and the user is logged out.

END OF STEPS
.....

□

Supporting information for “Administering user logins”

Configuration options The following configuration options exist:

Option	Meaning	refer to
New User	This field is used to enter a new user login	“Valid user login” (13-7)
Existing User	an existing user ID which can be selected from the pull-down menu.	
Enter/Confirm Password	This fields are to be used to enter/confirm a new NE password.	“Valid password” (13-8)
Password Aging Interval	the number of days between required NE password changes (7-999) for this user login. This option can be disabled as well.	“Password aging” (13-17)
Inactivity Timeout	the number of minutes (1-999) after which this user login logged out if there’s no activity by the user. This option can be disabled as well.	“Inactivity time-out period” (13-16)
User Class	the user class for this user login, and can have the following values: • OTHER • MEMADMIN	“User class” (13-16)

Option	Meaning	refer to
User Type	the user type for this user login, thereby automatically assigning the authorization levels. The levels range from 0 (no authorization) to 5 (full authorization). Possible Values are: • 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 • Other Any authorization levels that do not map to one of the five predefined user types above.	“Predefined user types” (13-10)
Provisioning	the authorization level for provisioning functions (no authorization or levels 1-5).	
Security	the authorization level for security functions (levels 1-5).	
Maintenance	the authorization level for maintenance functions (no authorization or levels 1-5).	
Performance Management	the authorization level for performance management functions (no authorization or levels 1-5).	
Test	the authorization level for test functions (no authorization or levels 1-5).	

Option	Meaning	refer to
Notification List	the notification registration list used to specify which types of messages this user login will receive. Multiple items are concatenated. Possible values are: • DBCHG (database changes) • STCHG (state changes) • PSCHG (protection switch notification) • ALARMS (alarm notification) • ALL (all the notification registrations as listed above) • OWN (user receives his/her own command responses only) Always select and deselect DBCHG and STCHG together. Both attributes are internally used as synonyms for data base change notifications.	“Notification list” (13-15)



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:

- [“Super user logins and passwords” \(13-7\)](#).
- [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 super user 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” \(13-4\)](#).
- [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 (refer to [“Valid password” \(13-8\)](#)).
-

Note

The new password can be any valid combination of characters as long as it is not the same as the old one.

- 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	2-31
Modifying user security parameters by admin	2-33
Provision global security parameters	2-35



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” \(13-15\)](#).
- [“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:

Change Notification

USER ID: LUC01

☒ Database Changes ☒ Alarm Notification

☒ State Changes

☒ Protection Switch Notification

☐ All the notification registrations as listed above

☐ User receives his/her own command responses only

☐ For OPS/INS memory administration user only

OK Cancel Help

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

Important! Database Changes and **State Changes** can only be selected and deselected together. Both attributes are internally used as synonyms for data base change notifications.

-
- 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” \(13-4\)](#)

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” \(13-4\)](#).

-
- 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: ***“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 that window without adopting the *WaveStar* CIT security database.

END OF STEPS



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” \(13-17\).](#)
- [“User id lockout interval” \(13-17\).](#)
- [“User id lockout aging period” \(13-17\).](#)
- [“User id aging period” \(13-18\).](#)
- [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 currently set to the value "2".
- User ID Lockout Interval:** Two radio buttons, "Disable" (which is selected) and "Enable". To the right is a spin box set to "40" followed by the text "Minutes".
- User ID Aging Period:** Two radio buttons, "Disable" (which is selected) and "Enable". To the right is a spin box set to "10" followed by the text "Days".
- User ID Lockout Aging Period:** A spin box currently set to the value "99" followed by the text "Minutes".

At the bottom 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

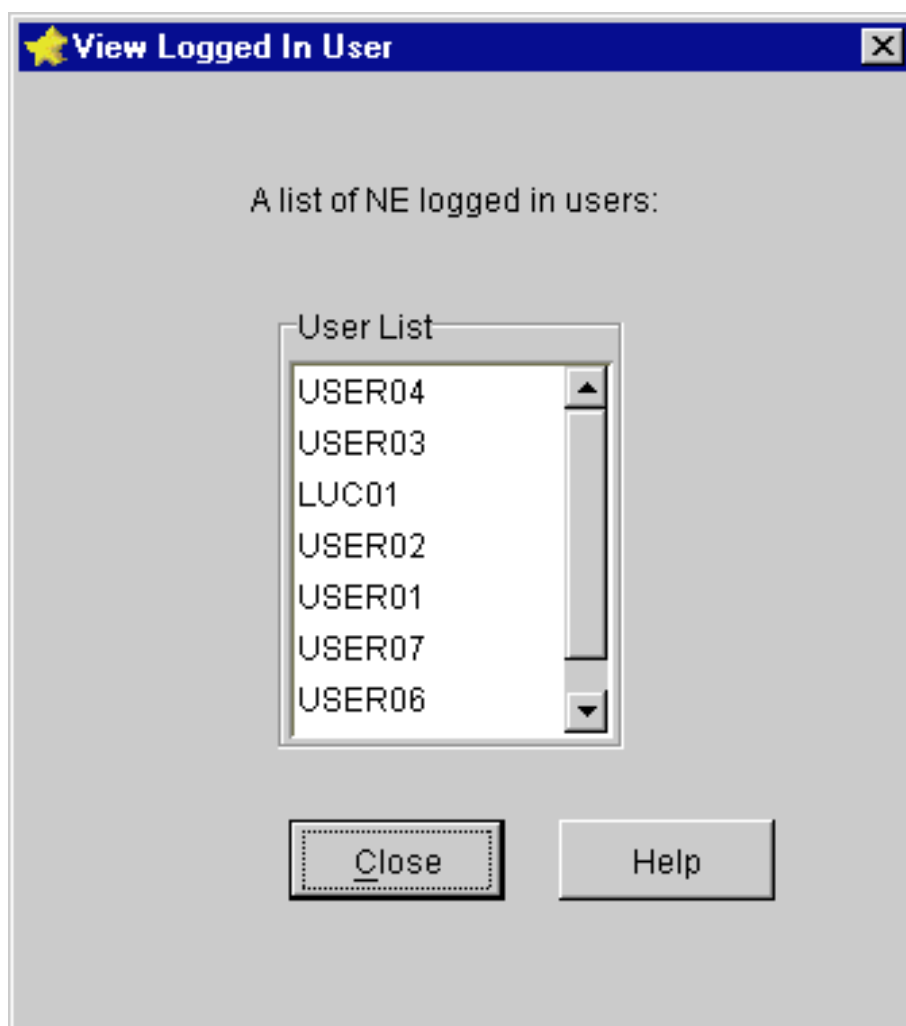
Displaying a list of all users logged into an NE	2-38
Displaying login information for an NE	2-40
Retrieve system wide security parameters	2-42
Retrieve security info of own user	2-44
Retrieve security info of other users	2-46



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 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 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

.....

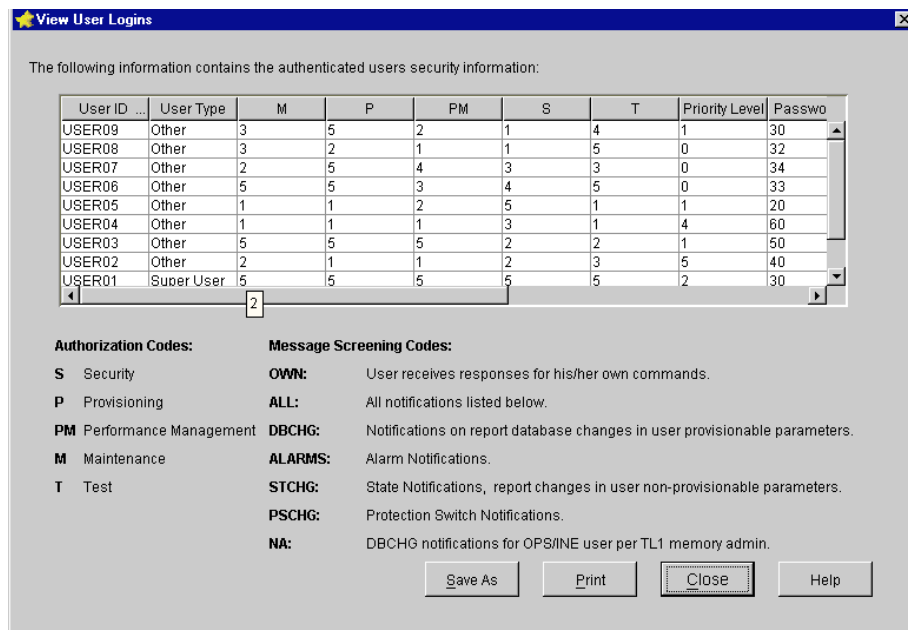


Displaying login information for an NE

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 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” \(13-17\).](#)
- [“User id lockout interval” \(13-17\).](#)
- [“User id lockout aging period” \(13-17\).](#)
- [“User id aging period” \(13-18\).](#)
- [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 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 Windows-style dialog box titled "Provision NE Security". It contains four configuration sections:

- User ID Lockout Threshold:** A numeric spinner box set to the value "2".
- User ID Lockout Interval:** Two radio buttons, "Disable" (selected) and "Enable". To the right is a numeric spinner box set to "40" followed by the text "Minutes".
- User ID Aging Period:** Two radio buttons, "Disable" (selected) and "Enable". To the right is a numeric spinner box set to "10" followed by the text "Days".
- User ID Lockout Aging Period:** A numeric spinner box set to "99" followed by the text "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:

Change Notification

USER ID: LUC01

☒ Database Changes ☒ Alarm Notification

☒ State Changes

☒ Protection Switch Notification

☐ All the notification registrations as listed above

☐ User receives his/her own command responses only

☐ For OPS/INS memory administration user only

OK Cancel Help

Reference:

Refer to [“Notification list” \(13-15\)](#).

END OF STEPS



Retrieve security info of other users

When to use Use this procedure to retrieve security info of 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” \(13-4\)](#).

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 WaveStar® CIT	3-11
Supporting information for “Configuring the basic DCN parameters for the WaveStar CIT”	3-14
Configuring the LDB timers for the WaveStar CIT	3-16
Supporting information for “Configuring the LDB timers for the WaveStar CIT”	3-18
Administering the address list at the WaveStar CIT	3-19
Supporting information for “Administering the address list at the WaveStar CIT”	3-23
Configuring the basic DCN parameters for an NE	3-28
Supporting information on the “LAN Management” tab	3-35

Supporting information on the “Network Layer” tab	3-37
Configuring a NE as T-TD Gateway	3-39
Supporting information on the “TCP/IP Gateway” tab	3-44
Configuring an NE as FTAM-FTP Gateway	3-47
Provisioning OSI nodes	3-50
Supporting information on the “OSI Nodes” tab	3-54
Configuring data communication channels	3-57
Supporting information for “Configuring data communication channels”	3-60
Supporting information on the “View DCC Terminations” window	3-61
Supporting information on the “Configure DCC Terminations” window	3-63
Configuring the TARP parameters for an NE	3-65
Supporting information on the “TARP” tab of the “Data Communications” window	3-68
Assigning TARP manual adjacencies	3-69
Supporting information on the “TARP Manual Adj.” tab of the “Data Communications” window	3-73
Viewing MAC Addresses	3-74



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” \(14-41\).](#)
- [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”).
 - Each NE name must be at most 20 characters in length.

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 *LambdaUnite*[™] MSS network elements and the *WaveStar*[®] CIT.

Related information For related information, please refer to:

- [Chapter 14, “Management communication setup concepts”](#)
- [Chapter 22, “WaveStar CIT Tutorial”](#)

Before you begin Please refer to the individual procedures for information about the required privileges.

Required equipment

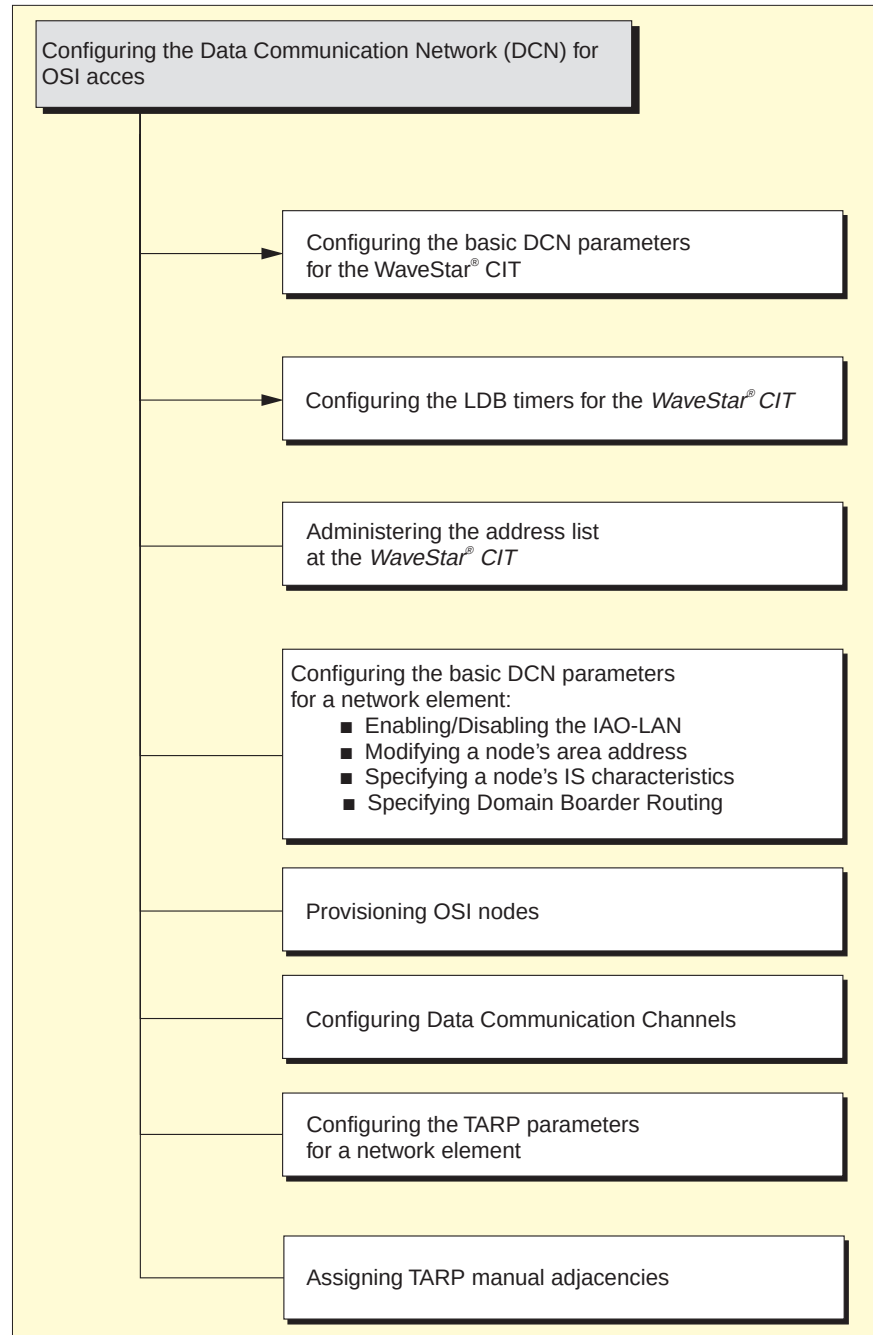
The following equipment is required to perform this task:

- *WaveStar* CIT

Configuring the DCN for OSI access

Important! The sequence of carrying out these procedures is optional, and each of the procedures may also be carried out separately.

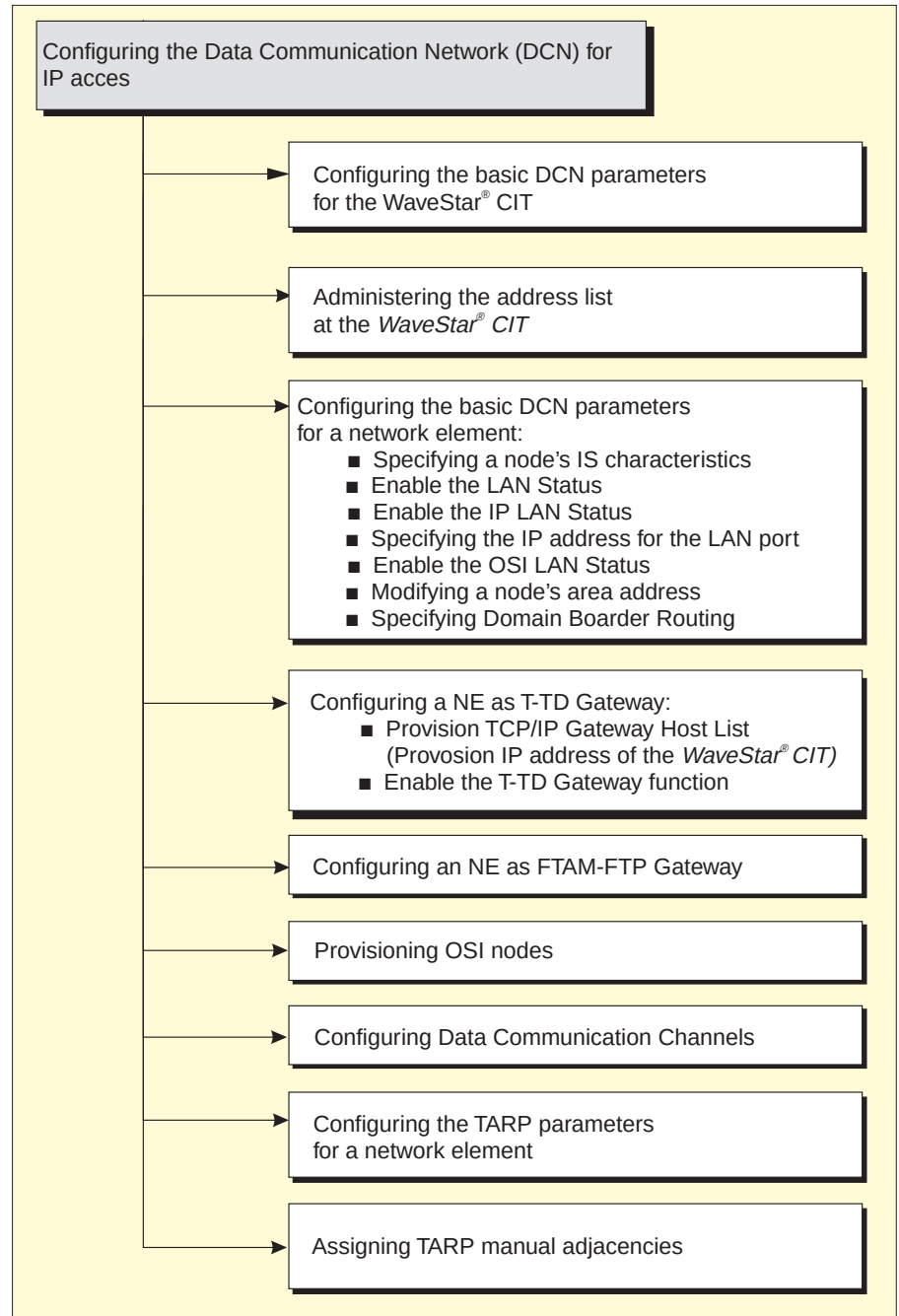
Configuring the Data Communication Network (DCN) for *LambdaUnite* MSS network elements and the *WaveStar* CIT consists of the procedures listed below.



**Configuring the DCN for
IP access**

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” \(3-11\)](#)
- [“Configuring the LDB timers for the WaveStar CIT” \(3-16\)](#)
- [“Administering the address list at the WaveStar CIT” \(3-19\)](#)
- [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)
- [“Configuring a NE as T-TD Gateway” \(3-39\)](#)
- [“Configuring an NE as FTAM-FTP Gateway” \(3-47\)](#)
- [“Provisioning OSI nodes” \(3-50\)](#)
- [“Configuring data communication channels” \(3-57\)](#)
- [“Configuring the TARP parameters for an NE” \(3-65\)](#)
- [“Assigning TARP manual adjacencies” \(3-69\)](#)



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.

The network layer parameters are to be set according to the type of connection between the WaveStar CIT and the NE (refer to [“Concepts for connecting the WaveStar CIT to the NE” \(22-12\)](#)).

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”](#)
- [“Concepts for connecting the WaveStar CIT to the NE” \(22-12\)](#)

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	IF	THEN
	you are going to connect the WaveStar CIT directly to an NE via the user panel of the NE (IP or OSI),	1. make sure that the Auto-Learn NSAP box is checked (refer to “Auto-Learn NSAP function” (3-14)). 2. Continue with Step 8 .
	you are going to connect to NEs via TCP/IP or remotely via an OSI-connection not using TARP (refer to “Concepts for connecting the WaveStar CIT to the NE” (22-12)),	continue with Step 4 .

- 4 Disable the **Auto-Learn NSAP** function,
-

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

If you like to change the area address select **Modify...** in the **Primary Area Address** segment.

Result:

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

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

Important! If you are changing the WaveStar CITs NSAP according to a new Node NSAP then you have to restart the CIT executable.

- 7 Click **OK** to confirm your changes.

Result:

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

-
- 8** If desired, change the maximum value of the routing metric in the **Max Link Metric** spin box.
-
- 9** If desired, change the value of ESCT in the **End System Config. Timer** spin box.
-
- 10** 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 <i>WaveStar</i> CIT” (3-16) . END OF STEPS
you want to save your changes and close the window,	click OK and continue with Step 11 .

-
- 11** 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

Important! Precondition is that the *WaveStar* CIT is directly connected to an NE via the user panel of the NE (IP or OSI). For connecting to NEs via TCP/IP this function must not be used.

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. 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 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.

Elements of the *Network Layer* tab

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**).

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

Option	Meaning
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 (via an OSI connection, if the network element supports TARP (refer to “TARP” (14-38)) for Name/Address resolution). Please refer to the explanation above. The following values are possible: • Enabled (default) • Disable
Primary Area Address	The complete area address in hexadecimal representation.
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. The possible value range is 1 to 63 (default: 14)
End System Config. Timer	The <i>WaveStar</i> CIT’s end systems periodically generate ES Hellos (ESHs). The interval between two ESHs is determined by the End System Configuration Timer (ESCT). The following values are possible: • 10 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” \(14-37\)](#),
- [“TARP” \(14-38\)](#),
- [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.
-

- 3 If desired, enable the TARP 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”

The *TARP Parameters* tab The **TARP Parameters** tab of the **CIT Data Communication** window allows you to enable or disable the TARP TDC functionality by selecting the respective radio button. Additionally the values for the following timers can be set:

- Loop Detection Buffer Entry Timer
- Loop Detection Buffer Flush Timer



Administering the address list at the WaveStar® CIT

When to use Use this procedure to generate and maintain a local WaveStar CIT file containing the TIDs, TCP/IP and NSAPs addresses for NEs, if the WaveStar CIT is to be connected to this NEs

- via an OSI connection, if the network element does not support TARP (refer to [“TARP” \(14-38\)](#) for Name/Address resolution, or
- directly via TCP/IP (WaveStar CIT connected to the user panel of the NE), or
- remotely via TCP/IP on a gateway NE.

If an NE is to be connected via TCP/IP you can enter the needed IP addresses and select

- if the NE is to be used as TCP/IP gateway, or
- if the entered IP address is to be used for default TCP/IP connection for that NE.

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”](#)
- [“Network element selection and login using the address list” \(22-23\)](#)

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

Prerequisites for NEs to be connected via TCP/IP (directly or via TCP/IP gateway)

Prior to performing this task, the following preconditions have to be fulfilled for the NE:

- the NE must have an TCP/IP address,
- if necessary, the **TCP/IP Gateway Host List** has to be provisioned for the NE (refer to [“Configuring a NE as T-TD Gateway” \(3-39\)](#)),
- if necessary, the **TCP/IP Gateway Control** has to be enabled for the NE (refer to [“Configuring a NE as T-TD Gateway” \(3-39\)](#)),
- the **LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **IP LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **OSI LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).

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 .

3 Click **Add**.

Result:

The **Protocol Provisioning** window opens.

4 Enter the information for the NE to be added, and verify that your entries are correct (refer to [“The Protocol Provisioning window” \(3-24\)](#)).

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 [“The Protocol Provisioning window” \(3-24\)](#)).
-

- 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

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 **Address Provisioning** window includes the following parameters.

Parameter	Description
TID	Displays a list of existing TIDs in the local <i>WaveStar</i> CIT file.
NE Type	This field displays the NE type.
Vendor	This field displays the system vendor, e.g. Lucent.
Primary TCP/IP, Port, GW	Displays the primary transmission control protocol/internet protocol address and indicates whether the port and gateway functions are enabled or disabled.
Secondary TCP/IP, Port, GW	Displays the secondary transmission control protocol/internet protocol address and indicates whether the port and gateway functions are enabled or disabled.
Primary NSAP	Displays the primary network service access point NSAP address as a 40 character NSAP entry or 20 octets.
Secondary NSAP	Displays the secondary network service access point NSAP address as a 40 character NSAP entry or 20 octets..
Use TARP	Indicates whether the target identifier address resolution protocol is being used.

Buttons and Actions

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

OK	Use this button to save the Address List and to dismiss the window.
Cancel	Use this button to dismiss the window.

Add	Use this button to add a new TID 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 TID 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 TID and its accompanying data. This option is dimmed until you select an existing entry in the list.
Import...	not used for this release.
Export...	not used for this release.

The Protocol Provisioning window

The **Protocol Provisioning** window can be invoked from the **Address Provisioning** window by clicking on **Add**.

The **Protocol Provisioning** window consist of two tabs:

- **OSI tab**
This tab is used to provision the OSI related parameters, like the NSAP address, for NEs that do not support TARP (refer to [“TARP” \(14-38\)](#)) and are to be remotely connected to the WaveStar CIT via an OSI connection.
- **TCP/IP**
This tab is used to provision the TCP/IP related parameters for NEs, that are connected to the WaveStar CIT via TCP/IP.

The following configuration options (the designations refer to the corresponding WaveStar CIT windows) exist:

Parameter	Description
TID	The field is used to enter/modify/display 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.

Parameter	Description
NE Type	This field displays the NE type for the selected/entered NE name. You can select from a list of supported NE types or Other.
Vendor	This field displays and enables the user to enter or modify the system vendor, e.g. Lucent.
OSI tab	
Use LDAP/TARP for OSI Connection	Select this checkbox to use LDAP (lightweight direct access protocol) or TARP (target identifier address resolution protocol) to connect to the NE.
Primary OSI NSAP	This field displays a primary NSAP address as a 40 character NSAP entry or 20 octets. By clicking on the Modify button the Provision Primary OSI NSAP window is opened. In this window a displayed NSAP address can be modified or a new can be entered. You can enter this field either as a single string of 40 characters or in individual fields. The text boxes in this window represent the individual fields of an NE’s NSAP address. Please refer to “NSAP address format” (14-24).
Secondary OSI NSAP	This field displays a primary NSAP address as a 40 character NSAP entry or 20 octets. By clicking on the Modify button the Secondary Primary OSI NSAP window is opened. In this window a displayed NSAP address can be modified or a new can be entered. You can enter this field either as a single string of 40 characters or in individual fields. The text boxes in this window represent the individual fields of an NE’s NSAP address. Please refer to “NSAP address format” (14-24).
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.
TCP/IP tab	

Parameter	Description
Primary TCP/IP	
Use as default TCP/IP Connection	Radiobutton. The selected address is used for TCP/IP connections to this NE.
Use as TCP/IP Gateway	Radiobutton. If selected the connection is used as TCP/IP gateway.
Primary TCP/IP Address	This field displays the 32 bit IPv4 address. The format is a dotted decimal notation: 4 dot-separated decimal numbers ranging from 0 to 255, inclusive. By clicking on the Modify button the TCP/IP Configure window is opened. In this field the displayed TCP/IP address can be modified. You can enter this field either as a single string or in individual fields. If no IP address has been provisioned, this is set to the Default NE IP Address.
Primary Port Address	This field displays the 16 bit transport layer destination port number. Value range: 0 to 65535.
Secondary TCP/IP	
Use as default TCP/IP Connection	Radiobutton. The selected address is used for TCP/IP connections to this NE.
Use as TCP/IP Gateway	Radiobutton. If selected the address is used for TCP/IP connections to this Gateway NE.

Parameter	Description
Secondary TCP/IP Address	This field displays the 32 bit IPv4 address. The format is a dotted decimal notation: 4 dot-separated decimal numbers ranging from 0 to 255, inclusive. By clicking on the Modify button the TCP/IP Configure window is opened. In this field the displayed TCP/IP address can be modified. You can enter this field either as a single string or in individual fields. If no IP address has been provisioned, this is set to the Default NE IP Address.
Secondary Port Address	This field displays the 16 bit transport layer destination port number. Value range: 0 to 65535.

Buttons and Actions

The **Protocol Provisioning** window provides the following pushbuttons:

OK Use this button to save the new entry in the **Address List** and to dismiss the window.

Cancel Use this button to dismiss the window.

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 at most 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.



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 the IP address of a LAN (therefore LANx must be assigned to osinode1),
 - 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,
 - Specifying Domain Boarder Routing.

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” \(14-24\)](#)
 - [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** **Important!** If the DCN has to be configured for TCP/IP access, at first an IP address for the NE has to be provisioned before any other IP configuration (e.g entering the *WaveStar* CIT IP address

in the **TCP/IP Gateway Host List** (refer to [“Configuring a NE as T-TD Gateway” \(3-39\)](#))) is possible.

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 an osinode for which you want to configure the basic DCN parameters. Each of these object types have their own provisioning screen.

IF	THEN
you have selected an IAO LAN AID, the Data Communications window opens in which only the LAN Management tab is applicable.	Continue with Step 3 .
you have selected an osinode, the Data Communications window opens in which only the LAN Management tab is not applicable.	Continue with Step 13 .

- 3 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.

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

Restriction:

Please note that LAN1 cannot be disabled.

- 5 You may now assign an osinode to the selected LAN port.

Restriction:

For LAN1 only osinode1 can be selected.

For LAN2 and LAN 3: osinode1 ... osinode8 can be selected

- 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 You may now enable or disable the IP communication over the selected LAN port by selecting the respective radio button for the **IP LAN Status**.

- 8 According to the setting of the **IP LAN Status** you have to continue.

IF	THEN
you have enabled the IP LAN Status ,	continue with Step 9 .
you have disabled the IP LAN Status ,	continue with Step 12 .

- 9 You may now modify the **IP Address** for the selected LAN port.

Restriction:

For modifying the **IP Address** the selected LAN port must be assigned to osinode1 (refer to [Step 5](#)).

- 10 You may now modify the **IP Subnet Mask** for the selected LAN port.

- 11 You may now enable/disable OSI on the selected LAN port by selecting the respective radio button for the **OSI LAN Status**.

-
- 12** If you have made any changes in the **LAN Management** tab click **OK** and confirm your changes in the confirmation window.

Continue with [Step 22](#).

.....

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

- 14** 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 15 .
you want to leave the node's area address unchanged,	continue with Step 16 .

.....

- 15** In the **NSAPI/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 **NSAPI/Area Address Provision** window is closed.

Please note that subsequently the DCC controller is restarted. Wait until the restart has finished.

.....

- 16** 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.
-

- 17** You may now provide if the selected node is to be used for domain routing via setting the value **Domain Boundary**.

Depending on the selected OSI node the following values are possible:

- **osinode1** selected:
 - **No** (fixed value)
- **osinode2 ... osinode8** selected:
 - **No**
 - **Yes**

-
- 18** You may now modify the **Reachable Address Destination**, i.e. the osinode used for inter domain routing, for the selected osinode.

Depending on the selected osinode the following values are possible:

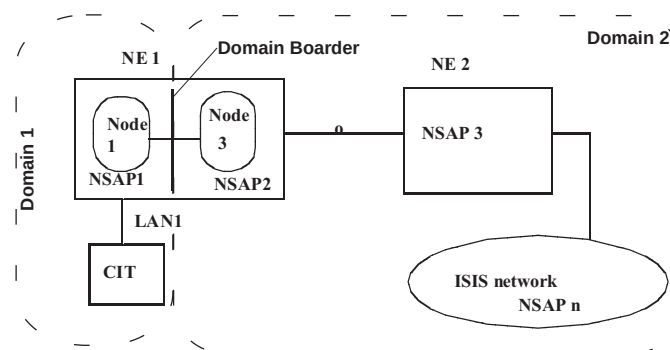
- **osinode1** selected:
 - **none**
 - **osinode2 ... osinode8**
- **osinode2 ... osinode8** selected:
 - **none**
 - **osinode1**

-
- 19** Click **OK** and confirm your changes in the confirmation window.

-
- 20** You may now provision the **Reachable Address Prefix**.

Guidelines for “Reachable Address Prefix”

The following figure gives an example of a multiple domain topology:



Below some rules that indicate how **Reachable Address Prefix** must be used in the SDH/SONET networks:

- Between osinode1 and osinode3, TARP manual adjacencies must be provisioned (refer to [“Assigning TARP manual adjacencies” \(3-69\)](#)).
- For TARP propagation over domain boundaries, the TARP manual adjacencies must be used, in addition to the Reachable Address Prefix.
- Reachable Address Prefix in osinode1 must match all NSAPs behind the domain boarder (NSAP 2, NSAP 3, NSAP n)
- Use unique area addresses in the multiple domain topology.
- Do not use a prefix that matches intra-domain NSAP's.
- When BLSR/MS-SPRING must pass a domain border to reach osinode-1 in the NE, the user must provision:
 - an **Reachable Address Prefix** from osinode1 to the node in an other routing domain.
 - an **Reachable Address Prefix** from the "node in an other routing domain" to osinode1.

Reference:

Refer to [“Domain border routing” \(14-9\)](#).

21 If you have made any changes in the **Network Layer** tab click **OK** and confirm your changes in the confirmation window.

22 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 ...	THEN ...
you want to save your changes and select another tab of the Data Communications window,	click OK and confirm your changes in the confirmation window, and refer to the corresponding task description.

IF ...	THEN ...
you want to save your changes and close the Data Communications window,	click OK 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 on the “LAN Management” tab

Overview 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 Management** 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.

Option	Meaning	Value range
MAC Address	MAC address of the selected IAO LAN port. This field is read only.	
LAN TARP Storm Suppression	This field allows you to enable or disable External LAN TARP Storm Suppression.	Enable or Disable
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 For LAN2 and LAN 3: osinode1 - 8
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
IP-LAN Status	This parameter indicates whether IP communication over the external LAN channel is enabled or disabled.	Enable or Disable
IP Address	This parameter indicates the assigned IP address for the LAN interface. 32-bit IPv4 address, four dot separated numeric strings.	For each numeric string: 0 .. 255

Option	Meaning	Value range
IP Subnet Mask	This parameter indicates the assigned IP subnet mask (32-bit IPv4) for the LAN interface. The value is made up of four dot-separated decimal numbers ranging from 0 to 255.	For each numeric string: 0 .. 255
OSI LAN Status	This parameter allows the user to enable/disable OSI on the selected LAN.	Depending on the selected LAN the following values are possible: • LAN1: Enable only • LAN2 Enable, Disable • LAN3: Enable, Disable



Supporting information on the “Network Layer” tab

Overview The **Network Layer** tab of the **Data Communications** window provides information on the actual network layer configuration and offers the opportunity to modify the NE’s area address and to specify the NE’s IS characteristics.

Elements of the *Network Layer* tab 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.

Option	Meaning	Value range
NSAP	This field displays the current NSAP dependent on the actual setting of the configurable NSAP address fields. The NSAP address can be modified. After clicking on Modify the NSAP Provisioning window opens.	please refer to “NSAP address fields” (14-25)
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
Domain Boundary		Depending on the selected OSI node the following values are possible: • osinode1 selected: - No (fixed value) • osinode2 ... osinode8 selected: - No - Yes

Option	Meaning	Value range
Reachable Address Destination Node	The parameter is actually an OSI node AID.	Depending on the selected OSI node the following values are possible: • osinode1 selected: - none - osinode2 ... osinode8 • osinode2 ... osinode8 selected: - none - osinode1
Reachable Address Prefix	This parameter shall be a hexadecimal string of 1 to 13 bytes or NONE. (An Area Address or part of it, beginning with the first byte - AFI.	The first byte is limited to the values [1-9][0-9]. Also the special value NONE can be used.



Configuring a NE as T-TD Gateway

When to use Use this procedure to configure a NE as T-TD gateway and to enter the *WaveStar*® CIT in the **TCP/IP Gateway Host List**.

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:

- [“T-TD Gateway” \(14-21\)](#)
- [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

Prerequisites

Prior to performing this task, the following preconditions have to be fulfilled:

- the NE must have an TCP/IP address (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **TARP Originator** functionality has to be enabled for the NE (refer to [“Configuring the TARP parameters for an NE” \(3-65\)](#)),
- the **IP LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),

- the **OSI LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).
- the IP address of the *WaveStar* CIT has to be investigated, How this can be done depends on the operating system installed on the *WaveStar* CIT PC. In general proceed as follows. From the *Windows*® **Start** button select **Settings** → **Control Panel**. In the **Control Panel** double-click **Network** and then select the **Protocols** tab. Select **TCP/IP Protocol** and click on **Properties**. In the **IP address** tab the IP address of the PC is displayed.

Instructions Complete the following steps to configure the T-TD Gateway function 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 the system.

Result:

The **Data Communications** window opens.

- 3 If you want to configure the T-TD Gateway function, then select the **TCP/IP Gateway** tab.
-

- 4 At first provision **TCP/IP Gateway Host List**.

This list contains the possible management systems that may set up management associations through the T-TD gateway. The list contains the IP addresses of the management systems and their host types that should be used in the association to the NE.

Investigating the IP address of the WaveStar CIT

In general proceed as follows:

- From the *Windows* **Start** button select **Settings** → **Control Panel**.
- In the **Control Panel** double-click **Network** and then select the **Protocols** tab.
- Select **TCP/IP Protocol** and click on **Properties**.
- In the **IP address** tab the IP address of the PC is displayed.

5 At first provision **TCP/IP Gateway Host List**.

IF	THEN
you want to add a host to the list	click on the symbol left of an empty entry in the list. The window Edit IP Address and OS type for system opens. Enter the IP address of the host in the field New IP Address and select the OS type in the New OS Types drop-down list box. Click on Add. Result: The window Edit IP Address and OS type for system is closed and the new entry is displayed in the TCP/IP Gateway Host List.
you want to modify a host on the list	click on the symbol left of the entry in the list. The window Edit IP Address and OS type for system opens. Enter the IP address of the host in the field New IP Address and select the OS type in the New OS Types drop-down list box. Click on Modify. Result: The window Edit IP Address and OS type for system is closed and the changed entry is displayed in the TCP/IP Gateway Host List.

IF	THEN
you want to delete a host on the list	click on the symbol left of the entry in the list. The window Edit IP Address and OS type for system opens. Click on Delete. Result: The window Edit IP Address and OS type for system is closed and the entry is removed from the TCP/IP Gateway Host List.

-
- 6 Provision the TCP port numbers that are used to listen for incoming TL1 connections in the field **Encoding Mode Port Numbers**.

Each TL1 encoding method has its own port, so three port numbers can be provisioned:

- **T-TD Length Value Port** (for Length Value (LV) encoding),
- **T-TD Raw Port** (for raw encoding),

-
- 7 You may now enable the T-TD Gateway function for the NE by clicking on the respective radio button in the field **TCP/IP Gateway Control**.

Important! Please note that you can lock out yourself from an NE without warning, if you are connected via TCP/IP and you disable the T-TD Gateway function.

-
- 8 If you have made any changes in the **TCP/IP Gateway** tab click **OK** and confirm your changes in the confirmation window.

-
- 9 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 ...	THEN ...
you want to save your changes and select another tab of the Data Communications window,	click OK and confirm your changes in the confirmation window, and refer to the corresponding task description.
you want to save your changes and close the Data Communications window,	click OK 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 on the “TCP/IP Gateway” tab

Overview The **TCP/IP Gateway** tab of the **Data Communications** window makes it possible to manage the TCP/IP Gateway function.

Configuration options The following configuration options (the designations refer to the corresponding *WaveStar*® CIT windows) exist:

Option	Meaning
TCP/IP Gateway Control	This field allows you to enable or disable TCP/IP to OSI conversion for the NE by selecting the according radion button.. The following values are possible: • Enable, • Disable Please note that you can lock out yourself from an NE without warning, if you are connected via TCP/IP and you disable the TCP/IP Gateway function.

Option	Meaning
TCP/IP Gateway Host List	Displays a list of the TCP/IP Gateway Hosts. The following information is displayed in the list: • IP Adress This field is the IP address of the OS. • Host Type This field displays the host type of the responding OS. - TL1MAINTENANCE Maintenance OS - TL1MEMORYADMINISTRATION Memory Administration OS - TL1TEST Test OS - TL1OTHER1 Other OS - TL1PEERCOM Peer Communications OS Any value can be used. A single entry is sufficient. To add, modify or delete an entry of the list, just click on the symbol left of the entry. Then the window Edit IP Address and OS type for system opens.
T-TD Length Value Port	This field allows you to set the port number over which the T-TD function is accessible using the Length Value Encoding method. Possible values: 0 ... 65535. For the Length Value Port encoding the <i>WaveStar</i> CIT uses the port number 3081 (default value). If other port numbers are used they are handled as Raw Ports.
T-TD Raw Port	This field allows you to set the port number over which the T-TD function is accessible using the raw-mode encoding method. Possible values: 0 ... 65535. For Raw Port encoding the <i>WaveStar</i> CIT uses the port number 3082 (default value). If other port numbers are used they are also handled as Raw Ports.



Configuring an NE as FTAM-FTP Gateway

When to use Use this procedure to configure an NE as FTAM-FTP Gateway. 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:

- [“FT-TD Gateway” \(14-22\)](#)
- [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

Prior to performing this task, you must:

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

Prerequisites

Prior to performing this task, the following preconditions have to be fulfilled by the NE:

- the NE must have an TCP/IP address,
- the **LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **IP LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **OSI LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).

Instructions Complete the following steps to enable/disable the TCP/IP Gateway function 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 the system.

Result:

The **Data Communications** window opens.

- 3 If you want to enable/disable the FTAM-FTP function for the NE, then select the **TCP/IP** tab.
-

- 4 You may now enable or disable the FTAM-FTP function for the NE by clicking on the respective radio button.
-

- 5 If you have made any changes in the **TCP/IP** tab click **OK** and confirm your changes in the confirmation window.
-

- 6 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 ...	THEN ...
you want to save your changes and select another tab of the Data Communications window,	click OK and confirm your changes in the confirmation window, and refer to the corresponding task description.

IF ...	THEN ...
you want to save your changes and close the Data Communications window,	click OK 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



Provisioning OSI nodes

When to use Use this procedure to provision OSI nodes.

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:

- [“T-TD Gateway” \(14-21\)](#)
- [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 provision OSI nodes.

- 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 the system.

Result:

The **Data Communications** window opens.

-
- 3 Select the **OSI Nodes** tab.
-

- 4 To provision OSI nodes perform the following:

IF	THEN
you want to add a OSI node,	click on the symbol left of an empty entry in the list. The window Create OSI Node opens. Enter the required parameters (refer to “Configuration options” (3-54)) Click on Add. Result: The window Create OSI Node is closed and the new entry is displayed in the OSI node List. Reference: Continue with Step 13.
you want to delete a OSI node on the list	continue with Step 5 .

- 5 Depending if the NE is used for domain routing proceed as follows:

IF	THEN
the NE is used for domain routing,	check which of the osinodes are used for domain routing. Additional info If an osinode is to be deleted in an NE in which domain routing is established, domain routing must be disabled before. Reference: Refer to Step 6.
the NE is not used for domain routing	click on the symbol left of the entry in the list. The window Delete OSI Node opens. Click on Delete. Result: The window Delete OSI Node is closed and the entry is removed from the OSI node List. Reference: Continue with Step 13.

-
- 6 For the osinodes in the NE used for domain routing set **Reachable Address Prefix** to '**NONE**' (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).

Reference:

Refer to [“Domain border routing” \(14-9\)](#).

- 7 For the osinodes in the NE used for domain routing set **Reachable Address Destination** to '**NONE**' (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).
-

- 8 For the osinodes in the NE used for domain routing set **Domain Boundary** to '**No**' (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).
-

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

Result:

The equipment selection window opens.

- 10 By means of the equipment selection window, select the system.

Result:

The **Data Communications** window opens.

- 11 Select the **OSI Nodes** tab.
-

- 12 Click on the symbol left of the osinode in the list you want to delete.

The window **Delete OSI Node** opens.

Click on **Delete**.

Result:

The window **Delete OSI Node** is closed and the entry is removed from the **OSI node List**.

-
- 13** If you have made any changes in the **OSI Node** tab click **Close** and confirm your changes in the confirmation window.
-
- 14** If needed re-establish domain routing (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).
-
- 15** 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 ...	THEN ...
you want to save your changes and select another tab of the Data Communications window,	click OK and confirm your changes in the confirmation window, and refer to the corresponding task description.
you want to save your changes and close the Data Communications window,	click OK 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 on the “OSI Nodes” tab

Overview The **OSI Nodes** tab of the **Data Communications** window allows to manage the OSI nodes.

Information field The **OSI Nodes** tab includes the OSI Nodes List.

Option	Description
	Clicking on this symbol either open the window Create OSI Node or Delete OSI Node depending if the corresponding Node field is empty or not.
Node	Display the osinodes defined for the NE.
NSAP	Displays the NSAP of the osinode (refer to “NSAP address format” (14-24))

Configuration options The elements of the **Create OSI Node** window 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.

Option	Meaning	Value range
OSI Node AID	AID of the selected osinode.	The following values can be selected: osinode1 ... osinode8
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” (14-25)

Option	Meaning	Value range
Domain Boundary		Depending on the selected OSI node the following values are possible: • osinode1 selected: - No (fixed value) • osinode2 ... osinode8 selected: - No - Yes
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

Option	Meaning	Value range
Reachable Address Destination Node	The parameter is actually an OSI node AID.	Depending on the selected OSI node the following values are possible: • osinode1 selected: - none - osinode2 ... - osinode8 • osinode2 ... osinode8 selected: - none - osinode1
Reachable Address Prefix	This parameter shall be a hexadecimal string of 1 to 13 bytes.	The first byte is limited to the values [1-9][0-9]. Also the special value NONE can be used.



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”” \(3-60\)](#)

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. [“Supporting information on the “View DCC Terminations” window” \(3-61\)](#)).

.....

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 [“Supporting information on the “Configure DCC Terminations” window” \(3-63\)](#).
-

- 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 12 .

.....

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

- 10** In the **DCC Channel Parameters** group box, choose the **LAPD Role** (either **USER-SIDE** (default) or **NETWORK-SIDE**) by selecting the respective radio button.
-

- 11** In the **DCC Channel Parameters** group box, choose the **LAPD Mode** (either **UITS** (default) or **AIMS**) by selecting the respective radio button.
-

END OF STEPS

- 12** 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.
-

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

Important! If **LAPD Mode** was set to **AIMS** the following has to be notified: 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” \(3-60\)](#) 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 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**



Supporting information on the “View DCC Terminations” window

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

This window can be invoked 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” \(14-29\)](#)). 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.
Protection Port AID	This field is greyed out. If a port is protected, this field displays the corresponding protection port AID from the protection group of which the selected port is a member.

Parameter	Meaning
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-256, STM-64, STM-16, STM-4, STM-1.
LADP Role	The assigned LAPD role. This can be either USER-SIDE or NETWORK-SIDE. NETWORK-SIDE has to be chosen for interworking with not-UNITE NEs.
LAPD Mode	The assigned LAPD mode. This can be either UITS (default) (unacknowledged service) or AIMS (acknowledged service).
OSI Node	Assignment of LANs to an OSI-node in a NE. This field value can be osinode1 to osinode8.
Channel Enable	This can be either Enabled Disabled
DCC protection type	This field is not used in this release.



Supporting information on the “Configure DCC Terminations” window

Overview 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” \(14-29\)](#)). If applicable, the permitted value range as well as the default setting of the parameters are also given.

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
Protection 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-256, STM-64, STM-16, STM-4, STM-1.	no default setting; read-only

Window element	Value range	Default Setting
DCC Channel Parameters		
DCC 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. The possible values are ENABLE and DISABLE	Disabled (default)
LAPD Role	The assigned LAPD role. This can be either USER-SIDE or NETWORK-SIDE. NETWORK-SIDE has to be chosen for interworking with not-UNITE NEs.	USER-SIDE
LAPD Mode	This parameter indicates the type of LAPD service: • AIMS • UITS	UITS
OSI Node	osinode 1...osinode 8	osinode1 ... 8;
DCC protection type	This field is not used in this release.	



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 originator functionality, or 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”](#)
- [“TARP” \(14-38\)](#)
- [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 originator functionality according to your needs by selecting the corresponding check box in the **TARP Originator** group box. The TARP originator functionality is enabled by default.
- Important!** Editable only on osinode1, on other nodes always Disabled.
-
- 5 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.
-
- 6 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.
-
- 7 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 ...	then ...
save your changes and select another tab of the Data Communications window,	click OK and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS

If you want to ...	then ...
save your changes and close the Data Communications window,	click OK and then Close . and confirm your changes in the confirmation window. END OF STEPS

.....
E N D O F S T E P S



Supporting information on the “TARP” tab of the “Data Communications” window

Overview This window is used to set the various TARP (Target Identifiers Address Resolution Protocol) parameters that are user provisionable.

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

- enable or disable the TARP propagation functionality,
- enable or disable the TARP responder functionality (editable only on osinode1, on other nodes always disabled.),
- enable or disable the TARP originator functionality (editable only on osinode1, on other nodes always disabled.)

for a selected node.

Elements of the *TARP* tab The elements of the **TARP** 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.

Option	Meaning	Value range
TARP Propagator	Used to enable or disable TARP propagation functions.	Enable or Disable
TARP Responder	Used to enable or disable TARP responder functions.	Enable or Disable
TARP Originator	Used to enable or disable TARP originator functions.	Enable or Disable



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 osinode.

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” \(14-25\)](#)).

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 field in the TARP Manual Adjacency Table .	continue with Step 5 .
modify an existing manual adjacency,	continue with Step 9 .
delete an existing manual adjacency,	continue with Step 13 .

- 5 Click on the symbol in the left column of the **TARP Manual Adjacency Table** beside the empty **Manual Adjacency Address**.

Result:

The **Manual Adjacency Address Provisioning** window opens.

- 6 Enter the individual fields of the TARP manual adjacency's NET into the corresponding text boxes in the **Manual Adjacency Address Provisioning** window.
-

- 7 Make sure that the NET is correct.

IF ...	THEN ...
the NET is correct,	continue with Step 8 .

IF ...	THEN ...
the NET is not correct,	correct the corresponding entries and continue with Step 8 .

- 8 Click **OK** in the **Manual Adjacency Address Provisioning** window.

Result:

The **Manual Adjacency Address Provisioning** window is closed.

Continue with [Step 16](#).

- 9 Click on the symbol besides the **Manual Adjacency Address** you want to modify.

Result:

The **Manual Adjacency Address Provisioning** 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 **Manual Adjacency Address Provisioning** 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 **Manual Adjacency Address Provisioning** window.

Result:

The **Manual Adjacency Address Provisioning** window is closed.

Continue with [Step 16](#).

-
- 13** Click on the symbol beside the **Manual Adjacency Address** you want to delete.

Result:

The **Manual Adjacency Address Provisioning** window opens.
In principle the window is the same as the window used in [Step 5](#).

.....

- 14** Click on **Clear** in the **Manual Adjacency Address Provisioning** window.
-

- 15** Click **OK** in the **Manual Adjacency Address Provisioning** window.

Result:

The **Manual Adjacency Address Provisioning** 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 OK 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 OK and then Close and confirm your changes in the confirmation window.

END OF STEPS

.....



Supporting information on the “TARP Manual Adj.” tab of the “Data Communications” window

Elements of the *TARP Manual Adj.* tab

The **TARP Manual Adj.** tab consists of a table displaying the two Manual Adjacency Addresses, which are shown in the right column of the table.

To enter a new or modify or delete an existing TARP manual adjacency address the user has to click on the according symbol in the left column of the table. Then the **Manual Adjacency Address Provisioning** window is opened.



Viewing MAC Addresses

When to use Use this procedure if you want to view the MAC Addresses of the NE.

Related Information For related information see [“Media Access Control \(MAC\)” \(18-45\)](#).

Instructions

- 1 Select **Administration** → **View MAC Addresses...** in the **System View**.

Result:

The LAN AIDs and the corresponding MAC Addresses are displayed in the window **View MAC Addresses**.

- 2 Via the buttons **Save As** and **Print** you can either save or print the MAC Addresses of the NE.
-

- 3 Click on **Close** to exit to the **System View**.

END OF STEPS





4 Equipment provisioning

Overview

Purpose This chapter describes the procedures to be carried out for the provisioning of the hardware components of a *LambdaUnite*[™] MSS network element (NE) by using the *WaveStar*[®] CIT.

Related information

Please also refer to [Chapter 15, “Equipment provisioning concepts”](#).

Provisioning hierarchy Some provisioning parameters relate to other provisioning parameters and must therefore be specified in a hierarchical fashion.

Provisioning of an NE with an empty database If an initial software download 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, or “name”) of the respective *LambdaUnite* MSS system 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 – overview procedure	4-4
Configuring the basic system parameters	4-5
Viewing equipment details of the system	4-10
Equipment details of the system	4-12
Configuring the shelf	4-14
Viewing equipment details of the backplane	4-16
Equipment details of the backplane	4-18
Viewing equipment details of the CI-CTL	4-20
Equipment details of the CI-CTL	4-22
Viewing equipment details of the user panel	4-24
Equipment details of the user panel	4-26
Viewing equipment details of a Timing Interface	4-28
Equipment details of a Timing Interface	4-30
Viewing equipment details of a Power Interface	4-32
Equipment details of a Power Interface	4-34
Viewing equipment details of the fan unit	4-36
Equipment details of the fan unit	4-38
Provisioning a slot	4-39
Preprovisioning a circuit pack	4-42
Provisioning a circuit pack	4-44
Reassigning a circuit pack	4-46
Configuring an optical SDH/SONET port	4-49
Configuring an optical SDH/SONET port	4-52

Viewing equipment details of an optical SDH/SONET port	4-72
Equipment details of an optical SDH/SONET port	4-74
Configuring an Ethernet port	4-81
Ethernet port parameters”	4-86
Configuring a VCG port	4-88
VCG port parameters	4-91
Configuring a tributary	4-92
Removing equipment from the system	4-94
Viewing an equipment protection group	4-96
Parameters for a 1+1 equipment protection	4-98
Protection Switch (1+1 Equipment)	4-99
Switching a 1+1 equipment protection	4-100
Retrieving an equipment list	4-102
Equipment list of a circuit pack/backplane	4-107
Equipment list of the shelf	4-108
Equipment list of a port	4-109
Equipment list of a virtual concatenation group (VCG)	4-111
Equipment list of a tributary	4-113
Equipment list of the Miscellaneous Discretes	4-114
Configuring Miscellaneous Discrete Outputs	4-115
Activating or deactivating Miscellaneous Discrete Outputs manually	4-117
Replacing an XC320 circuit pack by an XC320/A circuit pack	4-119



Initial equipment provisioning – overview procedure

Purpose This overview procedure lists the individual provisioning procedures 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 procedures, you must:

- have a valid user login and password,
- be connected to the corresponding NE, and
- have proper access privileges to perform these procedures.

Required privilege code

The required privilege codes are given with the individual provisioning procedures.

Required equipment

The following equipment is required to perform the tasks below:

- WaveStar® CIT

Instructions Subsequently perform the following provisioning procedures:

- 1 System provisioning
(cf. [“Configuring the basic system parameters” \(4-5\)](#))
- 2 Timing provisioning
(cf. [Chapter 6, “Timing provisioning”](#))
- 3 Port provisioning
(cf. [“Configuring an optical SDH/SONET port” \(4-49\)](#))
- 4 Tributary provisioning
(cf. [“Configuring a tributary” \(4-92\)](#))

END OF STEPS



Configuring the basic system parameters

- Purpose** Use this procedure to
- specify the basic configuration parameters related to the network element (NE, system) as a whole, and/or
 - define the system's date and time settings.
- Note:** The system's date and time must be set again after each power on or reboot.

- Related information** For related information, see:
- [“Provisioning of new components” \(15-6\)](#)

- 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 **P3 or M3** to set the basic system parameters.

Required equipment

The following equipment is required to configure the basic system parameters:

- WaveStar CIT

- Instructions** Proceed as follows to configure the basic system parameters:
-

- 1 Choose one of the following options to invoke the system provisioning window:
 1. From the WaveStar CIT **System View** main menu, select **Configuration** → **Provision...**
 2. Right-click on the white area of the WaveStar CIT **System View** window (**not** on the shelf display) and select **Provision System...** in the pop-up menu that opens.

Result:

The **Provision Parameters for Protection Groups or Equipment** window (option 1) or **Provision System** window (option 2) opens. In the case of the **Provision Parameters for**

Protection Groups or Equipment window, the **Equip** selection tab appears on the left-hand side.

If you have chosen option 1, then proceed with the next step. Otherwise proceed with [Step 3](#).

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

Result:

The selection window for the system parameters appears on the right-hand side of the window. This window consists of two tabs, **Settings** and **Date and Time**.

-
- 3 As it is up to your discretion whether to carry out only one out of the above mentioned provisioning activities or both, the corresponding procedures are described separately in the following:

If ...	then ...
you only want to specify the basic configuration parameters of the NE	refer to “Specifying the basic configuration parameters” (4-7) .
you only want to set the system’s date and time	refer to “Setting the system’s date and time” (4-9) .
you want to carry out both provisioning activities	subsequently perform both procedures in any desired sequence.

END OF STEPS

Specifying the basic configuration parameters

Proceed as follows to specify the basic configuration parameters:

- 1 Select the **Settings** tab.

- 2 In the **System Settings** group box, specify the **Optical Interface Standard**:

If ...	then ...
the system will interface predominantly with SDH equipment	select SDH . This is the default setting.
the system will interface predominantly with SONET equipment	select SONET .

- 3 In the **System Settings** group box, specify the **Tributary Mode Default**:

If ...	then ...
the fixed-rate tributary operation shall be the predominantly used tributary operation mode of a port	select Fixed-Rate . This is the default setting.
the adaptive-rate tributary operation shall be the predominantly used tributary operation mode of a port	select Adaptive-Rate .

- 4 In the **System Settings** group box, specify the **System Synchronisation Characteristics**. This parameter basically impacts the default settings for the expected external timing reference signals, the Synchronisation Status Message (SSM) handling, and the output timing mode of operation (please also refer to [Chapter 6, “Timing provisioning”](#) and [Chapter 17, “Timing provisioning concepts”](#)).

If ...	then ...
the system shall predominantly comply with SDH synchronisation requirements	select SDH . This is the default setting.
the system shall predominantly comply with SONET synchronisation requirements	select SONET .

-
- 5 In the **Fault Management** group box, specify the Alarm Severity Assignment Profile (ASAP) for unprotected equipment (ASAP type “Equipment unprotected”) by means of the **Equipment Alarm Severity Assignment Profile** drop-down list box.
-
- 6 In the **Fault Management** group box, specify the Alarm Severity Assignment Profile (ASAP) relating to the Data Communication Network (ASAP type “Data Communications Network”) by means of the **DCN Alarm Severity Assignment Profile** drop-down list box.
-
- 7 Click **Apply** (in the **Provision Parameters for Protection Groups or Equipment** window) or **OK** respectively (in the **Provision System** window) and confirm the resulting system message by clicking **Yes**.

END OF STEPS

Setting the system's date and time

Proceed as follows to set the system's date and time:

- 1 Select the **Date and Time** tab.
.....
- 2 In the **Date** group box, specify
 - the day by clicking on the desired date,
 - the month by means of the respective drop-down list box, and
 - the year by means of the respective drop-down list box......
- 3 In the **Time** group box, specify the time by means of the **Hour** and **Minute** drop-down list boxes and the **am** (ante meridiem) and **pm** (post meridiem) radio buttons.

Although the 12-hours time format is used when setting the system's date and time, the display format (12-hours format or 24-hours format) depends on the date and time configuration of the PC where the *WaveStar* CIT is installed. For example, 3:44 p.m. in the 12-hours format is equivalent to 15:44 in the 24-hours format.

.....
- 4 Click **Apply** (in the **Provision Parameters for Protection Groups or Equipment** window) or **OK** respectively (in the **Provision System** window) and confirm the resulting system message by clicking **Yes**.

END OF STEPS



Viewing equipment details of the system

Purpose	Use this procedure to retrieve and view the basic configuration parameters associated with the entire <i>LambdaUnite™</i> MSS system.
Related information	For related information, please refer to “Provisioning of new components” (15-6) .
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 to retrieve and view the basic system parameters. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Proceed as follows to retrieve and view the basic system parameters: 1 In the <i>WaveStar</i> CIT System View, select View → View Equipment Details... Result: The View Equipment Details window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components. 2 In the Equip tab of the selection tree, select the system (LambdaUnite(TM) MSS), and click Provision. Result: The current settings of the basic system parameters are displayed on the right-hand side of the View Equipment Details window. Reference: Please refer to “Equipment details of the system” (4-12) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** Click Close to close the **View Equipment Details** window.

END OF STEPS



Equipment details of the system

System parameters In the **View Equipment Details** window, invoked for a *LambdaUnite*[™] MSS system (see [“Viewing equipment details of the system” \(4-10\)](#)), you can view the current configuration parameters relating to the entire system.

The parameters displayed in the **View Equipment Details** window for a *LambdaUnite* MSS system are grouped as follows:

- **System Information**
- **Alarms**
- **Status**

System Information These parameters are displayed in the **System Information** group box:

Parameter	Meaning
System Type	The product family (<i>LambdaUnite</i> MSS) to which the system belongs.
TID	The Target Identifier (TID, or “name”) of the respective <i>LambdaUnite</i> MSS system.
Date/Time	The current date and time when the system information was retrieved.
Optical Interface Standard	An indication whether the system will interface predominantly with SDH or SONET equipment. Possible values are SDH (default setting) or SONET .

Alarms These parameters are displayed in the **Alarms** group box:

Parameter	Meaning
Alarm Level	The highest alarm severity of any alarm having the system as the source of alarm.
Equipment Alarm Severity Assignment Profile	The currently selected Alarm Severity Assignment Profile (ASAP) for unprotected equipment (ASAP type “Equipment unprotected”).

Parameter	Meaning
DCN Alarm Severity Assignment Profile	The currently selected Alarm Severity Assignment Profile (ASAP) relating to the Data Communication Network (ASAP type “Data Communications Network”).

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Maintenance Condition Status	An indication whether the system is currently in the maintenance condition or not. Possible values are Yes or No .
Tributary Mode Default	The configured default tributary operation mode. Possible values are Fixed-Rate (initial setting) or Adaptive-Rate .
System Synch Characteristics	The synchronisation model used. Possible values are SDH or SONET .



Configuring the shelf

Purpose	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” (15-15)
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 privilege codes of P3 and M1 to configure shelf parameters. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Proceed as follows to configure the shelf parameters: 1 Choose one of the following options to invoke the system provisioning window: 1. From the <i>WaveStar</i> CIT System View main menu, select Configuration → Provision... 2. In the <i>WaveStar</i> CIT System View shelf display, right-click on the shelf (not on a slot or circuit pack!), and select Provision Shelf 1-1... in the pop-up menu that opens. Result: The Provision Parameters for Protection Groups or Equipment window (option 1) or Provision Shelf 1-1 window (option 2) opens. In the case of the Provision Parameters for Protection Groups or Equipment window, the Equip selection tab appears on the left-hand side. If you have chosen option 1, then proceed with the next step. Otherwise proceed with Step 3.

-
- 2 Select the shelf (**Shelf 1 (DUR)**) in the **Equip** selection tab and click on **Provision**.

Result:

The selection window for the shelf parameters appears on the right-hand side of the window.

-
- 3 In the **Shelf Data** group box, set the **SS Bit Override** parameter using the respective radio button.

SS Bit Override

When **SS Bit Override** is enabled, the SS bits are set to “00” for all ports on a shelf. This setting overrides normal SS bit provisioning when interworking with non-compliant SONET network elements. When **SS Bit Override** is disabled, the SS bits are set to “10” for all ports on a shelf.

The default setting of the **SS Bit Override** parameter is **Disabled**.

-
- 4 Select the Alarm Severity Assignment Profile (ASAP) to be used for unprotected equipment (ASAP type “Equipment unprotected”; cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)) by means of the **Equipment Alarm Severity Assignment Profile (unprot.)** drop-down list box.

-
- 5 Select the Alarm Severity Assignment Profile (ASAP) to be used for protected equipment (ASAP type “Equipment with Protection State Dependence”; cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)) by means of the **Equipment Alarm Severity Assignment Profile (prot.)** drop-down list box.

END OF STEPS



Viewing equipment details of the backplane

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the backplane of a *LambdaUnite™* MSS 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 of **P1** to view the backplane parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the backplane parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **Backplane (LSRACK/BACK)**, and click **Select**.

Result:

The current settings of the backplane parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of the backplane” \(4-18\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of the backplane

Backplane parameters In the **View Equipment Details** window, invoked for the backplane, you can view the current configuration parameters relating to the backplane.

The parameters displayed in the **View Equipment Details** window for the backplane of the *LambdaUnite*[™] MSS system are grouped as follows:

- **Backplane Information**
- **Equipment Details**
- **Status**

Backplane information These parameters are displayed in the **Backplane Information** group box:

Parameter	Meaning
Backplane AID	The access identifier (AID) of the backplane.
Backplane Name	The name defined for the selected backplane.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular backplane by type and number.
Series Number	Series number of the backplane.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the backplane.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the backplane serial number representing the date and place of manufacturing.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The level of the highest alarm, either equipment, communications, or quality of service, associated with the backplane is displayed.



Viewing equipment details of the CI-CTL

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the CI-CTL (Connection Interface of the Controller) of a *LambdaUnite*[™] MSS 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 of **P1** to view the CI-CTL parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the CI-CTL parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **CI-CTL (CICTL_NCICTL_Q)**, and click **Select**.

Result:

The current settings of the CI-CTL parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of the CI-CTL” \(4-22\)](#) for an explanation of the CI-CTL parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of the CI-CTL

System parameters In the **View Equipment Details** window, invoked for the CI-CTL (Connection Interface of the Controller), you can view the current configuration parameters relating to the CI-CTL.

The parameters displayed in the **View Equipment Details** window for the CI-CTL of the *LambdaUnite™* MSS system are grouped as follows:

- **CI-CTL Information**
- **Equipment Details**
- **Status**

CI-CTL information These parameters are displayed in the **CI-CTL Information** group box:

Parameter	Meaning
CI-CTL AID	The access identifier (AID) of the CI-CTL.
CI-CTL Name	The name defined for the selected CI-CTL.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular ci-ctl by type and number.
Series Number	Series number of the CI-CTL.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the CI-CTL.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the ci-ctl serial number representing the date and place of manufacture.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The level of the highest alarm, either equipment, communications, or quality of service, associated with the ci-ctl is displayed.



Viewing equipment details of the user panel

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the user panel of a *LambdaUnite™* MSS 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 of **P1** to view the user panel parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the user panel parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View → View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **user panel (-/-)**, and click **Select**.

Result:

The current settings of the user panel parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of the user panel” \(4-26\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of the user panel

User panel parameters In the **View Equipment Details** window, invoked for the user panel, you can view the current configuration parameters relating to the user panel.

The parameters displayed in the **View Equipment Details** window for the user panel of the *LambdaUnite*[™] MSS system are grouped as follows:

- **User Panel Information**
- **Equipment Details**
- **Status**

User Panel information These parameters are displayed in the **User Panel Information** group box:

Parameter	Meaning
User Panel AID	The access identifier (AID) of the user panel.
User Panel Name	The name defined for the selected user panel.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular user panel by type and number.
Series Number	Series number of the user panel.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the user panel.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the user panel serial number representing the date and place of manufacture.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The level of the highest alarm, either equipment, communications, or quality of service, associated with the user panel is displayed.



Viewing equipment details of a Timing Interface

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the Timing Interface (TI) of a *LambdaUnite*TM MSS 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 of **P1** to view the Timing Interface parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the timing interface parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **Timing Interface (TI_N/TI_Q)**, and click **Select**.

Result:

The current settings of the Timing interface parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of a Timing Interface” \(4-30\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of a Timing Interface

System parameters In the **View Equipment Details** window, invoked for the Timing Interface, you can view the current configuration parameters relating to the Timing Interface.

The parameters displayed in the **View Equipment Details** window for the Timing Interface of the *LambdaUnite™* MSS system are grouped as follows:

- **Timing Interface Information**
- **Equipment Details**
- **Status**

Timing interface information These parameters are displayed in the **Timing Interface Information** group box:

Parameter	Meaning
Timing interface AID	The access identifier (AID) of the Timing Interface.
Timing interface Name	The name defined for the selected Timing Interface.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular Timing Interface by type and number.
Series Number	Series number of the Timing Interface.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the Timing Interface.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the Timing Interface serial number representing the date and place of manufacture.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The level of the highest alarm, either equipment, communications, or quality of service, associated with the Timing Interface is displayed.



Viewing equipment details of a Power Interface

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the Power Interface (PI) of a *LambdaUnite™* MSS 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 of **P1** to view the Power Interface parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the Power Interface parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **Power Interface (PI_N/PI_Q)**, and click **Select**.

Result:

The current settings of the Power Interface parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of a Power Interface” \(4-34\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of a Power Interface

System parameters In the **View Equipment Details** window, invoked for the Power Interface, you can view the current configuration parameters relating to the Power Interface.

The parameters displayed in the **View Equipment Details** window for the power interface of the *LambdaUnite*[™] MSS system are grouped as follows:

- **Power Interface Information**
- **Equipment Details**
- **Status**

Power Interface Information These parameters are displayed in the **Power Interface Information** group box:

Parameter	Meaning
Power Interface AID	The access identifier (AID) of the Power Interface.
Power Interface Name	The name defined for the Power Interface.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular power interface by type and number.
Series Number	Series number of the Power Interface.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the Power Interface.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the Power Interface serial number representing the date and place of manufacture.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The level of the highest alarm, either equipment, communications, or quality of service, associated with the Power Interface is displayed.



Viewing equipment details of the fan unit

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with the fan unit of a *LambdaUnite™* MSS 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 of **P1** to view the fan parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the Fan parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select **Fan fan**, and click **Select**.

Result:

The current settings of the Fan parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of the fan unit” \(4-38\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of the fan unit

System parameters In the **View Equipment Details** window, invoked for the fan unit, you can view the current configuration parameters relating to the fan unit.

The parameters displayed in the **View Equipment Details** window for the fan unit of the *LambdaUnite*[™] MSS system are grouped as follows:

- **Fan Information**
- **Equipment Details**
- **Status**

Fan information These parameters are displayed in the **Fan Information** group box:

Parameter	Meaning
Fan AID	The access identifier (AID) of the fan unit.
Fan Name	The name defined for the selected fan unit.

Equipment details These parameters are displayed in the **Equipment Details** group box:

Parameter	Meaning
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular fan unit by type and number.
Series Number	Series number of the fan unit.
CLEI Code	Common Language Equipment Identifier (CLEI) code of the fan unit.
Equipment Carrier Code	This is the Equipment Carrier Code.
Serial Number	This is the fan unit serial number representing the date and place of manufacture.

Status These parameters are displayed in the **Status** group box:

Parameter	Meaning
Alarm Level	The severity of the most severe alarm associated with the fan unit.



Provisioning a slot

Purpose Use this procedure to provision a slot, i.e. to assign an Alarm Severity Assignment Profile (ASAP) of type “Equipment with Protection State Dependence” to the slot. This assignment is necessary for alarms which have the slot as the source of alarm, such as *Circuit Pack not Present* or *Circuit Pack Type Mismatch*.

Slot provisioning can be done before the slot is equipped (preprovisioning) or during operation (“normal” provisioning).

Related information For related information, see:

- [“Slot provisioning” \(15-16\)](#)

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 privilege codes of **P3 and M1** to provision a slot.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to configure the parameters of a slot:

- 1 Depending on which way of provisioning you want to perform:

If you want to ...	then ...
assign an ASAP to a slot for preprovisioning purposes	please refer to “Preprovisioning an unequipped slot” (4-40) .
change the ASAP assignment of a slot where a circuit pack is already present	please refer to “Provisioning an already equipped slot” (4-41) .

END OF STEPS

Preprovisioning an unequipped slot

Proceed as follows to preprovision an unequipped slot:

-
- 1 Choose one of the following options to invoke the system provisioning window:
 1. From the *WaveStar* CIT **System View** main menu, select **Configuration** → **Provision...**
 2. In the *WaveStar* CIT **System View** shelf display, right-click on a slot, and select **Provision Slot # ...** (“#” represents the slot number) in the pop-up menu that opens.

Result:

The **Provision Parameters for Protection Groups or Equipment** window (option 1) or **Provision Slot** window (option 2) opens. In the case of the **Provision Parameters for Protection Groups or Equipment** window, the **Equip** selection tab appears on the left-hand side.

If you have chosen option 1, then proceed with the next step.

If you have chosen option 2, then proceed with [Step 3](#).

-
- 2 Select a slot in the **Equip** selection tab and click **Provision**.

Result:

The configurable slot parameters appear on the right-hand side of the window.

-
- 3 Select the **Alarm Severity Assignment Profile** (ASAP) to be assigned to the slot (ASAP type: “Equipment with Protection State Dependence”, cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)).

-
- 4 Click **Apply** (in the **Provision Parameters for Protection Groups or Equipment** window) or **OK** respectively (in the **Provision Slot** window) and confirm the resulting system message by clicking **Yes**.

END OF STEPS

Provisioning an already equipped slot

Proceed as follows to configure the parameters of a slot:

- 1 Choose one of the following options to invoke the system provisioning window:
 1. From the *WaveStar* CIT **System View** main menu, select **Configuration** → **Provision...**
 2. In the *WaveStar* CIT **System View** shelf display, right-click on a circuit pack, and select **Provision Circuit Pack #...** (# represents the slot number) in the pop-up menu that opens.

Result:

The **Provision Parameters for Protection Groups or Equipment** window (option 1) or **Provision Circuit Pack** window (option 2) opens. In the case of the **Provision Parameters for Protection Groups or Equipment** window, the **Equip** selection tab appears on the left-hand side.

If you have chosen option 1, then proceed with the next step.

If you have chosen option 2, then proceed with [Step 4](#).

- 2 Select a circuit pack in the **Equip** selection tab and click **Provision**.

Result:

The configurable circuit pack parameters appear on the right-hand side of the window.

- 3 Select the **Slot** tab.

- 4 Select the **Alarm Severity Assignment Profile** (ASAP) to be assigned to the slot (ASAP type: “Equipment with Protection State Dependence”, cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)).

- 5 Click **OK**, and confirm the resulting system message by clicking **Yes**.

END OF STEPS



Preprovisioning a circuit pack

Purpose	Use this procedure to preprovision a circuit pack for a certain slot in a network element.
Related information	For related information, see: • “Provisioning of new components” (15-6)
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 privilege codes of P3 and M1 to preprovision a circuit pack. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Proceed as follows to create a new circuit pack: 1 Choose one of the following options to invoke the system provisioning window: 1. From the <i>WaveStar</i> CIT System View main menu, select Configuration → Create New → Circuit Pack... 2. In the <i>WaveStar</i> CIT System View shelf display, right-click on a slot, and select Create New Circuit Pack in the pop-up menu that opens. Result: The Create New Circuit Pack window (option 1) or Establish Circuit Pack window (option 2) opens. In the case of the Create New Circuit Pack window, the Equip selection tab appears on the left-hand side. If you have chosen option 1, then proceed with the next step. If you have chosen option 2, then proceed with Step 3. 2 Select an empty slot in the Equip selection tab, and click Select Slot.

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

Please notice that circuit pack types might, for preprovisioning purposes, be selectable from the **Select CP Type** drop-down list box which are prepared for future applications.

- 4** Select the Alarm Severity Assignment Profiles (ASAPs) to be assigned to the circuit pack from the respective **Alarm Severity Assignment Profile** drop-down list boxes (ASAP types: “Equipment with Protection State Dependence” and “Equipment unprotected”, cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)).

This assignment is necessary for alarms which have the circuit pack as the source of alarm, such as Circuit Pack Failure, Circuit Pack Comm Failure, or Unit Cooling Degraded for example.

By clicking on the **View Details** button, you can call up a table with details on the ASAPs.

- 5** Click **Apply**, and confirm the resulting system message by clicking **Yes**.
-

- 6** Click **Close**.

END OF STEPS



Provisioning a circuit pack

Purpose Use this procedure to provision a circuit pack, i.e. to assign Alarm Severity Assignment Profiles (ASAPs) of type “Equipment with Protection State Dependence” and “Equipment unprotected” to the circuit pack. This assignment is necessary for alarms which have the circuit pack as the source of alarm, such as Circuit Pack Failure, Circuit Pack Comm Failure, or Unit Cooling Degraded for example.

Related information For related information, see:

- [“Circuit pack provisioning” \(15-17\)](#)

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 privilege codes of **P3 and M1** to provision a circuit pack.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to provision a circuit pack:

- 1 Choose one of the following options to invoke the system provisioning window:
 1. From the *WaveStar* CIT **System View** main menu, select **Configuration → Provision...**
 2. In the *WaveStar* CIT **System View** shelf display, right-click on a circuit pack, and select **Provision Circuit Pack #...** (# represents the slot number) in the pop-up menu that opens.

Result:

The **Provision Parameters for Protection Groups or Equipment** window (option 1) or **Provision Circuit Pack** window (option 2) opens. In the case of the **Provision**

Parameters for Protection Groups or Equipment window, the **Equip** selection tab appears on the left-hand side.

If you have chosen option 1, then proceed with the next step.

If you have chosen option 2, then proceed with [Step 3](#).

-
- 2** Select a circuit pack in the **Equip** selection tab and click **Provision**.

Result:

The configurable circuit pack parameters appear on the right-hand side of the window.

-
- 3** In the **Circuit Pack** tab, select the Alarm Severity Assignment Profiles (ASAPs) to be assigned to the circuit pack from the respective **Alarm Severity Assignment Profile** drop-down list boxes (ASAP types: “Equipment with Protection State Dependence” and “Equipment unprotected”, cf. [“Alarm Severity Assignment Profiles” \(16-26\)](#)).

-
- 4** Click **OK**, and confirm the resulting system message by clicking **Yes**.

END OF STEPS



Reassigning a circuit pack

Purpose Use this procedure to change the assignment of a slot to 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).

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.

Related information For related information, see:

- [“Circuit pack provisioning” \(15-17\)](#)
- [“Deleting a cross-connection” \(7-31\)](#)
- [“Deleting a protection group” \(7-93\)](#)

Before you begin Please note that reassignment of mandatory (core) circuit packs is not possible.

Please observe the following rules concerning the exchangeability of circuit packs:

1. The system must not be in maintenance condition.
2. Both circuit packs (the currently provisioned as well as the new circuit pack) must be optical circuit packs.
3. Both circuit packs must have the same number of ports.
4. Both circuit packs must have the same transmission capacity.
5. The current port configuration concerning Forward Error Correction (FEC) must be supported by the new circuit pack.
6. Both circuit packs must support the same tributary rates.
7. The respective slot must be empty, or the new circuit pack must already be inserted.

Required privilege code

You must have at least privilege codes of **P3 and 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.

Proceed as follows to configure circuit pack parameters:

- 1 Physically remove the currently provisioned circuit pack and insert the new circuit pack, or leave the slot empty.

Result:

In the WaveStar CIT **System View**, the circuit pack is displayed with diagonal grey lines to show that the slot is still assigned to this circuit pack.

- 2 Choose one of the following options:
 1. From the WaveStar CIT **System View** main menu, select **Configuration** → **Exchange Circuit Pack...**
 2. In the WaveStar CIT **System View** shelf display, right-click on the circuit pack you removed in [Step 1](#), and select **Exchange Circuit Pack** in the pop-up menu that opens.

Result:

If you have chosen option 1, then the **Exchange Circuit Pack** window opens with the **Equip** selection tab on the left-hand side. Proceed with the next step.

If you have chosen option 2, then the **Exchange Circuit Pack** window opens. A list with the possible new circuit packs is displayed. Proceed with [Step 3](#).

-
- 3 From the **Equip** selection tab, select the circuit pack you removed in [Step 1](#).

Result:

The **Exchange Circuit Pack** window opens. A list with the acceptable new circuit packs is displayed.

-
- 4 Select the desired circuit pack type from the list of acceptable circuit packs.

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

Result:

The new circuit pack will be autoprovisioned.

END OF STEPS



Configuring an optical SDH/SONET port

Purpose Use this procedure to configure an optical SDH/SONET port according to the needs of the network environment.

Related information For related information, see:

- [“Port and tributary provisioning” \(15-18\)](#)
- [“Reassigning a circuit pack” \(4-46\)](#)

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. [“Circuit pack provisioning” \(15-17\)](#) and [“Reassigning a circuit pack” \(4-46\)](#)).

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

Required privilege code

You must have at least privilege codes of **P3** and **M1** to configure an optical SDH/SONET port.

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Proceed as follows to configure an optical SDH/SONET port:

- 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 **Equip** 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.

-
- 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-1, 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**.

-
- 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-1, 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**.

-
- 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



Configuring an optical SDH/SONET port

Purpose Use this procedure to configure an optical SDH/SONET port according to the needs of the network environment.

Related information For related information, see:

- [“Circuit pack provisioning” \(15-17\)](#)
- [“Port and tributary provisioning” \(15-18\)](#)
- [“Provisioning a circuit pack” \(4-44\)](#)
- [“Reassigning a circuit pack” \(4-46\)](#)

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.

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

Required privilege code

You must have at least privilege codes of **P3 and M1** to configure an optical SDH/SONET port.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Invoking the port provisioning window

Proceed as follows to configure an optical SDH/SONET port:

- 1 Choose one of the following two options to invoke a relevant *WaveStar* CIT window:
 1. From the *WaveStar* CIT **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 port AID in the **Enter AID** field directly.
 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.

Result:

The port configuration parameters appear on the right-hand side of the **Provision Parameters for Protection Group or Equipment** window (option 1) or the **Provision Port** window opens (option 2). The various configuration options are grouped by means of corresponding tabs. On top of these tabs there are selection options for the **Service Condition** and the **Optical Interface Standard** of the port.

- 2 As the service condition is only relevant for setting facility loopbacks:

If ...	then ...
you want to perform a facility loopback (cf. “Facility loopback” (18-49)).	set the Service Condition to Out Of Service .
you do not want to perform a facility loopback	set the Service Condition to In Service .

- 3 If required, change the **Optical Interface Standard** to either **SDH** or **SONET** by selecting the corresponding radio button:

If ...	then ...
the system shall predominantly comply with the SDH standard	select SDH .
the system shall predominantly comply with the SONET standard	select SONET .

- 4 It is up to your discretion whether you want to configure only particular or all port parameters:

If you want to configure ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .
Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61) .

If you want to configure ...	then ...
interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i>™ MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
timing parameters	please refer to xx.
trace identifier parameters	please refer to xx.

.....
 END OF STEPS

Configuring the transmission parameters of an optical SDH/SONET port

Proceed as follows to configure the fault management parameters of an optical SDH/SONET port:

-
- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Transmission** tab of the port provisioning window.

.....

- 2 Select the **Transmission** tab.
-

- 3

If ...	then ...
The Optical Interface Standard is SDH	proceed with Step 6 .
The Optical Interface Standard is SONET	proceed with the next step.

-
- 4 In the **Transmission** group box, specify the tributary operation mode:

If ...	then ...
the fixed-rate tributary operation mode shall be used	select Fixed-Rate , and then proceed with the next step. In the fixed-rate tributary operation mode, a specific tributary substructure is expected in the incoming signal.
the adaptive-rate tributary operation mode shall be used	select Adaptive-Rate . In the adaptive-rate tributary operation mode, no specific tributary substructure is expected in the incoming signal. The port automatically adapts to the signal structure of the incoming signal.

- 5 In the **Tributary Rates Lists** group box, specify the expected tributary substructure of the incoming signal (**Input Signal Rate List**) as well as the tributary substructure of the outgoing signal in the case of unequipped (**Unequipped Output Signal**).

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 **Tributaries** group box.

Substructuring should be made by clustering

- VC-3, VC-4, VC4-4C, VC4-16C, VC4-64C (SDH)
- STS-1, STS-3c, STS-12c, STS-48c, STS-192c (SONET)

tributaries, i.e. using subsequent timeslots in the signal. The final substructure is displayed in the **Input Signal Rate List** text box.

-
- 6** In the **Transmission** group box, you may set the port monitoring mode to either **Auto**, **Monitored** or **Not Monitored** in 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.

- 7** You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
configure Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
configure fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61).

If you want to ...	then ...
configure interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i> MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
configure timing parameters	please refer to xx.
configure trace identifier parameters	please refer to xx.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS

Configuring the Optical Channel parameters of an optical SDH/SONET port

Important! The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).

Proceed as follows to configure the Optical Channel parameters of an optical SDH/SONET port:

- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Optical Channel** tab of the port provisioning window.

- 2 Select the **Optical Channel** tab.

- 3 Enable or disable the Optical Channel according to your needs:

If ...	then ...
you want to make use of out-of-band FEC	select Enabled for Optical Channel Support .
you do <i>not</i> want to make use of out-of-band FEC	select Disabled for Optical Channel Support .

- 4 You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .
configure fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61) .

If you want to ...	then ...
configure interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i> MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
configure timing parameters	please refer to xx.
configure trace identifier parameters	please refer to xx.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS

Configuring the fault management parameters of an optical SDH/SONET port

Proceed as follows to configure the fault management parameters of an optical SDH/SONET port:

- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Fault Management** tab of the port provisioning window.

- 2 Select the **Fault Management** tab.

- 3 As an option, you may set the preferred mode of bit error monitoring to monitor the bit error performance during transmission by selecting the corresponding radio button next to **Signal Degrade/Fail Mode**.

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.

- 4 As an option, you may set the **Degraded Signal Interval** to a value between 2 and 10 seconds. The default setting is 7 seconds.

The **Degraded Signal Interval** defines the measurement interval for bursty errors.

Note:

This parameter can only be set in **Burst** mode.

- 5 As an option, you may set the **Degraded Signal Threshold** to a value between 5% and 50% (in steps of 5%).

The **Degraded Signal Threshold** defines the threshold value for bursty errors.

Note:

This parameter can only be set in **Burst** mode.

-
- 6** As an option, you may set the **Degraded Signal (BER) Threshold** to one of the following values:

- 10^{-5}
- 10^{-6} (default value)
- 10^{-7}
- 10^{-8}
- 10^{-9}

The configured threshold defines the bit error ratio (BER) that must be exceeded before a **Degraded Signal** alarm is reported.

Note:

This parameter can only be set in **Poisson** mode.

-
- 7** As an option, you may set the **Excessive BER Threshold** to one of the following values:

- 10^{-3} (default value)
- 10^{-4}
- 10^{-5}

The configured threshold defines the bit error ratio (BER) that must be exceeded before an **Excessive Bit Error Ratio** alarm is reported.

Note:

This parameter can only be set in **Poisson** mode.

Important! Modifying the Forward Error Correction (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.

- 8** For ports supporting FEC, you may now configure all relevant FEC parameters.

If ...	then ...
you want to configure FEC parameters	continue with the next step.

If ...	then ...
you do not want to configure FEC parameters	continue with Step 12 .

Important! The Optical Channel needs to be enabled before out-of-band FEC can be enabled (cf. [“Configuring the Optical Channel parameters of an optical SDH/SONET port” \(4-59\)](#)).

- 9 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** radio buttons.

Possible FEC types are:

- **In-band** (default setting)
- **Out-band**

For circuit packs that do not support out-of-band FEC, the **In-band** radio button is preselected, and changing this setting is **not** possible.

-
- 10 Enable or disable FEC by selecting the **Enabled** or **Disabled** option for **FEC Encoding/Decoding**.

Enabling the **FEC Encoding/Decoding** 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.

-
- 11 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.

-
- 12 From the available ASAPs in the **Alarm Severity Profile** drop-down list box, select one according to your needs.

13 You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .
configure Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
configure interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i> MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
configure timing parameters	please refer to xx.
configure trace identifier parameters	please refer to xx.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS

Configuring the interworking parameters of an optical SDH/SONET port

Proceed as follows to configure the interworking parameters of an optical SDH/SONET port:

- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Interworking** tab of the port provisioning window.

- 2 Select the **Interworking** tab.

- 3 Specify the MS Remote Error Indication (REI) mode:

If ...	then ...
provision is made for interworking with older equipment	select Single for the MSREI Mode . Only the M1 byte is used for the Remote Error Indication.
no provision is made for interworking with older equipment	select Extended for the MSREI Mode . The M0 byte and the M1 byte are used for the Remote Error Indication.

- 4 You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .

If you want to ...	then ...
configure Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
configure fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61).
configure timing parameters	please refer to xx.
configure trace identifier parameters	please refer to xx.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS

Configuring the timing parameters of an optical SDH/SONET port

Proceed as follows to configure the timing parameters of an optical SDH/SONET port:

- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Timing** tab of the port provisioning window.

- 2 Select the **Timing** tab.

- 3

If ...	then ...
you wish to prevent the optical line from being used for synchronisation, e.g. because a timing loop might occur,	set the Force DUS to Enabled . The Synchronisation Status Message (SSM) transmitted from the port is forced to “Do not use for synchronisation” (DUS/DNU).
you wish the optical line to be used for synchronisation,	set the Force DUS to Disabled (default). In this case the actual Synchronisation Status Message (SSM) is transmitted from the port.

- 4 You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .

If you want to ...	then ...
configure Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
configure interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i> MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
configure fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61).
configure trace identifier parameters	please refer to xx.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS

Configuring the trace identifier parameters of an optical SDH/SONET port

Proceed as follows to configure the section trace identifier of an optical SDH/SONET port:

- 1 If not yet done, invoke the port provisioning window (see [“Invoking the port provisioning window” \(4-53\)](#)).

The following instructions refer to the **Trace Settings** tab of the port provisioning window.

- 2 Select the **Trace Settings** tab.

- 3 Select the format of the transmitted section trace identifier (J0 byte) from the **Transmitted Format** drop-down list box. The following formats are supported:

Specific Byte	A single byte (in hexadecimal format) using the printable T.50/ASCII character set (SONET mode).
Non-Specific Repeating Byte	A single byte with a fixed hexadecimal value of “0x01” (ITU/ETSI mode 2, for interworking with older SDH equipment).
Specific String	A 16-byte hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 checksum byte (ITU/ETSI mode 1)
64 Byte String	A 64-byte hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET mode).

- 4 Select the desired method of **CRC-7 Calculation**. Possible values are **Auto** or **Manual**.

- 5 Enter the value of the section trace identifier to be transmitted in the **Value** field.

The value is dependent on the trace identifier format and represents the information transferred in the trace identifier.

-
- 6 As an option, you may choose between a textual (**ASCII**) or a hexadecimal (**Hex.**) representation of the trace identifier value by selecting the corresponding radio button next to **Display Mode**.
-
- 7 Specify the read format of the section trace identifier by using the **Incoming Format** drop-down list box. The same formats as described for the transmitted format are available.
-
- 8 In the **Value** field in the **Incoming Identifier** group box, you can set the value of the accepted J0 byte.
-
- 9 As an option, you may choose between a textual (**ASCII**) or a hexadecimal (**Hex.**) representation of the trace identifier value by selecting the corresponding radio button next to **Display Mode**.
-
- 10 In an analogous way, specify the method of **CRC-7 Calculation**, the Value, and the Display Mode of the **Expected Identifier**.
The format of the expected section trace identifier is fix preset to **Specific String**.
-
- 11 In the **Regenerator Section** group box, enable or disable the monitoring function for trace identifier mismatches, and the consequent actions in case of a mismatch.
-
- 12 You may now proceed to configure the remaining port parameters:

If you want to ...	then ...
transmission parameters	please refer to “Configuring the transmission parameters of an optical SDH/SONET port” (4-55) .

If you want to ...	then ...
configure Optical Channel parameters	please refer to “Configuring the Optical Channel parameters of an optical SDH/SONET port” (4-59). The Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)).
configure fault management parameters	please refer to “Configuring the fault management parameters of an optical SDH/SONET port” (4-61).
configure timing parameters	please refer to xx.
configure interworking parameters	please refer to “Configuring the interworking parameters of an optical SDH/SONET port” (4-65). The interworking parameters are only applicable to STM-64/OC-192 circuit packs. <i>LambdaUnite</i> MSS systems support the extended MS REI mode (M0 and M1 byte are used for the Remote Error Indication). For interworking purposes with older equipment, the single-byte MS REI mode (M1 byte only) is also supported.
apply your settings	Verify your settings and correct if necessary. Then click Apply (in the Provision Parameters for Protection Groups or Equipment window) or OK respectively (in the Provision Slot window) and confirm the resulting system message by clicking Yes.

END OF STEPS



Viewing equipment details of an optical SDH/SONET port

Purpose Use this procedure to retrieve and view detailed equipment parameters associated with an optical port of a *LambdaUnite*[™] MSS 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 of **P1** to view the optical port parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the optical port parameters:

- 1 From the *WaveStar* CIT **System View** main menu, select **View** → **View Equipment Details...**

Result:

The **View Equipment Details** window opens. Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available system components.

- 2 In the **Equip** tab of the selection tree, select the desired port and click **Select**.

Result:

The current settings of the optical port parameters are displayed on the right-hand side of the **View Equipment Details** window.

Reference:

Please refer to [“Equipment details of an optical SDH/SONET port” \(4-74\)](#) for an explanation of the basic system parameters.

-
- 3** As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As** in the **View Equipment Details** window,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.
-

- 4** The window **View Equipment Details** contains two push buttons:
- **Refresh** to refresh the current view,
 - **Help** to invoke the online help.
-

- 5** Click **Close** to close the **View Equipment Details** window.

END OF STEPS



Equipment details of an optical SDH/SONET port

Description The optical interface standard is displayed on top of the window. This can either be SONET or SDH.

The window consists of six tabs, each describing a set of parameters:

- [“Port Data” \(4-74\)](#)
- [“Timing and Settings” \(4-75\)](#)
- [“Trace Settings” \(4-75\)](#)
- [“Optical Channel” \(4-79\)](#)
- [“Interworking” \(4-79\)](#)
- [“Port Rates” \(4-79\)](#)

Port Data The following table shows the status data which is shown in the tab **Port Data**.

Parameter	Values	Meaning
Port Information		
Port AID	–	This field displays the AID of the port.
Port Type	STM16, STM64, STM256, OC48, OC192, OC768	This field displays the type of the port.
Interface Standard	SONET, SDH	The current Interface Standard setting.
Protection type	Possible values are: • SDH 1+1 MSP, 2Fiber MS-SP, 4Fiber MS-SP • SONET 1+1, 2Fiber BLSR, 4Fiber BLSR • Unprotected	Indicate the protection scheme for this port.
Service Condition	In Service, Out of Service	The status concerning service involvement. "In Service" - Provisioning values for service shall be accepted. "Out of Service" - Provisioning values for service shall not be accepted.
Alarms		

Parameter	Values	Meaning
Highest Alarm	not alarmed, minor, major, critical	Displays the highest alarm of the port.
Alarm Severity Assignment Profile	–	The assigned Alarm Severity profile. Selection between the default and a specific ASAP.
Fault		
Loopback Status		
Port Mode	AUTO, MON (Monitored), NMON (Not Monitored)	The current port mode setting.
Eber AIS	TRUE, FALSE	When this parameter is set to FALSE, consequent actions of some maintenance signals such as line signal failure and signal degrade will not be inhibited.
Signal degrade/Fail Mode	POISSON, BURST	Displays the setting for the signal degrade/fail mode.
HP Degraded 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.
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.

Timing and Settings The following table shows the status data which is shown in the tab **Timing and Settings**.

Information field	Possible value	Meaning
Forced DUS	Enabled, Disabled	Displays wether Force DUS (Do Not Use for Synchronization) is enabled.

Trace Settings The following table shows the status data which is shown in the tab **Trace Settings**.

Information field	Possible value	Meaning
J0 (Section Trace)		

Information field	Possible value	Meaning
Transmitted Format	Values are • Specific Byte A single byte (in hexadecimal format) using the printable T.50/ASCII character set (SONET mode). • Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x01 (ITU/ETSI mode 2). • Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET mode).	The format of the trail trace is specified in this parameter.
Transmitted Identifier		
CRC-7 Calculation	AutoManual	This field displays the method of CRC-7 Calculation. • Auto - CRC is calculated and inserted by the WaveStar[®] CIT software. If the first byte of the trace is equal to the CRC over the trace, it is assumed that the value was auto-calculated. • Manual - CRC was entered manually by the user. If the first byte of the trace is not equal to the CRC over the trace, it is assumed that the value was manually inserted.
Value	–	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.

Information field	Possible value	Meaning
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· • In ASCII mode, if a series of two hexadecimal digits cannot be converted to ASCII characters, then the <i>WaveStar</i> CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). • In Hex mode, the <i>WaveStar</i> CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal digits, and so on until the full API is displayed.
Incoming Status	Normal Unavailable	This field shows the status of the Accepted TTI. If the status is not equal to "Normal", the corresponding Accepted TTI field (trace value) will be cleared and grayed out.
Incoming Format	Values are • Specific Byte A single byte (in hexadecimal format) using the printable T.50/ASCII character set (SONET mode). • Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x01 (ITU/ETSI mode 2). • Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET mode).	The format of the trail trace is specified in this parameter.
Incoming Identifier		
Value	—	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.

Information field	Possible value	Meaning
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· - In ASCII mode, if a series of two hexadecimal digits cannot be converted to ASCII characters, then the <i>WaveStar</i> CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). - In Hex mode, the <i>WaveStar</i> CIT displays the letters “hex”, a space, the two hexadecimal digits, a space, the next two hexadecimal digits, and so on until the full API is displayed.
Expected Format	Values are Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Expected Identifier		
CRC-7 Calculation	Auto Manual	This field displays the method of CRC-7 Calculation. - Auto - CRC is calculated and inserted by the CIT software. If the first byte of the trace is equal to the CRC over the trace, it is assumed that the value was auto-calculated. - Manual - CRC was entered manually by the user. If the first byte of the trace is not equal to the CRC over the trace, it is assumed that the value was manually inserted.
Value	—	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.

Information field	Possible value	Meaning
Regenerator Section		
Monitor	Enabled	This field allows to set the Regenerator Section monitor to enable or disable.
	Disabled	
Consequent Action	Enabled	This field allows to set the Regenerator Section Trace (J0) Identifier Mismatch (TIM) consequent action. to enable or disable.
	Disabled	

Optical Channel The following table shows the status data which is shown in the tab **Optical Channel**.

Information field	Possible value	Meaning
Optical Channel Support	Enabled, Disabled	This field displays whether the Optical Channel is enabled or not. Optical Channel parameters are only applicable to those circuit packs that support out-of-band FEC (OP40/9280XT ... 8650XT (KFA290 ... 353), OP10/9285XT ... 8650XT (KFA210 ... KFA482), OP10/01 ... 80/800G (KFA9, KFA81 ... 159)). The Optical Channel needs to be enabled for out-of-band FEC.

Interworking The following table shows the status data which is shown in the tab **Interworking**.

Information field	Possible value	Meaning
Insertion Mode	Fixed CChex, STS-Id	This field displays the insertion of the Z0 byte value. (Only applicable for OC48 and lower rate interfaces)
MS REI Mode	Single (M1 byte), Extended (M0/M1 byte)	This field displays the MS Remote Error Indication Mode. (Only applicable for OC192 interfaces)

Port Rates The following table shows the status data which is shown in the tab **Port Rates**.

Information field	Possible value	Meaning
Tributary Input Rate		

Information field	Possible value	Meaning
Rate	These are the possible values for: - SONET STS1, STS3c, STS12c, STS48c, STS192c - SDH VC3, VC4, VC4-4c, VC4-16c, VC4-64c	Displays the port rate.
Tributary Unequipped Output Rate		
Rate	These are the possible values for: - SONET STS1, STS3c, STS12c, STS48c, STS192c - SDH VC3, VC4, VC4-4c, VC4-16c, VC4-64c	Displays the port rate.
Port Constituent Rate (SONET Ports only)		
Rate	STS1, STS3c, STS12c, STS48c, STS192c	Displays the port rate.



Configuring an Ethernet port

Purpose Use this procedure to configure an Ethernet port(s) of the same type for the operation of a *LambdaUnite™* MSS system.

Related information For related information, see [“Gigabit Ethernet Interface” \(18-43\)](#).

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.

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

Required privilege code

You must have at least privilege codes of **P3 and M1** to configure an Ethernet 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 an Ethernet port:

- 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 **Equip** 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 Ethernet port unit. Double click on the port unit or click on the **+** in front of the unit name.
-

-
- 4 Select the desired Ethernet port. 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 [“Ethernet port parameters” \(4-86\)](#) for hints on the selection of the parameter values.
-

6	If ...	then ...
	you want to enable the repeater mode of this Ethernet port.	set the parameter Repeater Mode to Enabled . Result: In repeater mode, the “Admitted Frame Types” tab is greyed out. In Repeater mode, the VLAN Ids and Port VLAN Identifier have no meaning. When changing to repeater mode, the NE will also empty the VLAN list and reset the PVID. Reference: Continue with Step 11 .
	you want to disable the repeater mode of this Ethernet port.	set the parameter Repeater Mode to VLAN .

- 7 Click on **Apply** to change to **VLAN mode**.

Important! Before any VLAN settings can be done the port has to work in **VLAN mode**.

- 8 Select the **Admitted Frame Types** tab.

9

If ...	then ...
you want to enter a Port VLAN Identifier PVID for the VLAN-untagged incoming frames,	1. select the radio button Admitted in the field Untagged VLAN Frames. 2. In the field Port VLAN Identifier enter the Port VLAN Identifier (. Possible values: • 1 ... 4093 • No PVID Used to define that no default value is to be used. 3. In the field Default Priority select the priority for the untagged incoming frames. Possible values: • High • Low (default)
you don't want to enter a Port VLAN Identifier PVID for the VLAN-untagged incoming frames,	deselect the radio button Admitted in the field Untagged VLAN Frames .

- 10** The information field **Valid Tagged VLANs** provides a list of valid tagged VLANs. This list contains only user VLAN-tagged frames to be accepted by the ingress LAN port. The PVID, if used for VLAN-untagged frames, is not included in this list.

If ...	then ...
you want to add an entry to this list	1. Select the radio button Add in the information field VLAN List. Enables the VLAN ID List to be editable. Initially the list is filled with the current values. 2. Enter the new entry to the list. Additional info A VLAN range is denoted with two VLAN identifiers separated by a dash (-); for example, 1-3 means 1, 2 and 3. Commas and dashed can be combined; for example, "1,3-5,7" means 1, 3, 4, 5, and 7.
you want to delete an entry from this list	1. Select the radio button Delete in the information field VLAN List and enter the value to be deleted. Enables the VLAN ID List to be editable. Initially the list is filled with the current values. 2. Delete the desired entry from the list.

11

If ...	then ...
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,	1. Select the Port Data tab. 2. Set in the drop-down list box Port Mode the value to Auto. This is the default value.
there is a valid signal present at the port and you want the port to cause alarms,	1. Select the Port Data tab. 2. set in the drop-down list box Port Mode the value to Monitored .
you do not want the port to cause alarms,	1. Select the Port Data tab. 2. set in the drop-down list box Port Mode the value to Not Monitored.

-
- 12** Select the Alarm Severity Profile in the respective drop-down list box. You can choose between the default and a specific ASAP.
-

- 13** Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Ethernet port parameters”

Description The following fields/parameters are displayed on top of the window:

Parameter ...	Displays...
Port AID	the access identifier of the selected port.
Port Type	the rate of the corresponding port. Possible value: 1 GE.

The window consists of two tabs, each describing a set of parameters:

- [“Port Data” \(4-86\)](#)
- [“Admitted Frames Types” \(4-86\)](#)

Port Data The following table shows the status data which is shown in the tab **Port Data**.

Information field	Possible value	Meaning
Port Information		
Service Condition	In Service (Radio button) Out Of Service (Radio button)	This field allows to set the service condition of the port.
Protection Type	Unprotected (fixed value)	This field displays the protection scheme for this Ethernet port.
Repeater Mode	VLAN (Radio button) Repeater (Radio button)	This field allows to set the Ethernet transport to VLAN mode or to repeater mode.
Fault		
Port Mode	Auto Monitored Not Monitored	This field displays the current monitoring mode setting.
Ethernet Port PM Enabled	Enabled (Radio button) Disabled (Radio button)	This field enables or disables performance monitoring for the Ethernet port.
Alarms		
Alarm Severity Assignment Profile	<ASAP name> (24 characters max.), Default	Selection between the default and a specific ASAP

Admitted Frames Types The following table shows the status data which is shown in the tab **Admitted Frames Types**.

Information field	Possible value	Meaning
Untagged VLAN Frames		
Admitted (Checkbox)	Admitted Not Admitted	
Port VLAN Identifier,	An integer in the range 1-4093	VLAN-untagged incoming frames are tagged with a VLAN Id = PVID.
Default Priority (Drop-down list box)	High Low	Priority for untagged incoming frames.
Valid Tagged VLANs		
VLAN Id	An integer in the range [1 .. 4093]	This list contains only user VLAN-tagged frames to be accepted by the ingress LAN port. The PVID, if used for VLAN-untagged frames, is not included in this list.
Edit VLAN List		
–	Add (Radio button) Delete (Radio button)	The radio buttons Add and Delete enable to edit the “VLAN ID List” so that the user can edit this list. Additionally there is a text box to enter the VLAN ID’s to be added or deleted.



Configuring a VCG port

Purpose	Use this procedure to configure a Virtual Concatenation Group (VCG) port.
Related information	For related information, see: • “VCG Port Details” (7-105) • “Gigabit Ethernet Interface” (18-43)
Before you begin	You must be logged into the <i>WaveStar</i>® CIT and the respective network element. Required privilege code You must have at least privilege codes of P3 and M1 to configure a VCG port. Required equipment The following equipment is required to perform this task: • <i>WaveStar</i> CIT
Instructions	Complete the following steps in order to configure the parameters of a VCG port: 1 In the System View of the <i>WaveStar</i> CIT, via Configuration → Provision call up the Provision Parameters for Protection Groups or Equipment window. Result: On the left side of the window, the Equip 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 circuit pack. Double click on the circuit packt or click on the **+** in front of the unit name.
-

- 4 Select the desired VCG. 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 [“Ethernet port parameters” \(4-86\)](#) for hints on the selection of the parameter values.
-

- 6 Select the **LCAS** tab.
-

7

If ...	then ...
you want to enable the Link Capacity Adjustment Scheme for this VCG.	Select the Enabled radio button besides LCAS Mode .
you want to disable the Link Capacity Adjustment Scheme for this VCG.	Select the Disabled radio button besides LCAS Mode . Reference: Continue with Step 9 .

- 8 Enter the desired values for the parameters **WTR Time** and **Hold-Off Time**.
-

9

If ...	then ...
you want to set the Interface Standard for the selected VCG to SDH,	1. Select the VCG Data tab. 2. Select the SDH radio button.
you want to set the Interface Standard for the selected VCG to SONET,	1. Select the VCG Data tab. 2. Select the SONET radio button.

10

If ...	then ...
you want the VCG to cause alarms during normal operation, but not if there is no valid signal present at the VCG, e.g. during preprovisioning,	1. Select the VCG Data tab. 2. Set in the drop-down list box VCG Monitoring Mode the value to Auto. This is the default value.
there is a valid signal present at the port and you want the port to cause alarms,	1. Select the VCG Data tab. 2. set in the drop-down list box VCG Monitoring Mode the value to Monitored .
you do not want the port to cause alarms,	1. Select the VCG Data tab. 2. set in the drop-down list box VCG Monitoring Mode the value to Not Monitored.

11 Select the Alarm Severity Profile in the respective drop-down list box. You can choose between the default and a specific ASAP.

12 Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



VCG port parameters

Description The following fields/parameters are displayed on top of the window:

<i>Parameter ...</i>	<i>Displays...</i>
VCG AID	the access identifier of the selected VCG port.
Port Type	the rate of the corresponding port. Possible value: VCG.

The **View VCG Port Details** window consists of two tabs, each describing a set of parameters:

- [“VCG Data” \(4-91\)](#)
- [“LCAS” \(4-91\)](#)

VCG Data The following table shows the status data which is shown in the tab **VCG Data**.

Information field	Possible value	Meaning
Interface Standard	SONET SDH	This field displays the current interface standard.
VCG Monitoring Mode	Monitored Not Monitored	This field displays the current monitoring mode setting.

LCAS The following table shows the status data which is shown in the tab **LCAS**.

Information field	Possible value	Meaning
LCAS Mode	Enabled Disabled	This parameter shows the operation mode of the Link Capacity Adjustment Scheme for this VCG.
WTR (Wait To Restore) Time	0 ... 60 min in steps of 1 min	This parameter shows the delay time which is applied before the active path switches back to the original one after restoration.
Hold-Off Timer	0 ... 10 sec in steps of 0.1 sec.	Via different hold-off times it can be defined which protection should switch first.



Configuring a tributary

Purpose Use this procedure to configure tributaries belonging to optical signals.

Related information For related information, see:

- [“Reassigning a circuit pack” \(4-46\)](#)
- [“Configuring an optical SDH/SONET port” \(4-52\)](#)

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” \(4-46\)](#) and [“Configuring an optical SDH/SONET port” \(4-52\)](#)).

Required privilege code

You must have at least privilege codes of **P3 and 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 **Equip** selection tab is displayed. The shelf belonging to the system is shown.

- 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 [“VCG tributary details” \(7-99\)](#) for supporting information on the parameters.
-

- 7** Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Removing equipment from the system

Purpose 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” \(7-31\)](#))
- Delete protection groups in which the equipment you want to delete is involved (cf. [“Deleting a protection group” \(7-93\)](#))
- Physically remove the equipment.

Required privilege code

You must have at least a privilege code of **P3** 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.

Proceed as follows 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 **Equip**. You can delete 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



Viewing an equipment protection group

Purpose Use this procedure to query the status of an equipment protection group.

Related information For related information, see:

- [“Protection mechanisms” \(18-13\)](#)
- [“Protection configurations” \(18-52\)](#)
- [“XC320 equipment protection” \(15-19\)](#)

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 privilege codes of **M1 and P1** to query the status of an equipment protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows 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 **1+1 Equipment estgrp** in the tab **Ptn Grp** on the left side of the window and click on the push-button **Select..**

Result:

The right part of the window opens, the status data for the protection group are displayed.

Reference:

The displayed parameters are described in [“Parameters for a 1+1 equipment protection” \(4-98\)](#).

-
- 3** Click the **Refresh** button on this right side, the status data are updated.

END OF STEPS



Parameters for a 1+1 equipment protection

Fields and Parameters 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” (15-9)	The AID defined for the selected protection group.
Protection Type	Switch Fabric	
Circuit Pack Type(s)	XC320	The circuit pack type for which the equipment protection has been established.
Working AID(s)	cf. “Overview of access identifiers” (15-9)	The circuit pack AID(s) of the worker.
Protecting AID(s)	cf. “Overview of access identifiers” (15-9)	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	EF or NONE	The fault reason associated with worker/protection side.
Active Unit	WKG, PROTN	The unit (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.



Protection Switch (1+1 Equipment)

Purpose This window is used to display the settings for the selected protection group.

After expanding of the bay and shelf categories from the equipment explorer and highlighting the desired pack the Select button should be pressed.

Fields and Parameters The following fields/parameters are available:

<i>Parameter ...</i>	<i>Displays...</i>
Protection Group AID	the access identifier (AID) for the selected protection group.
Protection Type	the type of protection group for which details are being displayed.
Side 0 AID(s)	the circuit pack AID(s) of side 0.
Circuit Pack Type(s)	the value of the selected circuit pack type.
Side 0 Alarm Status	the highest alarm status associated with Side 0.
Side 1 AID(s)	the circuit pack AID(s) of side 1.
Circuit Pack Type(s)	the value of the selected circuit pack type.
Side 1 Alarm Status	the highest alarm status associated with Side 1.
Active Side	whether Side 0 or Side 1 is active.

Buttons and Actions The following options are available:

<i>If you select ...</i>	<i>then ...</i>
Switch Type	From the pull down menu a switch type can be selected. Possible values are: Clear Forced, Forced to Side 0, Forced to Side 1, Manual to Side 0, Manual to Side 1.



Switching a 1+1 equipment protection

Purpose 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” \(18-13\)](#)
- [“Protection configurations” \(18-52\)](#)
- [“Viewing an equipment protection group” \(4-96\)](#)

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.

Please also observe the recommendations given in [“Important protection switching details” \(15-20\)](#).

Required privilege code

You must have at least privilege codes of **M4 and P1** to switch a 1+1 equipment protection.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Proceed as follows 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 **1+1 Equipment estgrp** in the tab **Ptn Group** on the left side of the window and click on the push-button **Select**.

Result:

Some data of the protection group are displayed.

Important! Do not apply a manual or forced equipment protection switch command less than one minute after a previous equipment protection switch event to prevent traffic hits.

- 3** Select the desired switch request in the field **Switch Type**. The following options are available:

- **Clear**
- **Forced To Working**
- **Forced To Protection**
- **Manual To Working**
- **Manual To Protection**

-
- 4** Click on **Apply**.

END OF STEPS



Retrieving an equipment list

When to use Use this procedure to retrieve and view the basic equipment lists of the *LambdaUnite™* MSS 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 of **S1** or **P1** to view the equipment details lists.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to view the equipment lists:

1	If you want to...	then ...
	retrieve the Pack/Backplane List .	select Reports → Equipment Lists → Pack/Backplane... in the <i>WaveStar</i> CIT System View. • The Circuit Pack List window opens. • Highlight the shelf in the equipment tab by clicking on it and click Select. • The Circuit Pack List - UNITE-LambdaUnite(TM)MSS window opens. The parameters of this window are described in: “Equipment list of a circuit pack/backplane” (4-107)

If you want to...	then ...
retrieve the Shelf List .	select Reports → Equipment Lists → Shelf... in the <i>WaveStar</i> CIT System View. • The Shelf List window opens. • Highlight the system (UNITE-LambdaUnite(TM)MSS) or the bay by clicking on it and click Select. • The Shelf List - UNITE-LambdaUnite(TM)MSS window opens. The parameters of this window are described in: “Equipment list of the shelf” (4-108)
retrieve the Pack List .	select Reports → Equipment Lists → Pack... in the <i>WaveStar</i> CIT System View. • The Circuit Pack List window opens. • Highlight the shelf in the equipment tab by clicking on it and click Select. • The Circuit Pack List - UNITE-LambdaUnite(TM)MSS window opens. The parameters of this window are described in: “Equipment list of a circuit pack/backplane” (4-107)

If you want to...	then ...
retrieve the Port List .	select Reports → Equipment Lists → Port... in the <i>WaveStar</i> CIT System View. • The Port List window opens. • Highlight the desired circuit pack by clicking on it and click Select. • The Transmission Port List - UNITE-LambdaUnite(TM)MSS window opens and the data for the ports of the selected circuit pack are shown. The parameters of this window are described in: “Equipment list of a port” (4-109)
retrieve the VC Group List .	select Reports → Equipment Lists → VCG... in the <i>WaveStar</i> CIT System View. • The VC Group List window opens. • Highlight the desired ethernet circuit pack by clicking on it and click Select. • The VC Group List - UNITE-LambdaUnite(TM)MSS window opens and the data for the virtual concatenation groups of the selected circuit pack are shown. The parameters of this window are described in: “Equipment list of a virtual concatenation group (VCG)” (4-111)

If you want to...	then ...
retrieve the Tributary List .	select Reports → Equipment Lists → Misc.Discretes... in the <i>WaveStar</i> CIT System View. • The Tributary List window opens. • Highlight the desired circuit pack by clicking on it and click Select. • The Tributary List - UNITE-LambdaUnite(TM)MSS window opens and the data for the tributaries of the selected circuit pack are shown. The parameters of this window are described in: “Equipment list of a tributary” (4-113)
retrieve the Miscellaneous Discretes .	select Reports → Equipment Lists → Miscellaneous Discretes... in the <i>WaveStar</i> CIT System View. • The Miscellaneous Discretes List window opens. • Highlight the Misc. Discretes by clicking on it and click Select to display all miscellaneous discretes or highlight Input or Output to display either only the input or the output miscellaneous discretes. • The Miscellaneous Discretes List - UNITE-LambdaUnite(TM)MSS window opens. The parameters of this window are described in: “Equipment list of the Miscellaneous Discretes” (4-114)

-
- 2 As an option, you may store the current system parameters as a standard text file (“*.txt”) by:
1. clicking **Save As**,
 2. specifying the file name and its location in the **Save As Dialog** window that opens, and
 3. finally clicking **Save** in the **Save As Dialog** window.

3 The report list windows also contain the following push buttons:

- **Print** to print the current list,
- **Refresh** to refresh the current view,
- **Help** to invoke the online help.

4 Click **Close** to close the window.

END OF STEPS



Equipment list of a circuit pack/backplane

Purpose The **Pack/Backplane List** window shows a list of all circuit packs in the shelf.

Parameters The following table shows the parameters of the **Pack/Backplane List** window of the *LambdaUnite*[™] MSS system:

Parameter	Meaning
Circuit Pack Type	The name and qualifier of the circuit pack that has been provisioned for the slot. (It may or may be not the circuit pack type that is inserted.)
AID	The AID defined for the selected circuit pack/backplane.
Equip. unprot. ASAP	Displays the name of the provisioned Alarm Profile.
Apparatus Code	ASCII name assigned by the manufacturer to identify a particular circuit pack by pack type and number or the backplane.
Series Number	Series number of the circuit pack/backplane. (Indicates interchangeability among the circuit packs of the same circuit pack type.)
CLEI Code	CLEI code of the circuit pack/backplane.
ECI Code	Equipment Carrier Code (ECI) code of the circuit pack/backplane.
Serial Number	Serial number of the circuit pack/backplane.



Equipment list of the shelf

Purpose The **Shelf List** window shows a list of all parameters of the shelf..

Parameters The following table shows the parameters of the **Shelf List** window of the *LambdaUnite*[™] MSS system:

Parameter	Meaning
Shelf AID	The access identifier (AID) of the shelf.
ON Cable Pair Identifier	This is the physical shelf number.
Electrical DXI(1)	This is the Digital Cross Connect Interface.
Electrical DXI(2)	This is the Digital Cross Connect Interface.
Aisle Visual Alarm Interface Shelf	This is the AID of the shelf which has been user designated to display the alarms for this shelf.
Equipment Alarm Severity Assignment Profile	The name of the provisioned equipment alarm severity assignment profile (ASAP).
Shelf Type	The shelf type.



Equipment list of a port

Purpose The **Port List** window shows a list of all ports of a circuit pack.

Different parameters are displayed, depending on the port type:

- SDH/SONET ports
- Gigabit Ethernet ports

Parameters for SDH/SONET ports The following table shows the parameters of the **Port List** window for the SDH/SONET ports of the *LambdaUnite™* MSS system:

Parameter	Meaning
Port AID	The access identifier of the selected port.
Port Type	The type of the associated optical interface port.
Optical Wavelength	Displays the optical wavelength of the port.
Optical Distance	Displays the type of application to which the optical transmitter on this port is suited.
Constituent Rate	This is a list of the following rates bandwidth: • STS-1/3c/12c/48c/192c (SONET ports) • VC3/4/4C/16C/64C (SDH ports)
DCC Channel #	This is the DCC channel status of the port.
Force DUS	Shows the status of the function Force DNU or DUS.
Optical Interface Standard	Displays the optical interface standard: • SDH • SONET.
Signal Degrate Threshold	This threshold is the optical line bit error rate (signal degrade) threshold. If the value of Signal Degrade/Fail Mode is POISSON this field is displayed, If the Signal Degrade/Fail Mode is BURST this field is dimmed or removed.
Failure Threshold	This threshold is the optical line excessive bit error rate (signal failure). If the value of Signal Degrade/Fail Mode is POISSON this field is displayed, If the Signal Degrade/Fail Mode is BURST this field is dimmed or removed.

Parameter	Meaning
ASAP	The name of the incoming equipment alarm severity assignment profile (ASAP).

Parameters for Gigabit Ethernet ports

The following table shows the parameters of the **Port List** window for the Gigabit Ethernet ports of the *LambdaUnite* MSS system:

Parameter	Meaning
Port AID	The access identifier of the selected port.
Port Type	The type of the associated ethernet interface port.
Service Conditions	This field displays the current service conditions setting.
Protection Type	This field displays the protection scheme for this Ethernet port.
Repeater Mode	This field displays the current repeater mode setting.
Port Mode	This field displays the current monitoring mode setting.
Far Side Facility Loopback Status	This field displays the current facility loopback setting.
Remote Fault Status	This field shows the fault status of the remote link partner.
Ethernet Port PM Enable	This field displays the current ethernet port PM setting.
Alarm Level	This field displays the current alarm level.
Alarm Severity Profile	The name of the equipment alarm severity assignment profile (ASAP).
Auto Negotiation Status	This field displays the current auto negotiation setting.
Flow Control Mode	This field displays the current flow control mode setting.
Flow Control Mode Operation	This field displays the current flow control mode operation setting.
Port VLAN Identifier	VLAN-untagged incoming frames are tagged with a VLAN Id = PVID.
Default Priority	Priority for untagged incoming frames.
VLAN ID	This list contains only user VLAN-tagged frames to be accepted by the ingress LAN port. The PVID, if used for VLAN-untagged frames, is not included in this list.



Equipment list of a virtual concatenation group (VCG)

Purpose The **VC Group List** window shows a list of all virtual concatenation groups of a Gigabit Ethernet pack.

Parameters The following table shows the parameters of the **VC Group List** window of the *LambdaUnite™* MSS system:

Parameter	Meaning
VCG AID	The access identifier of the selected VCG port.
Interface Standard	This field displays the current interface standard.
VCG Trib AID	The access identifier of the selected VCG tributary.
Transmitted Sequence Number	This is a list with the Transmitted Sequence Number of the VCG Tributaries.
Accepted Sequence Number	A received sequence number is considered an accepted sequence number, if it is identical in three consecutive MF1s. Sequence numbers are not evaluated when the Link Capacity Adjustment Scheme (LCAS) protocol is active.
Input VCG Membership	This list shows whether the tributary takes part in the transmission of its owning VCG in input direction.
Input VCG Membership Status	This field shows the status of the tributary related to its VCG membership in input direction.
Output VCG Membership	This list shows whether the tributary takes part in the transmission of its owning VCG in output direction.
Output VCG Membership Status	This field shows the status of the tributary related to its VCG membership in output direction.
VCG Monitoring Mode	This field displays the current monitoring mode setting.
Tributary Input Signal Rate List	This field shows the tributary structure of the VCG port in input direction.
Tributary Unequipped Output Signal Rate List	This field shows the tributary structure of the VCG port in output direction.
LCAS Mode	This parameter shows the operation mode of the Link Capacity Adjustment Scheme for this VCG.
WTR Time	This parameter shows the delay time which is applied before the active path switches back to the original one after restoration.

Parameter	Meaning
Hold-off Time	Via different hold-off times it can be defined which protection should switch first.



Equipment list of a tributary

Purpose The **Tributary List** window shows a list of all tributaries of a port.

Parameters The following table shows the parameters of the **Tributary List** window of the *LambdaUnite*[™] MSS system:

Parameter	Meaning
AID	The access identifier of the selected tributary.
Port Type	The type of the associated port.
Trib Type	The type of the associated tributary.
Alarm Level	This field displays the current alarm level.
Loopback Status	This field displays the current loopback state.
Trib Mode	This field displays the current mode of the tributary.
Alarm Severity Profile	The name of the equipment alarm severity assignment profile (ASAP).
Path Trace Read Format	Read Format of Optical Channel Path trace message.



Equipment list of the Miscellaneous Discretes

Purpose The **Miscellaneous Discretes List** window shows a list of all (input and/or output) Miscellaneous Discretes.

Parameters The following table shows the parameters of the **Miscellaneous Discretes List** window of the *LambdaUnite™* MSS system:

Parameter	Meaning
AID	The access identifier of the selected Miscellaneous Discretes.
Name	This field displays the Input Miscellaneous Discrete provisioned name (or blank if not set).
ASAP	This field displays the Alarm Severity Assignment Profile (ASAP) assigned to the Miscellaneous Discrete Inputs.
Environment Message	This field displays the condition description associated to this MDI port. This description is sent with the alarm generated from the MDI port.
Environmental Alarm Inversion	This field displays the current state of the alarm inversion
Control Status	This field displays the Output Miscellaneous Discrete control status, the current On/Off state.
Probable Cause	This field displays the probable cause (type of alarm indication) which is assigned to the MDO port.



Configuring Miscellaneous Discrete Outputs

Purpose Use this procedure to provision Miscellaneous Discrete Outputs (MDOs).

Related information Please also refer to [“Miscellaneous Discretes” \(16-52\)](#).

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

Required privilege

You must have at least a privilege code of **M3** to provision MDOs.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar CIT

Instructions

- 1 From the WaveStar CIT **System View**, select **Configuration** → **Misc. Discretes...**

Result:

The **Configure Miscellaneous Discretes** window opens.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available Miscellaneous Discretes.

- 2 Select the desired MDO in the selection tree by clicking on the “+” sign next to **Misc Discretes**, then on the “+” sign next to **Output**, and finally selecting the MDO from the expanded list.

Alternatively, you may directly enter the AID of the desired MDO (misc_out1, misc_out2, ... misc_out8) into the **Enter AID** field.

- 3 Click **Select** in the lower left-hand corner of the window.

Result:

The MDO-related information is displayed on the right-hand side of the **Configure Miscellaneous Discretes** window.

-
- 4 As an option, you may assign a name to the selected MDO (or change an existing name) by entering the new name into the **Name** field.

The MDO name is an alphanumeric string of up to 26 characters. The following characters are permitted:

- Upper-case and lower-case letters (A ... Z, a ... z),
 - Spaces (“ ”),
 - Periods (“.”).
-

- 5 Proceed as follows depending on whether you want to operate the MDO in automatic or manual mode:

If ...	then ...
want to operate the MDO in <i>automatic</i> mode	make sure that the Assign Probable Cause checkbox is checked, and proceed with the next step.
want to operate the MDO in <i>manual</i> mode	make sure that the Assign Probable Cause checkbox is <i>not</i> checked, and proceed with Step 7 .

- 6 Select the probable cause of the alarm, which shall cause the MDO to switch, from the **Selected Probable Cause** drop-down list box.
-

- 7 Click **Apply** and confirm your settings by clicking **Yes** in the confirmation window that opens.
-

- 8 Repeat [Step 2](#) to [Step 7](#) for all other MDOs you want to configure.
-

- 9 Click **Close** to close the **Configure Miscellaneous Discretes** window.

END OF STEPS



Activating or deactivating Miscellaneous Discrete Outputs manually

Purpose Use this procedure to manually activate or deactivate Miscellaneous Discrete Outputs (MDOs).

Related information Please also refer to [“Miscellaneous Discretes” \(16-52\)](#).

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

Required privilege

You must have at least a privilege code of **M3** to activate or deactivate MDOs manually.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar CIT

Instructions

- 1 From the WaveStar CIT **System View**, select **Fault** → **Operate Output Misc. Discretes...**

Result:

The **Operate Miscellaneous Discrete Outputs** window opens.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available Miscellaneous Discrete Outputs.

- 2 Select the desired MDO in the selection tree by clicking on the “+” sign next to **Misc Discretes**, then on the “+” sign next to **Output**, and finally selecting the MDO from the expanded list.

Alternatively, you may directly enter the AID of the desired MDO (misc_out1, misc_out2, ... misc_out8) into the **Enter AID** field.

- 3 Click **Select** in the lower left-hand corner of the window.

Result:

The right-hand side of the **Operate Miscellaneous Discrete Outputs** window is populated.

-
- 4 From the **Control Status** drop-down list box, and depending on the actual state of the MDO, select:
- **On** to activate (switch on) an MDO currently switched off, or
 - **Off** to deactivate (switch off) an MDO currently switched on.

-
- 5 Click **Apply** and confirm your settings by clicking **Yes** in the confirmation window that opens.

-
- 6 Click **Close** to close the **Operate Miscellaneous Discrete Outputs** window.

END OF STEPS



Replacing an XC320 circuit pack by an XC320/A circuit pack

Purpose Use this procedure, for example during a reconfiguration of the shelf, to replace a circuit pack XC320 by a circuit pack XC320/A.

Before you begin You or a service technician need to be on-site at the NE to replace a circuit pack.

Make sure the required equipment listed below is available and within easy reach.

Required equipment

The following equipment is required to perform this procedure:

- A replacement circuit pack (XC320/A).
If the slot contains only one XC320 circuit pack, additionally one spare XC320 circuit pack is needed.
- Blank faceplates to cover unequipped slots.
- WaveStar® CIT.

Related Information For related information please refer to the *Alarm Messages and Trouble Clearing Guide, Chapter 1*.

NE with one XC320 circuit pack to exchange



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 as described in the “Alarm Messages and Trouble Clearing Guide, Chapter 1”.

Proceed as follows to replace a XC320 circuit pack by a XC320/A circuit pack:

- 1** Using the WaveStar CIT, preprovision the protection slot as an XC320 circuit pack.

-
- 2 Perform a forced switch to the worker XC320 circuit pack.
Important! Make sure to perform the forced switch not on the empty slot.
.....
- 3 Remove the blank faceplate of the protection slot.
Important! Do not leave unequipped slots uncovered for more than ten minutes.
.....
- 4 Insert the spare XC320 circuit pack into this preprovisioned protection slot and wait until it finished the boot-up and comes up properly.
Important! Make sure that you have inserted a XC320 circuit pack, not a XC320/A circuit pack.
.....
- 5 Release the forced switch to the worker XC320 circuit pack and perform a forced switch to this new XC320 circuit pack in the protection slot.
Check that the traffic is ok.
.....
- 6 Remove the other XC320 circuit pack of the worker slot and deprovision the slot by *WaveStar* CIT.
.....
- 7 Insert the new XC320/A circuit pack into this slot and wait until it finished the boot-up and comes up properly.
.....
- 8 Release the forced switch to the active XC320 and perform a forced switch to this new XC320/A circuit pack in the worker slot.
Check that the traffic is ok.
.....
- 9 Remove the XC320 circuit pack of the protection slot and deprovision this slot by *WaveStar* CIT.
.....
- 10 Cover the protection slot with a blank faceplate.
.....

Important! Do not leave unequipped slots uncovered for more than ten minutes.

-
- 11** Release the forced switch to the new XC320/A circuit pack.

END OF STEPS

**NE with two XC320 circuit
packs to exchange**



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 as described in the “Alarm Messages and trouble clearing Guide, Chapter 1”.

Proceed as follows to replace two XC320 circuit packs by two XC320/A circuit packs:

-
- 1** Using the *WaveStar* CIT, perform a forced switch to the worker XC320 circuit pack.
-
- 2** Remove the XC320 circuit pack of the protection slot and dep provision this slot by *WaveStar* CIT.

Important! Do not leave unequipped slots uncovered for more than ten minutes.

-
- 3** Insert the XC320/A circuit pack into this preprovisioned protection slot and wait until it finished the boot-up and comes up properly.
-
- 4** Release the forced switch to the worker XC320 circuit pack and perform a forced switch to this new XC320/A circuit pack in the protection slot, check, that the traffic is ok.
-

-
- 5 Remove the other XC320 circuit pack of the (now) protection slot and deprovision the slot by *WaveStar* CIT.

Important! Do not leave unequipped slots uncovered for more than ten minutes.

-
- 6 Insert the new XC320/A circuit pack into this slot and wait until it finished the boot-up and comes up properly.

-
- 7 Release the forced switch to the worker XC320.

.....
E N D O F S T E P S
.....





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.

Related information

Please also refer to [Chapter 16, “Alarm management concepts”](#).

Contents

Setting the view preferences	5-3
Retrieving the WaveStar[®] CIT NE Alarm List	5-6
The WaveStar CIT NE Alarm List	5-8
Retrieving the WaveStar CIT NE Alarm Log	5-12
The WaveStar CIT NE Alarm Log	5-14
Identifying SDH tributaries in alarm messages	5-19
Performing an LED test	5-23
Retrieving Alarm Severity Assignment Profile (ASAP) information	5-24
Creating a new Alarm Severity Assignment Profile (ASAP)	5-27
Creating non-reporting Alarm Severity Assignment Profiles (ASAPs)	5-29

<u>Modifying an existing Alarm Severity Assignment Profile (ASAP)</u>	<u>5-31</u>
<u>Deleting an Alarm Severity Assignment Profile (ASAP)</u>	<u>5-34</u>
<u>Assigning the same Alarm Severity Assignment Profile (ASAP) to all equipment components of a particular type</u>	<u>5-36</u>
<u>Setting the port monitoring mode</u>	<u>5-39</u>
<u>Configuring fault management parameters of an SDH/SONET port</u>	<u>5-41</u>
<u>Enabling or disabling autonomous alarm forwarding</u>	<u>5-46</u>
<u>Configuring Miscellaneous Discrete Inputs</u>	<u>5-48</u>

Setting the view preferences

Purpose Use this procedure to set various preferences concerning the signalling of alarms and the appearance of the *WaveStar*® CIT **System View**.

Setting the view preferences includes:

1. Setting the preferred alarm format for presenting alarm severities in the alarm status display, in the *WaveStar* CIT **NE Alarm List**, and in Alarm Severity Assignment Profiles (ASAPs) in either of the following two formats :
 - SONET format:
Critical/Major/Minor (**CR/MJ/MN**),
 - SDH format:
Prompt/Deferred/Info (**PR/DF/INF**).
 Please also refer to [“Alarm format preferences” \(16-13\)](#).
2. Enabling or disabling audible alarms.
3. Enabling or disabling the automatic adaptation of the *WaveStar* CIT **System View** window size.

Before you begin Prior to setting the view preferences, 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 privilege codes of **S1 and P1** to set the view preferences.

Required equipment

The following equipment is required to perform this procedure:

- *WaveStar* CIT

Instructions Proceed as follows to set the preferred alarm format:

- 1 From the *WaveStar* CIT **System View** main menu, select **View → Preferences...**

Result:

The **Preferences** window opens.

-
- 2 Select the preferred alarm format in the **LambdaUnite(TM) MSS Alarm Format** group box.

If ...	then ...
you prefer the SONET alarm format	choose SONET Format (CR/MJ/MN)
you prefer the SDH alarm format	choose SDH Format (PR/DF/INF)

-
- 3 Set your preferences concerning audible alarms in the **CIT Audible Alarm Alerting** group box.

If ...	then ...
you want alarms to be signalled by a beep (in addition to the standard alarm signalling)	choose CIT Audible Alarms Enabled
you do not want alarms to be signalled by a beep	choose CIT Audible Alarms Disabled

-
- 4 Select the preferred size of the *WaveStar* CIT **System View** window in the **System View Resizing** group box.

If ...	then ...
you want the size to be automatically adapted to the shelf display	choose Auto Resizing Enabled
the <i>WaveStar</i> CIT System View window shall always be displayed in its default size	choose Auto Resizing Disabled

-
- 5 You may now apply the selected preferences to the current session only (**not** possible for the alarm format!), or declare the preferences to

be your default settings.

If ...	then ...
you want to apply the selected preferences for CIT Audible Alarm Alerting and System View Resizing to the current session only (<i>not</i> possible for the alarm format!)	click OK .
you want to change the alarm format and/or declare the selected preferences to be your default settings	click Save , then OK .

Result:

The **Preferences** window is closed.

The preferences for **CIT Audible Alarm Alerting** and **System View Resizing** make an impact on the current *WaveStar* CIT session. The preferences for the **LambdaUnite(TM) MSS Alarm Format** make no impact on the current session but will affect future sessions provided that you have chosen the **Save** option.

END OF STEPS



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” \(5-8\)](#)

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 opens.

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 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 close the window	click Close button.
you want to update the alarm list	click Refresh (cf. Step 2).
you want to get online help information	click Help button.

END OF STEPS



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).

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. The possible values depend on the Preferences setting for the alarm format, cf. “Alarm format preferences” (16-13) .
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 also refer to “Overview of AIDs” (15-10)). Please note that a special display format is being used for SDH tributary AIDs, please refer to “Identifying SDH tributaries in alarm messages” (5-19).
Date Time	These two columns indicate the date and time of occurrence, i.e. the date and time the alarm was reported by the NE. The date and time format depends on the country in which the <i>WaveStar</i> CIT is being used. Please refer to “Configuring the basic system parameters” (4-5) for information on how to set the date and time of the system.
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 (-).

Column	Meaning
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.
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 (Miscellaneous Discrete Inputs) • EQPT Equipment • OC-3, OC-12, OC-48, OC-192, OC-768 Optical transport signals (SONET): OC-3 (155 Mbit/s), OC-12 (622 Mbit/s), OC-48 (2.5 Gbit/s), OC-192 (10 Gbit/s) or OC-768 (40 Gbit/s) • OUTT Output timing • STM-1, STM-4, STM-16, STM-64, STM-256 Optical transport signals (SDH): STM-1 (155 Mbit/s), STM-4 (622 Mbit/s), 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 (VCG) tributary

Column	Meaning
Alarm Type	This column indicates the alarm category. The alarm category indicates the functional area to which an alarm belongs. The NE alarms are assigned to the following alarm categories: • Communication This alarm category comprises DCN, synchronisation and transmission alarms. Therefore, the “Communication” alarm category is further divided into: - Communication (DCN) - Communication (Synchronisation) - Communication (Transport) • Environment This alarm category is used for environmental alarms, detected by means of Miscellaneous Discrete Inputs (MDIs). • Equipment This alarm category is used for hardware- and configuration-related alarms and alarms concerning the internal communication. • Processing error This alarm category is used for alarms related to problems or failures of the control system software, due to overload situations for example.
Description	This column describes the alarm’s probable cause in more detail.

Notes:

1. The sequence of alarm list columns in this table reflects the ordering of the columns (from left to right) in the default alarm list display.
2. The ordering of the columns in the alarm list display can be modified by clicking on the column header, holding down the mouse button, and dragging the column to the desired position.
3. The column width can be resized by selecting the small outside margin of a column with the mouse, holding down the mouse button, and adjusting the column’s width.

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 close 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 a similar fashion as in the NE alarm list; please refer to [“The WaveStar CIT NE Alarm List” \(5-8\)](#).

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 **Select Start Date/Time for NE Alarm Log** window opens.

There are two possible ways to retrieve the alarm log:

1. Retrieving the alarm log for a certain period of time by specifying the date and time for the alarm log to start.

Please note that there is no option to select a stop time. The alarm log is always returned up to the current time.

2. Retrieving the entire alarm log.

2

If ...	then ...
you want to retrieve the alarm log for a certain period of time	proceed as follows: 1. select the Retrieve for specified interval radio button in the Option group box, 2. select the start date and time using the corresponding window controls in the Start Date/Time group box, 3. click OK.
you want to retrieve the entire alarm log	proceed as follows: 1. select the Retrieve all radio button in the Option group box, 2. click OK.

END OF STEPS



The WaveStar[®] CIT NE Alarm Log

The “NE Alarm Log” window

The *WaveStar* CIT provides a list of history alarms, the **NE Alarm Log**, to retrieve 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.

Structure of the “NE Alarm Log”

The following table explains the structure of the *WaveStar* CIT **NE Alarm Log**:

Column	Meaning
Alarm Issue Point	This column indicates the alarm issue point, i.e. the access identifier (AID) of the component for which an alarm has being reported (“exttmg1”, “1-1-#-#-ctlw-nvm” or “1-1-#-#-12-v4” for example, please also refer to “Overview of AIDs” (15-10)). Please note that a special display format is being used for SDH tributary AIDs, please refer to “Identifying SDH tributaries in alarm messages” (5-19).

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 (Miscellaneous Discrete Inputs) • EQPT Equipment • OC-3, OC-12, OC-48, OC-192, OC-768 Optical transport signals (SONET): OC-3 (155 Mbit/s), OC-12 (622 Mbit/s), OC-48 (2.5 Gbit/s), OC-192 (10 Gbit/s) or OC-768 (40 Gbit/s) • OUTT Output timing • STM-1, STM-4, STM-16, STM-64, STM-256 Optical transport signals (SDH): STM-1 (155 Mbit/s), STM-4 (622 Mbit/s), 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 (VCG) tributary
Alarm Level	This column indicates the alarm severity. The possible values depend on the Preferences setting for the alarm format, cf. “Alarm format preferences” (16-13).

Column	Meaning
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.
Effect 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 (-).
Date/Time Reported	This column indicates the date and time of occurrence, i.e. the date and time the alarm was reported by the NE. The date and time format depends on the country in which the WaveStar CIT is being used. Please refer to “Configuring the basic system parameters” (4-5) for information on how to set the date and time of the system.
Condition State	This column indicates the state of the reported event or alarm. Possible values are: • Standing Condition • Transient Condition • Standing Condition Cleared
Observed Value	This column is only valid for Threshold Crossing Alerts (TCAs). It indicates the value of the performance parameter that has exceeded the configured threshold.
Threshold	This column is only valid for Threshold Crossing Alerts (TCAs). It indicates the configured threshold of the performance parameter for which a Threshold Crossing Alert (TCA) has been reported.
Time Period	This column is only valid for Threshold Crossing Alerts (TCAs). It indicates the time period of the threshold crossing.

Column	Meaning
Alarm Type	This column indicates the alarm category. The alarm category indicates the functional area to which an alarm belongs. The NE alarms are assigned to the following alarm categories: • Communication This alarm category comprises DCN, synchronisation and transmission alarms. Therefore, the “Communication” alarm category is further divided into: - Communication (DCN) - Communication (Synchronisation) - Communication (Transport) • Environment This alarm category is used for environmental alarms, detected by means of Miscellaneous Discrete Inputs (MDIs). • Equipment This alarm category is used for hardware- and configuration-related alarms and alarms concerning the internal communication. • Processing error This alarm category is used for alarms related to problems or failures of the control system software, due to overload situations for example.
Description	This column describes the alarm’s probable cause in more detail.

Notes:

1. The sequence of alarm log columns in this table reflects the ordering of the columns (from left to right) in the default alarm log display.
2. The ordering of the columns in the alarm log display can be modified by clicking on a column header, holding down the mouse button, and dragging the column to the desired position.
3. The column width can be resized by selecting the small outside margin of a column with the mouse, holding down the mouse button, and adjusting the column’s width.

Pushbuttons The **NE Alarm Log** window provides the following pushbuttons:

1. **Save As**
Use this button to store the currently displayed alarm log 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 log.
3. **Close**
Use this button to close the window.
4. **Refresh**
Clicking the **Refresh** button causes the *WaveStar* CIT to retrieve the alarm log information again.
5. **Help**
Use this button to get online help information specific to the **NE Alarm Log** window.



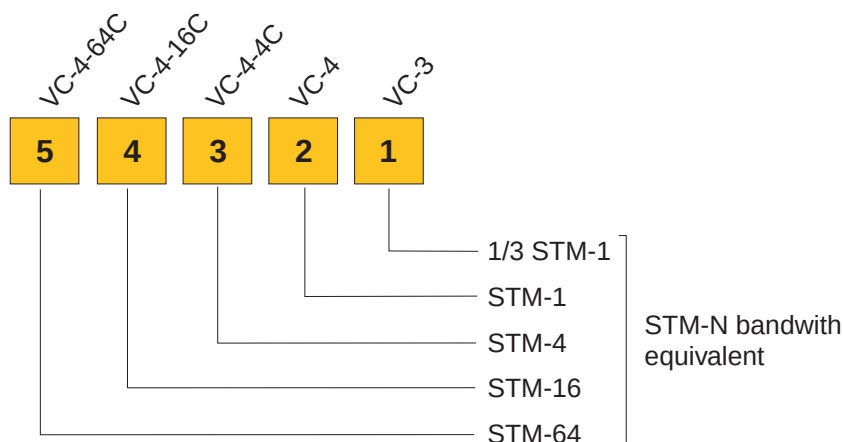
Identifying SDH tributaries in alarm messages

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

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” \(16-15\)](#).

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” (if the digit is required) or a fill character which can be ignored (if the digit is not required). Please also refer to “Required number of digits” (5-20) .
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” (if the digit is required) or a fill character which can be ignored (if the digit is not required). Please also refer to “Required number of digits” (5-20) .
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” (if the digit is required) or a fill character which can be ignored (if the digit is not required). Please also refer to “Required number of digits” (5-20) .
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” (if the digit is required) or a fill character which can be ignored (if the digit is not required). Please also refer to “Required number of digits” (5-20) .

Required number of digits

Depending on the STM level of an SDH interface 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 asterisks at position 3 and 4 each represent a “1”, the asterisk at positions 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” \(5-20\)](#)).

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” \(16-15\)](#).

END OF STEPS



Performing an LED test

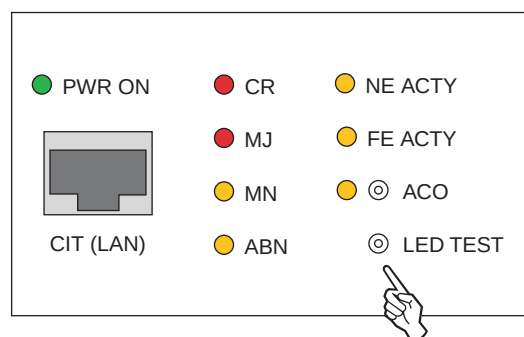
Purpose Use this procedure to test the correct functioning of the user panel and circuit pack LEDs.

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 An LED test can only be performed at the NE.

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 LEDs on the user panel (except the “PWR ON” LED) as well as the LEDs on the circuit packs (except the fan unit LEDs) should turn on for 5 seconds. Afterwards, the LED indications reflect to actual state of the network element which may either be the same state as before the test, or a new state, if changes occurred in the meantime.

After an LED test, the restoration of the LED state may be delayed for some seconds on single circuit packs.

END OF STEPS



Retrieving Alarm Severity Assignment Profile (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 *LambdaUnit*[™] MSS network elements:

- Automatic Protection Switch,
- Data Communications Network,
- Environmental (Miscellaneous Discrete),
- Equipment unprotected,
- Equipment with Protection State Dependence,
- Ethernet,
- MS-SPRing and Bilateral Switched Ring Protection Switch,
- Path MSA/NIM related,
- Path Termination,
- SDH/SONET ports,
- Sub-Network Connection Protection and Unidirectional Path Switched Ring,
- System Timing.

Related information Please also refer to [“Alarm Severity Assignment Profiles” \(16-26\)](#).

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**, select either
 - **View → View Alarms → View Alarm Severity Assignment Profile...** or
 - **Fault → View Alarm Severity Assignment Profile...**

Result:

The **View Alarm Severity Profile** window opens.

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 is 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** tab of any 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 Alarm Severity Assignment Profile (ASAP)

Purpose Use this procedure to create a new Alarm Severity Assignment Profile (ASAP).

Related information

Please also refer to [“Alarm Severity Assignment Profiles” \(16-26\)](#).

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 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 opens.

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),
- Digits (0 ... 9),
- Hyphens (-).

Lower case letters (a ... z) may also be entered. However, no distinction is made between lower case and upper case letters. ASAP names will always be displayed upper case.

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 Alarm Severity Assignment Profile \(ASAP\)” \(5-31\)](#), 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 Alarm Severity Assignment Profiles (ASAPs)

Purpose Use this procedure to create non-reporting Alarm Severity Assignment Profiles (ASAPs).

Related information

Please also refer to [“Alarm Severity Assignment Profiles” \(16-26\)](#).

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, and the **Create NonReporting ASAP Profiles** window is closed.

END OF STEPS



Modifying an existing Alarm Severity Assignment Profile (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” \(16-26\)](#).

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 opens.

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),
 - Digits (0 ... 9),
 - Hyphens (-).

Lower case letters (a ... z) may also be entered. However, no distinction is made between lower case and upper case letters. ASAP names will always be displayed upper case.

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



Deleting an Alarm Severity Assignment Profile (ASAP)

Purpose Use this procedure to delete an Alarm Severity Assignment Profile (ASAP).

Related information

Please also refer to [“Alarm Severity Assignment Profiles” \(16-26\)](#).

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.

Observe the following restrictions:

- The “DEFAULT” ASAPs **cannot** be deleted.
- An ASAP **cannot** be deleted if it is currently in use, i.e. assigned to any system component (a circuit pack or port for example).

Required privilege

You must have at least a privilege code of **M1** to delete an ASAP.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions **Important!** An attempt to delete a “DEFAULT” ASAP, or an ASAP, which is currently in use, will fail!

Proceed as follows to delete an ASAP:

- 1 If you are unsure whether the corresponding ASAP is currently in use or not, you may retrieve an equipment overview by selecting **Reports** → **Equipment Lists** from the WaveStar CIT **System View** main menu, and specifying the desired type of equipment (a circuit pack or port for example).

In the equipment overviews, the currently assigned ASAP is shown. Please also refer to [“Retrieving an equipment list” \(4-102\)](#).

- 2 From the WaveStar CIT **System View** main menu, select **Configuration** → **Alarms** → **Alarm Severity Assignment Profile...**
-

Result:

The **Provision Alarm Severity Profile** window opens.

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.

-
- 3** Select **Delete ASAP** in the upper left-hand corner of the window, next to **Operations**.
-

- 4** Select the ASAP to be deleted in the ASAP tree by clicking on the “+” sign next to the respective ASAP type and selecting the ASAP from the expanded list.
-

- 5** Click **Delete** 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.

-
- 6** If you are sure that the selected ASAP is the ASAP you want to delete, then click **Apply**, and confirm your selection by clicking **Yes** in the confirmation window that opens.
-

- 7** Click **Close** to close the **Provision Alarm Severity Profile** window.

END OF STEPS



Assigning the same Alarm Severity Assignment Profile (ASAP) to all equipment components of a particular type

Purpose Use this procedure to assign the same ASAP (either “NonReporting” or “DEFAULT”) to all equipment components of a particular type (port, tributary or circuit pack) within a shelf.

Related information Please also refer to [“Alarm Severity Assignment Profiles” \(16-26\)](#).

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 opens. Initially, the right-hand side of the window is empty.

- 2 In the left-hand side of the window, select **Shelf 1 (DUR)** and click **Select Shelf**.

Result:

The right-hand side 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 On the right-hand side 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.

If the list boxes contain no entries, this may be due to the following reasons:

- There is no “NonReporting” ASAP defined yet for the corresponding type of equipment.
 - All available ports, tributaries or circuit packs respectively already have the “DEFAULT” ASAP assigned.
-

- 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.

Assigning the same Alarm Severity
Assignment Profile (ASAP) to all equipment
components of a particular type

Alarm management

- 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” \(16-36\)](#).

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 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.

- 4 Click **Close** to close the window.

END OF STEPS



Configuring fault management parameters of an SDH/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 an SDH port:

- 1 Choose one of the following two options to invoke a relevant *WaveStar* CIT window for configuring the fault management parameters of a port:
 1. From the *WaveStar* CIT **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.
-

- 3 As an option, you may set the preferred mode of bit error monitoring to monitor the bit error performance during transmission by selecting the corresponding radio button next to **Signal Degrade/Fail Mode**.

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.
-

- 4 As an option, you may set the **Degraded Signal Interval** to a value between 2 and 10 seconds. The default setting is 7 seconds.

The **Degraded Signal Interval** defines the measurement interval for bursty errors.

Note:

This parameter can only be set in **Burst** mode.

-
- 5 As an option, you may set the **Degraded Signal Threshold** to a value between 5% and 50% (in steps of 5%).

The **Degraded Signal Threshold** defines the threshold value for bursty errors.

Note:

This parameter can only be set in **Burst** mode.

- 6 As an option, you may set the **Degraded Signal (BER) Threshold** to one of the following values:

- 10^{-5}
- 10^{-6} (default value)
- 10^{-7}
- 10^{-8}
- 10^{-9}

The configured threshold defines the bit error ratio (BER) that must be exceeded before a **Degraded Signal** alarm is reported.

Note:

This parameter can only be set in **Poisson** mode.

- 7 As an option, you may set the **Excessive BER Threshold** to one of the following values:

- 10^{-3} (default value)
- 10^{-4}
- 10^{-5}

The configured threshold defines the bit error ratio (BER) that must be exceeded before an **Excessive Bit Error Ratio** alarm is reported.

Note:

This parameter can only be set in **Poisson** mode.

Important! Modifying the Forward Error Correction (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.

- 8 For ports supporting FEC, you may now configure all relevant FEC parameters.

If ...	then ...
you want to configure FEC parameters	continue with the next step.
you do not want to configure FEC parameters	continue with Step 12 .

- 9 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** radio buttons.

Possible FEC types are:

- **In-band** (default setting)
- **Out-band**

For circuit packs that do not support out-of-band FEC, the **In-band** radio button is preselected, and changing this setting is **not** possible.

- 10 Enable or disable FEC by selecting the **Enabled** or **Disabled** option for **FEC Encoding/Decoding**.

Enabling the **FEC Encoding/Decoding** 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.

- 11 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.

.....

- 12** From the available ASAPs in the **Alarm Severity Profile** drop-down list box, select one according to your needs.
-

- 13** 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.
-

- 14** Click **Close** to close the window.

.....
E N D O F S T E P S
.....



Enabling or disabling autonomous alarm forwarding

Purpose Use this procedure to inhibit, temporarily, the forwarding of autonomously generated alarm notifications to management systems and/or to restart autonomous alarm forwarding again.

Related information Please also refer to [“Autonomous alarm forwarding” \(16-23\)](#).

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 for the current management session:

- 1 From the WaveStar CIT **System View** main menu, select **Fault** → **Inhibit/Allow Autonomous Message Reporting...** → **Current Session...**

Result:

The **Provision Autonomous Message Reporting for Current Session** window opens. The radio button (**allow** or **inhibit**) corresponding to the current setting is preselected. 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 according to your selection.

-
- 4** Click **Close** to close the window.

END OF STEPS



Configuring Miscellaneous Discrete Inputs

Purpose Use this procedure to provision Miscellaneous Discrete Inputs (MDIs).

MDI provisioning includes:

- Assigning names to the individual MDIs.
- Selecting an Alarm Severity Assignment Profile (ASAP) of type “Environmental (Miscellaneous Discrete)” to be applied to the MDIs.

Related information Please also refer to [“Miscellaneous Discretes” \(16-52\)](#).

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 configure Miscellaneous Discrete Inputs.

Required equipment

The following equipment is required to perform this procedure:

- WaveStar® CIT

Instructions

- 1 From the *WaveStar* CIT **System View**, select **Configuration** → **Misc. Discretes...**

Result:

The **Configure Miscellaneous Discretes** window opens.

Initially, the right-hand part of the window is empty, the left-hand part contains a selection tree of the available Miscellaneous Discretes.

- 2 Select the desired MDI in the selection tree by clicking on the “+” sign next to **Misc Discretes**, then on the “+” sign next to **Input**, and finally selecting the MDI from the expanded list.

Alternatively, you may directly enter the AID of the desired MDI (misc_in1, misc_in2, ... misc_in8) into the **Enter AID** field.

-
- 3 Click **Select** in the lower left-hand corner of the window.

Result:

The MDI-related information is displayed on the right-hand side of the **Configure Miscellaneous Discretes** window.

- 4 As an option, you may assign a name to the selected MDI (or change an existing name) by entering the new name into the **Name** field.

The MDI name is an alphanumeric string of up to 26 characters.

The following characters are permitted:

- Upper-case and lower-case letters (A ... Z, a ... z),
 - Spaces (“ ”),
 - Periods (“.”).
-

- 5 Select the Alarm Severity Assignment Profile (ASAP) to be applied to the MDIs from the **ASAP** drop-down list box in the **Alarm Severity Assignment Profile Name** group box.

Note:

You can view the current settings of **all** the available ASAPs of type “Environmental (Miscellaneous Discrete)” by clicking on the **View Details...** button.

- 6 As an option, you may assign a descriptive text to the selected MDI, explaining the environmental alarm in more detail, by entering this text into the **Environment Message** field.

This text will be displayed in the *WaveStar* CIT **NE Alarm List** when the corresponding environmental alarm is present.

The **Environment Message** is an alphanumeric string of up to 32 ASCII characters.

The default values are:

- Miscellaneous Discrete Input 1
 - Miscellaneous Discrete Input 2
-

- ...
- Miscellaneous Discrete Input 8

7 Define the **Environmental Alarm Inversion** parameter:

If ...	then ...
you want an alarm message to be generated if the relay associated to the MDI is switched on (activated)	select Normal
you want an alarm message to be generated if the relay associated to the MDI is switched off (deactivated)	select Inverted (default setting)

8 Click **Apply** and confirm your settings by clicking **Yes** in the confirmation window that opens.

9 Repeat [Step 2](#) to [Step 8](#) for all other MDIs you want to configure.

10 Click **Close** to close the **Configure Miscellaneous Discretes** 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
Synchronisation characteristics – External timing input ports	6-5
Synchronisation characteristics – External timing output ports	6-7
Synchronisation characteristics – Line timing references	6-13
Synchronisation characteristics – External timing references	6-15
Synchronisation characteristics – System timing	6-17
Configuring the external timing output ports (SDH mode)	6-20
Configuring the external timing output ports (SONET mode)	6-25
Configuring the external timing input ports (SDH mode)	6-29

<u>Configuring the external timing input ports (SONET mode)</u>	<u>6-31</u>
<u>Configuring the line timing references</u>	<u>6-33</u>
<u>Configuring the external timing references</u>	<u>6-36</u>
<u>Configuring the system timing</u>	<u>6-39</u>
<u>Switching between different clock modes</u>	<u>6-42</u>
<u>Switching to another timing reference for system timing</u>	<u>6-44</u>
<u>Switching to another timing reference for the external timing output ports</u>	<u>6-47</u>



Viewing the timing configuration

When to use Use this procedure to view the configuration of the external timing input and output ports, the timing references 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 Proceed as follows to query the data of the timing configuration:

- 1 In the **System View** of the *WaveStar* CIT, select **View** → **Timing/Sync**.

Result:

The **Synchronisation Characteristics** window appears.

- 2 You can query data on the following items:
 - [“Synchronisation characteristics – External timing input ports” \(6-5\)](#)
 - [“Synchronisation characteristics – External timing output ports” \(6-7\)](#)
 - [“Synchronisation characteristics – External timing references” \(6-15\)](#)
 - [“Synchronisation characteristics – Line timing references” \(6-13\)](#)
 - [“Synchronisation characteristics – System timing” \(6-17\)](#)

Click on the respective tab to query the data of these synchronisation characteristics. The corresponding parameters are described in the following chapters.

.....

- 3 Click on **Refresh** to update the displayed data. It is recommended to click on refresh each time the window is opened or if the timing settings have been changed during the session.
-

- 4 Click on **Help** in order to open the corresponding Online Help window.
-

- 5 Click on **Close** to quit the window.

END OF STEPS

.....



Synchronisation characteristics – External timing input ports

Overview The **External Input 1** or **External Input 2** tabs display the parameters of the external timing input ports.

LambdaUnite™ MSS provides two external timing input ports, for which the following parameters are displayed.

Input Signal Format The **Input Signal Format** drop-down list box displays the format of the incoming timing signal. These values are possible:

- SDH mode
 - **2 MHz** (default)
 - **2 Mbit - framed**
 - **2 Mbit - unframed**
- SONET mode
 - **SF** (Super Frame)
 - **ESF** (Extended Super Frame)

SSM Support The Synchronization Status Message (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**

SA bit Location This parameter is only supported for framed 2 Mbit/s signals which can be used for NEs working in SDH mode.

If the **SSM Support** parameter has the value **Not Supported**, then the value of the **SA bit Location** parameter is of no relevance. If the **SSM Support** parameter has the value **Supported**, then the SSM is extracted from the SA bits starting at the location defined by the **SA bit Location** parameter.

Possible values are:

- **SA4**
- **SA5**
- **SA6**

- **SA7**
- **SA8**



Synchronisation characteristics – External timing output ports

- Overview** The system provides two external timing output ports. Depending on the system timing mode (SDH mode or SONET mode) the output ports have different meanings:
- **SDH mode:**
The output signals of the two external timing output ports are identical. Therefore, only the first external timing output port (**External Output 1**) is displayed representing the parameters of the external timing output ports 1 and 2. The same is true for the provisioning of the external timing output ports.
 - **SONET mode:**
The output signals of the two external timing output ports are different. Therefore, each of the two external timing output ports (**External Output 1**, **External Output 2**) is displayed individually. The same is true for the provisioning of the external timing output ports.

The **Signal Format** of the output signals is the same as the signal format at the external timing input ports.

The output signal selected depends on the state of the **Provisioned Derived Output Timing Source Selection** parameter:

SETG	The output signal is derived from the system clock.
TLS	The output signal is derived from the Timing Link Switch (TLS).

- Availability of output signals** The availability of output signals depends on the system timing mode:
- **SDH mode:**
Both external timing output ports are connected to both XC320 switch units (Worker in slot 09, Protection in slot 10). If at least one of the two XC320 switch units is present, and if the external timing output ports are enabled, then there are output signals available at all times.
 - **SONET mode:**

Each external timing output port is connected to a particular XC320 switch unit. The **External Output 1** is connected to the XC320 in slot 09 (Worker) while the **External Output 2** is connected to the XC320 in slot 10 (Protection). If only one XC320 switch unit is present, then an output signal is available only at the corresponding external timing output port (provided that the output is enabled).

Parameters The following table describes the parameters which can be set for the external timing output ports:

Information field	Possible values	Meaning
Derived Output Timing		
Derived Output Timing Enable	Enable, Disable (default)	This parameter indicates whether a timing signal is forwarded to the output port.
Provisioned Derived Output Timing Source Selection	SDH mode: SETG (default) The timing output is derived from the system clock 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. SONET mode: Line 1 (→ output 1) The timing output is derived from line reference 1. Line 2 (→ output 2) The timing output is derived from line reference 2.	This parameter indicates from which source the external timing signal is derived.

Information field	Possible values	Meaning
Timing Output Equalization	The possible values are: • 20% (initial value) • 40% • 60% • 80% • 100%	This information field is available in SONET mode only. This parameter determines the adjustment (equalization) of the output signal to the used output cable length. These equalization options are provisionable for the DS1 timing reference signal: • 20% – 0 ft. to 131 ft. (max. 0.6 dB cable loss) • 40% – 131 ft. to 262 ft. (max. 1.2 dB cable loss) • 60% – 262 ft. to 393 ft. (max. 1.8 dB cable loss) • 80% – 393 ft. to 524 ft. (max. 2.4 dB cable loss) • 100% – 524 ft. to 655 ft. (max. 3.0 dB cable loss)
Alarming		
ASAP Name	<ASAP Name>	The assigned ASAP (Alarm Severity Assignment Profile) is displayed. Via the push-button ASAP Details... you can retrieve more detailed information on the ASAPs-
Signal Settings		
Output Quality Level	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)	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. Important: If the generating/transmitting HW resource is absent or in a recovery phase (operational state indicated as DISABLED), the values of the displayed SSM Bytes are not reliable. The real outgoing value depends on the recovery type of the related pack.

Information field	Possible values	Meaning
Signal Status	Normal, Disable, Unacceptable	This parameter describes the Status of the outgoing timing signal.
Signal Format	2 MHz (default), 2 Mbit/s-framed, 2 Mbit/s-unframed (SDH mode) SF (Super Frame), ESF (Extended Super Frame, default) (SONET mode)	This parameter shows the signal format of the outgoing timing signal.
Regenerator Parameters		
Regenerator Loop Delay	0 ... 60 s The default value is 0s.	Delay during which DNU/DUS (Do Not Use) is maintained after the Regenerator Loop conditions are no longer present.
Regenerator Loop (SONET mode)	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.	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 on the line, which is selected as timing reference for the external timing output port. This is the line defined in the value of the Provsioned Derived Output Timing Source Selection parameter (Line 1 or Line 2).

Information field	Possible values	Meaning
Regenerator Loop (SDH mode)	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 forwarded to the timing output which is selected as timing reference for the external timing output port (which can be Line 1 ... Line 6). • 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 forwarded to the timing output which is selected as timing reference for the external timing output port (which can be Line 1 ... Line 6). • Both The Regenerator Loop functionality is applied to both external timing inputs.	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, A timing loop can only be present if the input signal for the external timing output port is derived from the external line timing references (the Provisioned Derived Output Timing Source Selection parameter has the value TLS). DNU is forwarded to the timing output which is selected as timing reference for the external timing output port (which can be Line 1 ... Line 6).
SSM Parameters		
SA Bit Location	SA4, SA5, SA6, SA7, SA8	This parameter is only supported for framed 2-Mbit/s SDH signals. If the SSM Support parameter has the value Not Supported, then the value of the SA bit Location parameter is of no relevance. If the SSM Support parameter has the value Supported, then the SSM is extracted from the SA bits starting at the location defined by the SA bit Location parameter.

Information field	Possible values	Meaning
AIS Mode	AIS MODE, QL MODE (default)	This parameter is only supported for framed 2-Mbit/s output signals (SDH mode) and ESF output format signals (SONET mode). It specifies which type of signal (AIS or DNU/DUS) is inserted if the signal quality is below quality acceptance level.
Acceptance Quality Level for Output Threshold AIS	PRC, SSUT, SSUL, SEC (default) for SDH mode PRS, STU, ST2., ST3 (default) for SONET mode	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 in the output timing signal.
Sync Message Force DUS/DNU	Enable, Disable (default)	This parameter defines whether Sync Message Force DNU (SDH mode) respectively Sync Message Force DUS (SONET mode) is inserted in the outgoing timing signal.



Synchronisation characteristics – Line timing references

Overview The **Line Reference 1**, **Line Reference 2**, ... **Line Reference 6** tabs of the **Synchronisation Characteristics** window display data on the configured timing reference source.

A timing reference is an external signal to which the internal SDH/SONET equipment clock is locked.

These signals can be used as timing reference:

- External timing references
External net clock input signals (2048 kHz, 2048 kbit/s acc. to ITU-T or DS1 acc. to Telcordia Technologies standards)
- Line timing references
Six reference signals derived from the incoming line signals.

Settings The tab gives an overview of the possible settings of the line timing references.

Information filed	Possible values	Meaning
Signal Quality		
Input Quality Status	VALID, INVALID, NOT-SUPPORTED, NOT-APPLICABLE	Indicates if a valid timing input signal is available for the respective timing reference.
Quality Level (SDH mode)	DNU, PRC, SSUT, SSUL, SEC	Indicates the quality level of the timing reference port. If the Provisioned Quality Level has any value other than AUTO , then the Quality Level is the same as the Provisioned Quality Level . If the Provisioned Quality Level is equal to AUTO , then the Quality Level has the same value as the Incoming SSM value .
Quality Level (SONET mode)	DUS, PRS, STU, ST2, ST3	
Provisioned Quality Level (SDH mode)	PRC, SSUT, SSUL, SEC, AUTO	This is the quality level which can be provisioned. If the Provisioned Quality Level is equal to AUTO , then the Incoming SSM value is used as the Quality Level . If the Provisioned Quality Level has any value other than AUTO , then the Incoming SSM value is not used, but this provisioned value is used as the Quality Level .
Provisioned Quality Level (SONET mode)	PRS, STU, ST2, ST3, AUTO	
Incoming SSM value (SDH mode)	PRC, STUT, SSUL, SEC, DNU, SSM0, UNSTABLE, NONE	Indicates the Quality Level as received from the external signal when the signal has a valid SSM value.
Incoming SSM value (SONET mode)	PRS, STU, ST2, ST3, DUS, NONE	
Output Timing Switch Settings		

Information filed	Possible values	Meaning
Station Clock Output Reference Lockout State	Lockout	In SDH mode, the output signal at the external timing output ports can be derived from the line timing references (Line 1 ... Line 6) via the Timing Link Switch (Provsioned Derived Output Timing Source Selection = TLS).
	No Lockout	If this parameter is set to Lockout for a particular line timing reference, then using this line timing reference as output timing reference is inhibited.
Output Reference Priority	Disabled, 1, 2, 3, ..., 8	This parameters shows the priority assigned to the timing reference signal for the usage as output timing reference.
Alarming		
ASAP Name	DEFAULT, <ASAP Name>	Selection between a default and a specific Alarm Severity Assignment Profile (ASAP).
System Timing Switch Settings		
Lockout Status	Lockout	Determines if the respective line timing reference can be used as system timing reference (No Lockout) or not (Lockout).
	No Lockout	
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.
Provisionable Settings		
Assigned Port AID	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	0 (disabled, initial value) 1, 2, 3, ..., 8	Configured priority of the timing reference signals.
Timing Port Mode Monitoring	Monitored, Not Monitored	This parameter indicates whether timing alarms will be reported. If a timing port is set to Not Monitored , then no timing alarms will be reported for that port.

Only one of the timing references at a time can be selected as the active one.



Synchronisation characteristics – External timing references

Overview The **External Reference 1** and **External Reference 2** tabs of the **Synchronisation Characteristics** window display the parameters of the external timing input ports.

A timing reference is an external signal to which the internal SDH/SONET equipment clock is locked.

These signals can be used as timing reference:

- External timing references
External net clock input signals (2048 kHz, 2048 kbit/s acc. to ITU-T or DS1 acc. to Telcordia Technologies standards)
- Line timing references
Six reference signals derived from the incoming line signals.

Settings The tab gives an overview of the settings on the external timing references.

Information field	Possible values	Meaning
Signal Quality		
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.
Quality Level (SDH mode)	DNU, PRC, SSUT, SSUL, SEC	Indicates the quality level of the timing reference port. If the Provisioned Quality Level has any value other than AUTO , then the Quality Level is the same as the Provisioned Quality Level .
Quality Level (SONET mode)	DUS, PRS, STU, ST2, ST3	If the Provisioned Quality Level is equal to AUTO , then the Quality Level has the same value as the Incoming SSM value .
Provisioned Quality Level (SDH mode)	PRC, SSUT, SSUL, SEC, AUTO	This is the quality level which can be provisioned. If the Provisioned Quality Level is equal to AUTO , then the Incoming SSM value is used as the Quality Level .
Provisioned Quality Level (SONET mode)	PRS, STU, ST2, ST3, AUTO	If the Provisioned Quality Level has any value other than AUTO , then the Incoming SSM value is not used, but this provisioned value is used as the Quality Level .
Incoming SSM value (SDH mode)	PRC, STUT, SSUL, SEC, DNU, SSM0, UNSTABLE, NONE	Indicates the Quality Level as received from the external signal when the signal has a valid SSM value.
Incoming SSM value (SONET mode)	PRS, STU, ST2, ST3, DUS, NONE	

Information field	Possible values	Meaning
Alarming		
ASAP Name	Default, <ASAP Name>	Selection between the default and a specific External Timing Reference Alarm Severity Assignment Profile (ASAP). Via the push-button Info... you can open the window View ASAP Details which provides detailed information on the respective ASAP.
System Timing Switch Settings		
Lockout Status	Lockout	Determines if the respective external timing reference can be used as system timing reference (No Lockout) or not (Lockout).
	No Lockout	
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.
Provisional Settings		
System Timing Reference Priority	0 (disabled, initial value) 1, 2, 3, ..., 8	Configured priority of the timing reference signals.
Assigned Port AID	exttmg0, exttmg1, Not Connected	The external timing input port which is connected.
Timing Port Mode Monitoring	Monitored, Not Monitored	This parameter indicates whether timing alarms will be reported. If a timing port is set to Not Monitored , then no timing alarms will be reported for that port.



Synchronisation characteristics – System timing

Overview The **System Timing** tab on the **Synchronisation Characteristics** window displays data on the system timing state.

The tab consists of three tabs **System Timing Reference**, **System Timing** and **Output Timing Reference**.

The “System Timing” tab The following table lists the fields of the **System Timing** tab, the possible values and their meaning.

Information field	Possible value	Meaning
Alarming		
ASAP Name	Default, <ASAP Name>	Selection between the default and a specific System Timing Alarm Severity Assignment Profile (ASAP). Via the push-button Info... you can open the window View ASAP Details which provides detailed information on the respective ASAP.
General Parameters		
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 this parameter is set to QL Disable , then the optical interface will transmit DNU in SDH mode and STU in SONET mode.
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.
Warm Up Status	Normal (default), Warming-Up	Shows the status of the system. The system will be in the Warming-Up status for a temporary period of time before transitioning to Normal . In the Warming-Up status, the optical interface will transmit DNU in SDH mode and DUS in SONET mode.
System Quality Level Status (SDH Mode)	PRC, SSUT, SSUL, SEC, DNU	The current quality level of the system clock.
System Quality Level Status (SONET Mode)	STU, ST2, ST3, PRS, DUS	The current quality level of the system clock.
Clock		

Information field	Possible value	Meaning
System Clock Mode Status	Holdover (SDH) Autonomous Holdover (SONET)	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.
	Normal	The internal timing generator is not locked to an external timing reference signal. The system clock is generated by an internal oscillator.
	Forced Holdover	A forced switch to the holdover mode has been carried out.
	Fast Start	Indicates for fast pull-in of the clock when recovering from holdover (SONET mode only).
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.

System Timing Reference The tab gives an overview of the settings of the system timing references.

Information field	Possible values	Meaning
System Timing Reference AID	External Input 1, External Input 2 , <specific port AID> (for line timing references), for example “1-1-#-#-2-1”.	AID of the system timing reference.
Active Timing Reference	External Reference 1, External Reference 2, Line 1 ... Line 6	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 tab gives an overview of the settings of the output timing references.

Information field	Possible values	Meaning
Active Output Timing Reference (SDH mode only)	Line 1 ... 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 (SDH mode only)	No Request, Manual, Forced	Value of the switch request activated by the user or initiated by the system.
Output Timing Reference AID	Not Connected, <AID of the output timing reference>	Displays the AID of the output timing reference derived via the Timing Link Switch (TLS) connected to the station clock output. These values are only relevant when the Provisioned Derived Output Timing Source Selection is set to TLS . Otherwise the value of the Output Timing Reference AID is Not Connected .



Configuring the external timing output ports (SDH mode)

When to use Use the following procedures to configure the external timing output ports for an NE working in SDH mode.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – External timing input ports” \(6-5\)](#)
- [“Synchronisation characteristics – External timing output ports” \(6-7\)](#)

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 Proceed as follows to configure the external timing output ports:

- 1 Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronisation Characteristics** appears.

- 2 Select the **External Output 1** tab.

The configuration is valid for the external timing output ports 1 and 2. The timing signal is forwarded in parallel to both outputs.

-
- 3 Set the parameter **Regenerator Loop Delay** in the group box **Regenerator Parameter**. 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**.
-
- 4 Set the parameter **Regenerator Loop** in the group box **Regenerator Parameter** 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 **External Input 1** 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.
-
- 5 Set individual location of the Sa bit in the drop-down list box **SA Bit Location**.
-

The following values are possible:

- **SA4** (initial value)
- **SA5**
- **SA6**
- **SA7**
- **SA8**

This parameter is only supported for framed 2 Mbit/s signals.

- 6 In the drop-down list 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)
-

- 7 Select the value that will be sent if the outgoing signal is below the quality acceptance or if forced **DNU** is enabled in the drop-down list box **AIS mode**.

The following values are possible

- **AIS mode**
- **QL mode**

This parameter is only supported for framed 2 Mbit/s signals.

- 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** 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**
-
- 10** Select the **ASAP Name** in the group box **Alarming**. You can select the **Default** ASAP or a specific one.
-
- 11** Enable the use of the external outputs in the **Derived Output Timing** group box. Click on **Enable** in the drop-down list box.
- 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 that are physically available.
-
- 12** Select the timing output source from which the external timing signal is derived in the **Provisioned Derived Output Timing Source Selection** group box.
- The following selections are possible:
- **SETG** (default)
The external timing signal is derived from the system clock.
 - **TLS** (Timing Link Switch)
The external timing signal is derived from one of the six line 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**
- if the **System Synchronization Status Messaging Mode** is set to **QL Enable**, signals with a valid quality level not equal to **DNU**.

-
- 13** Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel** or **Undo**.

Result:

If you have clicked on **OK** or **Cancel**, the **Synchronization Characteristics** window closes. If you have clicked on **Apply** or **Undo** 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 an NE workign in SONET mode.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – External timing input ports” \(6-5\)](#)
- [“Synchronisation characteristics – External timing output ports” \(6-7\)](#)

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 Proceed as follows 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 the tab **External Output 1** or **External Output 2**. In SONET mode the external timing output port 1 is connected to the line signal 1 and the external timing output port 2 is connected to the line signal 2.

-
- 3 Set the parameter **Regenerator Loop Delay** in the group box **Regenerator Parameter**. 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**.
-

- 4 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.
-

- 5 In the **Acceptance Quality Level for Output Threshold AIS** drop-down list box, 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)**

-
- 6** Select the value that will be sent if the outgoing signal is below the quality acceptance or if forced **DUS** is enabled in the drop-down list box **AIS mode**.

The following values are possible

- **AIS mode**
- **QL mode**

This parameter is only supported for **ESF** output signals.

- 7** 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)
-

- 8** 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**
-

- 9** Select the **ASAP Name** in the group box **Alarming**. You can select the **Default** ASAP or a specific one.
-

- 10** Enable the use of the external outputs in the group box **Derived Output Timing**. Click on **Enable** in the drop-down list box.
-

- 11** Select the timing output source from which the external timing signal is derived in the **Provisioned Derived Output Timing Source Selection** group box.

This information field is greyed out, the following values are fixed:

- **Line 1** (for output 1)
- **Line 2** (for output 2)

-
- 12** Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel** or **Undo**.

Result:

If you have clicked on **OK** or **Cancel**, the **Synchronisation Characteristics** window closes. If you have clicked on **Apply** or **Undo** 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 an NE working in SDH mode.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – External timing input ports” \(6-5\)](#)

Before you begin Prior to performing this task, you must connect the external timing input ports to an external timing source.

Required 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 Proceed as follows to configure the external timing input ports:

- 1** In the **System View** of the WaveStar CIT select **Configuration** → **Timing/Sync**.

Result:

The **Synchronisation Characteristics** window appears with the active tab **External Input 1**. For port 2 select **External Input 2**.

- 2** Select the timing input format in the **Input Signal Format** group box 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 Sa bit in the group box **SA Bit Location**.

The following values are possible:

- **SA4** (initial value)
- **SA5**
- **SA6**
- **SA7**
- **SA8**

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** or **Undo**.

Result:

If you have clicked on **OK** or **Cancel**, the window **Synchronisation Characteristics** closes. If you have clicked on **Apply** or **Undo** 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 an NE working in SONET mode.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – External timing input ports” \(6-5\)](#)

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 Proceed as follows 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 Input 1**. For port 2, select **External Input 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 **Synchronisation Characteristics** closes. If you have clicked on **Apply** or **Undo** the window remains open and you can select another tab.

END OF STEPS



Configuring the line timing references

When to use Use this procedure to configure the line timing references.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – Line timing references” \(6-13\)](#)

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 (SONET mode or SDH 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 Proceed as follows to configure the timing references:

- 1 Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronisation Characteristics** appears.

- 2 Select the tab of the **Line Timing Reference** which you wish to configure. You can select an **SDH/SONET** signal via **Line Timing**

Reference 1 ... Line Timing Reference 6 for STM-N/OC-N line ports.

- 3 Select the port AID in the drop-down-list box **Assigned Port AID**. Click on **Browse...** in order to open the window **Select Line Timing Port AID**.

IF	THEN
the selected timing reference shall not be used,	select Not Connected
the selected timing reference is Line 1, Line 2, Line 3, Line 4, Line 5 or Line 6 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 **Provisioned Quality Level** drop-down list box. For **Line 1 ... Line 6**, it is recommended to select **AUTO**. This means that the Synchronization Status Message (SSM) is evaluated. You could also assign the actual quality level of the timing reference source (**PRC, SSUT, SSUL, SEC** for SDH mode or **PRS, STU, ST2, ST3** for SONET mode).

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
- **0** (disabled, 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.

If the **System Synchronization Status Messaging Mode** is set to **QL Enable**, then 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 the **System Synchronization Status Messaging Mode** is set to **QL Disable**, then only the priorities of the timing reference signals are evaluated.

If all possible timing reference signals fail, then the timing generator enters the holdover mode.

-
- 6** Select the **Timing Port Mode Monitoring**. The values **Monitored** or **Not Monitored** are possible. This defines whether alarms are raised for the timing signals or not.
-
- 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 **Info...** you can call up a table with details on the ASAPs.
-
- 8** Apply the changes by clicking on **Apply**. If you wish to discard the changes click on **Cancel** or **Undo**.
-
- 9** Repeat [Step 2](#) to [Step 8](#) until all timing references are configured. Click on **OK** to close the window.

END OF STEPS



Configuring the external timing references

When to use Use this procedure to configure the external timing references.

Related information For related information, see:

- [Chapter 17, “Timing provisioning concepts”](#)
- [“Viewing the timing configuration” \(6-3\)](#)
- [“Synchronisation characteristics – External timing references” \(6-15\)](#)

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 (SONET mode or SDH 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 Proceed as follows to configure the timing references:

- 1 Select **Configuration → Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronisation Characteristics** appears.

-
- 2 Select the tab of the **External Timing Reference** which you wish to configure. You can select two external timing signals from the external timing input ports. There is one tab for each port (**External Timing Reference 1** and **External Timing Reference 2**). 2 MHz or 2 Mbit/s signals for SDH mode or D1 timing signals for SONET mode can be used as external timing sources.
-

- 3 Select the timing quality belonging to the external timing reference in the **Provisioned Quality Level** drop-down list box.

These selections are possible:

- SDH mode
PRC, SSUT, SSUL, SEC or AUTO
- SONET mode
PRS, STU, ST2, ST3 or AUTO

If you want to use the incoming SSM value of the external timing reference (if supported), select **AUTO**, otherwise select a specific value. For external interfaces which do not support SSM, it is recommended to select a value other than **AUTO**.

Result:

The timing references are now used in the order of their quality level.

- 4 Select the port AID in the drop-down-list box **Assigned Port AID**. Select in the drop-down list box **Not Connected**, if the respective external timing signal should not be used or select **External Input 1** or **External Input 2** depending on the tab you have selected.
-

- 5 Select in the drop-down list box **System Timing Reference Priority** the priority of the selected timing reference. The values can be

- **0** (disabled, 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.

If the **System Synchronization Status Messaging Mode** is set to **QL Enable**, then 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 the **System Synchronization Status Messaging Mode** is set to **QL Disable**, then only the priorities of the timing reference signals are evaluated.

If all possible timing reference signals fail, then the timing generator enters the holdover mode.

-
- 6 Select the **Timing Port Mode Monitoring**. The values **Monitored** or **Not Monitored** are possible. This parameter defines whether alarms are raised for the timing signals or not.
-

- 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 **Info...** you can call up a table with details on the ASAPs.

- 8 Apply the changes by clicking on **Apply**. If you wish to discard the changes click on **Cancel** or **Undo**.
-

- 9 Repeat [Step 2](#) to [Step 8](#) 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” \(6-3\)](#)
- [“Synchronisation characteristics – System timing” \(6-17\)](#)

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 Proceed as follows to configure the system timing:

- 1 Select **Configuration** → **Timing/Sync** in the **System View** of the WaveStar CIT.

Result:

The window **Synchronisation Characteristics** appears.

- 2 Select the **System Timing Parameters** tab.
-

- 3 Select the **System Timing** tab.

-
- 4 Select the wait-to-restore time in the group box **Wait To Restore**. Click on the respective radio button. The values can be:
- **Zero**
 - 20 seconds (default value in SONET mode, available in SONET mode only)
 - 5 minutes (default value in SDH mode)
 - 1 minute to 60 minutes (in steps of 1 minute, selectable by means of a spin box)
 - **Infinite** (available in SONET mode only)

The wait-to-restore time specifies the time interval that has to elapse before every single switching from one timing reference to another is performed.

- 5 Enable or disable the use of **System Synchronisation Status Messaging 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 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.”

-
- 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 **Info...** you can call up a table with details on the ASAPs.

-
- 8** Apply the changes by clicking on **OK** or **Apply**. If you wish to discard the changes, click on **Cancel** or **Undo**.

END OF STEPS



Switching between different clock modes

When to use	Use this procedure to switch between different clock modes: • Clear Mode Switch Switching back from the holdover mode to the locked mode. • Force to Holdover Forcing the timing generator 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 <i>WaveStar</i>® CIT is connected and logged into the <i>LambdaUnite</i>™ 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: • <i>WaveStar</i> CIT
Instructions	Proceed as follows to change the clock mode: 1 Select Fault → Timing/Sync Protection Switch → Clock Mode Switch... in the System View of the <i>WaveStar</i> CIT. Result: The window System Timing Clock Mode Protection Switch appears. 2 Select the switch command by means of the Switch Type drop-down list box. Select either of these switch commands: • Clear Mode Switch

If the timing generator is currently operating in the holdover mode, then the Forced Switch condition will be reset, i.e. the timing generator is again synchronized (locked) to an external clock signal. 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 timing generator to be switched to the holdover mode regardless of the state of the timing references. When performing a forced switch to the holdover mode, the timing generator further on operates at that frequency that the stabilization process had at that time.

No clock mode switch will be carried out when the clock is provisioned for the free running mode.

-
- 3** Apply the changes by clicking on **Ok** or **Apply**. If you wish to discard the changes, click on **Cancel** or **Undo**.

Important! After a switch to the holdover mode or a clear mode switch, it takes the system up to 2 minutes (up to 8 minutes in the warming up phase) to stabilize the holdover filter. Therefore, it is recommended not to perform any further timing action during the holdover filter stabilization period.

END OF STEPS



Switching to another timing reference for system timing

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 To Reference**
- **Manual Switch To Reference**
- **Lockout**
- **Clear Lockout**
- **Clear Wait To Restore**

Related information For related information, see:

- [“Configuring the system timing” \(6-39\)](#)
[Chapter 17, “Timing provisioning concepts”](#)
- [“Synchronisation characteristics – Line timing references” \(6-13\)](#)
- [“Configuring the system timing” \(6-39\)](#)
- [“Configuring the line timing references” \(6-33\)](#)

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**, and then **External Reference 1, External Reference 2**(see [“Configuring the external timing references” \(6-36\)](#)), or
 - **Configuration** → **Timing/Sync**, and then **Line Reference 1, Line Reference 2, ... Line Reference 6** (see [“Configuring the line timing references” \(6-33\)](#)).
- verify that the timing generator is in the locked mode via **View** → **Timing/Sync** → **System Timing Parameters** (see [“Synchronisation characteristics – Line timing references” \(6-13\)](#))

When the system is provisioned to the free running mode, all currently active requests remain active, all switch requests can be performed and will be successful, and the Timing Link Switch (TLS) can be provisioned. However, these requests will have no effect, as

they are not considered by the system. The TLS provisioning will only be considered in locked mode.

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 Proceed as follows to switch to another timing reference:

- 1 Select **System Timing Reference Switch** via **Fault → Timing/Sync Protection Switch** in the System View of the *WaveStar* 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 (Forced and Manual Switch). It cannot be denied. 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 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.
A manual switch is only possible when the quality of the active reference is equal to the reference you want to switch to if **SSM** is enabled.
 - **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” \(6-39\)](#)).

-
- 3 Select the timing reference source to which you want to perform a switch request in the drop-down-list box **Destination**. This can be:

- **External Reference 1**
- **External Reference 2**
- **Line Reference 1 ... Line Reference 6**

Result:

The AID of the respective timing reference is displayed in the **Reference 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** or **Apply**. If you wish to discard the changes, click on **Cancel** or **Undo**.

Important! After a timing reference switch, it takes the system 2 minutes to stabilize the holdover filter. So don't do any further timing action during these 2 minutes. IF *LambdaUnite* MSS is in warm-up state, which takes about 6 minutes, you should wait these 6 minutes.

END OF STEPS



Switching to another timing reference for the external timing output ports

When to use Use this procedure to switch between different timing reference signals for the external timing references and to apply certain switch requests to a selected reference:

- **Clear Reference Switch**
- **Forced Switch To Reference**
- **Manual Switch To Reference**
- **Lockout**
- **Clear Lockout**
- **Clear Wait To Restore**

Related information For related information, see:

- [“Configuring the external timing references” \(6-36\)](#)
- [“Synchronisation characteristics – External timing references” \(6-15\)](#)
- [“Configuring the line timing references” \(6-33\)](#)
- [“Configuring the system timing” \(6-39\)](#)

Before you begin Prior to performing this task,

- verify that a *WaveStar*[®] CIT is connected and logged into the *LambdaUnite*[™] MSS system.
- configure the external timing references sources for the system via **Configuration** → **Timing/Sync** → **External Timing Reference 1/2...** (see [“Configuring the line timing references” \(6-33\)](#)).
- verify that the timing generator is in the locked mode via **View** → **Timing/Sync** → **System Timing Parameters** (see [“Synchronisation characteristics – System timing” \(6-17\)](#))

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, it is also possible to perform all switch requests. All requests will be successful (the timing link switch will be provisioned), but the system will not consider these

values. Only in **Locked mode** the system considers the **Timing Link Switch** provisioning.

Required privilege code

You must have at least privilege codes of **P1** and **M4** to perform the switch commands.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to switch to another timing reference:

- 1 Select **Output Timing Reference Switch** via **Fault → Timing/Sync Protection Switch** in the System View of the *WaveStar* CIT.

Result:

The window **Output Timing Link Switch** appears.

In the group box **Output Switch Parameter** the following values are displayed which show the current status of the timing output references:

- **Active Output Timing Reference:**
Line Reference 1 ... Line Reference 6
This parameter shows the current output timing reference
 - **Output Timing Reference Switch Request Status:**
No Request, Forced Switch To Reference, Manual Switch To Reference, Clear Reference Switch, Clear Lockout, Lockout
This parameters shows which switch request is currently applied to the active output timing reference.
-

- 2 Select the switch request (**Switch Command**) you want to perform in the group box **Switch Type**. The following switch requests are possible:

- **Clear Reference Switch**

removes any active external request (Forced and Manual Switch). It cannot be denied. 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 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.
A manual switch is only possible when the quality of the active reference is equal to the reference you want to switch to if **SSM** is enabled.
- **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” \(6-39\)](#)).

-
- 3 Select the timing reference source to which you want to perform a switch request in the drop-down-list box **Destination**. This can be:

- **Line 1 ... Line 6**

Result:

The AID of the respective timing reference is displayed in the **Reference 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** or **Apply**. If you wish to discard the changes, click on **Cancel** or **Undo**.

Important! After a timing reference switch, it takes the system 2 minutes to stabilize the holdover filter. So don't do any further timing action during these 2 minutes. IF *LambdaUnite* MSS is in warm-up state, which takes about 6 minutes, you should wait these 6 minutes.

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/APS, MS-SPRing/BLSR and SNCP/UPSR.

Contents

Viewing existing cross-connections	7-4
Parameters of the window “View Cross Connections”	7-6
Retrieve Cross-connection Lists	7-10
Supporting information on the “Cross Connection List”	7-12
Substructuring of input and output signals	7-14
Creating a new cross-connection	7-18
Modifying a cross-connection	7-23
Rolling a cross-connection	7-25
Bridging a cross-connection	7-28
Deleting a cross-connection	7-31
Viewing an existing protection group	7-34

<u>Parameters of the window “View Protection” for a 1+1 MSP or APS</u>	<u>7-35</u>
<u>Parameters of the window “View Protection” for a 2-Fiber MS-SPRing or 2-fiber BLSR</u>	<u>7-39</u>
<u>Parameters of the window “View Protection” for a 4-Fiber MS-SPRing or 4-fiber BLSR</u>	<u>7-42</u>
<u>Parameters of the window “View Protection” for SNCP and UPSR</u>	<u>7-46</u>
<u>Parameters of the window “View Protection” for a one way path protection</u>	<u>7-48</u>
<u>Creating a cross-connection in a 2- or 4-fiber MS-SPRing/BLSR network environment</u>	<u>7-50</u>
<u>Creating a new 1+1 MSP or 1+1 APS (NE level)</u>	<u>7-54</u>
<u>Creating a new 2-fiber MS-SPRing or 2-fiber BLSR (NE level)</u>	<u>7-57</u>
<u>Creating a new 4-fiber MS-SPRing or 4-fiber BLSR (NE level)</u>	<u>7-60</u>
<u>Creating an SNCP or UPSR (NE level)</u>	<u>7-63</u>
<u>Creating an unidirectional path protection</u>	<u>7-67</u>
<u>Provisioning path protection parameters</u>	<u>7-71</u>
<u>Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings</u>	<u>7-73</u>
<u>Creating an unidirectional DNI/DRI between two protected rings.</u>	<u>7-77</u>
<u>Creating a bidirectional DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR protected ring</u>	<u>7-86</u>
<u>Creating a bidirectional ring-to-ring SNCP</u>	<u>7-90</u>
<u>Deleting a protection group</u>	<u>7-93</u>
<u>Configuring VCG tributaries</u>	<u>7-95</u>
<u>Retrieving VCG/VCG tributary information</u>	<u>7-97</u>
<u>VCG tributary details</u>	<u>7-99</u>
<u>VCG Port Details</u>	<u>7-105</u>
<u>Retrieving current VCG delay</u>	<u>7-109</u>
<u>Parameters of the window “View VCG Delay”</u>	<u>7-111</u>

Retrieving current VCG tributary maintenance signal	7-113
Parameters of the window “View Current VCG Trib. Maintenance Signal”	7-115



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” \(18-21\)](#)
- [“Line Protection” \(18-19\)](#)
- [“Configuring an optical SDH/SONET port” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)

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”” \(7-6\)](#)

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 selection window View Cross Connections consists of three 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” (15-9))
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” (18-13) .
The <i>Path Ptn. Grp</i> tab	The tab Path Ptn. Grp. is similar to the tab Equipment . Any named path protection group established on the system can be selected on this tab. For further information on protection, please refer to “Protection mechanisms” (18-13) .
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.
Authorization level	You must have at least a P1 authorization level to access this dialog box.
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.
Validity	whether the NE name is valid or invalid.
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 , 1-Way Path Protected 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.

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
- 1-Way Path Protected
- UPSR/SNCP Ring Add, Drop
- BLSR/MS-SPRing, primary Node Ring Interworking, Drop, Continue
- BLSR/MS-SPRing, primary Nodes in same NE Ring Interworking, Drop, Continue
- UPSR/SNCP Ring-to-Ring, Single Node Interconnection in same NE

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” \(18-21\)](#)
- [“Line Protection” \(18-19\)](#)
- [“Configuring an optical SDH/SONET port” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)

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 **CrossConnection List** via **Reports** → **Cross Connection List...** 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 **CrossConnection List** opens. The displayed parameters are described in the chapter [“Supporting information on the “Cross Connection List”” \(7-12\)](#)

.....
E N D O F S T E P S



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 , 1-Way Path Protected 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 • 1-Way Path Protected • UPSR/SNCP Ring Add, Drop • BLSR/MS-SPRing, primary Node Ring Interworking, Drop, Continue • BLSR/MS-SPRing, primary Nodes in same NE Ring Interworking, Drop, Continue • UPSR/SNCP Ring-to-Ring, Single Node Interconnection in same NE
Source to Destination Cross Connection Number	Displays an up to 9 digit number associated with the cross connection.

Value	Meaning
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 • 1-Way Path Protected • UPSR/SNCP Ring Add, Drop • BLSR/MS-SPRing, primary Node Ring Interworking, Drop, Continue • BLSR/MS-SPRing, primary Nodes in same NE Ring Interworking, Drop, Continue • UPSR/SNCP Ring-to-Ring, Single Node Interconnection in same NE
Destination to Source Cross Connection Number	Displays an up to 9 digit number associated with the cross connection.
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” \(15-18\)](#)
- [“Reassigning a circuit pack” \(4-46\)](#)

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 provisioning” \(15-16\)](#) and [“Reassigning a circuit pack” \(4-46\)](#)).

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-1, STM-4, STM-16, STM-64 and STM-256 (in SDH Standard)
- STS-1c, STS-3c, STS-12c, STS-48c, STS-192c for OC-3, OC-12, OC-48, OC-192 and OC-768 (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, 256C** in SDH Standard. In SONET Standard X= **1, 3, 12, 48, 192, 768**. 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-1, STM-4, STM-16, STM-64 and STM-256 (in SDH Standard)
- STS-1c, STS-3c, STS-12c, STS-48c, STS-192c for OC-3, OC-12, OC-48, OC-192 and OC-768 (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, 256C** in SDH Standard. In SONET Standard X= **1, 3, 12, 48, 192, 768**. X is the transmission rate. N is the number of subsequent X.

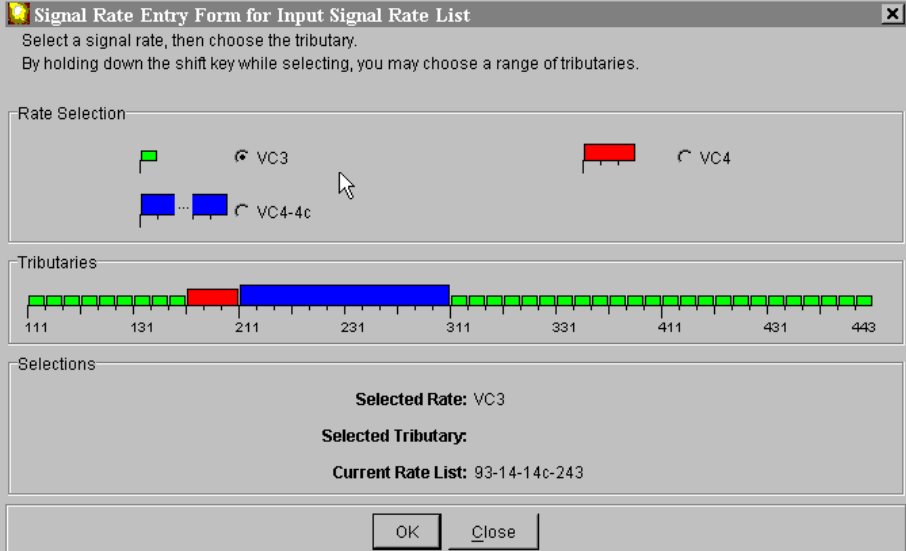
- 7 Select the destination port(s) in the **Apply To:** drop-down listbox. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack or to all ports on this type in the shelf. By using the latter options, you can decrease your 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". The window contains the following elements:

- Instructions:** "Select a signal rate, then choose the tributary. By holding down the shift key while selecting, you may choose a range of tributaries."
- Rate Selection:** A section with three radio buttons: "VC3" (selected), "VC4", and "VC4-4c".
- Tributaries:** A horizontal bar representing timeslots from 111 to 443. The bar is divided into segments: green for VC3, red for VC4, and blue for VC4-4c. The selected VC3 segment is highlighted in blue.
- Selections:** A section displaying the following information:
 - Selected Rate:** VC3
 - Selected Tributary:**
 - Current Rate List:** 93-14-14c-243
- Buttons:** "OK" and "Close" buttons at the bottom right.

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” \(18-21\)](#)
- [“Line Protection” \(18-19\)](#)
- [“Configuring an optical SDH/SONET port” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)
- [“Creating a cross-connection in a 2- or 4-fiber MS-SPRing/BLSR network environment” \(7-50\)](#)
- [“Creating an SNCP or UPSR \(NE level\)” \(7-63\)](#)

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**
- **1-Way Path-Protected**
- **UPSR/SNCP Ring Add, Drop**
- **Ring Interworking, Drop and Continue, BLSR/MS-SPRing Primary Node**
- **Ring Interworking, Drop and Continue, BLSR/MS-SPRing Primary Nodes in Same NE**
- **UPSR/SNCP Ring-to-Ring, Single Node Interconnection, Same NE**
- **Ring Interworking, Drop and Continue, UPSR/SNCP Node**

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- or 4-fiber MS-SPRing/BLSR network environment” \(7-50\)](#).

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 \(NE level\)” \(7-63\)](#).

- 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”” \(7-6\)](#).

- 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” \(7-4\)](#)

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” \(7-4\)](#))

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” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)

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) or BLSR (Bidirectional Line-Switched 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” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)

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” \(7-18\)](#)
- [“Configuring an optical SDH/SONET port” \(4-49\)](#)
- [“Configuring a tributary” \(4-92\)](#)

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” \(18-13\)](#)
- [“Line Protection” \(18-19\)](#)
- [“Ring Protection” \(18-21\)](#)
- [“Path Protection” \(18-14\)](#)

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 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” \(7-35\)](#).

END OF STEPS



Parameters of the window “View Protection” for a 1+1 MSP or APS

Description The **View Protection** window consists of four tabs, each describing a set of parameters:

- [“Protection Group” \(7-35\)](#)
- [“Alarm Status” \(7-35\)](#)
- [“Switch Status” \(7-36\)](#)
- [“Provisionable Parameters” \(7-37\)](#)

Protection Group The following table shows the status data which is shown in the tab **Protection Group** of 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” (15-9)	The AID defined for the selected protection group.
Protection Type	SDH: 1+1 MSP SONET: 1+1	Optical Port Protection Switching
Optical Line Rate	SDH: STM1, STM4, STM16, STM64, STM256 SONET: OC3, OC12, OC48, OC192, OC768	SDH or SONET line-rate associated with the port
Protocol	–	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.
Working AID	cf. “Overview of access identifiers” (15-9)	The port AID which has been assigned to be the working port.
Protection AID	cf. “Overview of access identifiers” (15-9)	The port AID which has been assigned to be the protection port.

Alarm Status The following table shows the status data which is shown in the tab **Alarm Status** of the **View Protection** window for an optical port protection (MSP or APS).

Information field	Possible value	Meaning
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”).
Working 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”).
Working Switch Fault Status	Signal Failure, Signal Degrade, None	Switch initiation reason associated with the working port
Protection 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”).
Protection Criteria Fault Status	Signal Failure, Signal Degrade, None	Switch initiation reason associated with the protection port

Switch Status The following table shows the status data which is shown in the tab **Switch Status** of the **View Protection** window for an optical port protection (MSP or APS).

Information field	Possible value	Meaning
Active Port	Working (<port AID>), Protection (<port AID>)	Indicates which port is carrying traffic
Switch Request State	Lockout, Forced Switch , Signal Failure, 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” (7-47) .
Near-End Outgoing APS Message	Lockout, Forced Switch, No Request, Signal Failure High Priority, Signal Failure Low Priority, Signal Degraded, Manual Switch, Do Not Revert	The outgoing Automatic Protection Switch Message, please refer to “Switch request state and APS messages” (7-37) .
Near-End Outgoing Request Selection	Working(<port AID>), Protection (<port AID>), None	

Information field	Possible value	Meaning
Far-End Incoming APS Message	Lockout, Forced Switch, No request, Signal Failure High Priority, Signal Failure Low Priority Signal Degraded High Priority, Signal Degraded Low Priority, Manual Switch, Do Not Revert	cf. “Switch request state and APS messages” (7-37)
Far-End Incoming Request Selection	Working/Working 1 (<port AID>), Protection/Working 2 (<port AID>), Invalid, None	Active port at the far end

Provisionable Parameters The following table shows the status data which is shown in the tab **Provisionable Parameters** of the **View Protection** window for an optical port protection (MSP or APS).

Information field	Possible value	Meaning
Alarm Severity Assignment Profile	<24-character string>	Designation of the corresponding ASAP

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.
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. SONET: Forced Switch is available for 1+1 APS only
Signal Failure High Priority	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 Failure Low Priority	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 Priority	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 Priority	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.

Switch Request State	Meaning
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 incoming K1 byte contains an invalid channel number outside the defined range for the MSP protocol/architecture or a code irrelevant for the specific switching operation.
Unavailable	In case of a signal failure condition of the protocol line or if the acceptance process for the received K-bytes fails, the value Unavailable is returned for K-byte retrievals.



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” \(7-39\)](#)
- [“Alarm Status” \(7-39\)](#)
- [“Provisionable Parameters” \(7-40\)](#)
- [“West Side and East Side” \(7-40\)](#)

Protection Group The following table shows the status data which is shown in the tab **Protection Group** of the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
Protection Group AID	<two-digit character string> (cf. “Overview of access identifiers” (15-9))	The AID defined for the selected protection group.
Protection Type	SDH: 2-Fiber MS-SPRING SONET: 2-Fiber BLSR	This field displays the Protection Type.
Optical Line Rate	SDH: STM16, STM64, STM256 SONET: OC48, OC192, OC768	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” (15-9)	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

Alarm Status The following table shows the status data which is shown in the tab **Alarm Status** of the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
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” (15-9))	The AID defined for the West and the East Port of the respective NE
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”).

Provisionable Parameters The following table shows the status data which is shown in the tab **Provisionable Parameters** of the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
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.

“West Side” and “East Side” The following table shows the status data which is shown in the tabs **West Side** and **East Side** of the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
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-S Reverse Request - Span RR-R Reverse Request - Ring NR No Request	Switch request for the outgoing west/east side Definition of the Switch Request State : A node reports the active switch state of a MS-SPRing/BLSR side, defined as the request currently associated with the concerned side, and accepted in the protocol as highest or coexisting priority. A request is associated to a side when it is detected on that side for automatic requests, when it is addressed to that side for external requests, or when that side is on the short path for received k-byte requests When no request is associated to a side (intermediate nodes), the active switch state is considered as a No-Request. ¹
East/West Last Protection Switch Attempt Status	Success, Denied, Failed	Status of the last switch action.

Information field	Possible value	Meaning
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-S Reverse Request - Span 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. K1byte, 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 route of the K-bytes to the other switching NE.
East/West Channel Status	Idle Bridged Bridged and Switched Not Used RDI-L AIS-L	The current channel status of the node.

Notes:

1. *LambdaUnite™* will have to interwork with other BLSR / MS SPRING products in mixed rings which will thus show different **Switch Request State** display behaviour.
2. In special multiple request scenarios it might happen that **East Switch Request State** and **West Switch Request State** are interchanged”.

Important! 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 a 4-Fiber MS-SPRing or 4-fiber BLSR

Description The **View Protection** window consists of five tabs, each describing a set of parameters:

- [“Protection Group” \(7-42\)](#)
- [“Alarm Status” \(7-42\)](#)
- [“Provisionable Parameters” \(7-43\)](#)
- [“West Side and East Side” \(7-43\)](#)

Protection Group The following table shows the status data which is shown in the tab **Protection Group** of the **View Protection** window for a 4-Fiber MS-SPRing.

Information field	Possible value	Meaning
Protection Group AID	<two-digit character string> (cf. “Overview of access identifiers” (15-9))	The AID defined for the selected protection group.
Protection Type	SDH: 4-Fiber MS-SPRING SONET: 4-Fiber BLSR	This field displays the Protection Type.
Interworking Type	SDH, SONET	-
Optical Line Rate	SDH: STM16, STM64, STM256 SONET: OC48, OC192, OC768	SDH or SONET line-rate associated with the port
Ring-ID	<ASCII character string> (up to 15 characters)	Ring ID for the selected protection group
Ring Node APS (Automatic Protection Switch) State	Idle, Switching, Passthrough, Suspended-Idle, Suspended-Switching, Suspended-Passthrough	Switch status of the NEs of the respective MS-SPRing
West (Working/Protection) Port AID/East (Working/Protection) Port AID	cf. “Overview of access identifiers” (15-9)	Working/Protection port AID of the west/east side which has been provisioned for the protection group

Alarm Status The following table shows the status data which is shown in the tab **Alarm Status** of the **View Protection** window for a 4-Fiber MS-SPRing.

Information field	Possible value	Meaning
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” (15-9))	The AID defined for the West and the East Port of the respective NE
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”).

Provisionable Parameters The following table shows the status data which is shown in the tab **Provisionable Parameters** of the **View Protection** window for a 4-Fiber MS-SPRing.

Information field	Possible value	Meaning
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.
Protection Switch Mode	4-Fiber MS-SPRING - Ring Loopback - Shortened Path Used for the transoceanic protocol. TOP (refer to “Transoceanic protocol” (18-25)). 4-Fiber BLSR - Loopback	Displays the selected setting for the Protection Switch Mode.
Span Wait To Restore	0 ... 12 minutes, Infinite	Displays the selected Span-Wait-to-Restore time of the selected protection group.

“West Side” and “East Side” The following table shows the status data which is shown in the tabs **West Side** and **East Side** of the **View Protection** window for a 4-Fiber MS-SPRing.

Information field	Possible value	Meaning
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-S Reverse Request - Span RR-R Reverse Request - Ring NR No Request	Switch request for the outgoing west/east side Definition of the Switch Request State : A node reports the active switch state of a MS-SPRing/BLSR side, defined as the request currently associated with the concerned side, and accepted in the protocol as highest or coexisting priority. A request is associated to a side when it is detected on that side for automatic requests, when it is addressed to that side for external requests, or when that side is on the short path for received k-byte requests When no request is associated to a side (intermediate nodes), the active switch state is considered as a No-Request. ¹
East/West Last Protection Switch Attempt Status	Success, Denied, Failed	Status of the last switch action.
East/West Active Unite State	Working or Protection and the corresponding port AID.	Displays the East/West Active Unit State
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-S Reverse Request - Span 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. K1byte, 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 route of the K-bytes to the other switching NE.
East/West Channel Status	Idle Bridged Bridged and Switched Not Used RDI-L AIS-L	The current channel status of the node.

Notes:

1. *LambdaUnite™* will have to interwork with other BLSR / MS SPRING products in mixed rings which will thus show different **Switch**

Request State display behaviour.

2. In special multiple request scenarios it might happen that **East Switch Request State** and **West Switch Request State** are interchanged”.

Important! 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” (15-9)	The AID defined for the selected protection group.
Protection Type	Path	This field displays the Protection Type. For UPSR/SNCP Path Protection is displayd.
Path Protection Group Name	<ASCII string with up to 24 characters>	The Names of the Path Protection Group which has been assigned with the creation of the cross connection.
Cross Connection Rate	VC-3, VC-4, VC-4-4c, VC-4-16c, STS-1, STS-3, STS-12, STS-48, STS-192	The rate of the cross connection associated with this protection group.
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, VC-4-64c, STS-1, STS-3c, STS-12c, STS-48c, STS-192c	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” (15-9)	Displays the path of the protection. This includes both, the source tributary AID and the destination tributary AID.
Protection Constituent	<source tributary AID>, <destination tributary AID>, cf. “Overview of access identifiers” (15-9)	Displays the path of the protection. This includes both, the source tributary AID and the destination tributary AID.
Switch Request State	cf. “Switch request state” (7-47)	Displays the switch request state.
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	Displays the settings wether revertive mode is enabled or disabled.

Information field	Possible value	Meaning
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	Displays the settings whether the holdoff timer is enabled or disabled.
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.



Parameters of the window “View Protection” for a one way path protection

Status data The following table shows the status data which is shown in the **View Protection** window for a one way path protection.

Information field	Possible value	Meaning
Portection Group		
Protection Group AID	cf. “Overview of access identifiers” (15-9)	The AID defined for the selected protection group.
Protection Type	Path	This field displays the Protection Type.
Path Protection Group Name	<ASCII string with up to 24 characters>	The Names of the Path Protection Group which has been assigned with the creation of the cross connection.
Cross Connection Rate	VC-3, VC-4, VC-4-4c, VC-4-16c, VC-4-64c, STS-1. STS-3c, STS-12c, STS-48c, STS-192c	Cross-connection rate
Constituent Member List		
Constituent	<source tributary AID>, <protection tributary AID>, <destination tributary AID>	Displays the path of the protection.
CST (Constituent Signal Type)	VC-3, VC-4, VC-4-4c, VC-4-16c, VC-4-64c, STS-1. STS-3c, STS-12c, STS-48c, STS-192c	Cross-connection rate
Active	Working, Protection	Shows which path is actually active
Working Source	<source tributary AID>, cf. “Overview of access identifiers” (15-9)	The source tributary AID.
Protection Source	<protection tributary AID>, cf. “Overview of access identifiers” (15-9)	The protection tributary AID.
Destination	<destination tributary AID> “Overview of access identifiers” (15-9)	The destination tributary AID.
SWREQ (Switch Request State)	cf. “Switch request state” (7-49)	Displays the switch request state.
Working Fault	Signal Failed (SF), Signal Degraded (SD), None	Displays the failure condition of the working path
Protection Fault	Signal Failed (SF), Signal Degraded (SD), None	Displays the failure condition 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.

Information field	Possible value	Meaning
Provisional Parameters		
Revertive Mode	Enabled, Disabled	Displays the settings whether revertive mode is enabled or disabled.
Alarm Severity Assignment Profile	<ASCII string with up to 24 characters>	Displays the Path Protection Switch Alarm Severity Assignment Profile
SNC Protection Type	SNC-I, SNC-N	This field is only applicable for an SDH path protection. It displays the type of path protection.
Holdoff Timer	Enabled, Disabled	Displays the settings whether holdoff timer is enabled or disabled.
Wait To Restore time	0 ... 60 minutes	Defines the time interval before the system switches back to the working path after restoration

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- or 4-fiber MS-SPRing/BLSR network environment

When to use Use this procedure to create cross-connections for traffic which is protected via a MS-SPRing/BLSR.

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 MS-SPRing/BLSR, 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

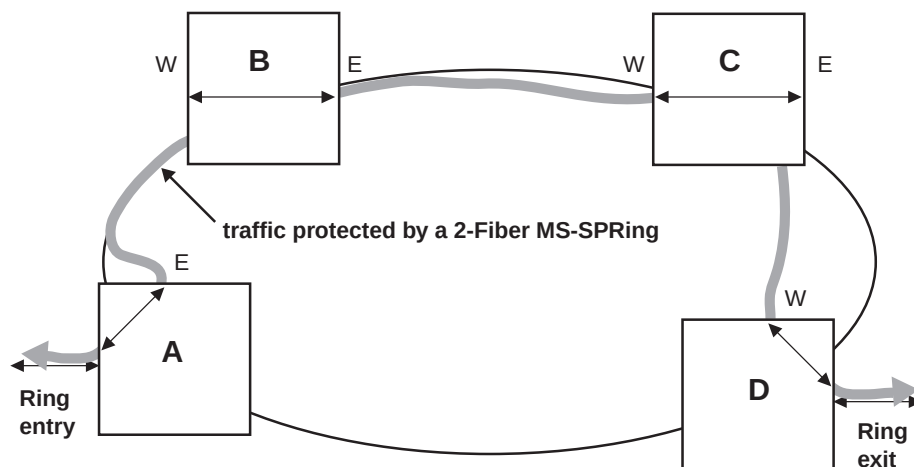
The following equipment is required to perform this task:

- WaveStar® CIT

Related information For related information, see:

- [“Creating a new cross-connection” \(7-18\)](#)
- [“Creating a new 2-fiber MS-SPRing or 2-fiber BLSR \(NE level\)” \(7-57\)](#)

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-256 ring,	select as cross-connection Destination the AID of a tributary belonging to an STM-256 port.

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.
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.
the NE belongs to an OC-768 ring,	select as cross-connection Destination the AID of a tributary belonging to the OC-768 port which is interface to the BLSR.
the NE belongs to an OC-192 ring,	select as cross-connection Destination the AID of a tributary belonging to the OC-192 port which is interface to the BLSR.
the NE belongs to an OC-48 ring,	select as cross-connection Destination the AID of a tributary belonging to the OC-48 port which is interface to the BLSR.

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/BLSR 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-256/OC-768 ring,	select as cross-connection Source the AID of a tributary belonging to an STM-256/OC-768 port. In the example the ring exit is NE D. In the example the ring exit is NE D.
the NE belongs to an OC-768 ring,	select as cross-connection Source the AID of a tributary belonging to an OC-768 port.
the NE belongs to an STM-64/OC-192 ring,	select as cross-connection Source the AID of a tributary belonging to an STM-64/OC-192 port.
the NE belongs to an STM-16/OC-48 ring,	select as cross-connection Source the AID of a tributary belonging to the STM-16/OC-48 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-1, STM-4, STM-16, STM-64 and STM-256 ports. The APS can be established for optical OC-3, OC-12, OC-48, OC-192 and OC-768 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” \(15-7\)](#), [“Preprovisioning a circuit pack” \(4-42\)](#) and [“Reassigning a circuit pack” \(4-46\)](#)).
- Complete the port provisioning for any optical port which is involved in the protection group (cf. [“Configuring an optical SDH/SONET port” \(4-49\)](#) and [“Configuring a tributary” \(4-92\)](#)).
- 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/APS 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/APS between 2 ports on the same circuit pack. An 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.

An MSP/APS can only be provisioned successfully, if no line timing reference is assigned to the protection port of the MSP/APS group.

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” \(18-13\)](#)
- [“Line Protection” \(18-19\)](#)

Instructions Complete the following steps to create a new MSP/APS:

- 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 or 2-fiber BLSR (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” \(18-13\)](#)
- [“Ring Protection” \(18-21\)](#)
- [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” \(15-7\)](#), [“Preprovisioning a circuit pack” \(4-42\)](#) and [“Reassigning a circuit pack” \(4-46\)](#)).
- Complete the port provisioning for any optical port which is involved in the protection group (cf. [“Configuring an optical SDH/SONET port” \(4-49\)](#) and [“Configuring a tributary” \(4-92\)](#)).
- Verify that no cross-connections have been made on any port to be included in the protection group (cf. [“Viewing existing cross-connections” \(7-4\)](#)).
- 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. 3 digits, a value from **1** to **999** 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” \(15-7\)](#) and [“Overview of access identifiers” \(15-9\)](#)).
-

-
- 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” \(3-57\)](#)). 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” \(3-57\)](#)).

-
- 11** Repeat [Step 1](#) to [Step 10](#) for each network element in the ring.

END OF STEPS



Creating a new 4-fiber MS-SPRing or 4-fiber BLSR (NE level)

When to use	Use this procedure to create a new 4-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. 4-fiber Rings are only possible for STM-64 or OC-192 interfaces.
Related information	For related information, see: • “Protection mechanisms” (18-13) • “Ring Protection” (18-21) • Chapter 3, “Management communication setup”
Configuration Rules	A 4-fiber MS-SPRing/BLSR group can only be provisioned successfully, if there is no line timing reference assigned to the protection port of the spans of the MS-SPRing/BLSR group (east protection port or west protection port).
Before you begin	Prior to performing this task, you must: • Verify that all required circuit packs are installed (cf. “Shelf configuration” (15-7), “Preprovisioning a circuit pack” (4-42) and “Reassigning a circuit pack” (4-46)). • Complete the port provisioning for any optical port which is involved in the protection group (cf. “Configuring an optical SDH/SONET port” (4-49) and “Configuring a tributary” (4-92)). • Verify that no cross-connections have been made on any port to be included in the protection group (cf. “Viewing existing cross-connections” (7-4)). • 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 or BLSR:

.....

- 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 **4Fiber MS-SPRing** (SDH) or **4 Fiber BLSR** (SONET).

Result:

The parameter fields for the 4-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. 3 digits, a value from **1** to **999** 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 Working Port**, **West Working Port**, **East Protection Port** and **West Protection Port** in the respective drop-down list boxes in the group box **Group Member**. The values correspond to the slot designations (cf. [“Shelf configuration” \(15-7\)](#) and [“Overview of access identifiers” \(15-9\)](#)).
-

- 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** or **SWTR (Spanning Wait To Restore)** 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” \(3-57\)](#)). 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 **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” \(3-57\)](#)).
-

- 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” \(18-14\)](#)

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, 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 or UPSR:

- 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.
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 **1** and **60 min** are allowed.
-

- 16** Click on the **Finish** button to apply your settings.

END OF STEPS

.....



Creating an unidirectional path protection

When to use Use this procedure to create a one way path-protection in a network element. The one way path-protection can be used to protect a signal. Configure the one way path-protection for the two NEs between which the protected cross connection is to be established.

Related information For related information, see

- [“Path Protection” \(18-14\)](#)
- [“Dual Node Ring Interworking \(DNI\)/Dual Ring Interworking \(DRI\) for MS-SPRing or BLSR” \(18-29\)](#)

Before you begin Prior to performing this task, you must be logged into the WaveStar® CIT and the respective network element. You must also complete the configuration of the rings which are involved in the DNI/DRI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected. Please note that for an interworking between one SNCP/UPSR protected ring and one MS-SPRing/BLSR protected ring (primary node) with both rings in the same NE (collapsed nodes), the interconnection in the direction from the SNCP/UPSR ring to the MS-SPRing/BLSR has to be realized through an external connection, i.e. through an additional tributary interface. Note that this does not apply to the secondary node. (cf. [“DNI/DRI between MS-SPRing and SNCP or BLSR and UPSR” \(18-36\)](#)).

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 one way path-protection:

- 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 **1-Way-Path-Protected** 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 one way path-protection is displayed.

- 6 Select the first leg source (A), the destination (B) and the second leg source (C) as described in the window via the buttons **Select...**

Proceed as described in the windows **First Leg Source Tributary**, **Destination Tributary** and **Second Leg Source Tributary**.

-
- 7 Define the working leg and the protection leg by clicking on the respective check box.
-

- 8 Click on the **Next>** button.

Result:

Screen 3 opens.

- 9 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.
-

- 10 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.
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.
-

- 11 Select the **Wait To Restore Time** if the one way path protection is working in revertive mode. Values between **1** and **60 min** are possible.

-
- 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 one way path protection shall operate in revertive or non-revertive mode.

-
- 15** Click on the **Finish** button to apply your settings.

END OF STEPS



Provisioning path protection parameters

When to use Use this procedure to provision parameters for an existing path-protection like SNCP, UPSR or an unidirectional path protection.

Related information For related information, see

- [“Path Protection” \(18-14\)](#)

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, 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 provision parameters on existing path-protections:

- 1 Call up the window **Provision Parameters for Protection Group or Equipment** via **Configuration** → **Provision...** 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. Click on the **Provision** button.

Result:

The window **Provision Parameters for Protection Group or Equipment** opens.

- 3 If you want to enter a new protection group name, insert a name with up to 24 characters for the protection group in the text box **New Protection Group Name**.

-
- 4 Define whether the path protection shall operate in revertive or non-revertive mode.
-

5 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.
-

- 6 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.

- 7 Select the **Wait To Restore Time** if the path protection is working in revertive mode. Values between **1** and **60 min** are possible.
-

- 8 Select the **Path Protection Switch ASAP** .
-

- 9 Click on **Apply** then click on **Close**.

END OF STEPS



Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings

When to use Use this procedure to create a bidirectional DNI (Dual Node Ring Interworking)/DRI (Dual Ring Interworking) protection between two rings with a 2-fiber or a 4-fiber MS-SPRing or BLSR.

Related Information For related information see:

- [“Dual Node Ring Interworking \(DNI\)/Dual Ring Interworking \(DRI\) for MS-SPRing or BLSR” \(18-29\)](#)

Before you begin Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI/DRI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected.

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:

- *LambdaUnite*[™] CIT

Instructions 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 *LambdaUnite* 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**

Please note that it is not possible to proceed to the next window before selecting the cross connection rate.

-
- 4 Define the type of DNI/DRI by clicking on the respective radio button in the group box **Type of Cross-Connection**. The following values are possible:

- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing Primary Node** for the interconnection of two rings via four DNI/DRI nodes
This type of DNI/DRI is realized by a connection between two different nodes (primary nodes) each belonging to one of the two protected rings. The broadcast and the switch function are located in two different network elements. Furthermore there are two or three other network elements involved in the DNI/DRI which realize the rerouting of the protected signals (secondary nodes).
- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing Primary Node in Same NE** for a DNIDRI with collapsed nodes
In this type of DNI/DRI the broadcast and the switch function are implemented in one network element, and there may be also only one secondary node.

-
- 5 Click on **Next>** to proceed to the next window.

Result:

Screen 2 appears. A depiction of the cross connections in the primary node (the NE to which you are connected and for which you are creating the DNI/DRI connections) is displayed automatically.

-
- 6 Select the connection to the secondary node(s) via the button **Select....** Proceed as described in the windows **From/To Secondary (Ring1/Ring2) Node Tributary**.

Result:

The tributaries which establish the connection to the terminating nodes (B, D) are displayed.

7	<table><tr><th>IF</th><th>THEN</th></tr><tr><td>you have selected the DNI/DRI with collapsed nodes,</td><td>go to Step 9.</td></tr><tr><td>you have selected the DNI/DRI with four nodes,</td><td>go to Step 8.</td></tr></table>	IF	THEN	you have selected the DNI/DRI with collapsed nodes,	go to Step 9 .	you have selected the DNI/DRI with four nodes,	go to Step 8 .
IF	THEN						
you have selected the DNI/DRI with collapsed nodes,	go to Step 9 .						
you have selected the DNI/DRI with four nodes,	go to Step 8 .						

- 8 Select the connection to the second ring (C) via the button **Select....** Proceed as described in the window **From/To Other Ring Tributary**.

Result:

The complete implementation of the DNI/DRI protection is displayed.

-
- 9 Define the role of the tributaries as working or protection tributary by clicking on the respective check box(es).

In a DNI/DRI with collapsed nodes, the STM-64 line port is the working port!

-
- 10 Click on the **Next>** button.

Result:

Screen 3 opens.

-
- 11** Select the terminating node TID and the secondary node TID in the drop-down list boxes **Term Node NE Name:** and **Sec Node NE Name:**.
-
- 12** Insert a name for the protection group in the text box **PPG Name**.
-
- 13** Define in the drop-down list box **PP Reversion Behavior**, whether the DNI/DRI shall operate in revertive or in non-revertive mode .
-
- 14** Define in the drop-down list box **PP Holdoff Behavior**, whether a Holdoff time shall pass before a protection switch is performed. This is necessary to avoid a double switch of MS-SPRing/BLSR and DNI/DRI.
- The default value is 100 ms, but the holdoff time can be modified in the window **Path Protection Type Provisioning**. The selected value is valid for all path protection which are configured for the network element.
-
- 15** Click on the **Finish** button to apply your settings.
-
- 16** If required, set the holdoff time in the window **Path Protection Type Provisioning** which is accessible via **Configuration → Path Protection Type....** Note that the setting is valid for all path protections in the network element.

END OF STEPS



Creating an unidirectional DNI/DRI between two protected rings.

When to use Use this procedure to create a unidirectional DNI/DRI protection (1-way path protection) between two rings with a 2-fiber or 4-fiber MS-SPRing/BLSR or one MS-SPRing/BLSR protected ring and one SNCP/UPSR protected ring.

Related Information For related information see:

- [“Creating a cross-connection in a 2- or 4-fiber MS-SPRing/BLSR network environment” \(7-50\)](#)
- [“Bridging a cross-connection” \(7-28\)](#)
- [“Creating an unidirectional path protection” \(7-67\)](#)

Before you begin Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI/DRI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected.

You have to distinguish between several possibilities of the network topology which are listed below:

- Two MS-SPRing/BLSR protected rings (with or without collapsed nodes)
- One MS-SPRing/BLSR protected ring, 1 SNCP/UPSR ring
 - with an interconnection via four NEs; the direction of the protected 1-way cross-connection is from SNCP/UPSR ring to MS-SPRing/BLSR
 - with an interconnection via four NEs; the direction of the protected 1-way cross-connection is from MS-SPRing/BLSR to SNCP/UPSR ring
 - with an interconnection via collapsed nodes; the direction of the protected 1-way cross-connection is from SNCP/UPSR ring to MS-SPRing/BLSR
 - with an interconnection via collapsed nodes; the direction of the protected 1-way cross-connection is from MS-SPRing/BLSR to SNCPUPSR ring

Please note that for an interworking between one SNCP/UPSR protected ring and one MS-SPRing/BLSR protected ring (primary node) with both rings in the same NE (collapsed nodes), the interconnection in the direction from the SNCP/UPSR ring to the MS-SPRing/BLSR has to be realized through an external connection, i.e. through an additional tributary interface. Note that this does not apply to the secondary node. (cf. [“DNI/DRI between MS-SPRing and SNCP or BLSR and UPSR” \(18-36\)](#)).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections and the DNI/DRI.

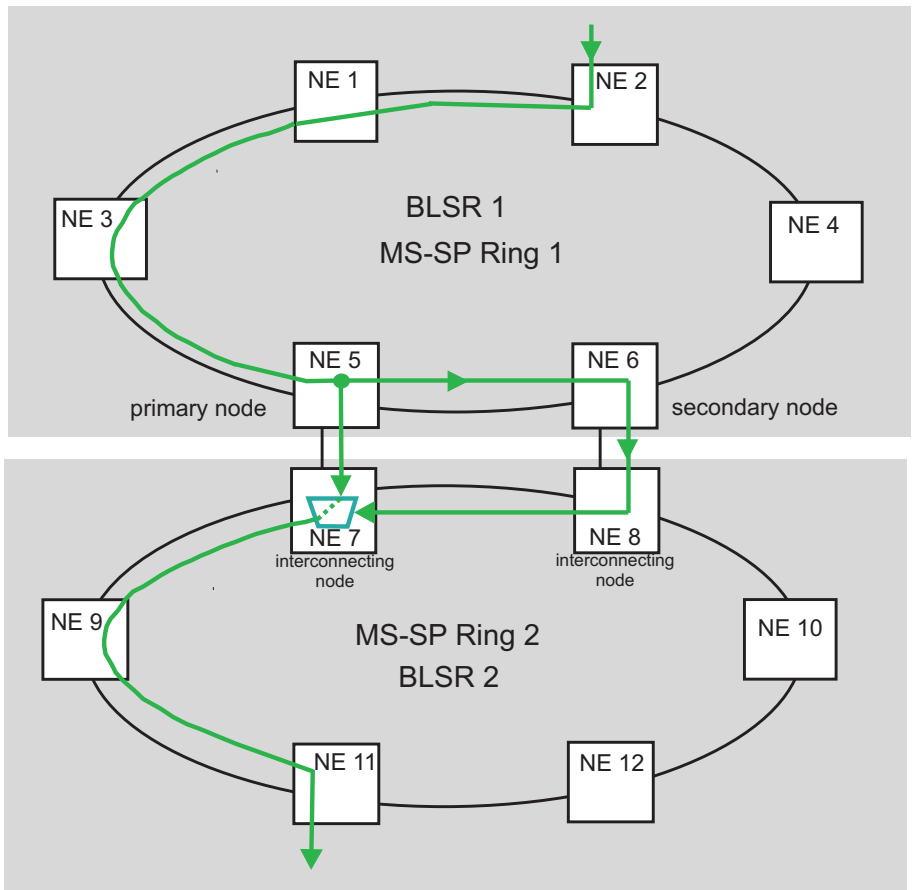
Required equipment

The following equipment is required to perform this task:

- *LambdaUnite*[™] CIT

**DNI/DRI between two
MS-SPRing/BLSR
protected rings**

1



As shown in the graphic above, switch 1-way cross-connections in all network elements (NE2, NE 1) belonging to the first ring (MS-SPRing/BLSR 1), cf. [“Creating a new cross-connection” \(7-18\)](#).

- 2 In the primary node (NE 5) create a broadcast (bridge) to the secondary node (NE 6) and one interconnecting node (NE 7), cf. [“Bridging a cross-connection” \(7-28\)](#).
- 3 Create through-connections in the secondary node (NE 6) and the second interconnecting node (NE 8), cf. [“Creating a new](#)

[cross-connection” \(7-18\)](#). In a network topology with collapsed nodes only one through connection is necessary.

.....

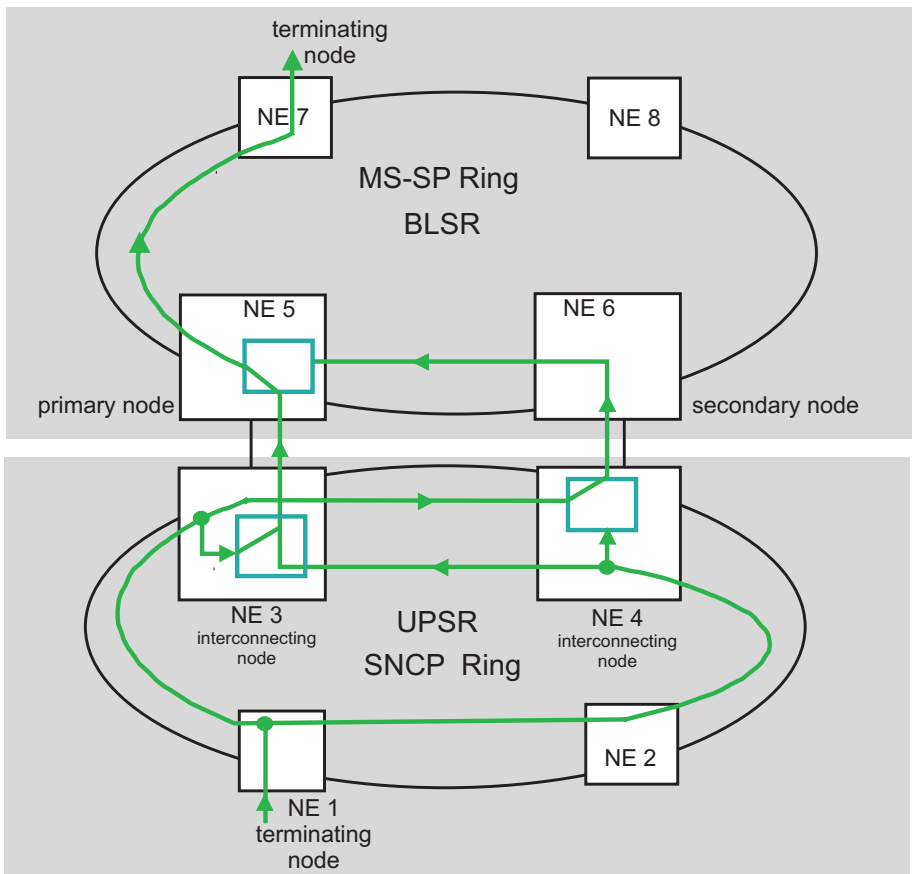
- 4 Create a 1-way path protection in the first interconnecting node (NE 7) which establishes the selector between the signal from the primary node (NE 5) and the other interconnecting node (NE 8), cf. [“Creating an unidirectional path protection” \(7-67\)](#). In a network topology with collapsed nodes, the broadcast and the 1-way path protection are in the same network element.
-

- 5 Create 1-way cross-connections in all network elements (NE 9, NE 11) belonging to the second ring (MS-SPRing/BLSR 2), cf. [“Creating a new cross-connection” \(7-18\)](#).

END OF STEPS

.....

**DNI/DRI between one
MS-SPRing/BLSR
protected ring and one
SNCP/UPSR ring via four
NEs (direction SNCP/UPSR
→ MS-SPRing/BLSR)**



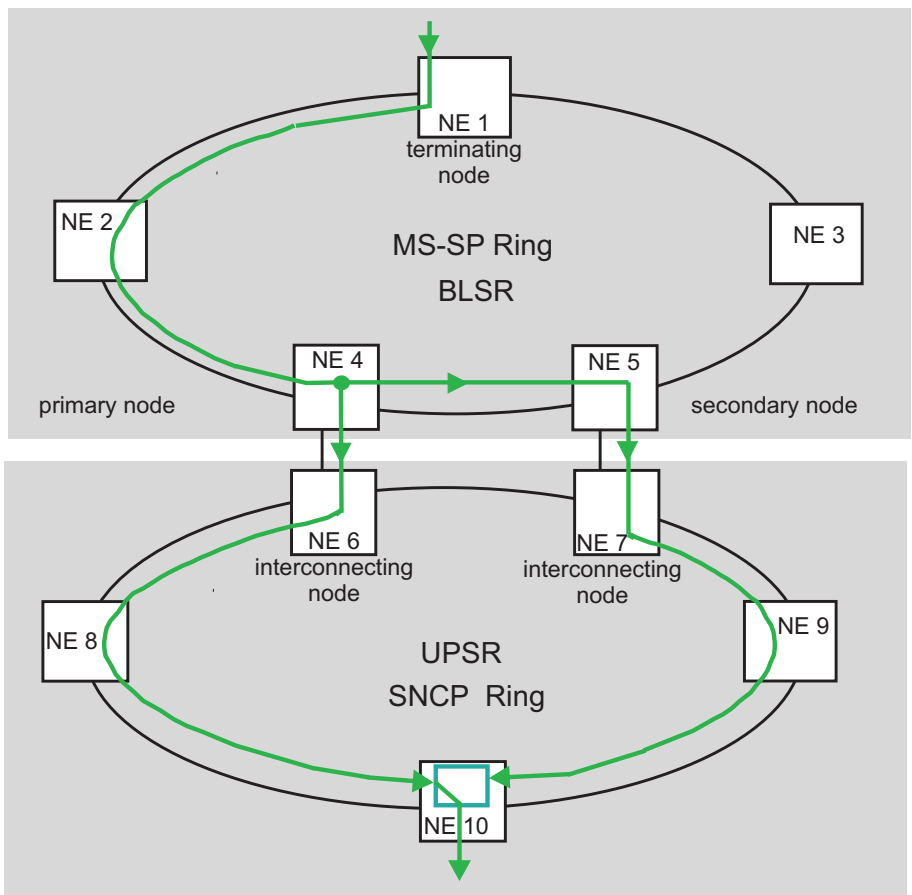
As shown in the graphic above, switch a broadcast (bridge) in the terminating node of the SNCP/UPSR ring, where the cross-connection starts (NE 1), cf. [“Bridging a cross-connection” \(7-28\)](#).

- 2 In the first interconnecting node (NE 3) create a 1-way path protection between the two signals broadcasted at the terminating node (NE 1), cf. [“Creating an unidirectional path protection” \(7-67\)](#).
- 3 Create additionally a one-way cross-connection to the second interconnecting node (NE 4).

-
- 4 Create through-connections in all network elements of the SNCP/UPSR ring which are not involved in the DNI/DRI (e.g. NE 2), cf. [“Creating a new cross-connection” \(7-18\)](#).
.....
- 5 In the second interconnecting node (NE 4) create a 1-way path protection between the broadcasted signal from the first interconnecting node (NE 3) and the signal which is received via the SNCP/UPSR ring (from NE 2), cf. .
.....
- 6 Create additionally a one-way cross-connection to the first interconnecting node (NE 3).
.....
- 7 Create a through-connection in the secondary node (NE 6), cf. [“Creating a new cross-connection” \(7-18\)](#).
.....
- 8 Create a 1-way path protection between the primary node (NE 5) between the signal from the secondary node (NE 6) and from the neighbour interconnecting node (NE 3), cf. .
.....
- 9 Create 1-way cross-connections in all network elements between the primary node and the terminating node (NE 7) of the MS-SPRing/BLSR protected ring, cf. [“Creating a new cross-connection” \(7-18\)](#).

.....
E N D O F S T E P S
.....

**DNI/DRI between one
MS-SPRing/BLSR¹
protected ring and one
SNCP/UPSR ring via four
NEs (direction
MS-SPRing/BLSR →
SNCP/UPSR)**



Create a 1-way cross-connection in the terminating node (NE 1) of the MS-SPRing/BLSR protected ring, cf. [“Creating a new cross-connection” \(7-18\)](#).

- 2 Create through-connections in all network elements between the terminating node and the primary node of the MS-SPRing/BLSR protected ring (e.g. NE 2), cf. [“Creating a new cross-connection” \(7-18\)](#).
- 3 Create a broadcast (bridge) in the primary node (NE 4) with one leg to the secondary node (NE 5) and one to the neighbour interconnecting node (NE 6), cf. [“Bridging a cross-connection” \(7-28\)](#).

- 4 Create a through-connection through the secondary node (NE 5), cf. [“Creating a new cross-connection” \(7-18\)](#).
- 5 Create a through-connection in each interconnecting node (NE 6, NE 7) of the SNCP/UPSR ring in a way that the signals are distributed via the ring in opposite directions, cf. [“Creating a new cross-connection” \(7-18\)](#).
- 6 Create through-connections in all network elements of the SNCP/UPSR ring (e.g. NE 8, NE 9), cf. [“Creating a new cross-connection” \(7-18\)](#).
- 7 Create a 1-way path protection in the terminating node (NE 10) of the SNCP/UPSR ring, cf. .

END OF STEPS

**DNI/DRI between one
MS-SPRing/BLSR
protected ring and one
SNCP/UPSR ring with
collapsed nodes (direction
SNCP/UPSR →
MS-SPRing/BLSR)**

Proceed as described in [“DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR ring via four NEs \(direction SNCP/UPSR → MS-SPRing/BLSR\)” \(7-81\)](#). Please note that the primary node (NE 5) and the first interconnecting node (NE 3) are the same network element in this case.

- 2 Create a 1-way through-connection through the primary node/interconnecting node as an external connection via an additional port unit.

END OF STEPS

**DNI between one
MS-SPRing protected ring
and one SNCP ring with
collapsed nodes (direction
MS-SPRing → SNCP)**

.....

Proceed as described in [“DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR ring via four NEs \(direction MS-SPRing/BLSR → SNCP/UPSR\)” \(7-83\)](#). Please note that the primary node (NE 4) and the first interconnecting node (NE 6) are the same network element in this case.

.....

- 2** Create a 1-way through-connection through the primary node/interconnecting node as an external connection via an additional port unit.

.....

END OF STEPS

.....



Creating a bidirectional DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR protected ring

When to use Use this procedure to create a bidirectional DNI/DRI protection (2-way path protection) between one ring which is protected by a 2-fiber or 4-fiber MS-SPRing/BLSR and one ring which is protected by an SNCP/UPSR. The following procedure has to be carried out in the interconnecting nodes of the SNCP/UPSR protected ring. In the primary and secondary node belonging to the MS-SPRing/BLSR protected ring the DNI/DRI has to be established as described in [“Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings” \(7-73\)](#).

Related Information For related information see:

- [“Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings” \(7-73\)](#)

Before you begin Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI/DRI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected. Please note that for a DNI/DRI with both rings in the same NE you need an additional pair of tributary ports to establish the interconnection via external connections. This procedure describes the creation of the DNI/DRI in the NEs belonging SNCP/UPSR protected ring. For the complete configuration of the interworking between the two rings the creation of the DNI/DRI in the primary and secondary node belonging to the MS-SPRing/BLSR protected ring as described in is necessary as well.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections and the DNI/DRI.

Required equipment

The following equipment is required to perform this task:

- *LambdaUnite™* CIT

Instructions Complete the following steps to create a DNI/DRI-protected cross-connection:

- 1 In the **System View** of the *LambdaUnite* CIT, via **Configuration** → **Cross Connection...**, call up the **Cross Connection Wizard**.

- 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**

Please note that it is not possible to proceed to the next window before selecting the cross-connection rate.

- 4 Select **Ring Interworking, Drop and Continue, UPSR/SNCP Node** by clicking on the respective radio button in the group box **Type of Cross-connection**.

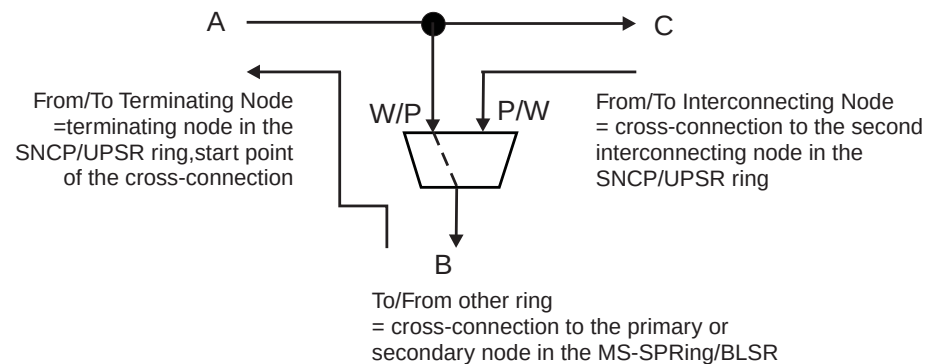
- 5 Click on **Next>** to proceed to the next window.

Result:

Screen 2 appears. A depiction of the DNI/DRI cross-connection in the NE to which you are connected is displayed.

-
- 6 The following figure shows an example for interworking between a MS-SPRing protected ring and a SNCP ring.

Via the buttons **Select...**, select the first leg source (A) defining the connection to the terminating node where the VC has been coupled in, the destination tributary (B) defining the connection to the MS-SPRing protected ring and the second leg source (C) defining the connection to the second interconnecting node.



Proceed as described in the windows **From/To Terminating Node**, **From/To Interconnecting Node** and **To/From Other Ring**.

-
- 7 Define the working leg and the protection leg by clicking on the respective check box.

-
- 8 Click on the **Next>** button.

Result:

Screen 3 opens.

-
- 9 Select the **Terminating Node NE Name**, which is the TID of the terminating node in the SNCP/UPSR ring.

-
- 10** Select the **Other Ring Node NE Name**, which is the TID of the terminating node in the MS-SPRing/BLSR protected ring.
-
- 11** Select the **Interconnecting Node NE Name**, which is the TID of the second interconnecting node of the DNI/DRI.
-
- 12** Select the **Output Mode**. 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.
-
- 13** Insert a name with up to 24 characters for the protection group in the text box **PPG Name**.
-
- 14** Define in the drop-down list box **PP Reversion Behavior**, whether the DNI/DRI shall operate in revertive or in non-revertive mode.
-
- 15** Define in the drop-down list box **PP Holdoff Behavior**, whether a Holdoff time shall pass before a protection switch is performed.
- The default value is 100 ms, but the holdoff time can be modified in the window **Path Protection Type Provisioning**. The selected value is valid for all path protection which are configured for the network element.
-
- 16** Click on the **Finish** button to apply your settings.
-
- 17** If required, set the holdoff time in the window **Path Protection Type Provisioning** which is accessible via **Configuration → Path Protection Type...** Note that the setting is valid for all path protections in the network element.

END OF STEPS

.....



Creating a bidirectional ring-to-ring SNCP

When to use Use this procedure to create two SNCPs within one NE which protect a bidirectional connection that is routed via two rings. Each SNCP protects the connection in one ring.

Related information For related information, see

- [“Path Protection” \(18-14\)](#)

Before you begin Prior to performing this task, you must complete the configuration of the rings which are involved in the SNCP. Furthermore you must have a detailed knowledge on the ring topology of the rings involved and the paths to be protected.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections protected with an SNCP.

Required equipment

The following equipment is required to perform this task:

- *LambdaUnite*[™] CIT

Instructions 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 *LambdaUnite* 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**

-
- 4 Select **UPSR/SNCP Ring-to-Ring, Single Node Interconnection, Same NE** 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-connections in the NE to which you are connected and for which you are creating the SNCP is displayed.

- 6 Select the tributaries as described in the window via the buttons **Select....** Proceed as described in the windows **PPG2 Output Tributary, Adjunct PPG2 Output Tributary, PPG1 Output Tributary** and **Adjunct PPG1 Output Tributary**.
-

- 7 Define the two working paths by clicking on the respective check boxes.
-

- 8 Click on the **Next>** button.

Result:

Screen 3 opens.

- 9 Select the **PPG1 Wkg Source NE Name**, the **PPG2 Wkg Source NE Name**, the **PPG1 Prot Source NE Name** and the **PPG2 Prot Source NE Name** in the respective drop-down list boxes. This is necessary, if the network element is part of and MS-SPRing. Otherwise proceed to [Step 10](#).

-
- 10** Select the **Output Mode** for the protection groups PPG1 and PPG2 in the respective group boxes. 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** Insert a name with up to 24 characters for the protection group in the text box **PPG Name**.
-
- 12** Define in the drop-down list box **PP Reversion Behavior**, whether the SNCP shall operate in revertive or in non-revertive mode.
-
- 13** Define in the drop-down list box **PP Holdoff Behavior**, whether a Holdoff time is to expire before a protection switch is performed.
-
- 14** Click on the **Finish** button to apply your settings.

END OF STEPS

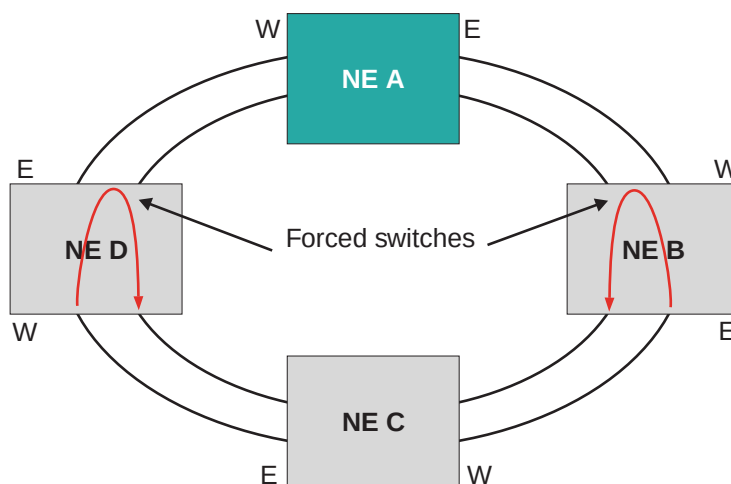


Deleting a protection group

When to use Use this procedure to delete protection groups which have been provisioned for the system. This can be 1+1 MSPs/APSs, 2-fiber MS-SPRings/2-fiber BLSRs or 4-fiber MS-SPRings/4-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” \(8-7\)](#)). In NE B, the destination side for the forced switch (**Direction**) is West, in NE D the destination side (**Direction**) is East.



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 delete a protection group 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



Configuring VCG tributaries

When to use Use this procedure to configure a VCG tributary.

Related information For related information, see:

- [“VCG tributary details” \(7-99\)](#)
- [“Gigabit Ethernet Interface” \(18-43\)](#)

Before you begin You must be logged into the WaveStar® CIT and the respective network element.

Required privilege code

You must have at least privilege codes of **P3 and M1** to configure a VCG tributary.

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 VCG 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 **Equip** 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 circuit pack. Double click on the circuit pack or click on the **+** in front of the unit name.

-
- 4 Select the desired VCG.
-

- 5 Select the desired VCG tributary. Click on the **Provision** pushbutton.

Result:

On the right side of the window the provisionable parameters are displayed.

- 6 Set the parameters according to your needs. Please refer to [“VCG tributary details” \(7-99\)](#) for hints on the selection of the parameter values.
-

- 7 Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**.

END OF STEPS



Retrieving VCG/VCG tributary information

When to use Use this procedure to retrieve information on a virtual concatenation group.

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

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps in order to view information on a virtual concatenation group:

- 1 In the **System View** of the *LambdaUnite*™ CIT, via **View** → **View Equipment Details...** call up the **View Equipment Details...** window.

Result:

On the left side of the window, the **Equipment** selection tab is displayed. 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 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 VCG. Double click on the VCG or click on the + in front of the VCG.

Result:

The list of tributaries which are available becomes visible below the VCG.

5

IF	THEN
you want to display the information on the VCG	select the desired VCG and click on Select. Result: On the right side of the window, the parameters of the selected VCG are displayed. Reference: Please refer to “VCG Port Details” (7-105) for the description of the parameters.
you want to display the VCG tributary parameters	select the desired tributary and click on Select. Result: On the right side of the window, the parameters of the selected tributary are displayed. Reference: Please refer to “Parameters of the window “View Current VCG Trib. Maintenance Signal”” (7-115) for the description of the VCG tributary specific parameters.

END OF STEPS



VCG tributary details

Description The following fields/parameters are displayed on top of the window:

Field/parameter ... Displays...

Tributary AID the access identifier of the selected VCG tributary.

The window consists of four tabs, each describing a set of parameters:

- [“Transmission” \(7-99\)](#)
- [“Trail Trace Identifier” \(7-100\)](#)
- [“Trail Signal Label” \(7-103\)](#)
- [“VCG Membership” \(7-103\)](#)

Transmission Configure the tributary according to the needs of the network environment. Especially the alarm behaviour is concerned.

The following table shows for VCG 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.
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
HP Degraded 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.
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.
HP Excessive BER 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.

Parameter	Values	Meaning
HP Degraded Signal (BER) 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.
Tributary Alarm Severity Assignment Profile	<ASAP name> (24 characters max.), Default	Selection between the default and a specific ASAP

Trail Trace Identifier The following table shows the status data which is shown in the tab **Trail Trace Identifier**.

Information field	Possible value	Meaning
J1 (Path Trace)		
Transmitted Format	Values are • Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Transmitted Identifier		
CRC-7 Calculation	AutoManual	This field displays the method of CRC-7 Calculation. • Auto - CRC is calculated and inserted by the CIT software. If the first byte of the trace is equal to the CRC over the trace, it is assumed that the value was auto-calculated. • Manual - CRC was entered manually by the user. If the first byte of the trace is not equal to the CRC over the trace, it is assumed that the value was manually inserted.

Information field	Possible value	Meaning
Value	–	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· • In ASCII mode, if a series of two hexadecimal digits cannot be converted to ASCII characters, then the <i>WaveStar</i>® CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). • In Hex mode, the <i>WaveStar</i> CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal digits, and so on until the full API is displayed.
Incoming Status	Normal Unavailable	This field shows the status of the Accepted TTI. If the status is not equal to "Normal", the corresponding Accepted TTI field (trace value) will be cleared and grayed out.
Incoming Format	Values are • Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Incoming Identifier		
Value	–	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.

Information field	Possible value	Meaning
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· - In ASCII mode, if a series of two hexadecimal digits cannot be converted to ASCII characters, then the <i>WaveStar</i> CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). - In Hex mode, the <i>WaveStar</i> CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal digits, and so on until the full API is displayed.
Expected Format	Values are Non-Specific Repeating Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Expected Identifier		
CRC-7 Calculation	Auto Manual	This field displays the method of CRC-7 Calculation. - Auto - CRC is calculated and inserted by the CIT software. If the first byte of the trace is equal to the CRC over the trace, it is assumed that the value was auto-calculated. - Manual - CRC was entered manually by the user. If the first byte of the trace is not equal to the CRC over the trace, it is assumed that the value was manually inserted.
Value	—	This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. In the textbox the value can be edited.

Information field	Possible value	Meaning
HP TIM		
Monitor	Enabled	This field allows to set the Trace Identifier Mismatch (TIM) monitor to enable or disable.
	Disabled	
AIS Insertion	Enabled	This field allows to set the Trace Identifier Mismatch (TIM) AIS insertion to enable or disable.
	Disabled	

Trail Signal Label The following table shows the status data which is shown in the tab **Trail Signal Label**.

Information field	Possible value	Meaning
Trail Status	Normal AIS Unavailable	This field shows the accepted trail status.
Accepted Signal Label (C2)	Two hexadecimal digits: • 0x00 "Unequipped" • 0x01 "Equipped" • 0x02 "TUG Structure" • 0x03 "Locked TU" • 0x04 "34 Mbit/s or 45 Mbit/s, asynchronous" • 0x12 "140 Mbit/s, asynchronous" • 0x13 "ATM" 0x14 "MAN-DQDB" • 0x15 "FDDI" • 0x1B "GFP Mapping" • 0x1F "Ethernet Frame" • other	This field shows the accepted trail signal label (C2). If the Trail Status is not equal to "Normal", this field is grayed out and empty.
Trail Signal Label Descriptive	Equipped Unequipped	
TSL Mismatch Monitor	Enabled Disabled	This field shows the status of the monitoring of the Trail Signal Label Mismatch defect.

VCG Membership The following table shows the status data which is shown in the tab **VCG Membership**.

Information field	Possible value	Meaning
Input Direction		

Information field	Possible value	Meaning
VCG Membership	Enabled Disabled	This column in the list shows whether the tributary shall take part in the transmission of its owning VCG in input direction.
VCG Membership Status	Values are: • Add The tributary is in the LCAS state "Wait-for-Add" or "Wait-for-Data" • Active The tributary is member of the VCG and working • Failed The tributary is member of the VCG but not working due to a failure condition. Includes period during "Hold-Off". • Not Applicable The trib. is no member of the VCG. • Unavailable The trib. is member of the VCG but the current data is not retrievable for any reason.	This field shows the status of the tributary related to its VCG membership in input direction. If the VCG Membership for this VCG Tributary is disabled, this field is greyed out.
Output Direction		
VCG Membership	Enabled Disabled	This column in the list shows whether the tributary shall take part in the transmission of its owning VCG in output direction.
VCG Membership Status	• Add The tributary is in the LCAS state "Wait-for-Add" or "Wait-for-Data" • Active The tributary is member of the VCG and working • Failed The tributary is member of the VCG but not working due to a failure condition. Includes period during "Hold-Off". • Not Applicable The trib. is no member of the VCG. • Unavailable The trib. is member of the VCG but the current data is not retrievable for any reason.	This field shows the status of the tributary related to its VCG membership in output direction. If the VCG Membership for this VCG Tributary is disabled, this field is greyed out.

WTR Timer

This window also contains the push button **Clear** to clear the wait to restore timer (**WTR Timer**).



VCG Port Details

Description The following fields/parameters are displayed on top of the window:

Field/parameter ... Displays...

VCG AID the access identifier of the selected VCG port.

Port Type the rate of the corresponding port. Possible value: VCG.

The **View VCG Port Details** window consists of five tabs, each describing a set of parameters:

- [“VCG Data” \(7-105\)](#)
- [“VCG Trib. Information” \(7-105\)](#)
- [“VCG Membership” \(7-106\)](#)
- [“Port Rates” \(7-107\)](#)
- [“LCAS” \(7-107\)](#)

VCG Data The following table shows the status data which is shown in the tab **VCG Data**.

Information field	Possible value	Meaning
<i>Interface Standard</i>		
Interface Standard	SONET SDH	This field displays the current interface standard.
<i>Fault</i>		
VCG Monitoring Mode	Monitored Not Monitored	This field displays the current monitoring mode setting.

VCG Trib. Information The following table shows the status data which is shown in the tab **VCG Trib. Information**.

Information field	Possible value	Meaning
VCG Trib AID	cf. “Overview of access identifiers” (15-9)	This field shows the tributary AID (access identifier) or the respective VCG tributary.
Transmitted Sequence Number	[0 .. 20] (step = 1) Not Applicable Not Available	This parameter shows the value of the Transmitted Sequence Number of the tributary within the VC Group.

Information field	Possible value	Meaning
Accepted Sequence Number	[0 .. 255] (step = 1) Not Applicable Not Available	This parameter shows the value of the Accepted Sequence Number of the tributary within the VC Group.

VCG Membership The following table shows the status data which is shown in the tab **VCG Membership**.

Information field	Possible value	Meaning
<i>Input Direction</i>		
VCG Trib AID	cf. “Overview of access identifiers” (15-9)	This field shows the tributary AID (access identifier) or the respective VCG tributary.
VCG Membership	Enabled Disabled	This column in the list shows whether the tributary shall take part in the transmission of its owning VCG in input direction.
VCG Membership Status	Add The tributary is in the LCAS state “Wait-for-Add” or “Wait-for-Data” Active The tributary is member of the VCG and working Failed The tributary is member of the VCG but not working due to a failure condition. Includes period during “Hold-Off”. Not Applicable The trib. is no member of the VCG. Unavailable The trib. is member of the VCG but the current data is not retrievable for any reason.	This field shows the status of the tributary related to its VCG membership in input direction. If the VCG Membership for this VCG Tributary is disabled, this field is greyed out.
<i>Output Direction</i>		
VCG Trib AID	cf. “Overview of access identifiers” (15-9)	This field shows the tributary AID (access identifier) or the respective VCG tributary.
VCG Membership	Enabled Disabled	This column in the list shows whether the tributary shall take part in the transmission of its owning VCG in output direction.

Information field	Possible value	Meaning
VCG Membership Status	• Add The tributary is in the LCAS state "Wait-for-Add" or "Wait-for-Data" • Active The tributary is member of the VCG and working • Failed The tributary is member of the VCG but not working due to a failure condition. Includes period during "Hold-Off". • Not Applicable The trib. is no member of the VCG. • Unavailable The trib. is member of the VCG but the current data is not retrievable for any reason.	This field shows the status of the tributary related to its VCG membership in output direction. If the VCG Membership for this VCG Tributary is disabled, this field is greyed out.

Port Rates The following table shows the status data which is shown in the tab **Port Rates**.

Information field	Possible value	Meaning
Tributary Input Signal Rate List		
Rate	Numeric string of the form NX. N specifies the count of container type X specifies the container type (or envelope) • SDH: N = 7, X = 4 (VC4) • SONET: N = 21, X = 1 (STS-1)	This field shows the tributary structure of the VCG port in input direction. This implicitly gives the maximum capacity of the VCG port.
Tributary Unequipped Output Signal Rate List		
Rate	Numeric string of the form NX. N specifies the count of container type X specifies the container type (or envelope) • SDH: N = 7, X = 4 (VC4) • SONET: N = 21, X = 1 (STS-1)	This field shows the tributary structure of the VCG port in output direction. This implicitly gives the maximum capacity of the VCG port.

This window also contains a legend to explain the port rates.

LCAS The following table shows the status data which is shown in the tab **LCAS**.

Information field	Possible value	Meaning
LCAS Mode	Enabled Disabled	This parameter shows the operation mode of the Link Capacity Adjustment Scheme for this VCG.
WTR (Wait To Restore) Time	0 ... 60 minutes	This parameter shows the delay time which is applied before the active path switches back to the original one after restoration.
Hold-Off Timer	0 ... 10 sec	Via different hold-off times it can be defined which protection should switch first.



Retrieving current VCG delay

When to use Use this procedure to retrieve information on the current VCG delay.

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

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Instructions Complete the following steps in order to view the current VCG delay:

- 1 In the **System View** of the *LambdaUnite*™ CIT, via **Fault** → **Analysis** → **View Current VCG Tributary delays within VC Group...** call up the **View VCG Delay** window.

Result:

On the left side of the window, the **Equipment** selection tab is displayed. The shelves belonging to the system are listed.

- 2 Select the desired shelf. 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 VCG. Double click on the VCG or click on **Select**.

Result:

On the right side of the window, the parameters of the selected VCG are displayed.

Reference:

Please refer to [“Parameters of the window “View VCG Delay”” \(7-111\)](#) for the description of the parameters.

END OF STEPS



Parameters of the window “View VCG Delay”

Fields and parameters The following table shows the status data which are shown in the **View VCG Delay** window.

Information field	Possible value	Meaning
VCG Trib. AID		The AID (access identifier) of the VCG tributaries.
Transmitted Sequence Number	0 .. 20] (step = 1) Not Applicable Unavailable	This parameter shows the value of the Transmitted Sequence Number of the tributary within the VC Group.
Accepted Sequence Number	0 .. 255] (step = 1) Not Applicable Unavailable	This parameter shows the value of the Accepted Sequence Number of the tributary within the VC Group.
VCG Membership (Input Direction)	Enabled Diabled	This parameter shows whether the tributary shall take part in the transmission:of its owning VCG in input direction.
VCG Membership Status (Input Direction)	Values are • Active The tributary is member of the VCG and working • Do Not Use The tributary is member of the VCG but taken off by LCAS • Not Available The trib. is member of the VCG but the current data is not retrievable for any reason • Not Applicable The trib. is no member of the VCG.	Status of the tributary related to its VCG membership in input direction.
VCG Membership (Output Direction)	Enabled Diabled	This parameter shows whether the tributary shall take part in the transmission:of its owning VCG output direction.

Information field	Possible value	Meaning
VCG Membership Status (Output Direction)	Values are • Active The tributary is member of the VCG and working • Do Not Use The tributary is member of the VCG but taken off by LCAS • Not Available The trib. is member of the VCG but the current data is not retrievable for any reason • Not Applicable The trib. is no member of the VCG.	Status of the tributary related to its VCG membership in output direction.
Relative Differential Delay (ms)	Values • Number, [0 .. 511.875] ms step = 125 ms • Unavailable The value cannot be retrieved • Not Applicable Defect conditions, or the VCG Trib is not part of the VCG	Shows the relative differential delay of the VCG Tribs in ms. The fastest trib has a delay of 0 ms. The delay of the other tribs is relative to the fastest one.



Retrieving current VCG tributary maintenance signal

When to use Use this procedure to retrieve information on the current VCG tributary maintenance signal.

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

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps in order to view the path trace at a specific tributary:

- 1 In the **System View** of the *LambdaUnite*™ CIT, via **View** → **View Equipment Details...** call up the **View Equipment Details...** window.

Important! If you only want to display the actual value of the path trace at a specific tributary you can also use the menu option **Fault** → **Analysis** → **View Current VCG Tributary Maintenance Signal**.

Result:

On the left side of the window, the **Equipment** selection tab is displayed. The shelves belonging to the system are listed.

- 2 Select the desired shelf. 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 parameters of the selected tributary are displayed.

Reference:

Please refer to [“Parameters of the window “View Current VCG Trib. Maintenance Signal”” \(7-115\)](#) for the description of the parameters.

END OF STEPS



Parameters of the window “View Current VCG Trib. Maintenance Signal”

Description The **View Current VCG Trib. Maintenance Signal** window consists of four tabs, each describing a set of parameters:

- [“VCG Membership” \(7-115\)](#)
- [“Trail Trace Identifier” \(7-116\)](#)
- [“Trail Signal Label” \(7-118\)](#)
- [“Sequence Number” \(7-118\)](#)

VCG Membership The following table shows the status data which is shown in the tab **VCG Membership** of the **View Current VCG Trib. Maintenance Signal** window.

Information field	Possible value	Meaning
Input Direction		
VCG Membership	Enabled Diabled	This parameter shows whether the tributary shall take part in the transmission:of its owning VCG in input direction.
VCG Membership Status	Values are • Active The tributary is member of the VCG and working • Do Not Use The tributary is member of the VCG but taken off by LCAS • Not Available The trib. is member of the VCG but the current data is not retrievable for any reason • Not Applicable The trib. is no member of the VCG.	Status of the tributary related to its VCG membership in input direction.
Output Direction		
VCG Membership	Enabled Diabled	This parameter shows whether the tributary shall take part in the transmission:of its owning VCG output direction.

Information field	Possible value	Meaning
VCG Membership Status	Values are • Active The tributary is member of the VCG and working • Do Not Use The tributary is member of the VCG but taken off by LCAS • Not Available The trib. is member of the VCG but the current data is not retrievable for any reason • Not Applicable The trib. is no member of the VCG.	Status of the tributary related to its VCG membership in output direction.

Trail Trace Identifier The following table shows the status data which is shown in the tab **Trail Trace Identifier** of the **View Current VCG Trib. Maintenance Signal** window.

Information field	Possible value	Meaning
Accepted TTI		
Accepted TTI Status	Enabled Diabied	The AID defined for the selected protection group.
Accepted TTI (J1) Read Format	Values are • Specific Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Accepted TTI (J1) Value		This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. The textbox is not editable.

Information field	Possible value	Meaning
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· - In ASCII mode, if a series of two hexadecimal digits cannot be con-verted to ASCII characters, then the <i>WaveStar</i>® CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). - In Hex mode, the <i>WaveStar</i> CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal dig-its, and so on until the full API is displayed.
Expected TTI		
Expected TTI (J1) Format	Values are Specific Byte A single byte (hexadecimal format using the printable T.50/ ASCII character set) (SONET). A single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). Specific String A 16-byte hexadecimal format using the printable T.50/ ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). 64 Byte String A 64-byte hexadecimal format using the printable T.50/ ASCII character set, with the last two bytes being a carriage return, line feed (SONET).	The format of the trail trace is specified in this parameter.
Expected TTI (J1) Value		This parameter shows the value of the trace. The value is dependent on the trace format and represents the information transferred in the trace. The textbox is not editable.
Display Mode	ASCII Hex	The display mode of a textbox is selectable via a radio button to the values hex or ASCII (default). The following behavior is expected:· - In ASCII mode, if a series of two hexadecimal digits cannot be con-verted to ASCII characters, then the <i>WaveStar</i> CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]). - In Hex mode, the <i>WaveStar</i> CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal dig-its, and so on until the full API is displayed.

Information field	Possible value	Meaning
HP TIM Monitor	Enable Disable	Trace Identifier Mismatch (TIM) monitor enable

Trail Signal Label The following table shows the status data which is shown in the tab **Trail Signal Label** of the **View Current VCG Trib. Maintenance Signal** window.

Information field	Possible value	Meaning
Trail Status	Normal AIS Not Available	This field shows the accepted trail status.
Accepted Signal Label (C2)	Two hexadecimal digits: 0x00 "Unequipped" 0x01 "Equipped" 0x02 "TUG Structure" 0x03 "Locked TU" 0x04 "34 Mbit/s or 45 Mbit/s, asynchronous" 0x12 "140 Mbit/s, asynchronous" 0x13 "ATM" 0x14 "MAN-DQDB" 0x15 "FDDI" 0x1B "GFP Mapping" 0x1F "Ethernet Frame" - other	This field shows the accepted trail signal label (C2). If the Trail Status is not equal to "Normal", this field is grayed out and empty.
TSL Mismatch Monitor	Enabled Diabled	This field shows the status of the monitoring of the Trail Signal Label Mismatch defect.

Sequence Number The following table shows the status data which is shown in the tab **Sequence Number** of the **View Current VCG Trib. Maintenance Signal** window.

Information field	Possible value	Meaning
Transmitted Sequence Number	0 .. 20] (step = 1) Not Applicable Unavailable	This parameter shows the value of the Transmitted Sequence Number of the tributary within the VC Group.
Accepted Sequence Number	0 .. 255] (step = 1) Not Applicable Unavailable	This parameter shows the value of the Accepted Sequence Number of the tributary within the VC Group.





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	8-3
Supporting information on the “Switching an MSP or APS”	8-5
Switching a 2-fiber MS-SPRing or 2-fiber BLSR	8-7
Supporting information on the “Switching a 2-fiber MS-SPRing or 2-fiber BLSR”	8-9
Switching a 4-fiber MS-SPRing or 4-fiber BLSR	8-11
Supporting information on the “Switching a 4-fiber MS-SPRing or 4-fiber BLSR”	8-13
Switching a DNI, UPSR or SNCP	8-15
Switching a path protection	8-17
Clearing a protection switch request	8-19
Retrieve protection switch reports	8-21
Supporting information on the “BLSR Protection Switch List”	8-22

Supporting information on the “NE Protection Switch Activity Log”	8-23
Retrieving current optical tributary maintenance signal	8-24
Supporting information on the “View Current Optical Trib. Maintenance Signal”	8-26
Performing facility loopbacks	8-27
Releasing a facility loopback	8-30



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” \(18-13\)](#)
- [“Line Protection” \(18-19\)](#)

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 switch a 1+1 MSP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* 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 or lockout of protection 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



Supporting information on the “Switching an MSP or APS”

Information fields The following are the parameters displayed for a selected MSP or APS (the designations refer to the corresponding *WaveStar*® CIT windows).

Parameter	Description
Protection Group AID	the AID (access identifier) for the selected protection group.
Protection Type	the type of protection group. Possible values: • 1 +1 Port Protection
Active Port	indicates the port carrying traffic. Possible values: • Side 1 • Side 2 Additionally the corresponding port AID is displayed.
Protocol	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.
Optical Line Rate	SDH: STM1, STM4, STM16, STM64, STM256 SONET: OC3, OC12, OC48, OC192, OC768
Working AID	The port AID which has been assigned to be the working port. cf.: “Overview of access identifiers” (15-9)
Protection AID	The port AID which has been assigned to be the protection port. cf. “Overview of access identifiers” (15-9)

Configuration options The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist:

Option	Meaning
Switch Type	Enables the user to select a switch type. The following options are possible: • Clear • Lockout of Protection • Forced to Working • Forced to Protection • Manual to Working • Manual to Protection



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” (18-13) • “Ring Protection” (18-21)
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 side to which the switch shall be applied in the field Direction.

The following options are possible:

- **East**
- **West**

When applying a protection switch, the parameter **Direction** (**EAST** or **WEST**) states the side to which the switch is applied to, the traffic will then be routed to the other side.

-
- 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



Supporting information on the “Switching a 2-fiber MS-SPRing or 2-fiber BLSR”

Information fields The following are the parameters displayed for a selected 2 Fiber MS-SPRing or 2 Fiber BLSR (the designations refer to the corresponding *WaveStar*® CIT windows).

Parameter	Description
Protection Group AID	the AID (access identifier) for the selected protection group.
Protection Type	the type of protection group. Possible values: • 2 Fiber MS-SPRing • 2Fiber BLSR
Ring ID	Ring ID of the BLSR/MS-SPRING protection group.
Optical Line Rate	the optical line rate values, depending on the rate associated with this ports. Possible values: • OC48 • OC192 • OC768 • STM16 • STM64 • STM256
East Port AID	the east port AID provisioned for the protection scheme.
West Port AID	the west port AID provisioned for the protection scheme.

Configuration options The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist:

Option	Meaning
Direction	the desired direction. Possible values are: • East • West. When applying a protection switch, the parameter Direction (EAST or WEST) states the side to which the switch is applied to, the traffic will then be routed to the other side.
Switch Type	Enables the user to select a switch type. The following options are possible: • Clear • Lockout of Protection, Span • Forced to Protection, Ring • Manual to Protection, Ring



Switching a 4-fiber MS-SPRing or 4-fiber BLSR

When to use	Use this procedure to switch from one section to the other in a 4-fiber MS-SPRing or from one line to the other in a 4-fiber BLSR.
Related information	For related information, see: • “Protection mechanisms” (18-13) • “Ring Protection” (18-21)
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 4-fiber MS-SPRing. Required equipment The following equipment is required to perform this task: • WaveStar® CIT
Instructions	Complete the following steps to switch a 4-fiber MS-SPRing or 4-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 (refer to “Supporting information on the “Switching a 4-fiber MS-SPRing or 4-fiber BLSR”” (8-13)).

-
- 3 Select the side to which the switch shall be applied in the field **Direction**.

The following options are possible:

- **East**
- **West**
- **Both (LP-S only)** (not applicable for *LambdaUnite*[™] MSS NEs)

When applying a protection switch, the parameter **Direction** (**EAST** or **WEST**) states the side to which the switch is applied to. In case of span-switches the traffic will be routed to the protection span of the chosen side. In case of ring-switches the traffic will be routed to the protection span of the opposite side.

-
- 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**
- **Forced to Protection, Span**
- **Manual to Protection, Ring**
- **Manual to Protection, Span**

-
- 5 Click on **Apply**.

END OF STEPS



Supporting information on the “Switching a 4-fiber MS-SPRing or 4-fiber BLSR”

Information fields The following are the parameters displayed for a selected 4 Fiber MS-SPRing or 4 Fiber BLSR (the designations refer to the corresponding *WaveStar*® CIT windows).

Parameter	Description
Protection Group AID	the AID (access identifier) for the selected protection group.
Protection Type	the type of protection group. Possible values: • 4 Fiber MS-SPRing • 4Fiber BLSR
Ring ID	Ring ID of the BLSR/MS-SPRING protection group.
Optical Line Rate	the optical line rate values, depending on the rate associated with this ports. Possible values: • OC48 • OC192 • OC768 • STM16 • STM64 • STM256:
West Working Port AID	the west working port AID provisioned for the protection scheme.
West Protection Port AID	the west protection port AID provisioned for the protection scheme.
East Working Port AID	the east working port AID provisioned for the protection scheme.
East Protection Port AID	the east protection port AID provisioned for the protection scheme.

Configuration options The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist:

Option	Meaning
Direction	the desired direction. Possible values are: East or West. When applying a protection switch, the parameter Direction (EAST or WEST) states the side to which the switch is applied to. In case of span-switches the traffic will be routed to the protection span of the chosen side. In case of ring-switches the traffic will be routed to the protection span of the opposite side.
Switch Type	Enables the user to select a switch type. The following options are possible: • Clear • Lockout of Protection, Span • Forced to Protection, Ring • Forced to Protection, Span • Manual to Protection, Ring • Manual to Protection, Span



Switching a DNI, UPSR or SNCP

When to use Use this procedure to switch from one path to the other in a DNI, UPSR or SNCP.

Related information For related information, see:

- [“Path Protection” \(18-14\)](#)

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 M4, Maintenance, to switch a DNI, UPSR or SNCP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* 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 DNI, 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



Switching a path protection

When to use Use this procedure to switch from one path to the other in a one way path protection.

Related information For related information, see:

- [“Path Protection” \(18-14\)](#)

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 M4, Maintenance, to switch a one way path protection.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to switch a one way path protection:

- 1 Call up the **Protection Switch** window either in the **System View** via **Fault → Protection Switch** .
 - 2 Select the desired **Path Protection** in the tab **Ptn Grp** on the left side of the window.
-

Result:

The window **Switch Protection** 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” \(18-13\)](#)
- [“Path Protection” \(18-14\)](#)
- [“Parameters of the window “View Cross Connections”” \(7-6\)](#)
- [“Ring Protection” \(18-21\)](#)
- [“Switching an MSP or APS” \(8-3\)](#)
- [“Switching a 2-fiber MS-SPRing or 2-fiber BLSR” \(8-7\)](#)
- [“Switching a 4-fiber MS-SPRing or 4-fiber BLSR” \(8-11\)](#)
- [“Switching a DNI, UPSR or SNCP” \(8-15\)](#)

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” \(18-13\)](#)
- [“Ring Protection” \(18-21\)](#)
- [“Switching an MSP or APS” \(8-3\)](#)
- [“Switching a 2-fiber MS-SPRing or 2-fiber BLSR” \(8-7\)](#)
- [“Switching a DNI, UPSR or SNCP” \(8-15\)](#)

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.



Retrieving current optical tributary maintenance signal

When to use Use this procedure to retrieve information on the current optical tributary maintenance signal.

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

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps in order to view the path trace at a specific tributary:

- 1 Call up the window for viewing the desired tributary in the **Shelf View**, clicking with the right mouse button on a specific port of a specific circuit pack and then selecting the option **View Tributary Details** in the pop-up menu.

Continue with step [Step 7](#)

- 2 In the **System View** of the *LambdaUnite*™ CIT, via **View → View Equipment Details...** call up the **View Equipment Details...** window.

Important! If you only want to display the actual value of the path trace at a specific tributary you can also use the menu option **Fault → Analysis → View Current Optical Trib. Maintenance Signal**.

Result:

On the left side of the window, the **Equipment** selection tab is displayed. The shelves belonging to the system are listed.

- 3 Select the desired shelf. 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.

-
- 4 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.

-
- 5 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.

-
- 6 Select the desired tributary (type).

Result:

On the right side of the window, the parameters of the selected tributary are displayed.

-
- 7 Select the **Trace Settings** tab.

Reference:

Please refer to [“Supporting information on the “View Current Optical Trib. Maintenance Signal”” \(8-26\)](#) for the description of the parameters.

END OF STEPS



Supporting information on the “View Current Optical Trib. Maintenance Signal”

Purpose This window is used to display the current optical maintenance signal for a selected tributary.

Displayed data The following values are displayed:

Value	Description
Tributary AID	The AID of the tributary.
Path Trace (J1 byte)	the value of the path trace identifier on the incoming path overhead J1 byte of a non-terminated tributary.
Signal Label (C2 byte)	Overhead C2 byte of a non-terminated STS-1 tributary.



Performing facility loopbacks

When to use Use this procedure to operate near-side or far-side facility loopbacks.

Related information For related information, see:

- [“Facility loopback” \(18-49\)](#)

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 task.

Required privilege

You must have at least privilege codes of **S1 and P1 and M3** to perform facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions **Important!** If you want to switch a facility loopback on a port involved in a Line/MS protection scheme (Line protection, MSP), it is highly recommended to put the corresponding protection group in the lockout or forced switch state before switching the facility loopback to avoid an unintended protection switch or failure of protocol (FOP) events.

Proceed as follows to operate a near-side or far-side facility loopback:

- 1 Make sure that the port on which you want to operate a facility loopback is ***not assigned/locked as timing reference***, and that ***no DCC is enabled*** for that port.

-
- 2 By using the *WaveStar* CIT, set the port into the out-of-service state proceeding according to one of the following options:
- Option 1
 - Select **Configuration** → **Provision...** from the **System View** main menu,
 - choose the port on which you want to operate a facility loopback from the equipment selection window, and
 - click **Provision**.
 - In the **Provision Parameters for Protection Group or Equipment** window, set the **Service Condition** to **Out Of Service**.
 - Option 2
 - In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.
 - In the pop-up menu that opens, select the **Provision Port #** menu item (“#” represents the port number).
 - In the **Provision Port** window, set the **Service Condition** to **Out Of Service**.
-
- 3 Proceed according to one of the following options to invoke the **Facility Loopback** window from the *WaveStar* CIT:
- Option 1
 - Select **Fault** → **Analysis** → **Facility Loopback...** from the **System View** main menu,
 - choose the port on which you want to operate a facility loopback from the equipment selection window that will be opened, and
 - click **Select**.
 - Option 2
 - In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.
 - In the pop-up menu that opens, select the **Facility Loopback** menu item.

-
- 4 By means of the read-only fields in the upper region of the window (**Port AID**, **Port Type/Rate**, **Facility Loopback Status**), verify that you selected the desired port, and that no loopback is currently active.
-

- 5 Select the type of facility loopback to be operated by means of the **Facility Loopback Type** checkboxes:

- **Nearside Facility** or
 - **Farside Facility**.
-

- 6 Click the button in the lower left-hand-side corner of the window which may be labelled either **Operate** or **Force**.

The button will be labelled **Operate** if the corresponding port is an optical port, is protected and *not* active, and if the switch request state is “Lockout of protection”. Otherwise it will be labelled **Force**.

Important! Operating a facility loopback may be service affecting!

- 7 If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window that will be opened.

END OF STEPS



Releasing a facility loopback

When to use Use this procedure to dismantle (release) a facility loopback.

Related information For related information, see:

- [“Facility loopback” \(18-49\)](#)

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 task.

Required privilege

You must have at least privilege codes of **S1 and P1 and M3** to perform or release facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- WaveStar® CIT

Instructions Proceed as follows to dismantle a facility loopback:

- 1 Proceed according to one of the following options to invoke the **Facility Loopback** window from the WaveStar CIT:
 - Option 1
 - Select **Fault** → **Analysis** → **Facility Loopback...** from the **System View** main menu,
 - choose the port on which you want to dismantle a facility loopback from the equipment selection window that will be opened, and
 - click **Select**.
 - Option 2
 - In the shelf display, right-click on the alarm LED of the port on which you want to dismantle a facility loopback.
 - In the pop-up menu that opens, select the **Facility Loopback** menu item.

Result:

The **Facility Loopback** window will be opened. The read-only fields in the upper region of the window (**Port AID**, **Port Type/Rate**, **Facility Loopback Status**) indicate the selected port and whether a facility loopback is currently active. In the **Facility Loopback Type** field, the type of facility loopback currently being active is shown.

-
- 2 Click the **Release** button if you want to dismantle the indicated type of facility loopback on the respective port.

END OF STEPS





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	9-5
Retrieving performance monitoring reports	9-11



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.
 - To enable or disable Ethernet performance monitoring, you need to select a LAN port (Ethernet port) or a WAN port (VCG port).
- 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 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.

-
- 2 In the **Equipment Selection** window, open the required bay and shelf details, then select the required port or tributary.
-

- 3 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.

- 4 Proceed as follows, depending on your selection in [Step 2](#):

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 near-end and/or far-end path performance monitoring data collection by selecting Enable or Disable respectively for Near End Path PM Activation and/or Far End Path PM Activation .

IF	THEN
you selected an Ethernet port (for example Port 2 (1GE)) or VCG port (for example VCG v1)	Proceed as follows: 1. Make sure that the Port Mode is set to Monitored. 2. Enable or disable Ethernet performance monitoring data collection by selecting Enable or Disable respectively for Ethernet PM Activation and/or VCG PM Activation. 3. Proceed with Step 6.

- 5 Depending on your selection in [Step 2](#), you may now change the respective values of the SES declaration threshold (cf. [“SES declaration threshold” \(19-10\)](#)) by means of the corresponding spin box:

- SDH port
 - **Multiplex Section Near End SES Threshold**
 - **Multiplex Section Far End SES Threshold**
 - **Regenerator Section Near End SES Threshold**
- SONET port
 - **Line Section Near End SES Threshold**
 - **Line Section Far End SES Threshold**
 - **Section Near End SES Threshold**
- SDH or SONET tributary
 - **Higher-order Path Far-end SES Threshold**
 - **Higher-order Path Near-end SES Threshold**

The value of the SES declaration threshold is preset to a meaningful default value. Increasing this value means that a lower signal quality is acceptable before a second is declared severely errored. Decreasing the value means that great demands are made on the signal quality.

- 6 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.
 - To retrieve Ethernet performance monitoring settings, you need to select a LAN port (Ethernet port) or a WAN port (VCG port).
- 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
Port AID	Indicates the AID of the selected port.
Port Rate	Indicates the transport capacity of the selected port.
Regenerator Section PM Activation	Indicates whether Regenerator Section performance monitoring is enabled or not.
Regenerator Section SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for Regenerator Section performance monitoring.
Near End Multiplex Section PM Activation	Indicates whether near-end Multiplex Section performance monitoring is enabled or not.
Near End Multiplex Section SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end Multiplex Section performance monitoring.
Far End Multiplex Section PM Activation	Indicates whether far-end Multiplex Section performance monitoring is enabled or not.

Far End Multiplex Section SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for far-end Multiplex Section performance monitoring.

If a SONET port has been selected, the following parameters can be viewed:

Parameter	Meaning
Port AID	Indicates the AID of the selected port.
Port Rate	Indicates the transport capacity of the selected port.
Section PM Activation	Indicates whether Section performance monitoring is enabled or not.
Section SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for Section performance monitoring.
Near End Line PM Activation	Indicates whether near-end Line performance monitoring is enabled or not.
Near End Line SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for near-end Line performance monitoring.
Far End Line PM Activation	Indicates whether far-end Line performance monitoring is enabled or not.
Far End Line SES Threshold	Indicates the threshold set for the detection of Severely Errored Seconds (SES) for far-end Line performance monitoring.

If an SDH or SONET tributary has been selected, the following parameters can be viewed:

Parameter	Meaning
Tributary AID	Indicates the AID of the selected tributary.

Port Rate	Indicates the transport capacity of the corresponding port.
Near End Path PM Activation	Indicates whether near-end path performance monitoring is enabled or not.
Far End Path PM Activation	Indicates whether far-end 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.

If a LAN port or WAN port has been selected, the following parameters can be viewed:

LAN port (Ethernet port):

Parameter	Meaning
Port AID	Indicates the AID of the selected LAN port.
Port Rate	Indicates the transport capacity of the selected LAN port (for example: “1 GE”).
Port Monitoring Mode	Indicates the current setting of the port monitoring mode (Auto , Monitored or Not Monitored) of the selected LAN port.
Ethernet PM Enable	Indicates whether Ethernet performance monitoring is enabled or not for the selected LAN port.

WAN port (VCG port):

Parameter	Meaning

VCG AID	Indicates the AID of the selected WAN port.
VCG Monitoring Mode	Indicates the current setting of the VCG monitoring mode (Monitored or Not Monitored) for the selected WAN port.
VCG PM Enable	Indicates whether Ethernet performance monitoring is enabled or not for the selected WAN port.

If a VCG tributary has been selected, the following parameters can be viewed:

Parameter	Meaning
Tributary AID	Indicates the AID of the selected VCG tributary.
VCG Monitoring Mode	Indicates the current setting of the VCG monitoring mode (Monitored or Not Monitored) for the selected VCG port.
Tributary Monitoring Mode	Indicates the current setting of the tributary monitoring mode (Monitored or Not Monitored) for the selected VCG tributary.
Near End Path PM Activation	Indicates whether near-end path performance monitoring is enabled or not.
Far End Path PM Activation	Indicates whether far-end path performance monitoring is enabled or not.
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.
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.

4 Click **Close** to exit.

E N D O F S T E P S



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
- Ethernet

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**

7. **Performance** → **Reports** → **Ethernet**

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” \(19-14\)](#).

- 5 Click **Apply**.

Result:

The corresponding ... **PM Report** window opens.

- 6 View the report, then perform one of the following:

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 .

IF	THEN
you want to refresh the screen display,	Click Refresh .
you 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 109088708). 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).
2. Acquire the CD-ROM that contains the new generic/version of the NE software (ComCode 109088708).
3. Connect the *WaveStar* CIT to the local area network (LAN) of the subject 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:

- Empty 256 Mb *CompactFlash* card (as delivered from manufacturer)
- CD-ROM that contains the new generic/version of the NE software
- *WaveStar* CIT PC with *CompactFlash* or PCMCIA slot. For the second case an adapter is required.

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 (or PCMCIA slot with adapter) 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 *WaveStar* CIT.
.....
- 16** In the *WaveStar* CIT Main Window, choose the option **Administration** → **Prepare PCMCIA Disks...**

Result:

The **Prepare PCMCIA Disk** window appears.

-
- 17** In the left list, under **Available Generics**, click the version of network element software you are installing.
-

- 18** In the right list, click on the drive letter that represents the *CompactFlash* card.
-

- 19** Click on **Copy Generic**.

Result:

The file copy function starts and you see a **Copying files...** message.

-
- 20** The “Coying files...” message will disappear when the file transfer is complete. Click the **Close** button to exit the **Prepare PCMCIA Disk** window.
-

- 21** If the *CompactFlash* card driver software you are using requires you to stop the *CompactFlash* card before ejecting it, stop the card now. If the software you are using does not allow for this procedure, make sure that the used slot is not being accessed (the LED is not blinking) before continuing.
-

- 22** Eject the *CompactFlash* card from the *CompactFlash* slot (or PCMCIA slot with adapter) of the *WaveStar* CIT PC.
-

- 23** 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:

- [“Software download for upgrade purposes” \(20-4\)](#)
- [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).
2. Acquire the CD-ROM that contains the new generic/version of the NE software.
3. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE.
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 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 According on how the NE is connected to the WaveStar CIT select the responding option in the **Download From/Via** drop down list box

IF	THEN
the WaveStar CIT is connected to the NE via DCC or OSI LAN	1. in the Download From/Via drop down list box select CIT. A file selection screen appears showing that the software will downloaded from C:\Program Files\Lucent Technologies\Wavestar CIT\generics. The directory of the file selection screen is automatically pre-populated. 2. 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.
the WaveStar CIT is connected to the NE viaTCP/IP	1. in the Download From/Via drop down list box select FTTD. 2. Enter the required parameters as described in “Remote download of software generics via FTTD” (20-5). Specify the Source directory path.
the download of the software generic shall be performed using FTAM,	1. in the Download From/Via drop down list box select FTAM. 2. Enter the required parameters as described in “Remote download of software generics using FTAM” (20-7). Specify the Source directory path.

- 17 Click the **Download** push-button.

Result:

A warning screen appears.

-
- 18** Read the text in the warning screen and if you are sure, confirm with **OK**.

Result:

A second warning screen appears.

-
- 19** 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 less than 60 minutes (remotely via the LAN/DCC network) or approx. 10 minutes (via direct LAN).

-
- 20** 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

Important! On the *CompactFlash*[™] card, there is room for two databases, the current and the previous one. If a *CompactFlash* card never contained a second database, the content of the previous partition is reported wrongly: The allocated size parameter for the previous database is missing (“size=0”) and a serial number for that non-existing database is reported.

The following information is displayed in the window for each file selected by the user:

Object	Description/Behavior
Current generic	the software release which is currently active for the <i>WaveStar</i> CIT or network element.
NVM	Selected file. If resident on the NE, the file description indicates whether the file is • Current, • Previous, or • Secondary 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.

Object	Description/Behavior
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. Possible values are integers from 0...999,999,999, inclusive.
Source	Source of the original download. Examples at this time include CIT, EMS and FTDD along with a file path and file name. If the source system is either CIT, EMS or FTDD 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” (14-19) and “NSAP address format” (14-24)).
State	State of this software release. It may take the values: • Corrupt • Downloaded • In Progress • Failed • Previous • Running • Initial.
Free NVM Space	n/a (not applicable)
Unavailable NVM Space	n/a (not applicable)

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 WaveStar[®] CIT	11-3
Retrieving NE database information	11-6
Supporting information for NSAPRetrieving NE database information	11-7
Restoring a database to a network element	11-9



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	<table><tr><th>IF</th><th>THEN</th></tr><tr><td>you want to backup the database via FTAM,</td><td>in the Backup To/Via drop down list box select FTAM. Reference: Continue with step Step 3.</td></tr><tr><td>the connection to the NE is through a TCP/IP Gateway,</td><td>in the Backup To/Via drop down list box select FTTD. Reference: Continue with step Step 4.</td></tr><tr><td>you want to backup the database directly to the CIT,</td><td>in the Backup To/Via drop down list box select CIT. Result: A file selection screen appears showing that the database will back up to a specified folder under C:\Program Files\Lucent Technologies\Wavestar CIT\.... The directory of the file selection screen is automatically pre-populated. Reference: Continue with step Step 7.</td></tr></table>	IF	THEN	you want to backup the database via FTAM,	in the Backup To/Via drop down list box select FTAM . Reference: Continue with step Step 3 .	the connection to the NE is through a TCP/IP Gateway,	in the Backup To/Via drop down list box select FTTD . Reference: Continue with step Step 4 .	you want to backup the database directly to the CIT,	in the Backup To/Via drop down list box select CIT . Result: A file selection screen appears showing that the database will back up to a specified folder under C:\Program Files\Lucent Technologies\Wavestar CIT\.... The directory of the file selection screen is automatically pre-populated. Reference: Continue with step Step 7 .
IF	THEN								
you want to backup the database via FTAM,	in the Backup To/Via drop down list box select FTAM . Reference: Continue with step Step 3 .								
the connection to the NE is through a TCP/IP Gateway,	in the Backup To/Via drop down list box select FTTD . Reference: Continue with step Step 4 .								
you want to backup the database directly to the CIT,	in the Backup To/Via drop down list box select CIT . Result: A file selection screen appears showing that the database will back up to a specified folder under C:\Program Files\Lucent Technologies\Wavestar CIT\.... The directory of the file selection screen is automatically pre-populated. Reference: Continue with step Step 7 .								

- 3 In the **FTAM** tab specify the TID, PSEL, SSEL, TSEL and NSAP for the FTAM information (refer to [“Backup database using FTAM” \(21-5\)](#)).

Reference:

Continue with step [Step 6](#).

- 4 In the **FTTD** tab specify the TID, PSEL, SSEL, TSEL and NSAP for the FTTD information (refer to [“Backup database via FTTD” \(21-3\)](#)).
-

- 5 In the **FTP** tab specify the Server, IP or Name, Port (optional), User Name (optional) and User Password (optional) for FTP information (refer to [“Backup database via FTTD” \(21-3\)](#)).
-

-
- 6** Specify the **Destination directory path**.
-

- 7** Record the path/destination of the backup folder/files and click on **Backup**.

Result:

The NE Data Backup in Progress Screen appears.

- 8** When the NE Data Backup in Progress screen disappears and the backup is complete, select **View → NE Data...**

Result:

The File Selection Screen appears.

- 9** Select CIT in the Look in: field and double click on C:, Program Files, Lucent Technologies, WaveStar CIT, and Backups. Then click on the backup folder number and on OK.

Result:

The Database Info Screen appears.

- 10** 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 NSAPRetrieving NE database information” \(11-7\)](#).

END OF STEPS



Supporting information for NSAPRetrieving 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	the software release which is currently active for the craft interface terminal (CIT) or network element.
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. Possible values: integers ranging from 0 to 999,999,999 inclusive.
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 Location	Destination of the most recent backup. Examples at this time include FTTD, 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, <i>WaveStar</i> ® CIT and FTTD plus a file name/path. If there has been no restoral, this field is blank.



Restoring a database to a network element

Purpose Use this procedure to restore a previously saved database to a network element.

Before you begin Before you begin this task:

- Obtain the work instructions for this task and note the database to be restored and the location of the most recent backup files.
- Verify that a *WaveStar*® CIT is connected and logged in to the *LambdaUnite*™ MSS network element (NE) where the database is to be restored.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

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.



CAUTION

Possible material damage due to electrostatic discharge

Handling circuit packs or working on a LambdaUnite MSS system can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a LambdaUnite MSS system.

Important! If provisioning changes were made after the last backup files were created, use the appropriate *WaveStar* CIT commands to manually apply the recent provisioning changes to the just-restored database.

Instructions Complete the following steps to manually restore a database to a network element:

- 1 From the **System View** main menu, enter the maintenance condition via **Fault → Enter/Exit Maintenance Condition... → Enter Maintenance Condition...**

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

- 3 Select **Configuration → Software → Remote Restore...** from the **System View** main menu.

Result:

The **Restore Database** window will be opened.

- 4 Proceed as follows:

IF	THEN
you want to restore the database directly from the PC where the <i>WaveStar</i> CIT is installed,	select CIT in the Restore From/Via drop down list box. Result: A file selection screen appears showing that the database will back up to a specified folder under <i>C:\Program Files\Lucent Technologies\Wavestar CIT\...</i>. The directory of the file selection screen is automatically pre-populated. Reference: Proceed with Step 5.
the connection to the NE is through a TCP/IP gateway,	select FTTD in the Restore From/Via drop down list box. Reference: Proceed with Step 6.

- 5 Select “CIT” in the **Look in** field and double click successively on *C:*, *Program Files*, *Lucent Technologies*, *Wavestar CIT*, and *backups*. Proceed [Step 8](#).

-
- 6 Select the **FTTD** tab and specify the **TID**, presentation selector (**Psel**), session selector (**Ssel**), transport selector (**Tsel**) and the **NSAP Address** for the FTTD information.
-

- 7 Select the **FTP** tab and specify the **Server** (IP address or server name), port information (optional), User name (optional) and password (optional) for the FTP information.

Proceed with [Step 8](#).

Important! Be careful to select the correct backup files to restore to the NE.

- 8 Specify the path to the folder where the backup files reside.

Important! The NE does not restore a backup file properly if the release number of the backup file is not the same as the release number of the running SW.

Restoring a backup file with a different release number

To restore a backup file with a different release number as the running software you have to perform the following:

- open the file named db (in the *WaveStar* CIT) or db.dci (in the *Navis*® Optical EMS) in the directory where the backedup information (list of files) are stored, using a text editor
 - in this file change the release number of the backup file to the release number of the running SW,
-

- 9 Verify your settings and correct if necessary. Then click **Restore**.
-

- 10 Confirm the resulting system message by clicking **YES**.

Result:

The **NE Data Restore in Progress** window appears. When the database restore is complete, the system will perform a 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.

.....

11 Connect to the NE again.

.....

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

.....

13 Confirm the resulting system message by clicking **OK**.

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

.....





12 Periodic activities

Overview

Purpose This section describes periodic activities for maintaining the system.

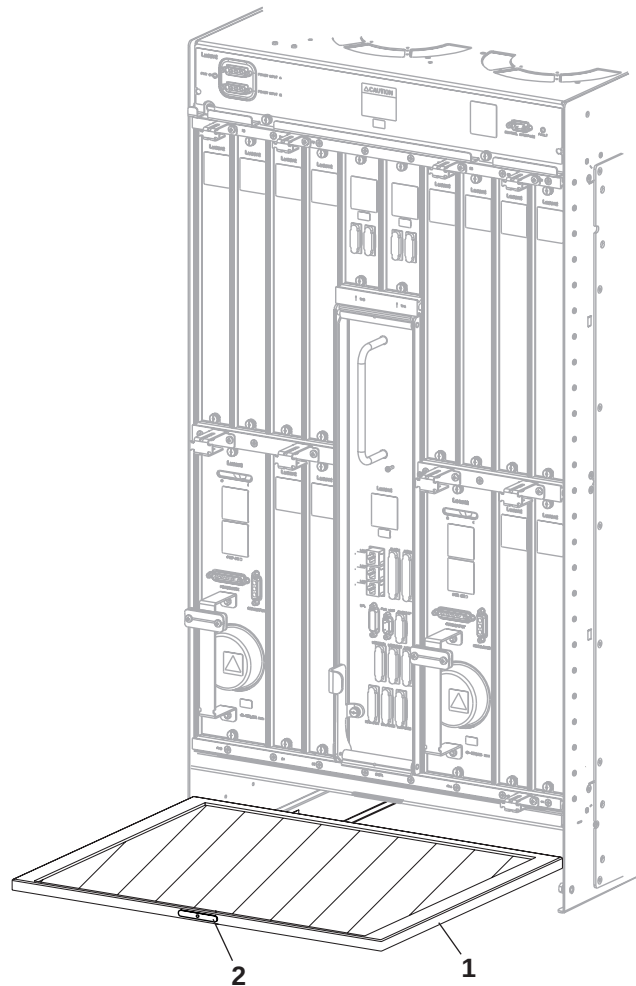


Replacing the air filter

When to use Use this procedure:

- Every 3 months, as a part of routine fan maintenance.
- When construction work is done near the equipment in service the filters should be inspected during and short after the construction work on a weekly interval.
- 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

<u>Security management</u>	<u>13-2</u>
<u>Security management concept</u>	<u>13-3</u>
<u>User administration</u>	<u>13-4</u>
<u>User administration concept</u>	<u>13-5</u>
<u>User login and password</u>	<u>13-7</u>
<u>User provisioning</u>	<u>13-10</u>
<u>History logs</u>	<u>13-19</u>
<u>NE alarm log</u>	<u>13-20</u>
<u>NE protection switch activity log</u>	<u>13-21</u>



Security management

Overview

Purpose This section describes the security management concept.

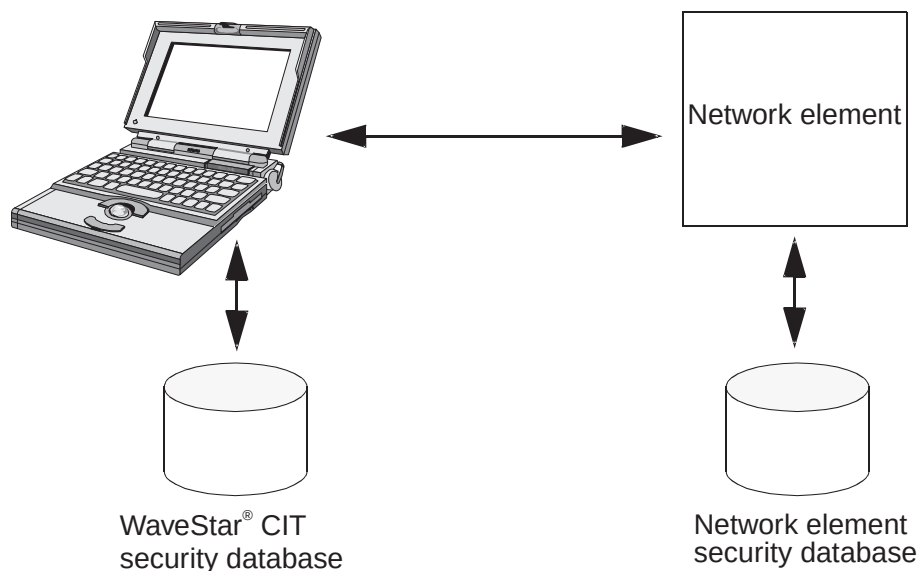


Security management concept

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.

□

User administration

Overview

Purpose 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.

Contents

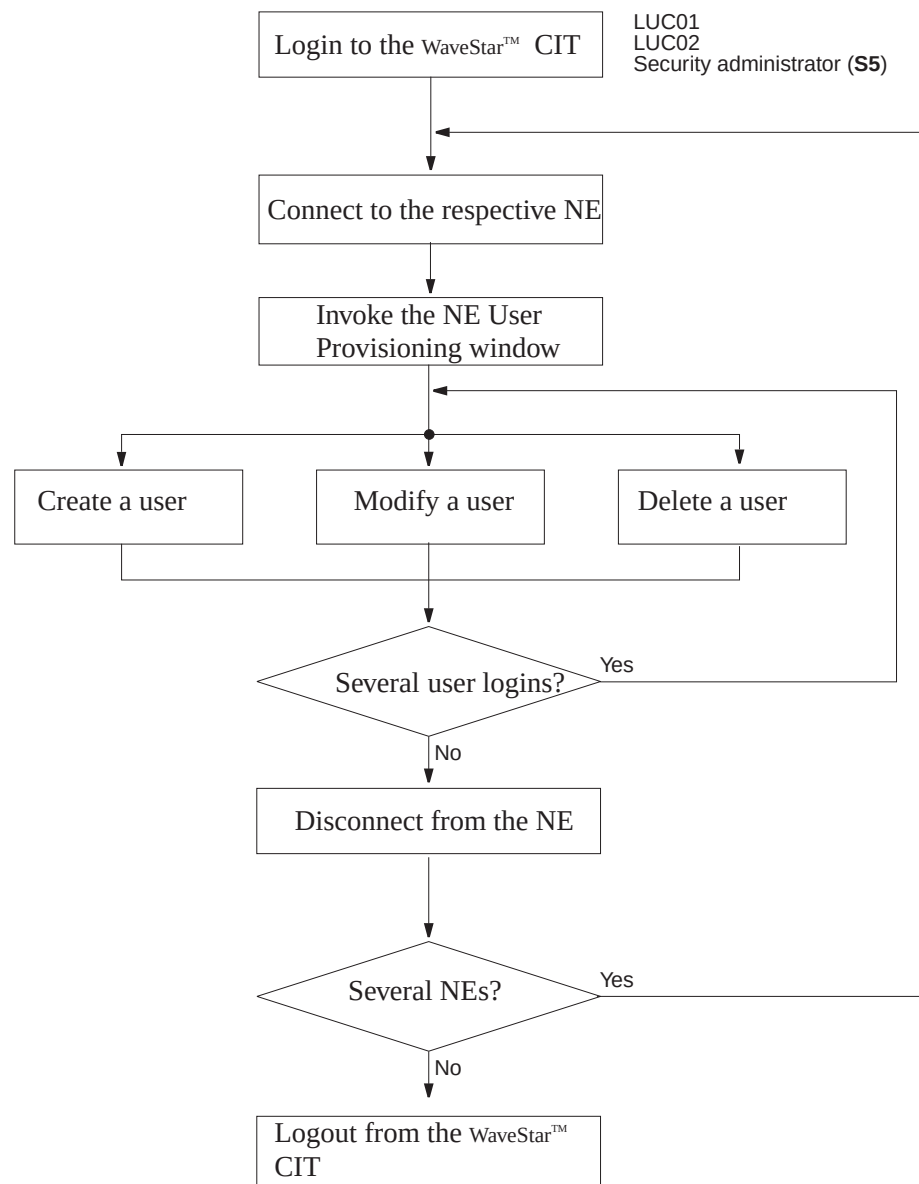
User administration concept	13-5
User login and password	13-7
User provisioning	13-10



User administration concept

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 <i>WaveStar</i> [®] 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” \(2-6\)](#)).



User login and password

Overview 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.

Super user logins and passwords

Two super user logins are preinstalled: “LUC01” and “LUC02”. Please note that the super user logins can be renamed.

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” \(13-10\)](#)).

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.

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
 - } right curly brace
 - | vertical bar
 - } right cruelly brace
 - < less than
 - > greater than
 - ~ tilde

The following characters are ***not allowed*** in a password:

- space

Spaces are ignored, so they are not stored with the password, they are not evaluated for password validity and they do not count for the password length.

- @ commercial add
- , 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 provisioning

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.

Please note that the predefined users are a definition for *WaveStar*[®] CIT. If one of the predefined user types is created, then on the NE a user is created with the privileges as defined for this user type. The NE has no knowledge about the predefined users.

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

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” \(13-7\)](#)) no other user can have an authorization level of '5' for all functional categories.

The following table describes which user privilege codes are required for the tasks defined in this manual:

User task	User Privilege Codes				
	M	P	PM	S	T
Activating or deactivating Miscellaneous Discrete Outputs manually	M3				
Activating an NE software generic				S4	
Administering the address list at the WaveStar CIT				S3	
Assigning TARP manual adjacencies				S4	
Bridging a cross-connection	M1	P3			
Changing super user IDs				S5	
Changing the NE name (TID)	M4	P1		S4	
Changing the user password on the NE				S1	
Clearing a protection switch request	M4				
Configuring a NE as T-TD Gateway				S4	
Configuring a slot	M1	P3			
Configuring a tributary	M1	P3			
Configuring a VCG port	M1	P3			
Configuring an Ethernet port	M1	P3			
Configuring an NE as FTAM-FTP Gateway				S4	
Configuring an optical SDH/SONET port	M1	P3			
Configuring data communication channels				S4	
Viewing data communication channels				S1	
Configuring fault management parameters for a SONET port		P3			
Configuring fault management parameters for an SDH port		P3			
Configuring Miscellaneous Discrete Inputs	M3				
Configuring Miscellaneous Discrete Outputs	M4				

User task	User Privilege Codes				
	M	P	PM	S	T
Configuring the basic DCN parameters for an NE				S4	
Configuring the basic DCN parameters for the WaveStar CIT				S3	
Configuring the external timing input ports (SDH mode)		P3			
Configuring the external timing input ports (SONET mode)		P3			
Configuring the external timing output ports (SDH mode)		P3			
Configuring the external timing output ports (SONET mode)		P3			
Configuring the external timing references		P3			
Configuring the LDB timers for the WaveStar CIT				S3	
Configuring the line timing references		P3			
Configuring the shelf	M1	P3			
Configuring the system	M1	P3			
Configuring the system timing		P3			
Configuring the TARP parameters for an NE				S4	
Configuring VCG tributaries	M1	P3			
Creating a bidirectional DNI/DRI between one MS-SPRing/BLSR protected ring and one SNCP/UPSR protected ring		P3			
Creating a bidirectional DNI/DRI between two MS-SPRing/BLSR protected rings		P3			
Creating a bidirectional ring-to-ring SNCP		P3			
Creating a cross-connection in a 2-fiber or 4 fiber MS-SPRing/BLSR network environment		P3			
Creating a new 1+1 MSP or 1+1 APS (NE level)	M4				
Creating a new ASAP	M3				
Creating a new circuit pack	M1	P3			
Creating a new cross-connection	M1	P3			
Creating a new 2-fiber MS-SPRing or 2fiber BLSR (NE level)	M4				
Creating a new 4-fiber MS-SPRing or 4-fiber BLSR (NE level)	M4				
Creating a user login				S5	
Creating an SNCP or UPSR (NE level)		P3			
Creating an unidirectional DNI/DRI between two protected rings.		P3			

User task	User Privilege Codes				
	M	P	PM	S	T
Creating an unidirectional path protection		P3			
Creating non-reporting ASAPs	M3				
Database backup				S4	
Deleting a cross-connection	M1	P3			
Deleting a protection group	M4				
Deleting a user login 2-10				S5	
Disabling user logins 2-11				S5	
Displaying a list of all users logged into an NE				S4	
Displaying login information for an NE				S4	
Enabling or disabling autonomous alarm forwarding	M3				
Enabling or disabling performance monitoring data collection	M1	P3			
Enabling user logins 2-13				S5	
Identifying SDH tributaries in alarm messages	M1				
Limiting the number of saved backups				S4	
Logging out NE users				S5	
Manually backup database to the WaveStar CIT				S4	
Modifying a cross-connection		P3			
Modifying a user login				S5	
Modifying a users own notification list				S1	
Modifying an existing ASAP	M1				
Modifying user security parameters by admin				S5	
Performing a software download for upgrade purposes using the WaveStar				S4	
Performing an initial software download using the CIT				S1	
Performing facility loopbacks	M3	P1		S1	
Provision global security parameters				S5	
Provisioning OSI nodes				S4	
Provisioning path protection parameters		P3			
Reassigning a circuit pack	M1	P3			
Releasing a facility loopback	M3	P1		S1	

User task	User Privilege Codes				
	M	P	PM	S	T
Removing equipment from the system		P3			
Restoring a database to a network element				S4	
Retrieve Cross-connection Lists		P1			
Retrieve protection switch reports	M1				
Retrieve security info of other users				S4	
Retrieve security info of own user				S1	
Retrieve system wide security parameters				S4	
Retrieving ASAP information	M1				
Retrieving current optical tributary maintenance signal	M1				
Retrieving current VCG delay		P1			
Retrieving current VCG tributary maintenance signal		P1			
Retrieving current VCG tributary maintenance signal		P1			
Retrieving equipment info for circuit packs	M1	P1			
Retrieving equipment info for optical SDH/SONET ports	M1	P1			
Retrieving equipment info for slots	M1	P1			
Retrieving equipment info for the backplane	M1	P1			
Retrieving equipment info for the shelf	M1	P1			
Retrieving equipment info for the system	M1	P1	PM1	S1	
Retrieving equipment info for tributaries	M1	P1			
Retrieving NE database information				S1	
Retrieving NE software generic information				S1	
Retrieving performance monitoring reports			PM1		
Retrieving performance monitoring settings for individual ports or tributaries			PM1		
Retrieving the WaveStar CIT NE Alarm List	M1				
Retrieving the WaveStar CIT NE Alarm Log	M1				
Retrieving VCG/VCG tributary information					
Rolling a cross-connection	M1	P3			
Setting ASAPs for a shelf	M1				
Setting the port monitoring mode		P3			

User task	User Privilege Codes				
	M	P	PM	S	T
Substructuring of input and output signals	M1	P3			
Switching a 1+1 equipment protection	M4	P1			
Switching a DNI, UPSR or SNCP	M4				
Switching a path protection	M4				
Switching aiber MS-SPRing oriber BLSR	M4				
Switching aiber MS-SPRing oriber BLSR	M4				
Switching an MSP or APS	M4				
Switching between different clock modes	M4				
Switching to another timing reference for system timing	M4	P1			
Switching to another timing reference for the external timing output ports	M4	P1			
Viewing an equipment protection group	M1	P1			
Viewing an existing protection group	M4				
Viewing existing cross-connections		P1			
Viewing MAC Addresses		P1			
Viewing the timing configuration		P1			

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.) **Database Changes** and **State Changes** are internally used as synonyms for data base change notifications and are to be selected and deselected together.
- State changes (STCHG) (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.) **Database Changes** and **State Changes** are internally used as synonyms for data base change notifications and are to be selected and deselected together.
- 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 1 to 999, or 'Disable'. The default is 30.

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 Automatic Tag (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 interval	The User Id Lockout Interval 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 1 to 99. The User Id Lockout can be disabled .
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 indicating the number of days within which a non-Super user needs to login or their login is automatically disabled on the NE. This parameter provides a means for removing inactive logins. The range of values is 1-999 days, or 'Disable'.



History logs

Overview

Purpose History logs are used to display history data that is maintained in the network element database.

Types of history logs The *LambdaUnite*[™] MSS system provides the following history logs:

- NE alarm log
- NE protection switch activity log

User dependency Which history logs will be retrievable by a user depends on the user privileges.

Contents

NE alarm log	13-20
NE protection switch activity log	13-21



NE alarm log

Purpose The NE alarm log provides a chronological history of all of the most recent anomalous behaviour detected by a *LambdaUnite*[™] MSS network element. The NE alarm log may contain up to 1024 entries.

Invocation The NE alarm log can be invoked via **Reports** → **NE Alarm Log...** from the **System View** or **Shelf View** main menu of the *WaveStar*[®] CIT.



NE protection switch activity log

Purpose 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.

Invocation 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 *WaveStar*[®] 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	14-14
Partition repair guidelines	14-15
DCN protocols and services	14-19
NSAP address format	14-24
Data communication channels	14-29
LAN access	14-36
Name-to-address translation	14-37
NE name administration	14-41
System provisioning	14-42



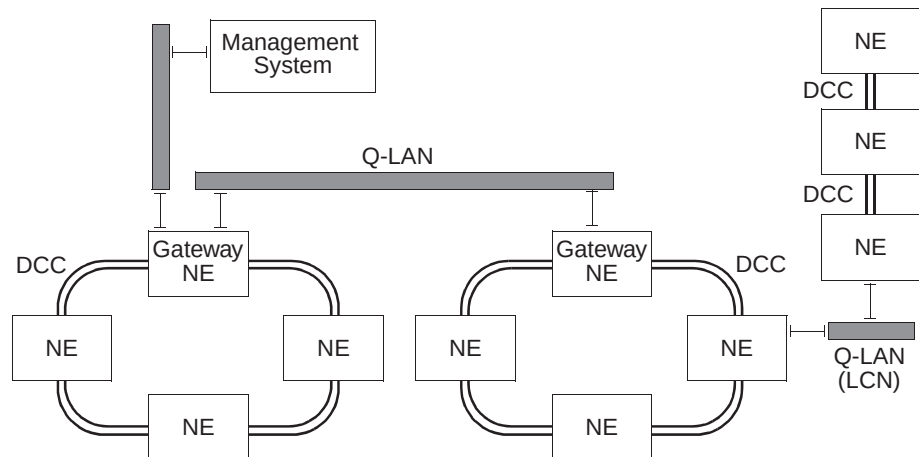
Basic DCN principles

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” \(14-29\)](#)) 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).

Multiple OSI nodes An Network Element can consist of multiple OSI nodes (OSI node–1 til OSI node–8). An OSI node is a fully provisionable OSI routing node, which can be seen externally via the routing data base. The default node is OSI node–1, which is the only node to offer the 7 Layer OSI services to all application parts. Only node-1 is represented by the NSAP address. All other OSI nodes only provide the TARP and the Network Layer services and are represented by their NET.

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). The ESCT can be only provisioned for the <i>WaveStar</i>® CIT not for <i>LambdaUnite</i> NEs, because they are no end systems.
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).
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 <i>OSI Routing Map</i> and the <i>OSI Neighbor Map</i> information that can be retrieved by using the <i>WaveStar</i> 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 <i>OSI Routing Map</i> and the <i>OSI Neighbor Map</i> 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 <i>LambdaUnite</i> 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 <i>LambdaUnite</i> MSS <i>TL1 Reference Manual</i>.



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” \(14-24\)](#)).

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.

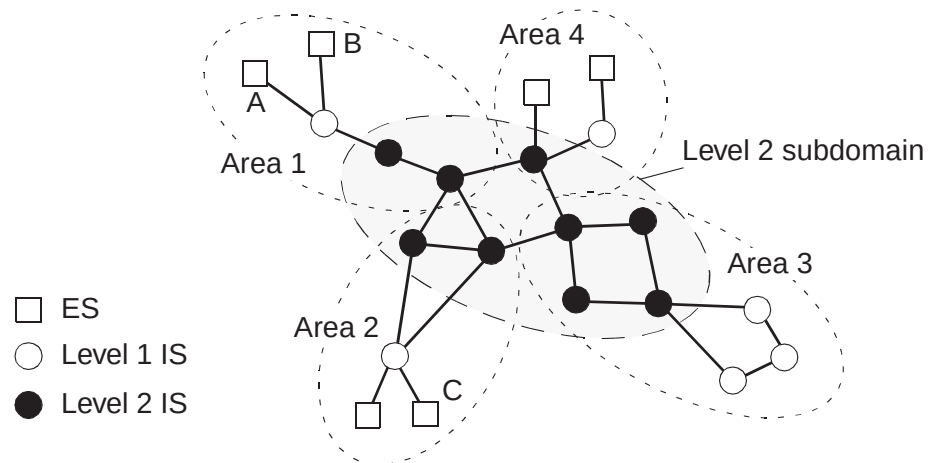
Level-2 subdomain The adjacent set of level-2 ISs is also referred to as the level-2 subdomain. All areas in a network are connected via the level-2 subdomain.

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.

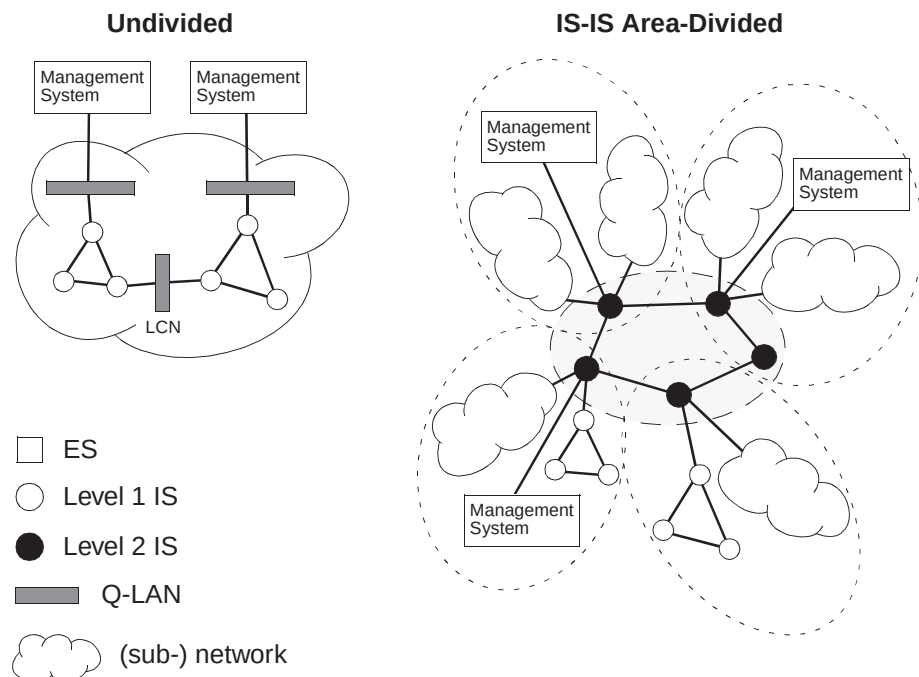
Alternatively, if the desired destination is in a different area (“C” in [“Area-divisioning of a DCN” \(14-7\)](#)), the messages are sent to a second, higher level (level-2) intermediate system. This level-2 IS routes the messages coming from node “A” to other level-2 ISs until they reach a level-2 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” \(14-7\)](#)).

Domain border routing

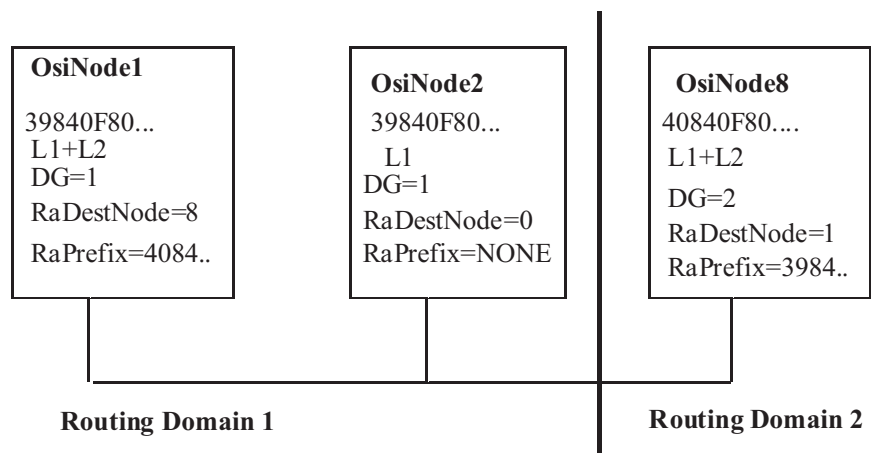
In order to facilitate the construction of multiple-domain topologies, inter domain routing information can be provided via the Reachable Address Prefix at the domain boundary. The prefix indicates that any node whose NSAP address matches the prefix, is reachable via the SNPA (of the Reachable Address Destination node) with which the prefix is associated. The address prefixes are handled (flooded etc.) by the level-2 routing algorithm. NPDU's with a destination address matching any of the prefixes present in the level-2 subdomain can therefore be relayed (using level-2 routing) and delivered outside the domain.

Routing information is not exchanged (IS-IS is disabled) across the routing domain boundary. The routing information related to a circuit connected to an other routing domain is specified via the Reachable Address Prefix. This causes NPDU's destined for NSAPs which are included in the prefix to be relayed to the node where the prefix is provisioned.

Reachable address routes have lower precedence than the intra-domain routes. For two routes with equal precedence, the shortest path is preferred, using the COST values of the default metric.

A multiple-domain topology can be used for the following purposes:

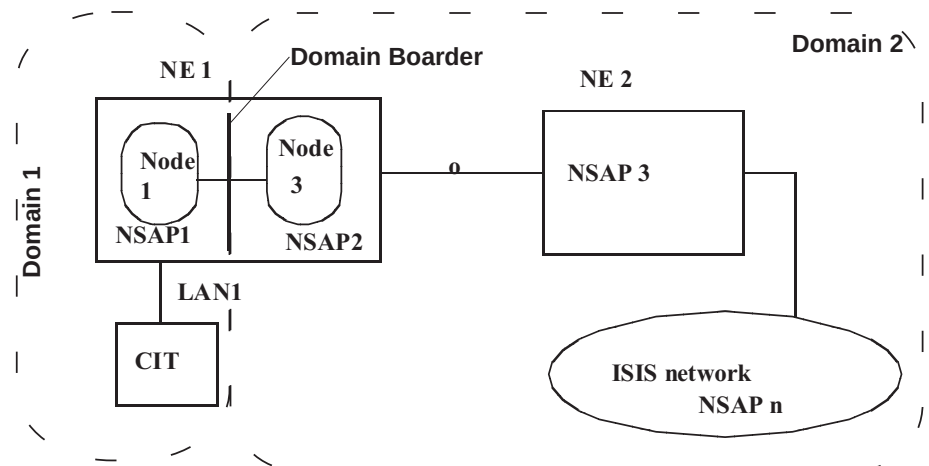
- Share an external network to interconnect several (vendors) routing domains with the office where all management equipment is located. This would require to support this feature on external LAN's (possible future enhancement - with SPOF).
- Enlarge the Lucent Management domain and manage NE's in several Lucent routing domains by the same manager (supported via requirements below - no SPOF).

Example of a domain boarder routing configuration

The following recommendations have to be fulfilled for domain boarder routing:

- Between different routing domains there is NO ISIS traffic.
- Static Routing is performed via Reachable Address Prefix!
- Domain boarder routers (osinode1 and osinode8) must be Level1+2 routers.
- Only one osinode is allowed to be in DomainGroup 2 (DG=2).
- The Reachable Address Prefix of an osinode should not match with it's own NSAP.
- Domain boarder Routers must point to each other (using Reachable Address Destination Node)
- The Router in Routing Domain 2 MUST specify Node1 as Reachable Address Destination Node.

Guidelines for configuring the “Reachable Address Prefix”



The following rules have to be observed for configuring Reachable Address Prefixes:

- Between osinode1 and osinode3, TARP Manual adjacencies must be provisioned (refer to [“Assigning TARP manual adjacencies” \(3-69\)](#)).
- Reachable Address Prefix in osinode1 must match all NSAPs behind the domain boarder (NSAP 2, NSAP 3, NSAP n).

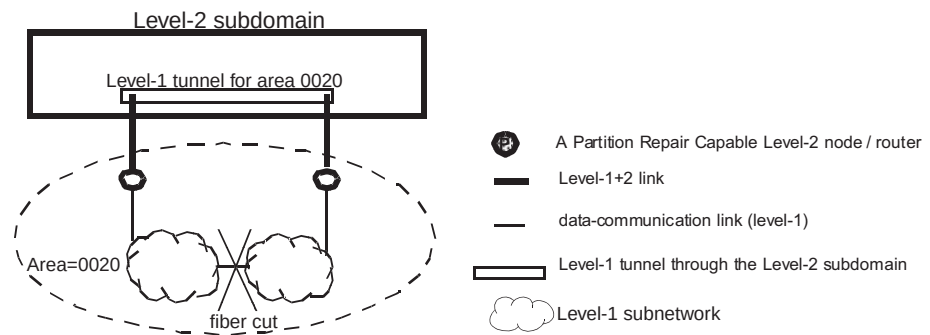
Deleting domain boarder routing

The following steps have to be performed to delete domain boarder routing:

1. Set **Reachable Address Prefix** to **none** with valid Reachable Address Destination Node in both osinodes.
2. Set **Reachable Address Destination** to **none** in both osinodes
3. Set Domain Group (**Domain Boundary**) back to no in the former Domain Boarder Router.

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 250 nodes (i.e. NSAP addresses) is supported in an area.
 - A maximum of 50 areas is supported in a subnetwork.
 - All nodes in an area must have the same area address (cf. [“ISO-DCC NSAP address format” \(14-25\)](#)).
 - All nodes in an area must have DCC or LAN 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.

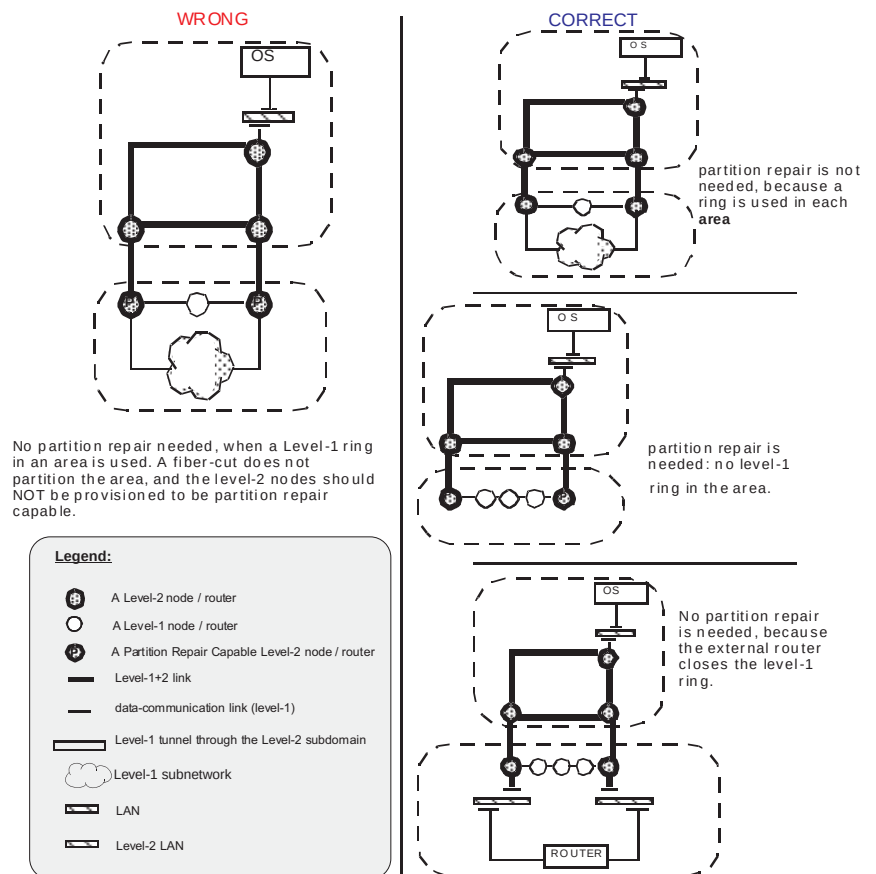
For example, a perfectly balanced subnetwork of 200 nodes would include 20 nodes per area in each of 10 areas and 20 level-2 ISs in the level-2 subdomain (two level-2 ISs per area).
- Related information** Please refer to [“NSAP address format” \(14-24\)](#) and to [“Data communication channels” \(14-29\)](#) 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.



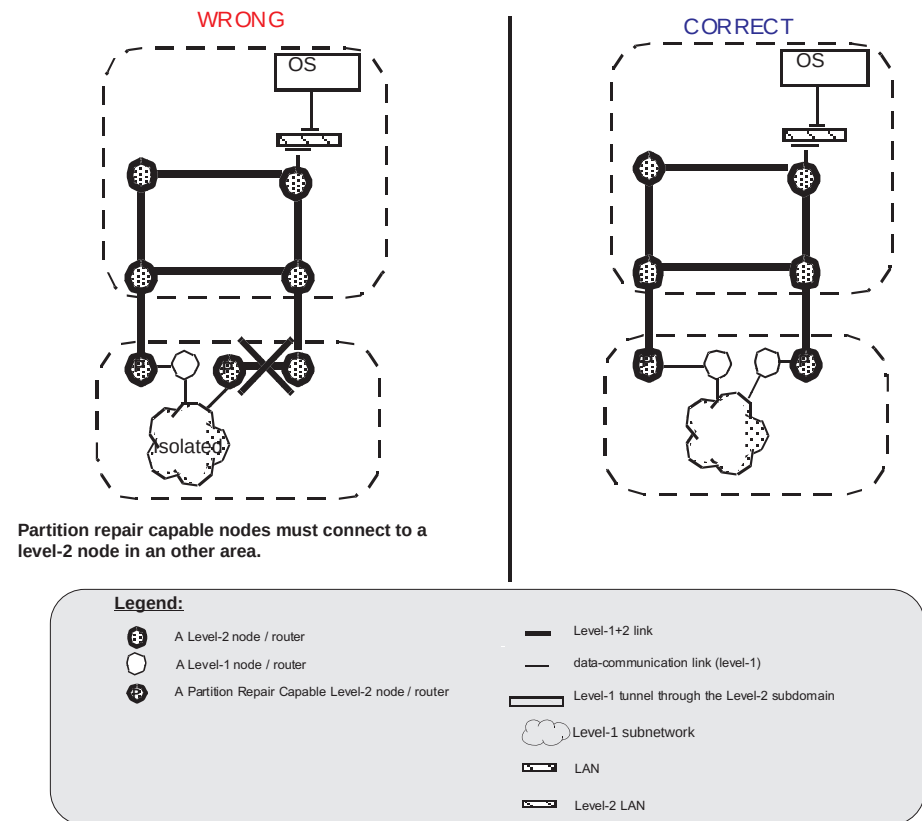
How to use partition repair

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 SPF'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 (*WaveStar*® CIT/ *Navis*® Optical EMS) 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/*Navis* Optical EMS) 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 10 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, OSI LAN or TCP/IP. The DCC and OSI LAN network operations capabilities use 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 or 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:

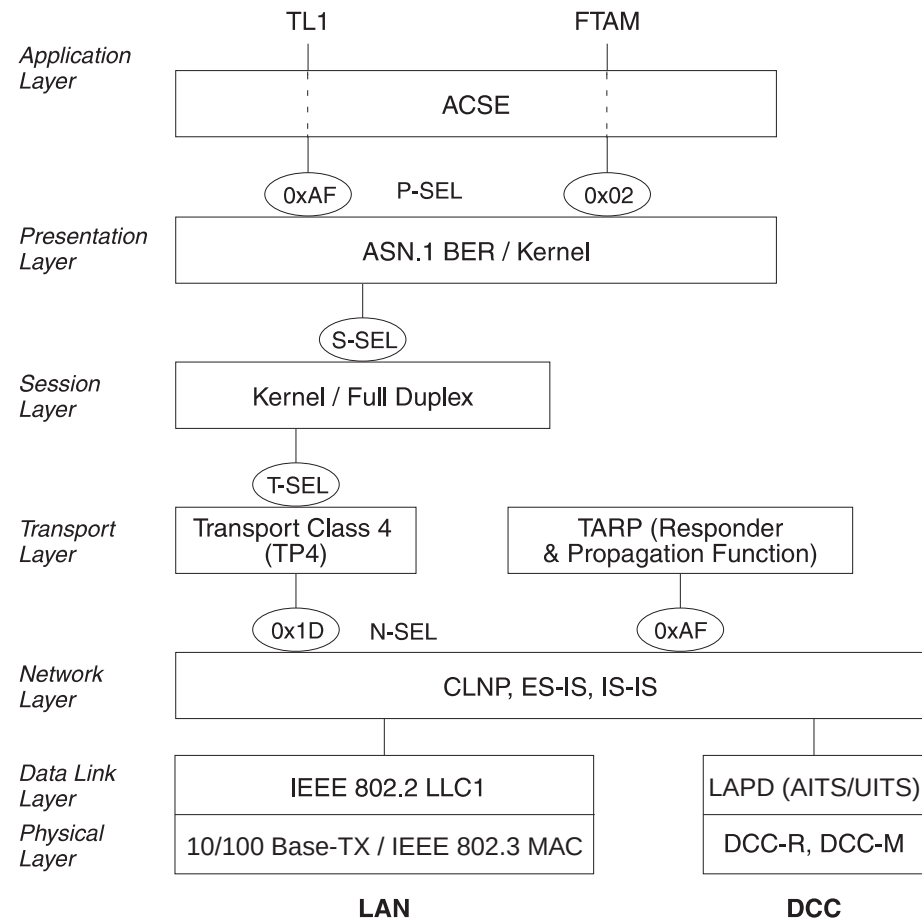
- OSI LAN/WAN
- TL1 TCP/IP (using the internal gateway function)
- File Transfer, Access and Management (FTAM) protocol (for software download, database backup and restore.)
- FTP (for software download, database backup and restore).

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 OSI 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).

TCP for support of IP access networks

TCP provides a connection-oriented, reliable, full duplex byte stream service. There are always exactly two peers (end points) communicating with each other on a TCP connection. Concepts like broadcasting and multi-casting are not applicable to TCP. A TCP connection is set up between an IP-address-and-port-number on one end, and an IP-address-and-port-number on the other end. A combination between an IP address and a port number is called a socket. Using this terminology, a TCP connection is uniquely identified by a pair of sockets. TCP uses IP as the basis for providing its services.

TL1 over TCP/IP

A TL1 TCP/IP gateway (refer to [“T-TD Gateway” \(14-21\)](#)) may be used to connect multiple collocated *LambdaUnite* MSS systems to a remote OS equipped to communicate through a TCP/IP WAN. Since the OS communicates through TCP/IP, a gateway is required to provide a mapping between TCP/IP and OSI. That gateway function is included as a feature of the *LambdaUnite* MSS system.

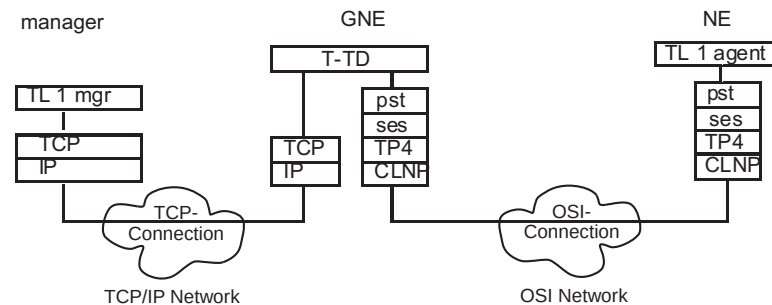
The gateway is provisioned to provide a TL1 TCP/IP gateway between TCP/IP and OSI. This process is bidirectional, mapping messages originating in the OS to the proper NE NSAP, as well as mapping messages originating in the NE to the proper OS IP address and returning then to the OS.

This interface supports TL1 messages only.

T-TD Gateway

The TL1 Translation Device (T-TD) is a device that translates TL1 over TCP to TL1 over OSI presentation. By doing so, it enables the OSs which are located in the IP-based network to manage the NEs that are located in the OSI-based network. Thus, T-TD is essentially a TL1 TCP-OSI gateway, and it requires the support of both the TCP/IP stack and the OSI stack. The T-TD may be an NE or it may be a separate device. It encompasses both the TL1 initiator and TL1 responder aspect.

The T-TD gateway resides in an NE and operates as shown in the figure below.



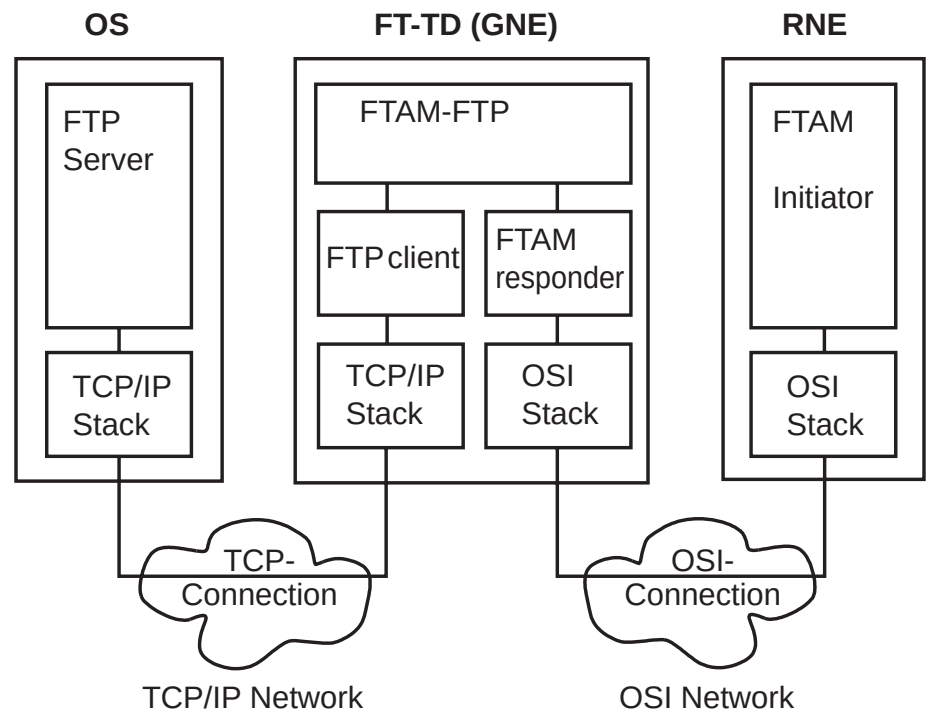
FT-TD Gateway

The FTAM-FTP Gateway is a gateway that translates FTAM over OSI presentation to FTP over TCP/IP. It requires the support of both the TCP/IP stack and the OSI stack. It is also referenced as FT-TD (File Transfer Translation Device).

The FT-TD is used in a mixed OSI and IP network, where the access DCN is IP, and the NEs being managed are in an OSI network. While different approaches exist to solve the file transfer problem in a mixed network, the system will be using an FTAM-FTP On-The-Fly Gateway. Other approaches are IP Tunneling or an FTAM-FTP Store and Forward Gateway.

The FT-TD acts as a gateway with connection set-up in a single direction - from FTAM to FTP, and not the other way. Even though an OS sends the initial TL1 message requesting a file transfer, it is the FTAM initiator residing on the remote NE (RNE) that creates an FTAM association with an FTAM responder on the Gateway NE (GNE). The FTAM-FTP Gateway translates the FTAM requests into FTP requests that are passed to the FTP Client on the GNE. The file transfers are supported in both directions (download, backup, restore). The FT-TD does not require FTP Server functionality on the NE.

The FT-TD gateway resides in an NE and operates as shown in the figure below.



Refer to [“Configuring an NE as FTAM-FTP Gateway” \(3-47\)](#)

□

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”](#).

***LambdaUnite™* MSS NE addressing**

A *LambdaUnite* MSS NE that runs OSI has at least one node, which is referred to as node-1. Additional nodes can be added, with a subset of the functionality of 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” \(14-28\)](#)). 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.

In TL-1 messages towards the user interfaces, the NSAP for TL-1 management via node-1 will be presented. For the other nodes the NET is used.

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 aux-profile1="future" address.

The meaning of the individual fields of the ISO-DCC NSAP address is explained in ["NSAP address fields" \(14-25\)](#).

NSAP address fields

The following table lists the NSAP address fields and describes their meaning.

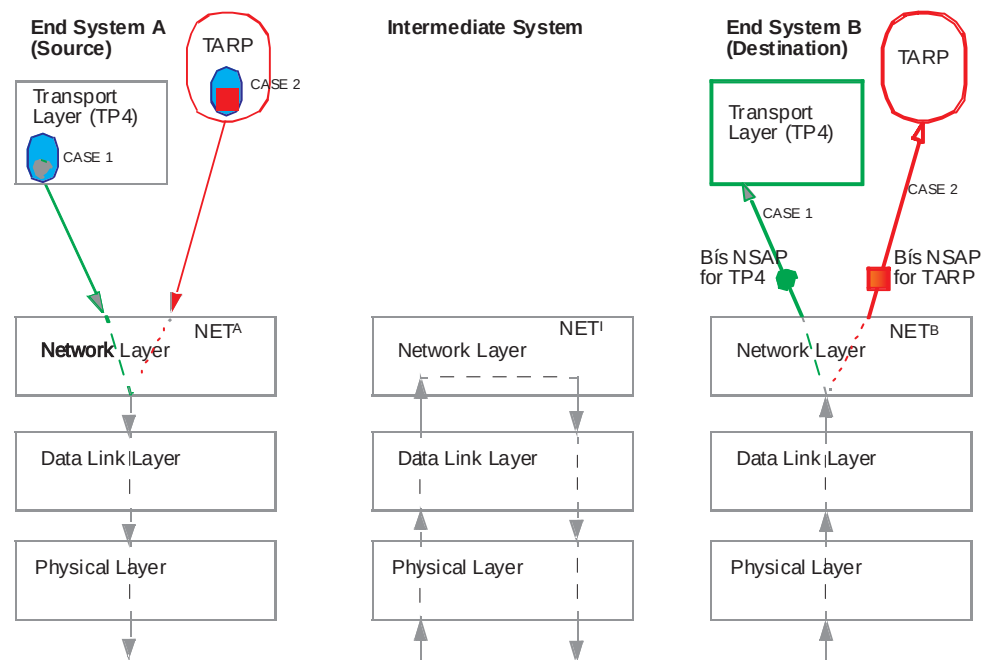
Field	Meaning	Description
Initial Domain Part (IDP):		
AFI	Authority and Format Identifier specifying the NSAP address format.	The predefined value is 0x39 (hex.), indicating that the ISO Data Country Code (ISO-DCC) is the address format. This field is configurable.

Field	Meaning	Description
IDI	Initial Domain Identifier specifying the country code.	The predefined value is 0x840F (hex.). This field is configurable.
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. 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

Field	Meaning	Description
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” (14-37)). 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” (14-25)).
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 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” \(14-14\)](#)).

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.

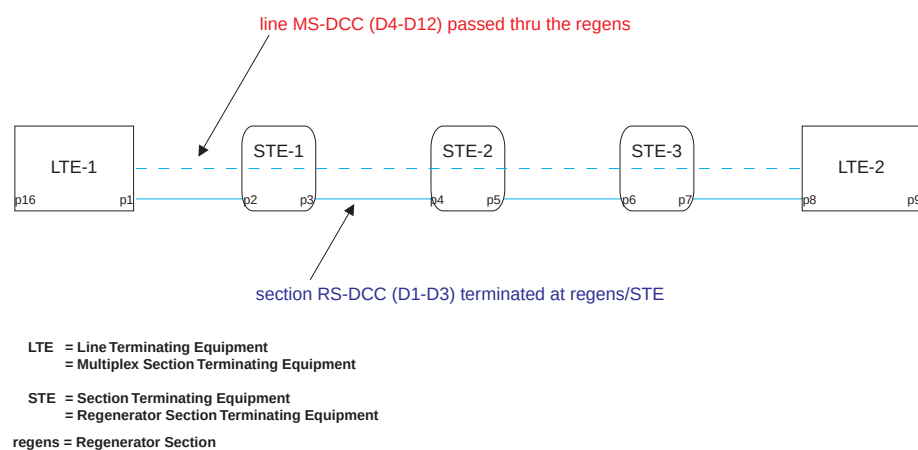
Termination of Data Communication Channels

The *LambdaUnite*[™] MSS system supports the 7-layer OSI protocol stack over the DCC links which terminate on the DCC controller DCF. The controller circuit pack (DCF and SCF in one 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-256, STM-64, STM-16. 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/s 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 8. Each DCC controller thus can support up to 8 active DCC links.

When a circuit pack is inserted into a slot, the RS/MS-DCC on a port are left in disabled state.

The User has to explicitly enable the RS/MS-DCC on a port.

DCC provisioned state

A Data Communication Channel (RS/MS-DCC) can be in one of the following provisioned states:

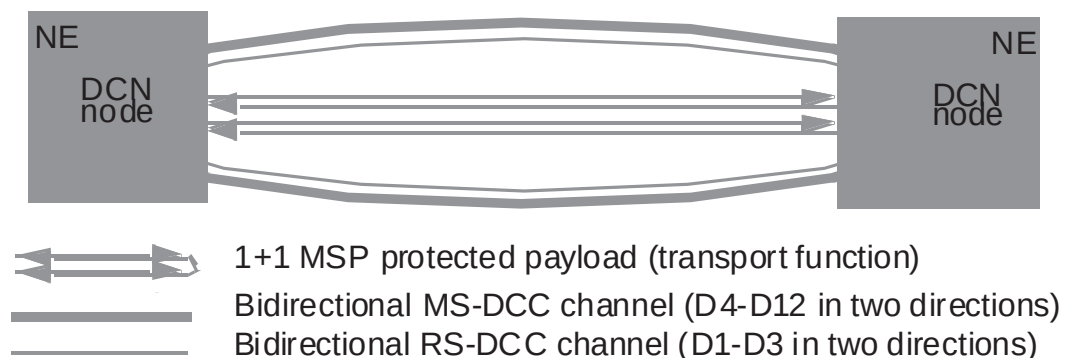
- **Enabled**
 - The corresponding DCC bytes are allocated to an optical interface port.
 - The DCC is assigned a LAPD channel.
- **Disabled**
 - The corresponding DCC bytes are no longer allocated to an optical interface port.
 - The DCC is no longer accessed by a LAPD channel.

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! The following has to be observed:

1. 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”.
2. If the neighboring node in an SDH MS-SPRing is an ADM-16/1, then you must enable the DCC-M on the side connected to the ADM-16/1.

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) 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 requirement 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) 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) 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) is available on that port.

Enabling of DCCs

When a circuit pack is inserted into a slot, the RS/MS-DCC on a port is in disabled state. Each RS/MS-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” \(3-57\)](#).

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” \(3-57\)](#).

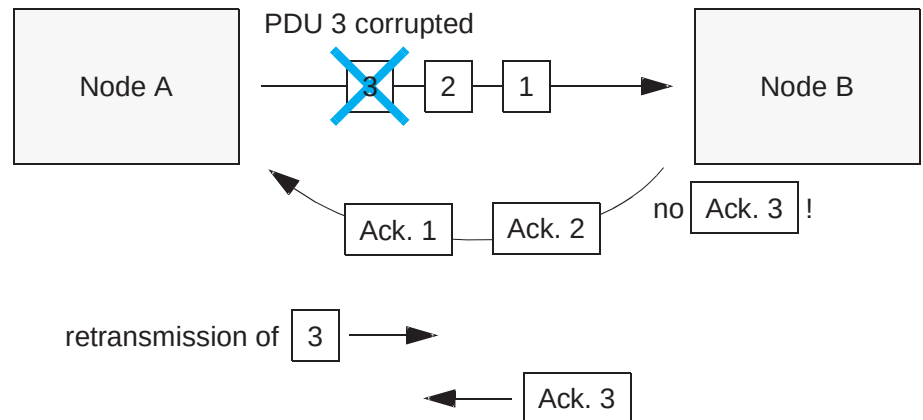
AIMS and UITS supported

LambdaUnite MSS network elements support the Acknowledged Information Transfer Service (AIMS) and the Unacknowledged Information Transfer Service (UITS) as the basis for the LAPD or LinkID 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” \(14-37\)](#) (starting below).
2. The TID Address Resolution Protocol (TARP); please refer to [“TARP” \(14-38\)](#).

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” \(14-24\)](#)). 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 and/or IP addresses for NEs that might be connected to the *WaveStar* CIT via OSI. Provisioning IP addresses into this local *WaveStar* CIT file does not set or change the NE’s IP address, which is done via the Data Communication, but provides a method for giving the CIT the IP addresses of an NE to which the CIT is to be connected in the absence of a DNS. This is necessary since there is no equivalent in TCP/IP to the OSI/TARP capability to broad-cast a TID on the network and receive back the NSAP from the NE that has that TID.

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 <i>WaveStar</i> 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 <i>WaveStar</i> CIT. Three basic TARP functionalities can be distinguished: • TARP originator functionality • TARP propagation functionality • TARP responder functionality
TARP originator functionality	The TARP originator functionality means the ability to spontaneously originate a TARP PDU type 1, 2 or 5 query (cf. “Types of TARP PDUs” (14-39)) and broadcast it over the OSI network.
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). 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” (14-39)).

Types of TARP PDUs

The following table shows the five defined types of TARP PDUs.

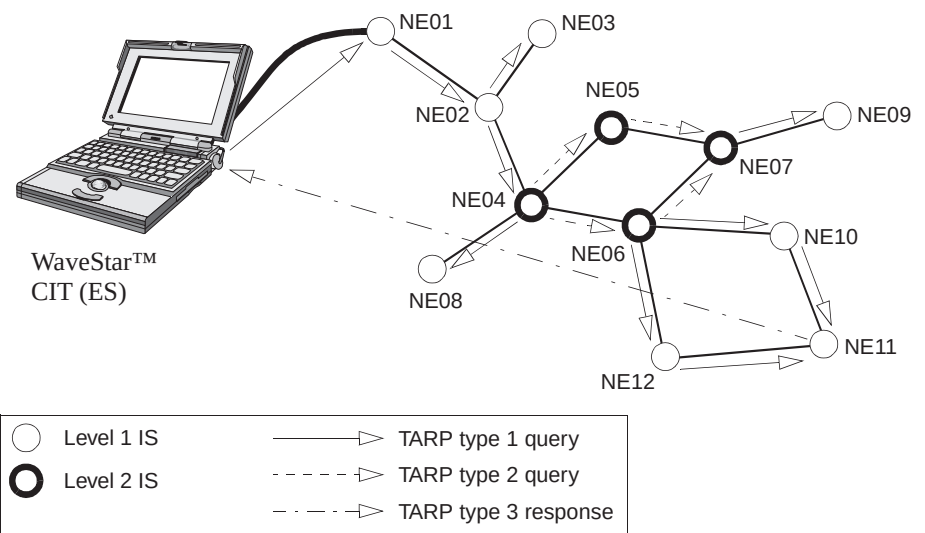
Type	Characteristic	Description
1	Query	Given an NE name (TID), the corresponding NSAP address is requested (restricted to IS-IS level-1 area).
2	Query	Given an NE name (TID), the corresponding NSAP address is requested (IS-IS level-1 and 2 areas).
3	Response	Response to a TARP Query.
4	Autonomous notification	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 originator, the TARP propagation and the TARP responder functionalities. These functionalities can be either enabled or disabled. If T-TD is used in a GNE the TARP originator functionality must be enabled for this NE.

TARP example

The following figure shows an example to illustrate the TARP functional principle.



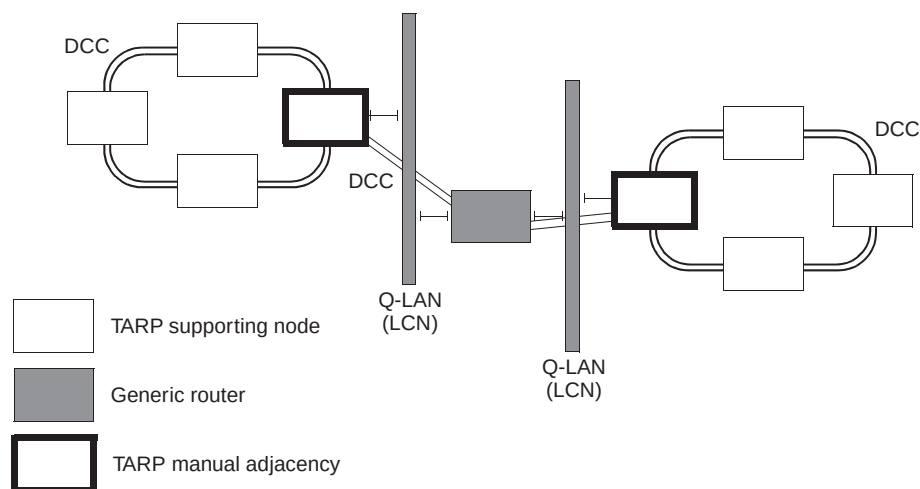
When a user requests to establish a management association to NE11 and the corresponding NSAP address cannot be found in the static routing table, then the *WaveStar* CIT originates a TARP type 1 query. This query will be propagated over the network until it reaches NE11. NE11 then sends a TARP-type-3 response directly back to the *WaveStar* CIT.

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” \(14-4\)](#)) to obtain information about the network neighbors of an NE.

TARP manual adjacencies

By using TARP manual adjacencies (cf. [“Assigning TARP manual adjacencies” \(3-69\)](#)) 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” \(14-28\)](#)) of a node that supports TARP.



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” \(3-65\)](#),
- [“Assigning TARP manual adjacencies” \(3-69\)](#),
- [“Configuring the LDB timers for the *WaveStar* CIT” \(3-16\)](#).



NE name administration

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").
- Each NE name must be at most 20 characters in length.

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 valid 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
WaveStar[®] CIT methods to perform provisioning	15-4
Provisioning of new components	15-6
Shelf configuration	15-7
Overview of access identifiers	15-9
Shelf provisioning	15-15
Slot provisioning	15-16
Circuit pack provisioning	15-17
Port and tributary provisioning	15-18
XC320 equipment protection	15-19



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 using the *WaveStar*[®] CIT or *Navis*[®] Optical EMS. The configuration data is placed in the NE and stored on a *CompactFlash*[™] card, the non-volatile memory (NVM) of the NE.

Equipment provisioning by means of the *Navis* Optical EMS is out of the scope of this manual. Please refer to the *Navis* Optical Element Management System (EMS) Provisioning Guide for *LambdaUnite* MultiService Switch (MSS).

Autoprovisioning

Some of the components are autoprovisioned. This means some system parameters are assigned automatically after installation and system start. These are:

- Controller (CTL)
System controller and DCC controller
- XC320 switch unit(s)
Switching and timing generator functions
- Synchronization default mode (free running)
- Equipment protection (if two XC320 switch units 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 other 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

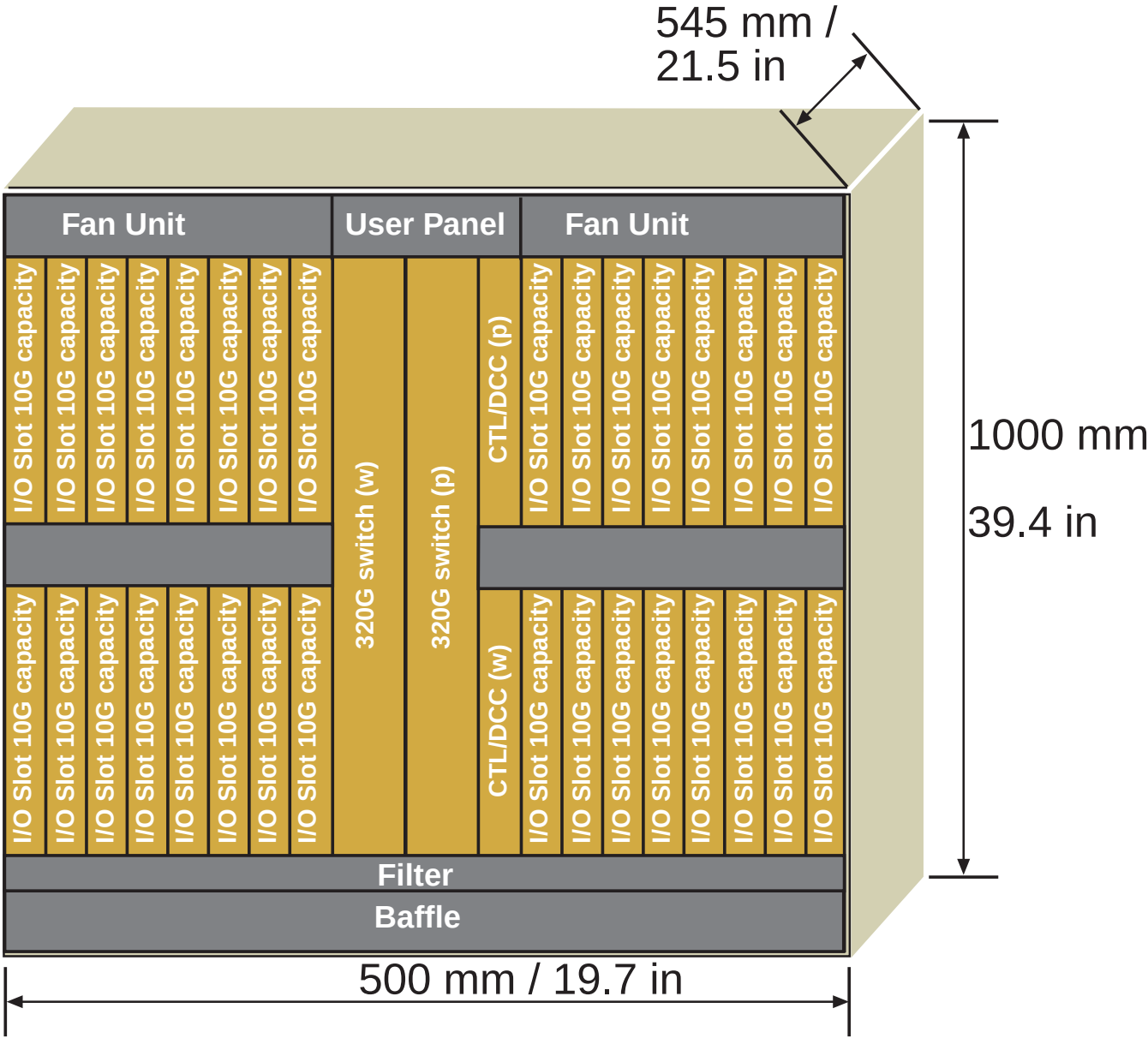
- Overview** You can add new components to an existing system. This can be necessary during reconfiguration or after installation. The following components can be added:
- Circuit packs
 - Protection groups
- Invocation** Select in the main menu **Configuration** → **Create New**. In the pop-up menu 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” \(18-13\)](#).



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.



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 • 622-Mbit/s port units • 2.5-Gbit/s port units • 10-Gbit/s port units • 40-Gbit/s port units • 1-Gigabit Ethernet interface (GE1/SX4) • 10-Gigabit Ethernet interface (realised on an OP10... port unit)
Controller slot (working)	CTL circuit pack. System controller including the non-volatile memory (NVM, <i>CompactFlash</i> [™] card) and DCC controller for the whole network element.
Controller slot (protection)	Reserved for future use.
320G switch slot (working)	The XC320 switch unit in this slot can make cross-connections for 6144 STS-1 / 2048 VC-4 equivalent circuits. This switch is paired with the XC320 switch unit in the protection slot 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 XC320 switch unit in this slot can make cross-connections for 6144 STS-1 / 2048 VC-4 equivalent circuits. This switch is paired with the XC320 switch unit in the working slot 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.

Minimum Complement of circuit packs

The minimum complement of circuit packs depends on the desired functionality: required for an operational *LambdaUnite* MSS shelf is

- To perform preprovisioning, it is sufficient to install the Controller (CTL).
- These circuit packs are required for transmission functionality:
 - The CTL for system controller and DCC controller functions
 - At least one XC320 for switching and timing functions
 - The respective port unit(s) for the transmission functions

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 the connection interface of the Controller (CI-CTL).



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” \(15-10\)](#) 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 is a certain value range possible for an entry, then it is given in curly braces (“{1-9}” or “{4, 8, 15, 19, 24, 28, 35, 39}” for example).

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 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 (XC) slots	1-1-#-#-xcp 1-1-#-#-xcw 1-1-#-#-xcall
Controller (CTL) 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 (XC) circuit packs	1-1-#-#-xcp-cp 1-1-#-#-xcw-cp 1-1-#-#-xcall-cp
Controller (CTL) circuit packs	1-1-#-#-ctlp-cp 1-1-#-#-ctlw-cp 1-1-#-#-ctlall-cp
Non-volatile memory (NVM)	
NVM	1-1-#-#-ctlp-nvm 1-1-#-#-ctlw-nvm 1-1-#-#-ctlall-nvm
Ports	

Entity	Access Identifier
SDH/SONET ports	The SDH/SONET port AIDs depend on the type of circuit pack: - OP155 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all - OP622 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all - OP2G5 - Any OP2G5 port unit other than the PWDM-compatible OP2G5-1...32PWDM (see below) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-4} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all - OP2G5-1...32PWDM (KFA20, with OM2G5/921...959PWDM module) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1, 3} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all Note: Due to architectural reasons, the two ports on the PWDM-compatible OP2G5 port unit are numbered “1” and “3”! - OP10 1-1-#-#{1-8, 12-19, 21-28, 32-39}-1 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all - OP40 1-1-#-#{4, 8, 15, 19, 24, 28, 35, 39}-1 1-1-#-#{4, 8, 15, 19, 24, 28, 35, 39}-all
Gigabit Ethernet LAN ports (Ethernet ports)	The Gigabit Ethernet LAN port AIDs depend on the transport capacity: 1 Gbit/s 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-4} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all 10 Gbit/s 1-1-#-#{1-8, 12-19, 21-28, 32-39}-1 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all
Gigabit Ethernet WAN ports (VCG ports)	The Gigabit Ethernet WAN port AIDs depend on the transport capacity: 1 Gbit/s 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{v1, v2, v3, v4} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-vall 10 Gbit/s 1-1-#-#{1-8, 12-19, 21-28, 32-39}-1 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all
External LAN ports	1-1-lan{1-3} 1-1-lanall
Miscellaneous Discrete Input (MDI) ports	misc_in{1-8} misc_inall
Miscellaneous Discrete Output (MDO) ports	misc_out{1-8} misc_outall

Entity	Access Identifier
User byte ports	1-1-ubio{1-6}
<i>Tributaries</i>	
VC-3/STS-1 Tributaries A specific tributary numbering format is used for SDH tributaries. Please refer to “SONET and SDH tributary numbering format” (16-15)	The VC-3/STS-1 tributary AIDs depend on the type of circuit pack: - OP155 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16}-{1-3} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16}-all - OP622 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16}-{1-12} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-16}-all - OP2G5 - Any OP2G5 port unit other than the PWDM-compatible OP2G5-1...32PWDM (see below) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-4}-{1-48} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1-4}-all - OP2G5-1...32PWDM (KFA20, with OM2G5/921...959PWDM module) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1, 3}-{1-48} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{1, 3}-all - OP10 1-1-#-#{1-8, 12-19, 21-28, 32-39}-1-{1-192} 1-1-#-#{1-8, 12-19, 21-28, 32-39}-all - OP40 1-1-#-#{4, 8, 15, 19, 24, 28, 35, 39}-1-{1-768} 1-1-#-#{4, 8, 15, 19, 24, 28, 35, 39}-all
VCG tributaries	1-1-#-#{1-8, 12-19, 21-28, 32-39}-{v1, v2, v3, v4}-{111, 112, 113, 121, 122, 123, 131, 132, 133, 141, 142, 143, 211, 212, 213, 221, 222, 223, 231, 232, 233, 241, 242, 243} (VC-3/STS-1 substructure) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{v1, v2, v3, v4}-{110, 120, 130, 140, 210, 220, 230} (VC-4/STS-3c substructure) 1-1-#-#{1-8, 12-19, 21-28, 32-39}-{v1, v2, v3, v4}-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>	

Entity	Access Identifier
Fan unit	1-1-fan 1-1-fanall
Timing references	
External timing reference	extref1 extref2 extrefall
Line timing references	line1 line2 line3 line4 line5 line6 lineall
Timing Ports	
External timing input port	exttmg0 exttmg1 exttmgall
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 parameters are available:

Parameter	Meaning	refer to
Shelf AID	Displays the AID (access identifier) of the shelf.	“Overview of access identifiers” (15-9)
Alarm Severity Assignment Profile	Displays a list of provisioned equipment ASAPs (alarm severity assignment profile) from which an ASAP can selected and set for the shelf. 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 <i>LambdaUnite</i>[™] MSS system.	“Alarm Severity Assignment Profiles” (16-26)



Slot provisioning

Purpose Slot provisioning allows the user to configure parameters associated with a specific slot.

Parameters The following parameters are available:

Parameter	Meaning	refer to
Slot AID	Displays the AID (access identifier) of the slot.	“Overview of access identifiers” (15-9)
Alarm Severity Assignment Profile	Displays a list of provisioned equipment ASAPs (alarm severity assignment profile) from which an ASAP can selected and set for the slot. 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 <i>LambdaUnite</i>TM MSS system.	“Alarm Severity Assignment Profiles” (16-26)



Circuit pack provisioning

Purpose Circuit pack provisioning allows the user to configure parameters associated with a specific circuit pack.

Parameters The following parameters are available:

Parameter	Meaning	refer to
Circuit Pack AID	Displays the AID (access identifier) of the circuit pack.	“Overview of access identifiers” (15-9)
Circuit Pack Type	Displays the type and qualifier of the circuit pack.	
Alarm Severity Assignment Profile	Displays a list of provisioned equipment ASAPs from which an ASAP can be selected and set for the slot/circuit pack. An Alarm Severity Assignment Profile (ASAP) is a list of alarms that can occur in an NE and which each have an alarm severity assigned. Several ASAPs for different functional categories are predefined for the <i>LambdaUnite™</i> MSS system.	“Alarm Severity Assignment Profiles” (16-26)



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” \(4-49\)](#)).

Tributary provisioning Tributary provisioning allows the user to configure parameters associated with a specific tributary belonging to a port (cf. [“Configuring a tributary” \(4-92\)](#)).



XC320 equipment protection

Introduction An active XC320 switch unit can be protected by a standby XC320. Both the cross-connect function as well as the timing function are protected on this way and form a single protection object. The equipment protection process of the XC320 is fully performed by a central process in the CTL.

Creation The equipment protection group is created automatically if

- the second XC320 unit is plugged in the shelf
- the two slots for the working and the protection XC320 are preprovisioned
- one of the two slots is autoprovisioned and the other one is preprovisioned

Mode of operation The XC320 equipment protection operates in 1+1 non-revertive mode.

Hot standby mode The standby XC320 switch unit works in the so-called hot-standby mode, 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.

Switch Info The following switch commands are denied and the error message `Command did not execute successfully. Execution of the following commands failed is displayed.`

Active Unite	Active Switch Request	Denied Switch Request
WKG	Forced Switch	Force To Protection
PROTN	Forced Switch	Force To Working
WKG	Equipment Failed	Manual To Working
PROTN	Equipment Failed	Manual To Working
WKG	Equipment Failed	Manual To Protection
PROTN	Equipment Failed	Manual To Protection
WKG	Manual Switch	Manual To Protection
PROTN	Manual Switch	Manual To Working
WKG	Forced Switch	Manual To Working

Active Unite	Active Switch Request	Denied Switch Request
PROTN	Forced Switch	Manual To Working
WKG	Forced Switch	Manual To Protection
PROTN	Forced Switch	Manual To Protection

Deletion The equipment protection groups are deleted automatically, if an XC320 is plugged-out and the respective slot is deprovisioned, or if a preprovisioned slot is deprovisioned.

Important protection switching details

Please observe these functional details with respect to XC320 equipment protection switching:

1. After an equipment protection switch, wait at least one minute before applying a manual or forced equipment protection switch command to prevent traffic hits.
2. When a standby XC320 switch unit is plugged into the system it enters the warming-up state for approximately five minutes. During this warming-up state the system timing quality level is explicitly set to DNU/DUS (Do not use for synchronization). When an equipment protection switch occurs during the warming-up period of the standby XC320 the quality level at the timing outputs of the system will change to DNU/DUS which could cause timing rearrangements in other NEs. Therefore, wait at least approx. five (5) minutes after the insertion of a standby XC320 switch unit before performing a manual or forced equipment protection switch.
3. On an XC320 switch unit, performance monitoring data is stored in the current bin and one recent bin. Both XC320 switch units 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. Prior to an (intentional) XC320 equipment protection switch the standby XC320 should have been present in the system for a full 24-hours binning period. Otherwise, performance monitoring data may be lost.





16 Alarm management concepts

Overview

Purpose This chapter provides information about the *LambdaUnite*[™] MSS alarm management.

Contents

<u>LambdaUnite MSS fault management</u>	<u>16-3</u>
<u>Basic fault management concepts</u>	<u>16-4</u>
<u>LambdaUnite MSS fault management principle</u>	<u>16-7</u>
<u>WaveStar[®] CIT alarm presentation formats</u>	<u>16-10</u>
<u>Alarm severities</u>	<u>16-11</u>
<u>Alarm format preferences</u>	<u>16-13</u>
<u>Signalling of alarms</u>	<u>16-18</u>
<u>WaveStar CIT visual alarm indicators</u>	<u>16-20</u>
<u>NE local indications</u>	<u>16-22</u>
<u>Impact of state changes on the signalling of alarms</u>	<u>16-23</u>
<u>Alarm provisioning</u>	<u>16-25</u>
<u>Alarm Severity Assignment Profiles</u>	<u>16-26</u>
<u>Port monitoring mode</u>	<u>16-36</u>
<u>Forward error correction</u>	<u>16-37</u>
<u>Operations interfaces</u>	<u>16-40</u>

<u>The <i>LambdaUnite</i> MSS user panel</u>	<u>16-41</u>
<u>ACO interaction with an alarm test</u>	<u>16-44</u>
<u>Circuit pack status indicators</u>	<u>16-46</u>
<u>Fan unit status indicators</u>	<u>16-49</u>
<u>Office alarm interfaces</u>	<u>16-50</u>
<u>Miscellaneous Discretes</u>	<u>16-52</u>



LambdaUnite[™] MSS fault management

Overview

Purpose The present section describes the behaviour of *LambdaUnite* MSS network elements with respect to fault management.

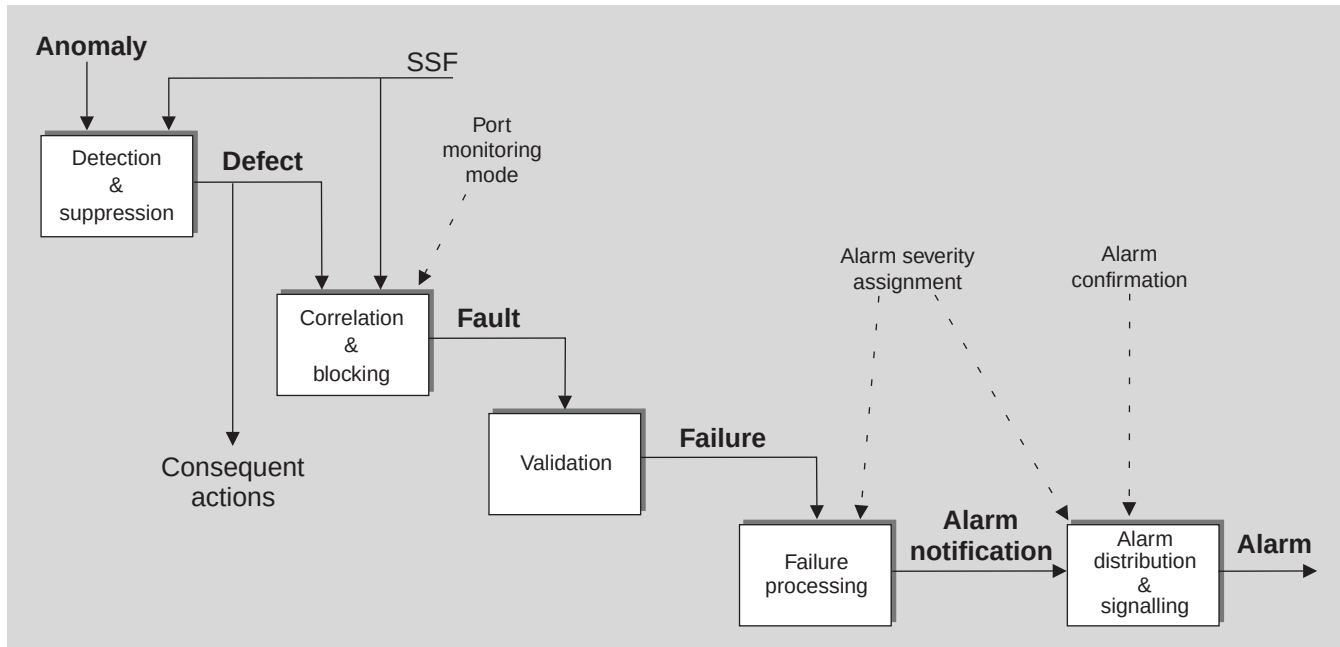
Fault management deals with the detection and the reporting of particular degraded conditions by the network elements and the resulting actions.



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. An SF 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 (blocked) when the corresponding server layer indicates a Signal Fail (SF) 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. A synonym for "blocking" is "masking" .

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” \(16-36\)](#).

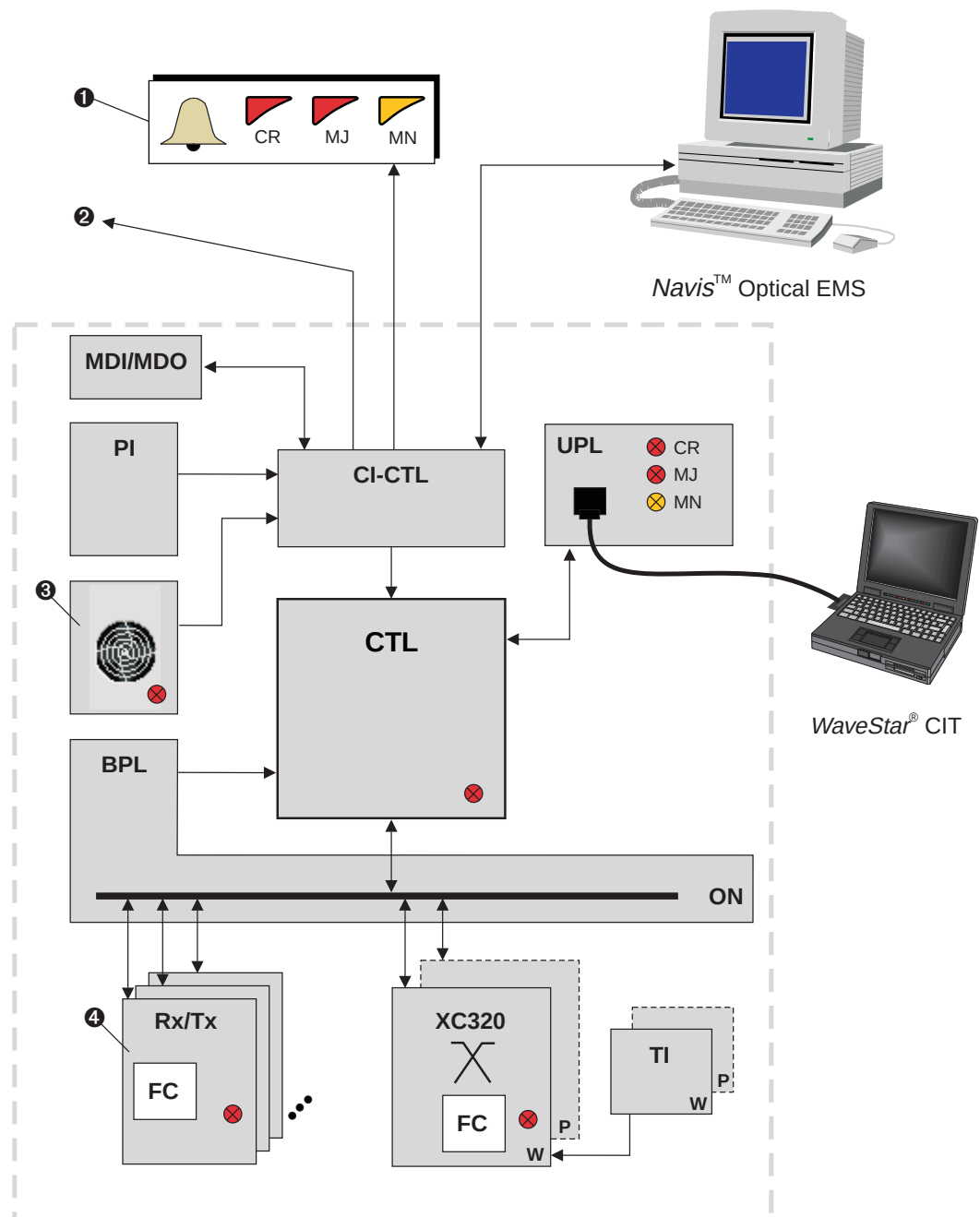
Alarm severity assignment Please refer to [“Alarm severities” \(16-11\)](#) and [“Alarm Severity Assignment Profiles” \(16-26\)](#).

Alarm confirmation Please refer to [“Alarm acknowledgment” \(16-42\)](#).



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, Miscellaneous Discrete Outputs
	PI	Power Interface
3		Fan unit
	BPL	Backplane (ON=Operations Network)
4	Rx/Tx ¹	Transceiver units For example optical port units (OP...) or GE1 Gigabit Ethernet port unit (FC=Function Controller)
	XC320 ¹	Cross connection unit (switch 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. Circuit packs with an on-board function controller are referred to as "subsystems".

Related information

Please also refer to ["Operations interfaces" \(16-40\)](#).

***LambdaUnite* MSS fault
processing**

Each subsystem (circuit pack with integrated function controller) contributes to the *LambdaUnite* MSS fault processing (cf. [“Fault management process” \(16-4\)](#)) 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.

□

WaveStar[®] CIT alarm presentation formats

Overview

Purpose In the following, the available *WaveStar* 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	16-11
Alarm format preferences	16-13



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 WaveStar® CIT to influence how alarm severities will be presented in the WaveStar CIT **NE Alarm List** or **NE Alarm Log**, please refer to [“Alarm format preferences” \(16-13\)](#).

Meaning of the alarm severities

The alarm severities have the following meanings:

Alarm severity	Meaning
Critical (CR) Major (MJ)	“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.
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” (16-18)). 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” \(16-26\)](#).



Alarm format preferences

Alarm formats A preference for presenting alarm severities in the alarm status display, in the WaveStar® CIT **NE Alarm List**, and in Alarm Severity Assignment Profiles (ASAPs) in either of the following two alarm formats can be specified:

- SONET format:
Critical/Major/Minor (**CR/MJ/MN**),
- SDH format:
Prompt/Deferred/Info (**PR/DF/INF**).

The 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. Please refer to:

- [“Setting the view preferences” \(5-3\)](#)

Navis® Optical EMS

In principle, the same preferences for the alarm presentation format can be set for Navis Optical EMS sessions. However, the procedure for accomplishing this setting is out of the scope of the present manual. Please refer to the Navis Optical EMS 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 (PR/DF/INF)	SONET format ¹ (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-3c/VC-4	1	10
	STS-1/VC-3	1, 2, 3	1, 2, 3
OC-12/STM-4	STS-12c/VC-4-4C	1	100
	STS-3c/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-48c/VC-4-16C	1	1000
	STS-12c/VC-4-4C	1, 13, 25, 37	100, 200, 300, 400
	STS-3c/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-192c/VC-4-64C	1	10000
	STS-48c/VC-4-16C	1, 49, 97, 145	1000, 2000, 3000, 4000
	STS-12c/VC-4-4C	1, 13, 25, 37, ... , 181	1100, 1200, 1300, 1400, 2100, 2200, ... , ... , 4300, 4400
	STS-3c/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
OC-768/STM-256	STS-192c/VC-4-64C	1, 193, 385, 577	10000, 20000, 30000, 40000
	STS-48c/VC-4-16C	1, 49, 97, 145, ... , 721	11000, 12000, 13000, 14000, 21000, 22000, ... , ... , 43000, 44000
	STS-12c/VC-4-4C	1, 13, 25, 37, ... , 757	11100, 11200, 11300, 11400, 12100, 12200, ... , ... , 44300, 44400
	STS-3c/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-3c/VC-4	1, 4, 7, 10, 13, 16, 19	110, 120, 130, 140, 210, 220, 230
	STS-1/VC-3	1, 2, 3, 4, ... , 24	111, 112, 113, 121, 122, 123, ... , 241, 242, 243

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” \(5-19\)](#).



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>Navis</i>[®] Optical EMS - <i>WaveStar</i>[®] CIT Please notice that administration, maintenance and provisioning activities via <i>Navis</i> Optical EMS are described in the separate <i>Navis</i> Optical EMS documentation set. • Alarm LEDs on the user panel • “FAULT” LED on the circuit pack faceplate (indicates the presence of <i>defects</i>, not alarms) • 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” (16-42).

Contents

WaveStar CIT visual alarm indicators	16-20

<u>NE local indications</u>	<u>16-22</u>
<u>Impact of state changes on the signalling of alarms</u>	<u>16-23</u>



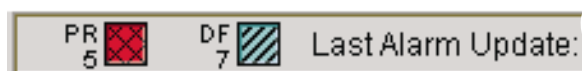
WaveStar[®] CIT visual alarm indicators

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 present on the NE at the date and time of the last update, 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 (cf. [“Alarm format preferences” \(16-13\)](#)).

These are examples of the alarm status display:



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, the **Last Alarm 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 (for example: ) to indicate the circuit pack's current alarm status.

Notice that a bell symbol will only be displayed if at least a deferred alarm is present for the corresponding circuit pack.

- Port unit LEDs

Furthermore, each port unit has an LED associated with each port which serves to indicate the alarm status of 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” \(5-8\)](#).



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” \(16-41\)](#).

Fault LED on circuit packs

A red “FAULT” LED is located on all *LambdaUnite* MSS circuit packs to indicate defects attributable to the circuit pack.

Please note that the indications via the red “FAULT” LED on the circuit pack faceplate is **controlled by defects**, not alarms (cf. [“Fault management process” \(16-4\)](#)).

The possible Fault LED states are shown in the following table.

Fault LED State	Meaning
On	indicates an equipment defect on the circuit pack
Off	indicates that no defects are present
Flashing	indicates an incoming signal defect, an external timing defect 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” \(16-50\)](#).



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” \(5-46\)](#)).

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” \(16-13\)](#).

ASAP types These ASAP types, listed in alphabetical order according to their *WaveStar* CIT representation, are defined for *LambdaUnite* MSS network elements:

ASAP Type ¹	Functional category
Automatic Protection Switch	Alarms related to Automatic Protection Switching (APS)
Data Communications Network	Alarms related to the Data Communication Network (DCN)
Environmental (Miscellaneous Discrete)	Environmental alarms (alarm conditions monitored by means of detectors connected to Miscellaneous Discrete Inputs)
Equipment unprotected	Circuit pack and other equipment alarms (unprotected components)
Equipment with Protection State Dependence*	Circuit pack and other equipment alarms (protected components)
Ethernet*	Alarms related to the transport of Ethernet data
MS-SPRing and Bilateral Switched Ring Protection Switch	Ring protection switching alarms (BLSR/MS-SPRing)
Path MSA/NIM related*	Path-related alarms (path monitoring)
Path Termination*	Path-related alarms (path termination)
SDH/SONET ports*	SDH/SONET port-related alarms
Sub-Network Connection Protection and Unidirectional Path Switched Ring	Path protection switching alarms (SNCP/UPSR)
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).

Alarm identifier “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
PSBINAPPR*	Prot. Switch Byte Inappropriate	Major
SCM*	Switch Channel Mismatch	Major
FESF*	Far End Signal Fail	Major

Notes:

1. Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present *LambdaUnite* MSS release. These alarms are prepared for future applications.

“Data Communications Network” ASAP

The following table lists the default alarm severity assignments of the “Data Communications Network” ASAP (service-independent).

Alarm identifier “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

Notes:

1. Alarms marked with an asterisk (“*”) in the “Probable cause” column

are not supported in the present *LambdaUnite* MSS release.

**“Environmental
(Miscellaneous Discrete)”
ASAP**

The following table lists the default alarm severity assignments of the “Environmental (Miscellaneous Discrete)” ASAP (service-independent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity
MISC_1	Miscellaneous Discrete Input 1	Not reported
MISC_2	Miscellaneous Discrete Input 2	Not reported
MISC_3	Miscellaneous Discrete Input 3	Not reported
MISC_4	Miscellaneous Discrete Input 4	Not reported
MISC_5	Miscellaneous Discrete Input 5	Not reported
MISC_6	Miscellaneous Discrete Input 6	Not reported
MISC_7	Miscellaneous Discrete Input 7	Not reported
MISC_8	Miscellaneous Discrete Input 8	Not reported

**“Equipment unprotected”
ASAP**

The following table lists the default alarm severity assignments of the “Equipment unprotected” ASAP (service-independent).

Alarm identifier “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
SYSCOMF	Comm Channel Failure	Major
CTLCOMF	CTL Comm Failure	Minor
BKUPMEMP*	IDE Flash Card Access Fail	Major
BKUPMEMO	NVM Shortage	Minor
CIPWRDWN	CICTL Powered Down	Minor
TIMM	TI Mismatch	Minor
CIMISS	CICTL not Present	Minor

Alarm identifier “Probable cause”	Alarm text	Alarm severity
CIF	CICTL Failure	Minor
CICOMF	CICTL Comm Failure	Minor
FANUNITMISS*	Fan Unit not Present	Critical
FANUNITCOMF	Fan Unit Comm Failure	Critical
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

Notes:

- Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present *LambdaUnite* MSS release. These alarms are prepared for future applications.

“Equipment with Protection State Dependence” ASAP

The following table lists the default alarm severity assignments of the “Equipment with Protection State Dependence” ASAP (service-dependent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
EQPT	Circuit Pack Clock Failure	Critical	Minor
CPTEMP	Unit Temperature too High	Major	Minor
PRCDRERR	Circuit Pack Type Mismatch	Major	Minor
REPLUNITMISS	Circuit Pack not Present	Critical	Minor
TXInF ¹	TXI Failure	Critical	Minor
CPFAIL	Circuit Pack Failure	Critical	Minor
PIEF	Power Interface Read Failure	Minor	Minor
PIMISS	Power Interface not Present	Major	Minor
POWF	System Power Failure	Major	Minor

Notes:

- “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).

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
VCGLOA	Loss of Alignment	Critical	Minor
VCGLOPC	Partial Transport Capacity Loss	Major	Minor
VCGLOTC	Total Transport Capacity Loss	Critical	Minor
VCGFOPT*	Source End Failure of Protocol	Major	Minor
VCGFOPR*	Sink End Failure of Protocol	Major	Minor
VCGSSF*	Server Signal Fail	Not reported	Not reported
GFPLOF	GFP Loss of Frame	Critical	Minor
LANLOS	LAN Loss of Signal	Critical	Minor
LANANM*	LAN Auto Negotiation Mismatch	Minor	Not alarmed

Notes:

- Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present *LambdaUnite* MSS release. These alarms are prepared for future applications.

“MS-SPRing and Bilateral Switched Ring Protection Switch” ASAP The following table lists the default alarm severity assignments of the “MS-SPRing and Bilateral Switched Ring Protection Switch” ASAP (service-independent).

Alarm identifier “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
RNG-OPEN	Open Ring	Major
SQMAP-CONFL	Local Squelch Map Conflict	Minor
RNG-INC	Ring Incomplete	Major
RNG-URT	Unknown Ring Type	Not alarmed

Alarm identifier “Probable cause”	Alarm text	Alarm severity
RNG-IRPM	Inconsistent Ring Protection Mode	Major
RNG-DSCVY	Ring Discovery in Progress	Not alarmed
ET-PREEMPT	Extra Traffic Preempted	Not alarmed

“Path MSA/NIM related” ASAP The following table lists the default alarm severity assignments of the “Path MSA/NIM related” ASAP (service-dependent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
AIS-P	Alarm Indication Signal	Not reported	Not reported
LOP-P	Loss of Pointer	Critical	Minor
SRM-P	Signal Rate Mismatch	Major	Minor
UNEQ-P	Unequipped	Critical	Minor
TIM-P	Trace Identifier Mismatch	Critical	Minor
EXC-P	Excessive Bit Error Ratio	Critical	Minor
DEG-P	Degraded Signal	Major	Minor
SSF-P	Server Signal Fail	Not reported	Not reported
RFI-P	Remote Defect Indication	Not reported	Not reported
PDI-P	Payload Defect Indication	Major	Minor

“Path Termination” ASAP The following table lists the default alarm severity assignments of the “Path Termination” ASAP (service-dependent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
THPSSF*	Server Signal Fail	Not reported	Not reported
THPLOP*	Loss of Pointer	Critical	Minor
THPUNEQ*	Unequipped	Critical	Minor
THPTIM*	Trace Identifier Mismatch	Critical	Minor
THPEXC*	Excessive Bit Error Ratio	Critical	Minor
THPDEG*	Degraded Signal	Major	Minor
THPRDI*	Remote Defect Indication	Not reported	Not reported
THPPLM	Payload Mismatch	Critical	Minor
VCLOM	Loss of Multiframe	Critical	Minor

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
VCSQM	Sequence Number Mismatch	Critical	Minor

Notes:

- Alarms marked with an asterisk (“*”) in the “Probable cause” column are not supported in the present *LambdaUnite* MSS release. These alarms are prepared for future applications.

“SDH/SONET ports” ASAP The following table lists the default alarm severity assignments of the “SDH/SONET ports” ASAP (service-dependent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity	
		SA	NSA
OCHLOF	OCh Loss of Frame	Critical	Minor
PREDCMLOS	Pre DCM Signal Loss	Critical	Minor
POSTDCMLOS	Post DCM Signal Loss	Critical	Minor
LOS	Loss of Signal	Critical	Minor
LOF	Loss of Frame	Critical	Minor
RSTIM	Trace Identifier Mismatch	Critical	Minor
MSEXC	Excessive Bit Error Ratio	Critical	Minor
MSDEG	Degraded Signal	Major	Minor
AIS-L	Alarm Indication Signal	Critical	Minor
MSSSF	Server Signal Fail	Not reported	Not reported
MSPSSF	Prot. Server Signal Fail	Not reported	Not reported
RFI-L	Remote Defect Indication	Not reported	Not reported
DCCRSF	RS DCC failure	– (not applicable)	Major
LIDRSM	RS Protocol Version Mismatch	– (not applicable)	Major
DCCMSF	MS DCC failure	– (not applicable)	Major
LIDMSM	MS Protocol Version Mismatch	– (not applicable)	Major

“Sub-Network Connection Protection and Unidirectional Path Switched Ring” ASAP The following table lists the default alarm severity assignments of the “Sub-Network Connection Protection and Unidirectional Path Switched Ring” ASAP (service-independent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity
PSI	Path Switch Inhibit	Not alarmed
FAILTOSW	Path Switch Denial	Not alarmed

“System Timing” ASAP The following table lists the default alarm severity assignments of the “System Timing” ASAP (service-independent).

Alarm identifier “Probable cause”	Alarm text	Alarm severity
SYNCRF	Timing Reference Failure	Major
SYNCLOSS	Loss of Synchronisation	Major
SYNCT4OUT	T4 quality insufficient	Major

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),
 - Digits (0 ... 9),
 - Hyphens (-).

Lower case letters (a ... z) may also be entered. However, no distinction is made between lower case and upper case letters.

ASAP names will always be displayed upper case.

Spaces in an ASAP name will be ignored.

Maximum number of ASAPs The total number of ASAPs is restricted to 64, including the “DEFAULT” ASAPs, and independent from the ASAP type, i.e. beyond the overall maximum number of 64, there is no specific restriction per ASAP type.

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 Alarm Severity Assignment Profile \(ASAP\)” \(5-27\)](#)
- [“Creating non-reporting Alarm Severity Assignment Profiles \(ASAPs\)” \(5-29\)](#)
- [“Modifying an existing Alarm Severity Assignment Profile \(ASAP\)” \(5-31\)](#)
- [“Assigning the same Alarm Severity Assignment Profile \(ASAP\) to all equipment components of a particular type” \(5-36\)](#)

Deleting ASAPs ASAPs which are no longer needed can be deleted.

The following general rules apply:

- The “DEFAULT” ASAPs **cannot** be deleted.
- An ASAP **cannot** be deleted if it is currently in use, i.e. assigned to any system component (a circuit pack or port for example).

Please refer to [“Deleting an Alarm Severity Assignment Profile \(ASAP\)” \(5-34\)](#).



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” \(5-39\)](#).



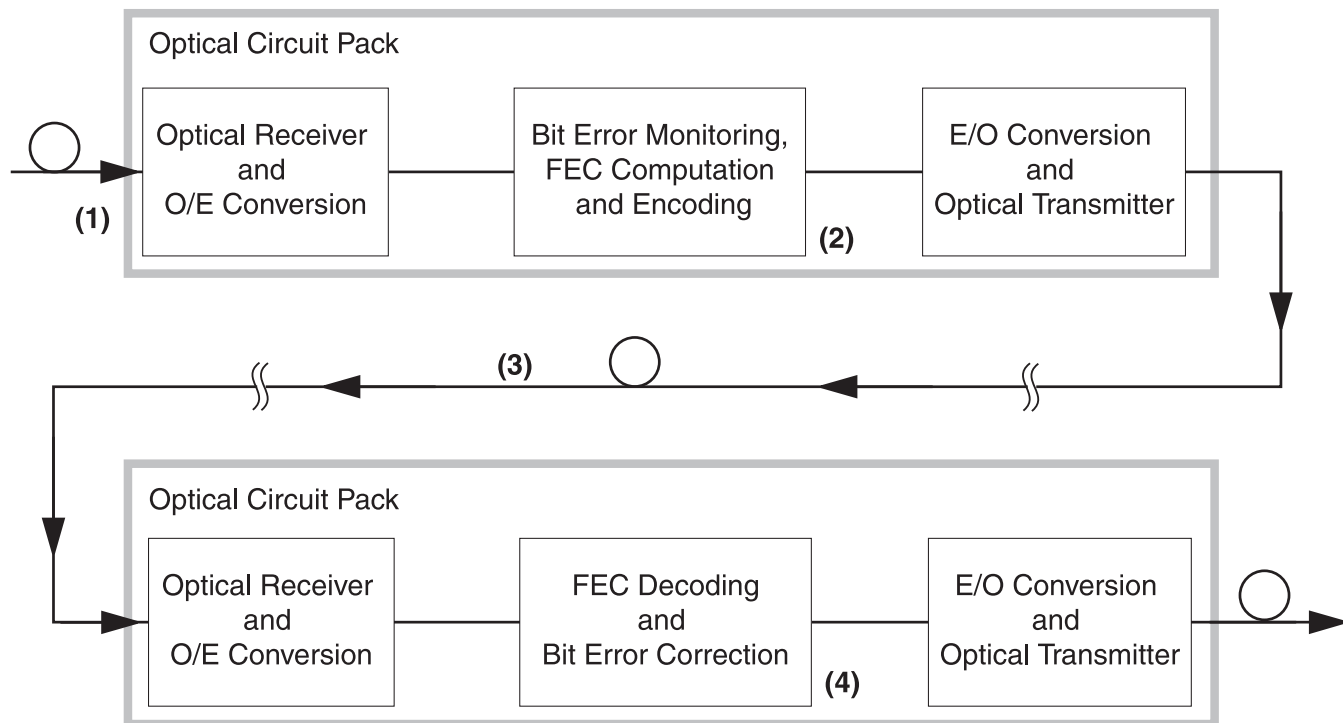
Forward error correction

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 algorithm is a 4-times bit-interleaved 2-bit error correcting Bose-Chaudhuri-Hocquenghem (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.

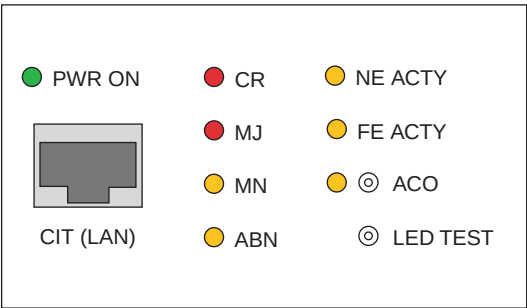
Contents

The <i>LambdaUnite</i> MSS user panel	16-41
ACO interaction with an alarm test	16-44
Circuit pack status indicators	16-46
Fan unit status indicators	16-49
Office alarm interfaces	16-50
Miscellaneous Discretes	16-52



The *LambdaUnite*TM 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” (16-42) .
MJ (red)	Indicates that at least one major alarm is present. Please refer to “User panel alarm LEDs” (16-42) .
MN (yellow)	Indicates that at least one minor alarm is present. Please refer to “User panel alarm LEDs” (16-42) .
ABN (yellow)	Indicates abnormal conditions – temporary conditions that may potentially be service affecting. Please refer to “Abnormal Conditions” (16-42) .
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” (16-42) .

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” (16-43) .
ACO	An alarm cut-off button to suppress both visual and audible alarm indications. Please refer to “Alarm acknowledgment” (16-42) .
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.

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 5 seconds. Afterwards, the LED indications reflect to actual state of the network element which may either be the same state as before the test, or a new state, if changes occurred in the meantime.

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.
-

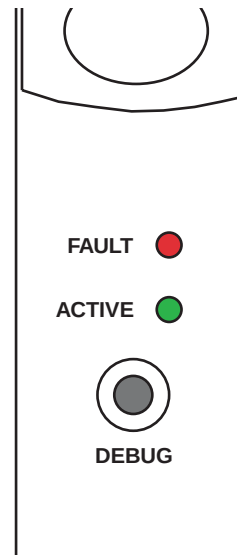
-
- 6** The control of the alarm indicators is returned to the control system to reflect the actual system status.



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.



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” \(16-47\)](#) or [“Fault LED on circuit packs” \(16-22\)](#).

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, after a delay of up to approximately 15 seconds, 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) ¹	●	—
	Initialization	—	✱
	Self-test		
	Software download		
	Failure detected during initialization, self-test or software download	●	—

Operational State	Status	“FAULT” LED	“ACTIVE” LED
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 ²	✱	–
Explanation: ● LED is continuously lit; – LED is off; ✱ LED flashes (0.5 s on, 0.5 s off)			

Notes:

1. This circuit pack state may possibly not be clearly recognizable depending on the duration of the power-up cycle and the time needed to start initialization.
2. 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 further information on *LambdaUnite* MSS circuit packs, please refer to the *LambdaUnite MSS Applications and Planning Guide*.



Fan unit status indicators

- LEDs on the fan unit** The fan unit is equipped with a red fault LED labelled “FAULT” and a green activity LED labelled “PWR ON”.
- Both LEDs are located on the rear side of the fan unit, the “PWR ON” LED on the left-hand side next to the two power supply connectors, the “FAULT” LED on the right-hand side next to the controller interface connector.
- Activity LED** The green “PWR ON” LED is lit as long as power is supplied to the fan unit by at least one of the two fan unit power feeders.
- Fault LED** The red “FAULT” LED is lit if one or more fans have failed (Fan Failure).
- Other failure conditions, like a disconnected or defective fan unit power feeder, an open circuit breaker on one of the two Power Interfaces, or a broken fuse in the fan unit power inputs, do **not** cause the red “FAULT” LED to be lit. These failure conditions are solely indicated by means of corresponding alarm messages and via the user panel alarm LEDs.
- Fan unit failure** None of the two fan unit LEDs will be lit in the case of a Fan Unit Failure.



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*.



Miscellaneous Discretes

Purpose Miscellaneous Discrete Inputs (MDIs) and Miscellaneous Discrete Outputs (MDOs) make it possible to use a *LambdaUnite*[™] MSS network element to monitor and control external equipment co-located with the system.

Miscellaneous Discrete Inputs (MDIs) *LambdaUnite* MSS systems feature a set of eight MDIs for user-defined applications.

MDIs can be used to **monitor** co-located equipment, a temperature sensor for example. MDIs can thus be used to trigger the reporting of application-specific environmental alarms.

Each MDI can be assigned a **Name** as well as a descriptive text (**Environment Message**) identifying the type of environmental alarm condition in more detail. The latter will be displayed in the *WaveStar*[®] CIT **NE Alarm List** when a corresponding alarm is present.

Furthermore, an **Environmental Alarm Inversion** parameter can be specified per MDI which indicates whether an alarm shall be generated if the relay associated to the MDI is switched on (activated) or if the relay is switched off (deactivated). A “door closed” contact for example would activate the connected MDI whereas it might be intended that an open door causes an alarm.

Miscellaneous Discrete Outputs (MDOs) *LambdaUnite* MSS systems feature a set of eight MDOs for user-defined applications. These MDOs are realized by means of relays (make contact latching type).

MDOs can be used to **control** external equipment, an additional fan or an air conditioning system for example.

Modes of operation

MDOs can be operated in two different modes:

- Automatic mode
The MDO has a probable cause assigned and becomes activated as soon as at least one alarm with this probable cause is active.
- Manual mode
The MDO is not bound to an alarm but can be activated/deactivated manually using a TL1 management command.

Transient behaviour in the case of a restart or reset

As the MDOs are initialized to a hardware-defined state after a system restart (power up) or a full reset of the Controller (CTL), they may transiently indicate a wrong state until the state before the reset is reestablished.

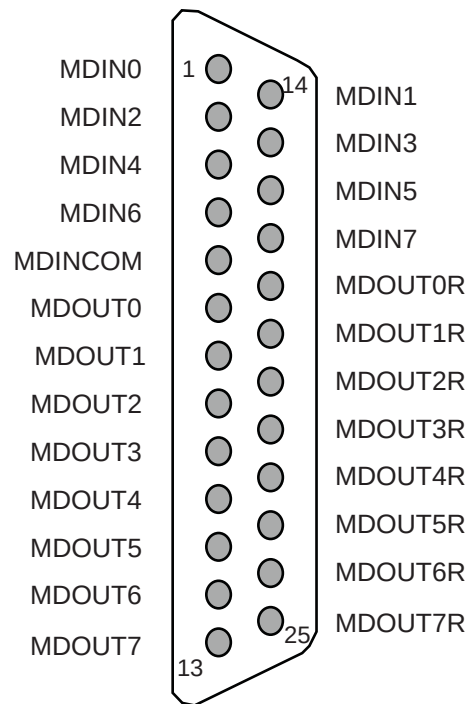
Electrical specifications

The MDI ports are sensitive to passive switches ($R_{on} \leq 50 \Omega$, $R_{off} \geq 20 \text{ k}\Omega$) or input voltages up to -72 V_{DC} (threshold voltage -3 V_{DC} to -10 V_{DC}) and are ESD safe up to 2 kV.

The MDO ports are capable to switch 500 mA at 72 V_{DC} and 2 A at 30 V_{DC} and are ESD safe up to 2 kV.

MDI/MDO interface

The MDI/MDO interface is realized on the CI-CTL (Connection Interface of the Controller) as a 25-pin female D-Subminiature connector. The pin assignment is as follows:



Pin assignment			Meaning
1		MDIN0	Miscellaneous Discrete Input 1

Pin assignment			Meaning
	14	MDIN1	Miscellaneous Discrete Input 2
2		MDIN2	Miscellaneous Discrete Input 3
	15	MDIN3	Miscellaneous Discrete Input 4
3		MDIN4	Miscellaneous Discrete Input 5
	16	MDIN5	Miscellaneous Discrete Input 6
4		MDIN6	Miscellaneous Discrete Input 7
	17	MDIN7	Miscellaneous Discrete Input 8
5		MDICOM	Miscellaneous Discrete Input - Common (connected to the negative polarity)
	18	MDOUT0R	Miscellaneous Discrete Output 1 - Return
6		MDOUT0	Miscellaneous Discrete Output 1
	19	MDOUT1R	Miscellaneous Discrete Output 2 - Return
7		MDOUT1	Miscellaneous Discrete Output 2
	20	MDOUT2R	Miscellaneous Discrete Output 3 - Return
8		MDOUT2	Miscellaneous Discrete Output 3
	21	MDOUT3R	Miscellaneous Discrete Output 4 - Return
9		MDOUT3	Miscellaneous Discrete Output 4
	22	MDOUT4R	Miscellaneous Discrete Output 5 - Return
10		MDOUT4	Miscellaneous Discrete Output 5
	23	MDOUT5R	Miscellaneous Discrete Output 6 - Return
11		MDOUT5	Miscellaneous Discrete Output 6
	24	MDOUT6R	Miscellaneous Discrete Output 7 - Return
12		MDOUT6	Miscellaneous Discrete Output 7
	25	MDOUT7R	Miscellaneous Discrete Output 8 - Return
13		MDOUT7	Miscellaneous Discrete Output 8

Provisioning MDIs and MDOs

Please refer to the following procedures for information on how to provision MDIs and MDOs:

- [“Configuring Miscellaneous Discrete Inputs” \(5-48\),](#)
- [“Configuring Miscellaneous Discrete Outputs” \(4-115\).](#)





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” \(17-3\)](#)). 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	17-3
Timing configuration	17-4
Timing quality	17-5
Timing protection	17-9
Timing with facility loopbacks	17-11
Timing slaved to MSP/APS groups	17-12

4-fiber MS-SPRing/BLSR protection switching	17-13

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)
 - An optical STM-16/OC-48 line 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 \(SDH mode\)” \(6-29\)](#) and [“Configuring the external timing input ports \(SONET mode\)” \(6-31\)](#))
- the configuration of the external output port (cf. [“Configuring the external timing output ports \(SONET mode\)” \(6-25\)](#) and [“Configuring the external timing output ports \(SDH mode\)” \(6-20\)](#))
- the selection and configuration of the timing references (cf. [“Configuring the line timing references” \(6-33\)](#))
- the configuration of the system timing, this means the configuration of the master timing generator (cf. [“Configuring the system timing” \(6-39\)](#))

□

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 (2.5 Gbit/s, 10 Gbit/s), the timing functions accept a timing reference signal from a port unit (2.5 Gbit/s, 10 Gbit/s) and derive the timing signals used to synchronize the transmission port units.
- If the **System Synchronization Status Messaging Mode** is set to **QL Enable**, then 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 the **System Synchronization Status Messaging Mode** is set to **QL Disable**, then only the priorities of the timing reference signals are evaluated.
- If all possible timing reference signals fail, then the timing generator 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”, when *LambdaUnite* MSS is in locked mode. Holdover mode is not available in free running mode.

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 Telcordia TR-1244
0010	Primary Reference Clock (PRC), acc. to ITU-T Rec. G.811	—
0100	Transit Node Clock (SSU-T), acc. to ITU-T Rec. G.812	—
0111	—	Stratum-2 clock (ST2), acc. to Telcordia TR-1244
1000	Local Node Clock (SSU-L), acc. to ITU-T Rec. G.812	—
1010	—	Stratum-3 clock (ST3), acc. to Telcordia 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 (→ **System Synchronization Status Messaging Mode**). Furthermore, you can define the quality level of the outgoing timing signal (→ **Provisioned Quality Level**).



Timing protection

Timing reference protection switching

If the **System Synchronization Status Messaging Mode** is set to **QL Enable**, then 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 the **System Synchronization Status Messaging Mode** is set to **QL Disable**, then only the priorities of the timing reference signals are evaluated.

If all possible timing reference signals fail, then 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 signals derived from the incoming STM-16/OC-48 or 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

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.

If only one cross-connection is present (worker) and the protection cross-connection is inserted, *LambdaUnite*[™] MSS is in a warm-up status for about 6 minutes. During this time the system quality is set to DNU in SDH mode or DUS in SONET mode. During this state is is not allowed to perform a manual switch command to the standby cross-connection.

Wait-to-restore time

If a timing signal is restored, then – after a defined time (wait-to-restore time, WTR) – a decision is made based the quality and priority selection criteria, which signal select. If the same signal has the best quality and/or highest priority, then the same signal will be selected, else another signal.



Timing with facility loopbacks

Overview *LambdaUnite*[™] MSS supports two types of facility loopbacks, [“Near-side facility loopbacks” \(18-49\)](#) and [“Far-side facility loopbacks” \(18-50\)](#).

When a near side facility-loopback is set, the signal received is transparently looped to the corresponding output. However the SSM received in the S1 byte of the overhead will be overwritten with the value “Do not use for synchronization (DNU/DUS)” in the outgoing S1 byte. This is done because a signal which is looped should not be used as a timing reference to avoid timing loops.

Configuration rules Consider the following configuration rules to set a facility loopback:

- When a facility loopback is set, no line timing references can be assigned.
- When a line timing reference is assigned, no facility loopbacks can be set
- Before a facility loopback can be set the port must be set out-of-service.

□

Timing slaved to MSP/APS groups

Overview When a line timing reference is assigned to a protection port of a 1+1 MSP/APS group, the system will internally reserve 2 timing references (one for the worker port and one for the protection port). For the user there is only one timing reference which is mapped to the worker port. But dependent of the protection switch status of the MSP/APS group, internal either the worker or the protection line is selected. This means that the timing follows the MSP/APS switching protocol.

If for instance the worker fibre is cut, the MSP/APS protection switch status shows an SF condition and the protection port is active. In this case timing will select the protection line as timing reference and the reference is not failed. When the timing reference is the active reference, in the outgoing S1 byte the quality DNU/DUS will be forwarded (in order to prevent timing loops when this signal is used as timing reference).

In the case that the timing reference is the active reference on a worker port of a MSP/APS group, in both worker and protection lines the quality DNU/DUS will be forwarded the outgoing S1 byte.

Configuration rules An MSP/APS group can only be provisioned successfully when no line timing reference is assigned to the protection port of the 1+1 MSP/APS group.

□

4-fiber MS-SPRing/BLSR protection switching

Overview	<i>LambdaUnite</i>[™] MSS supports two types protection switching in 4-fiber MS-SPRing/BLSR groups: • Timing slaved to the span switching protocol • Timing independent of the ring switching protocol
Timing slaved to the span switching protocol	The same as for MSP/APS groups also applies to 4-fiber MS-SPRing/BLSR groups. There are 2 MSP/APS groups (spans), an east span and a west span. So in this case timing is slaved to the span switching protocol.
Configuration rules	Consider the following configuration rules: • A 4-fiber MS-SPRing/BLSR group can only be provisioned successfully when no line timing reference is assigned to the protection port of the spans of the 4-fiber MS-SPRing/BLSR group (East/West protection port). • A line timing reference can only be assigned to the protection port of the East and West span.
Timing independent of the ring switching protocol	When line timing is used in a 4-fiber MS-SPRing/BLSR protection group, on both spans (East and West), line timing is assigned. If one of the spans is failed (say east, both the worker line and the protection line of the MSP/APS spans are failed), a transmission ring switch will occur. However timing will not follow the transmission ring switch. It will be detected that the east line timing reference is declared failed. Timing will then switch automatically to the assigned line timing reference on the west span and the ring timing will be derived via the west side of the ring. When the span failure has recovered, timing switches back to the east line timing reference of the recovered span and timing will be derived again from the east side. Please note, a span is only recovered when the worker line has no signal failure. When timing is switched back from the west side to the east side, always the worker line of the east side is selected.

□



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	18-7
Protection mechanisms	18-13
Path Protection	18-14
Line Protection	18-19
Ring Protection	18-21
Dual Node Ring Interworking (DNI)/Dual Ring Interworking (DRI) for MS-SPRing or BLSR	18-29
DNI/DRI SNCP or UPSR	18-35
DNI/DRI between MS-SPRing and SNCP or BLSR and UPSR	18-36
Gigabit Ethernet Interface	18-43
Facility loopback	18-49
Protection configurations	18-52



Cross-connection management

Overview The *LambdaUnite*[™] MSS add/drop multiplexer in its basic configuration is a single shelf that interfaces optical STM-1/OC-3, STM-4/OC-12, STM-16/OC-48, STM-64/OC-192 and STM-256/OC-768 lines to an SDH/SONET-standard MS-SPRing/BLSR 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. The following types of port protection groups are defined:

- 4-fiber MS-SPRing port protection group used for STM-64 1+1 MS-SPRing
- 4-fiber MS-SPRing port protection group used for STM-64 1+1 MS-SPRing Transoceanic Protocol
- 2-fiber MS-SPRing port protection group used for STM-256, STM-64 and STM-16 1+1 MS-SPRing
- 1+1 MSP port protection group used for STM-256, STM-64, STM-16, STM-4 and STM-1 1+1 Multiplex Section Protection (MSP)
- 2-fiber BLSR port protection group used for OC-768, OC-192 and OC-48 1+1 BLSR
- 4-fiber BLSR port protection group used for OC-192 1+1 BLSR
- 1+1 APS port protection group used for OC-768, OC-48, OC-48, OC-12 and OC-3 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/STS-1 or VC-4/STS-3 within an STM-N/OC-M port.

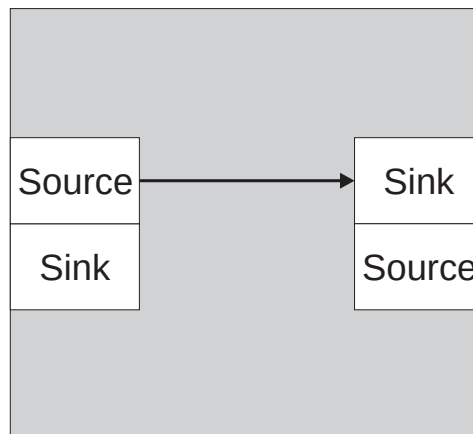
Cross-connection A reconfigurable SDH/SONET path-level interconnection within a network element between input and output tributaries of specific ports.

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.

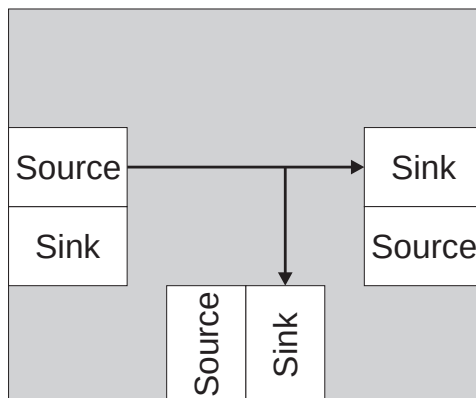
Cross-connection types

All meaningful cross-connection types can be reduced to three basic types:

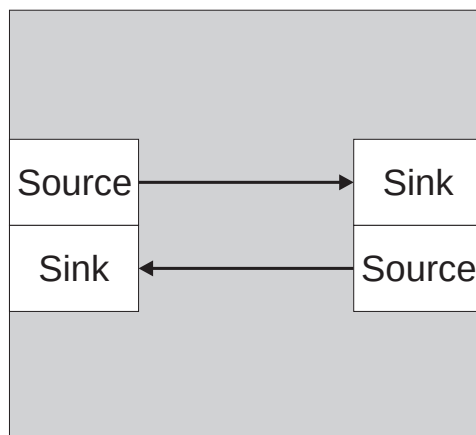
- Unidirectional point-to-point connection



- Unidirectional path protected connection



- 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
- 1-way path protected (DRI/DNI applications only)
- DRI/DNI (bidirectional) with four nodes
- DRI/DNI (bidirectional) with collapsed nodes
- Bidirectional Sub-Network Connection Protection (SNCP)

- Unidirectional Path Switched Ring UPSR
- Ring-to-ring SNCP/UPSR

Transmission interfaces *LambdaUnite* MSS includes the following optical port units:

Interface type	Transmission rate	Wavelength
Optical	STM-256/OC-768	1.5 long reach
		1.5 μm (intermediate reach)
		1.3 μm (intra office)
		OLS 800 G compatibel
		passive WDM compatible
		passive WDM compatible
	STM-64/OC-192	1.5 μm (intermediate reach)
		1.3 μm (intra office)
		OLS 800 G compatibel
		passive WDM compatible
		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 *LambdaUnite* 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 *LambdaUnite* 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 *WaveStar*® TDM 10G, *WaveStar* ADM-16/1, *WaveStar* BandWidth Manager, *Metropolis*™ DMX, *WaveStar* OLS 1.6T, *WaveStar* LambdaXtreme and *WaveStar* LambdaRouter systems today and in the future.



Cross-connection wizard

Overview	Cross-connections may be configured using the <i>WaveStar</i> ® 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. Rolling a Cross Connection is a special case of deleting a Cross Connection: a roll operation consists of moving the input (source) of an existing leg of a one-way or two-way point-to-point cross-connection from the current input (source) tributary to a new input (source) tributary, while leaving the output tributary unchanged.
- **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” \(15-9\)](#) 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 BLSR/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 or a protection channel.

Types The following types of network protection switching can be realized:

- STM-256, STM-64, STM-16 2-fiber Multiplex Section-Shared Protection Ring (MS-SPRing) or OC-768, OC-192, OC-48 2-fiber Bidirectional Line Switched Rings (BLSR)
- STM-64 4-fiber Multiplex Section-Shared Protection Ring (MS-SPRing), STM-64 4-fiber MS-SPRing transoceanic protocol or OC-192 4-fiber Bidirectional Line Switched Rings (BLSR)
- Multiple MS-SPRing/BLSR protection
- Sub-Network Connection Protection (SNCP) or Unidirectional Path Switched Rings (UPSR)
- STM-256, STM-64, STM-16, STM-4, STM-1 1+1 Multiplex Section Protection (MSP) or OC-768, OC-192, OC-48, OC-12, OC-3 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 (SF) 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.

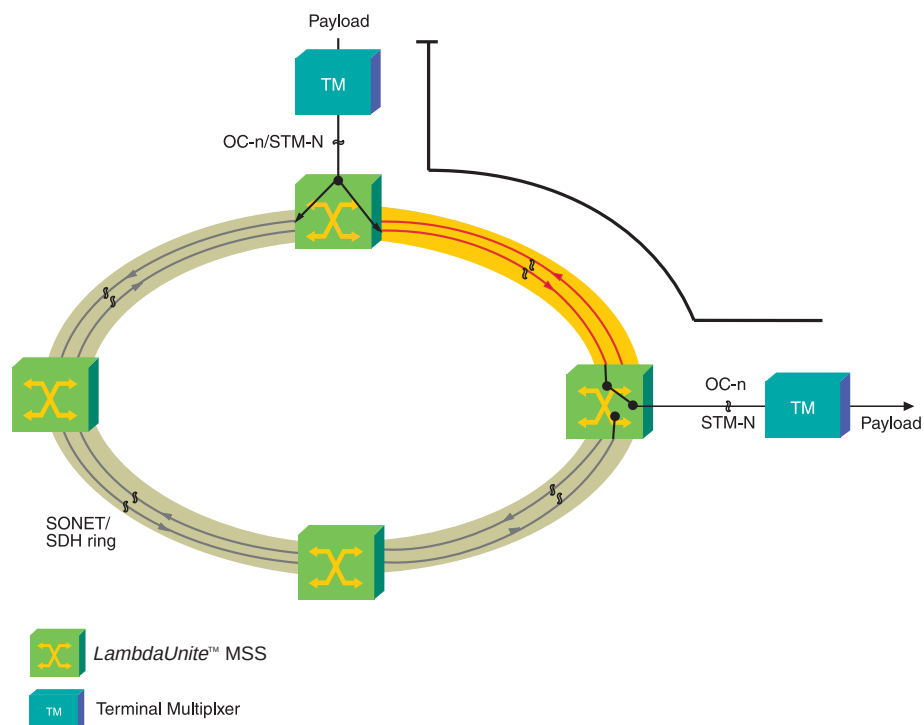
LambdaUnite MSS supports UPSR protection, also within logical ring applications.

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.

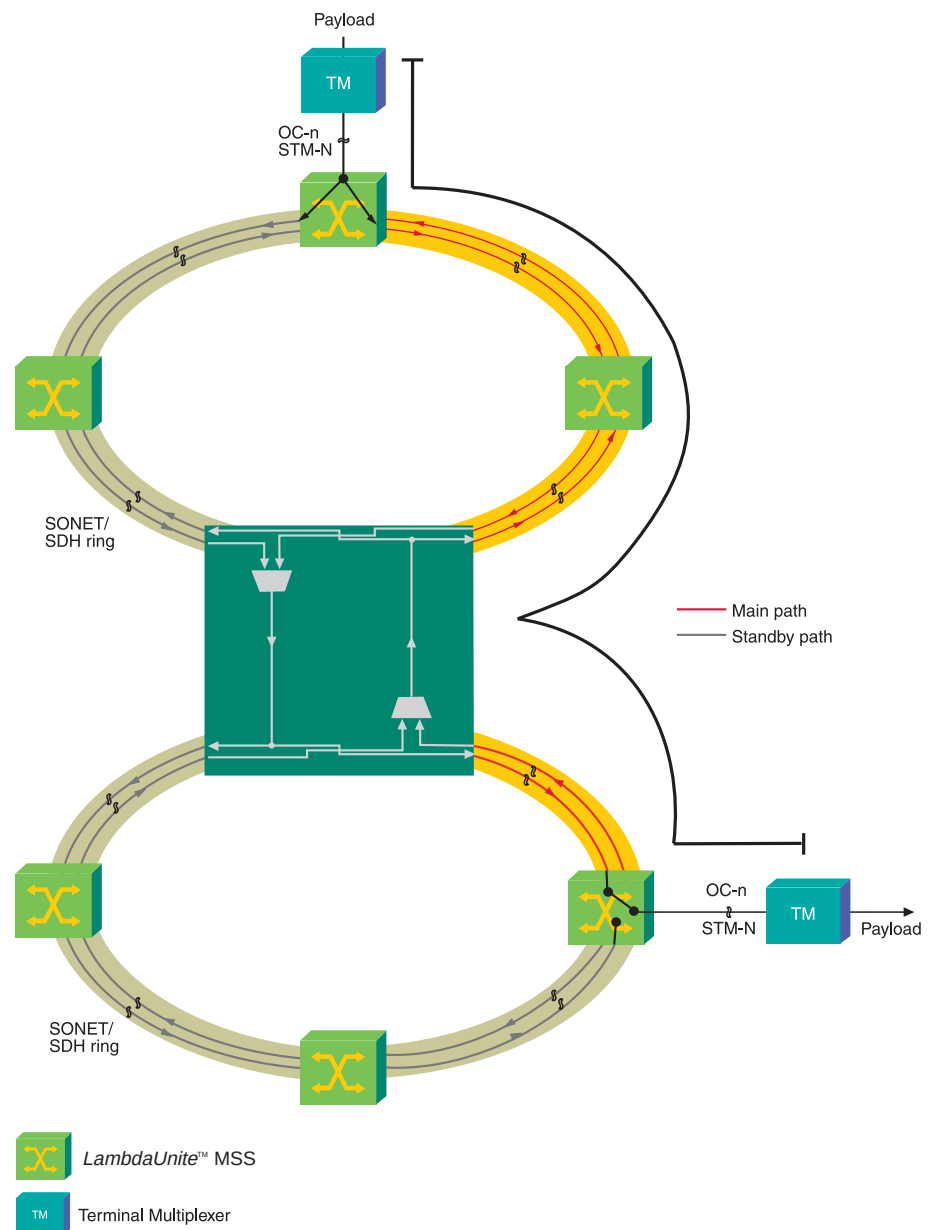
The following figure shows an example of a single ring UPSR/SNCP application. Path 1 is the working (main) path, path 2 is the protection (standby) path in this example. The path termination is always outside

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 *Navis*® Optical EMS:
- 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.

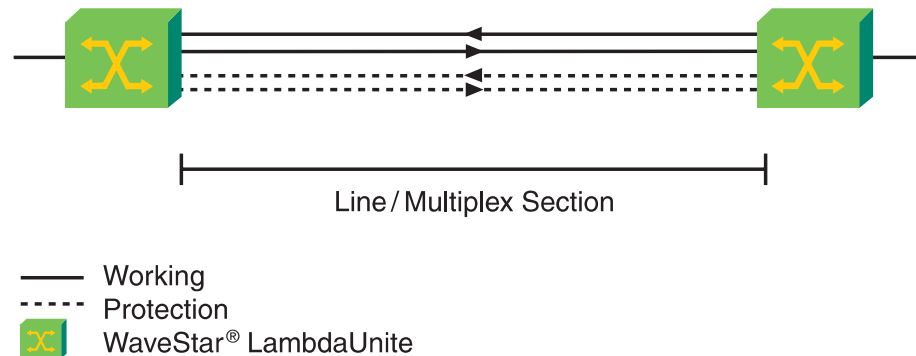
- SDH: 1+1 Multiplex Section Protection (MSP) on STM-256, STM-64, STM-16, STM-4 and STM-1 interfaces
- SONET: 1+1 Linear Automatic Protection Switch (APS) on OC-768, OC-192, OC-48, OC-12 and OC-3 interfaces

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 MSP functional block after evaluation of the SOH (section overhead):

- **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 *LambdaUnite* 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 MS-SPRing protection schemes can be configured:

- 2-fiber MS-SPRing on STM-256, STM-64 and on STM-16 interfaces
- 4-fiber MS-SPRing on STM-64 interfaces
- 4-fiber MS-SPRing with transoceanic protocol on STM-64 interfaces

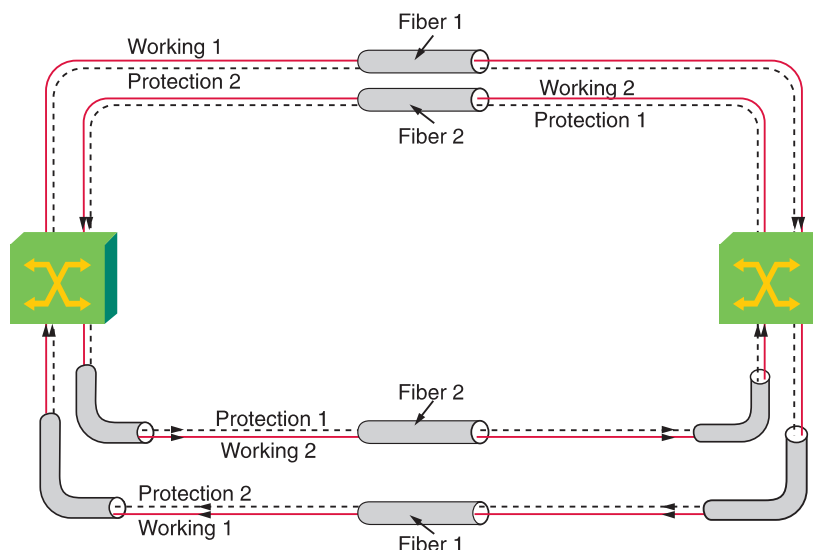
The protection scheme complies with ITU-T Rec. G.841 and provides in a future release also “extra traffic” on STM-64 and STM-16 interfaces in the MS-SPRing configuration. 4-fiber MS-SPRing for the STM-256 and on the STM-16 interfaces will be supported in future.

BLSR The following BLSR protection schemes can be configured:

- 2-fiber BLSR on OC-768, OC-192 and on OC-48 interfaces
- 4-fiber BLSR on OC-192 interfaces

The protection scheme complies with the ANSI T1.105.01 Standard and provides in a future release also pre-emptible protection access (PPA, refer to [“Pre-emptible protection access or extra traffic” \(18-25\)](#)). 4-fiber BLSR for the OC-768 and on the OC-48 interfaces will be supported in future.

Traffic disposition The following figure shows working and protection traffic disposition in a *LambdaUnite* MSS 2-fiber MS-SPRing/BLSR.



 *LambdaUnite*™ MSS

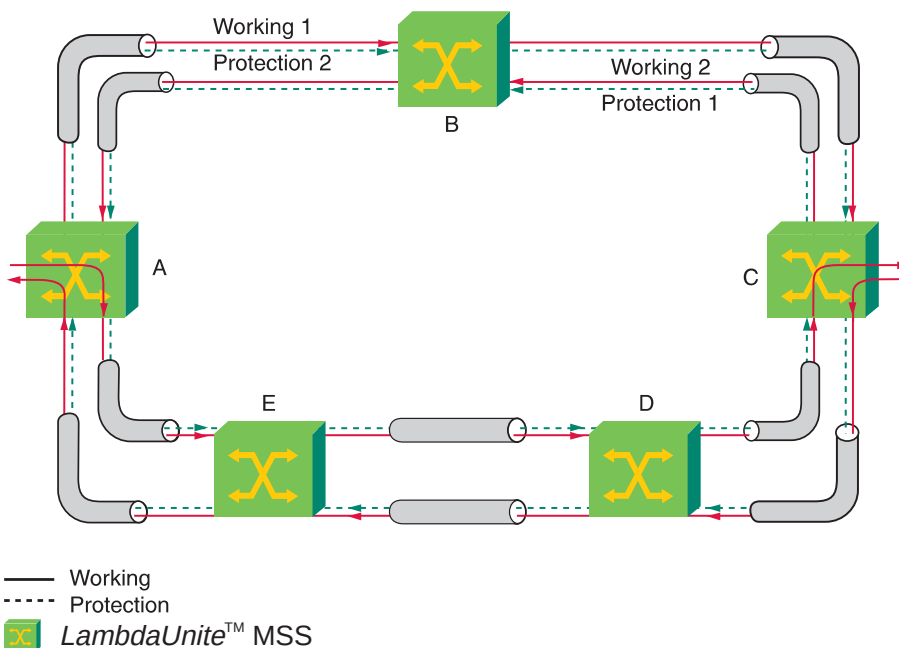
Self-healing rings *LambdaUnite* MSS MS-SPRings/BLSRs are self healing, that means transport is automatically restored after node or fiber failures.

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” \(18-23\)](#) and [“Fiber cut example” \(18-24\)](#).)

Traffic flow example

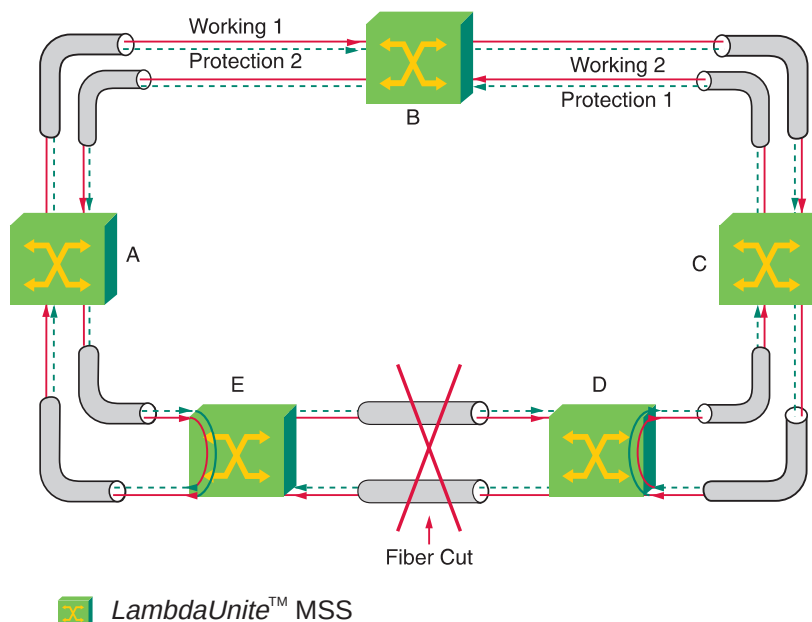
The following figure shows normal (non-protection-switched) traffic flow in a *LambdaUnite* MSS 2-fiber MS-SPRing/BLSR.

**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” \(18-24\)](#).) 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.

**Protection traffic flow**

In [“Fiber cut example” \(18-24\)](#), 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.

Pre-emptible protection access or extra traffic

Pre-emptible Protection Access (PPA) or extra traffic is a feature using the protection capacity of a BLSR or MS-SPRing in order to carry some extra “low priority” traffic. *LambdaUnite* MSS offers PPA / extra traffic in a future release in all supported ring protection features as an economical way to obtain more capacity for traffic that does not need to be protected. If a failure occurs, the protection capacity is taken back for normal protection use by the ring, and the low priority traffic is dropped.

Transoceanic protocol

A special feature of a future release of *LambdaUnite* MSS for very long-haul 4-fiber MS-SPRing applications is the transoceanic protocol. It shortens the protection path in rings, avoiding loops over very long distance spans. Thus it greatly reduces the impact of propagation delay on the signal quality, and it saves fiber resources.

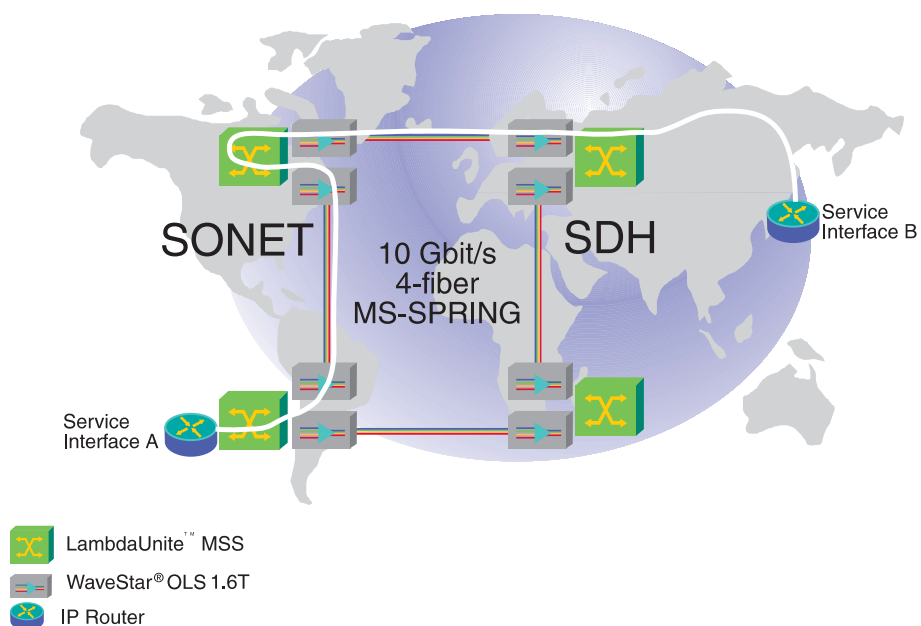
LambdaUnite MSS supports 4-fiber MS-SPRing transoceanic protocol protection schemes on the 10-Gbit/s interfaces. The protection scheme complies with ITU-T Rec. G.841.

Important! When using transoceanic protocol in combination with Time Slot Interchange (TSI) a significant increase of the restoration path length can occur for ring switching (the problem does not exist for span switching). Whether this effect occurs depends on the relative position of the failed span, the affected circuit, and the position of the TSI node. Therefore the configuration of TSI together with MS-SPRing transoceanic protocol is not recommended.

Transoceanic principle

The following figure provides a schematic view of *LambdaUnite* MultiService Switch (MSS) in a 4 fiber MS-SPRing very long distance configuration. The MS-SPRing is composed of four *LambdaUnite* MultiService Switch (MSS) elements. Under normal

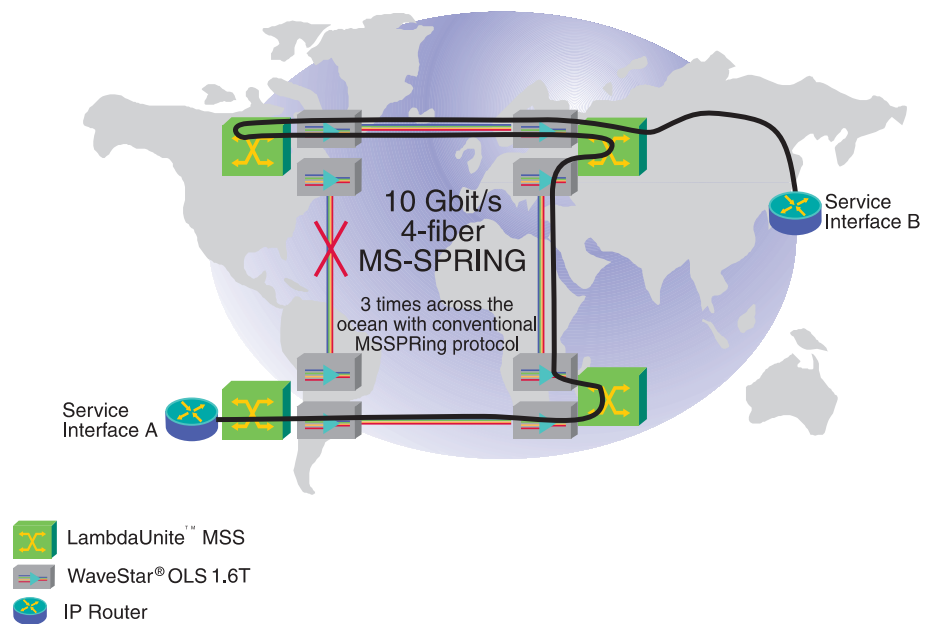
conditions (MS-SPRing idle) the traffic is routed from service interface A over two very long distance spans to service interface B.



Plain MS-SPRing switching case

The figure below shows the traffic flow in the MS-SPRing protection condition (switching case) **without** transoceanic protocol. In case of a

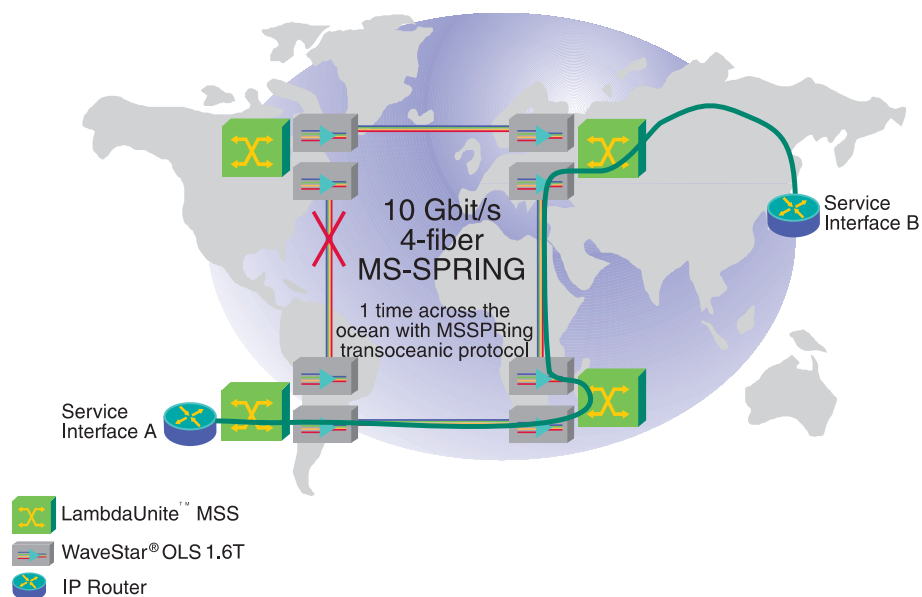
complete fiber cut as indicated by the red cross, the traffic is carried **three times across the ocean**.



MS-SPRing with transoceanic protocol, switching case

In the protection condition (switching case) **with** transoceanic protocol, the traffic **passes the ocean only once**, running through **two very long distance spans** only, as shown in the following figure.

LambdaUnite MultiService Switch (MSS) routes the traffic directly to the service interface B, avoiding the loop over the ocean.



In this way *LambdaUnite* MultiService Switch (MSS) in the MS-SPRing with transoceanic protocol shortens the protection path strikingly, improving significantly the signal quality and increasing the performance of fiber resources.

□

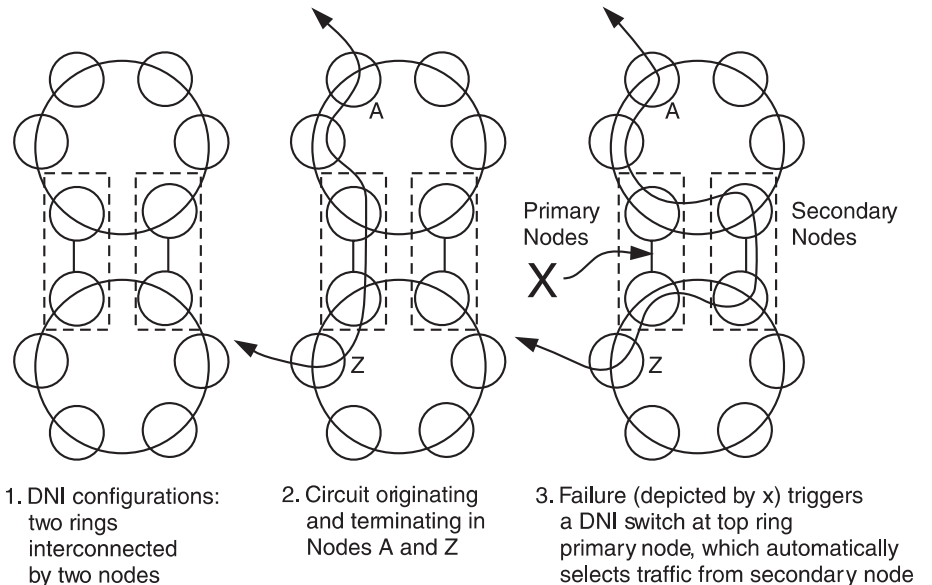
Dual Node Ring Interworking (DNI)/Dual Ring Interworking (DRI) for MS-SPRing or BLSR

Overview	Dual node ring interworking (DNI) and dual ring interworking are configurations that provide path-level protection for selected STM-N or OC-M circuits that are being carried through two rings. Protection for the route between the two rings is provided by interconnecting the rings at two places. Each circuit that is provisioned with DNI/DRI protection is dual-homed, meaning it is duplicated and subsequently terminated at two different nodes on a ring. The two interconnecting nodes in each ring do not need to be adjacent.
DNI/DRI protection	The self-healing mechanisms of the two rings remain independent and together protect against simultaneous single failures on both rings (not affecting the interconnections). The DNI/DRI configuration additionally protects against failures in either of the interconnections between the rings, whether the failure is in a facility or an interconnection node.
Transoceanic protocol	DNI is not yet supported in a 4-fiber MS-SPRing transoceanic protocol.
Interworking	All <i>LambdaUnite</i>[™] MSS tributary interfaces (STM-256, STM-64, STM-16, STM-4 and STM-1, OC-3, OC-12, OC-48, OC-192, OC-768) can support dual node ring interworking. A <i>LambdaUnite</i> MSS ring can interwork with MS-SPRing/BLSR, including rings using • <i>WaveStar</i>[®] TDM 10G • <i>LambdaManager</i>[™] Terabit MultiService Switch (TMSS) • <i>Metropolis</i>[™] DMX Access Multiplexer • <i>WaveStar</i> BandWidth Manager • <i>LambdaUnite</i> MultiService Switch (MSS) • <i>WaveStar</i> ADM16/1 STM-16 interfaces Additionally, there can be intermediate network elements in the interconnection routes between the two rings.

- Primary and secondary nodes** In the MS-SPRing, a bidirectional DNI-protected circuit to and from the terminating node is added and dropped at both a primary node and a secondary node, both of which interconnect with the other network. The primary and secondary nodes are defined and provisioned on a per-circuit basis.
- Drop and continue** *LambdaUnite* MSS supports the drop and continue method of DNI, in which the primary node is located between the terminating node and the secondary node and performs the drop-and-continue and path-selection functions. The primary node drops the circuit in the direction of the other network and also continues (bridges) the circuit to the secondary node. The secondary node drops the circuit in the direction of the other network and adds the circuit from the other network in the direction of the terminating node. The primary node either adds the circuit received on its tributary interface from the other network, or else passes through the duplicate signal received on the line from the secondary node, depending on standards-compliant path selection criteria.

Protection switching example

The following graphic illustrates a failure of the interconnection to a primary node at the point labeled “X” in the figure. The failure results in a DNI switch at the primary node in the top ring. A DNI protection switch in a *LambdaUnite* MSS occurs in ≤ 50 milliseconds (not counting the detection time) plus a provisionable hold-off time nominally of 100 milliseconds. The graphic shows a DNI configuration transporting traffic between nodes A and Z.



Sdh-10gapog-006

Types of connection

The two types of connections shown in Example: DRI/DNI via OC-3/STM-1 tributaries are

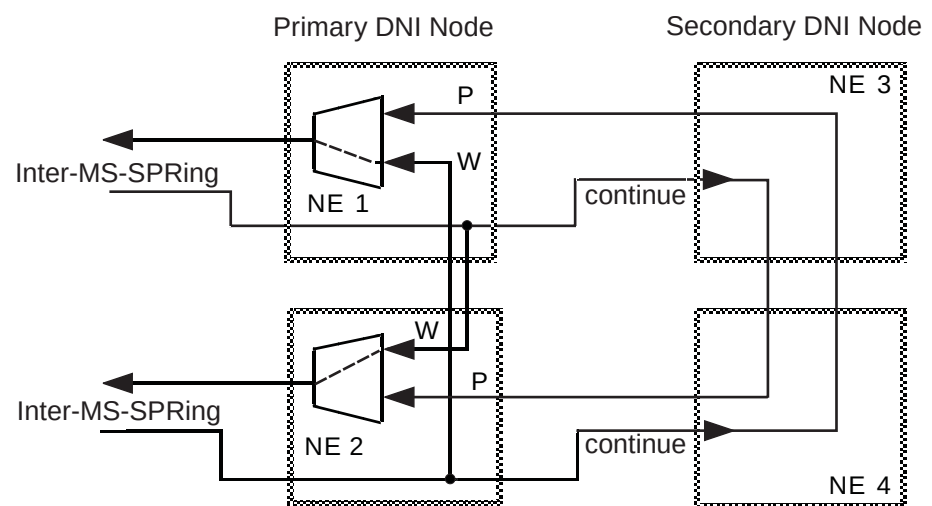
- a direct intraoffice connection between the primary nodes, Node 1 and Node 2, at the first central office (CO 1).
- an optically extended, direct secondary connection between the secondary nodes (Node 3 at the second central office (CO 2) and Node 4 of the *WaveStar* ADM16/1 2.5 Gbit/s ring). This type of connection is achieved through the 155 Mbit/s interfaces at the interconnected nodes and can go through other equipment.

Both types of connection can be used in either primary or secondary nodes.

Failure conditions In the illustrated configuration *LambdaUnite* MultiService Switch (MSS) protection switching results from the following failure conditions (grouped by priority, from highest to lowest):

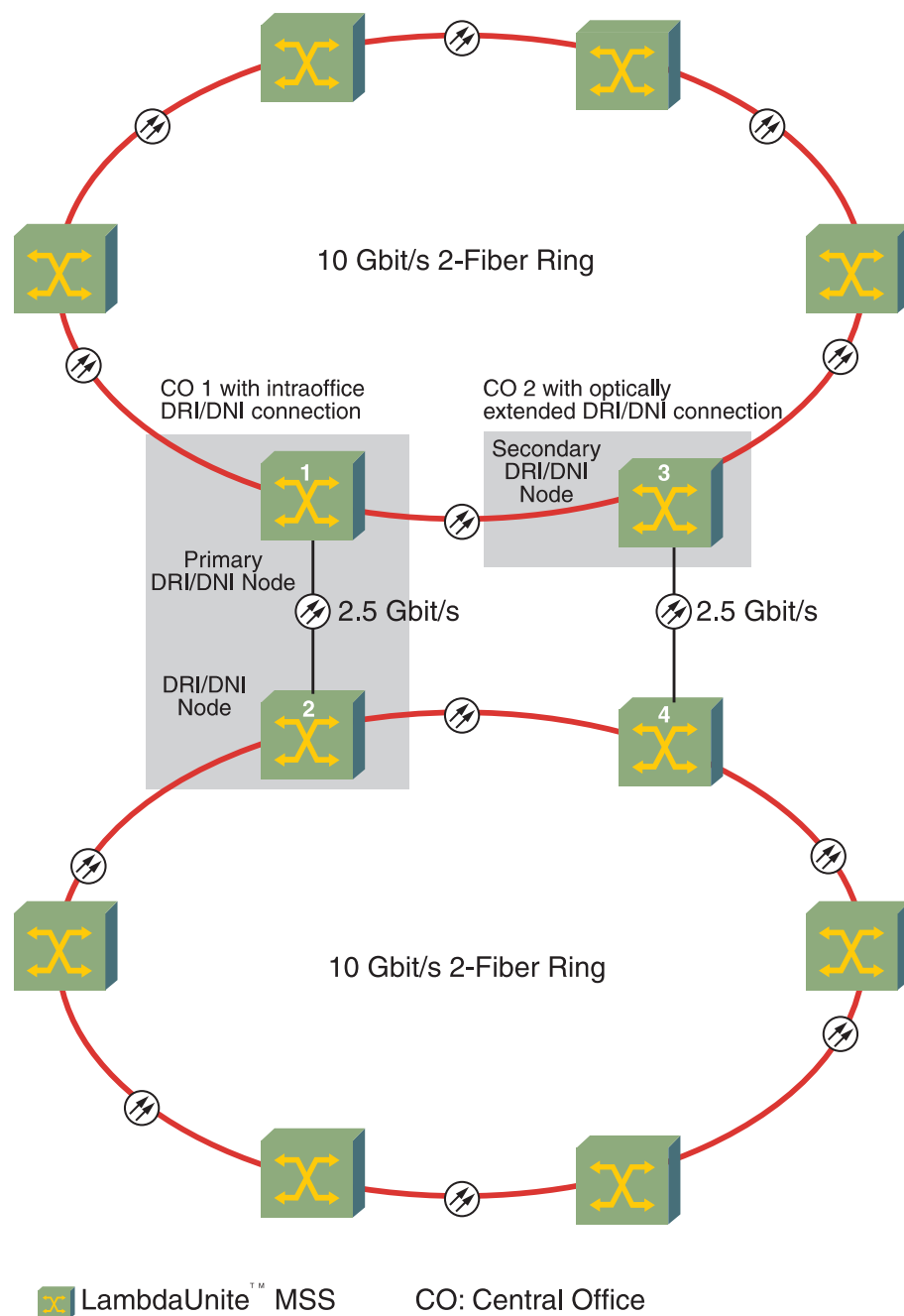
- LOP, P-AIS, or Unequipped
- Excessive Bit Error Ratio (EXC)
- Signal Degrade (DEG)

Implementation of the switch The following figure shows a detailed implementation of a protection switch in NE 1 and NE 2.

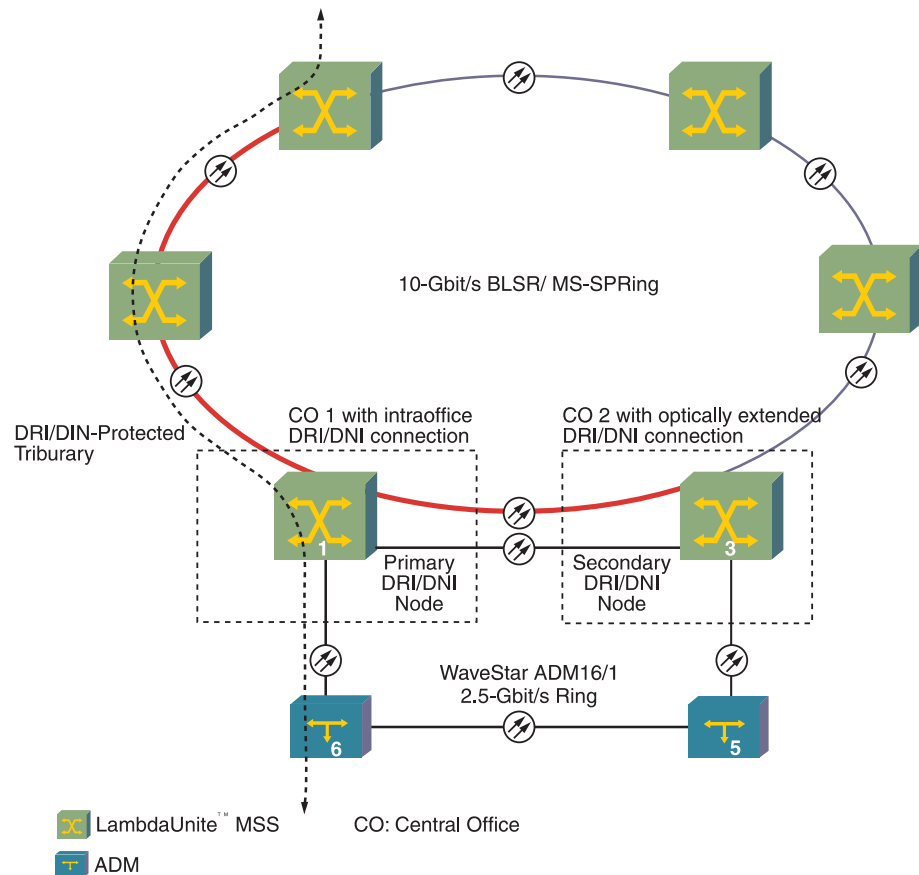


**Example: DRI/DNI via
OC-3/STM-1 tributaries**

The following figure illustrates a DRI/DN Iconfiguration that uses
2.5-Gbit/s interfaces between two *LambdaUnite* MSS 10-Gbit/srings.



Collapsed nodes A further, more sophisticated, possibility is to use the *LambdaUnite* MultiService Switch (MSS) itself as the DNI node. By means of the STM-16 interfaces, the STM-16 ring can be directly connected to the *WaveStar* TDM 10G (STM-64), as depicted in the following graphic. So, the complete DNI node is included in one network element.



DNI/DRI SNCP or UPSR

Overview	<i>LambdaUnite</i> [™] MSS supports DNI/DRI between two SNCP or UPSR protected rings.
Related Information	For related information please refer to “SNCP” (18-14) and “UPSR” (18-15) .
SDH Dual node ring interworking (DNI) for SNCP	<i>LambdaUnite</i> MSS supports SDH dual node interworking (DNI) for the purpose to protect between two SNC/I/N protected rings. The DNI feature is compliant with ITU-T Rec. G.842 standard. It provides a service selector for each VC-N tributary provisioned for DNI. The service selector selects the better of two received path-level signals in accordance with a given hierarchy of conditions. These conditions include VC Path Signal Fail. Multiple DNIs (up to the maximum system capacity) are supported.
SONET Dual ring interworking (DRI) for UPSR	<i>LambdaUnite</i> MSS supports SONET dual ring interworking (DRI) for the purpose to protect between two UPSR protected rings. The DRI feature is compliant with Telcordia GR-1400-CORE chapter 4.6 standard. It provides a service selector for each STS-M tributary provisioned for DRI. The service selector selects the better of two received path-level signals in accordance with a given hierarchy of conditions. These conditions include STS Signal Fail and PDI-P (Payload defect indicator path level), for drop and continue. Multiple DRIs (up to the maximum system capacity) are supported.

□

DNI/DRI between MS-SPRing and SNCP or BLSR and UPSR

Overview *LambdaUnite*[™] MSS supports DNI/DRI with the Drop-and-Continue method between a MS-SPRing/BLSR and a SNCP/UPSR ring.

Benefits This feature allows for

- highly survivable services where circuits are carried through interconnected rings with different protection schemes
- advanced networking capabilities with a single network element that supports OC-48/STM-16, OC-192/STM-64 and OC-768/STM-256 rings and interconnects traffic directly from one ring to another.

Transoceanic protocol DNI is not yet supported in a 4-fiber MS-SPRing transoceanic protocol.

Concept The ring interworking between a MS-SPRing/BLSR and a SNCP/UPSR ring provides a high degree of protection of the traffic crossing from one ring to the other.

It is capable of protecting against the failure of

- one interconnecting node
- two interconnecting nodes (each on different rings, but on the same interconnect)
- the connection between two interconnecting nodes.

Note that, within the MS-SPRing/BLSR, any line or node failure (including interconnecting node) will be protected at Multiplex Section level by the standard MS-SPRing/BLSR scheme, as described in ITU-T Recommendation G.842. The BLSR DRI feature is compliant with Telcordia GR-1230-CORE, GR-1400-CORE and ANSI T1.105.01

There are two variants of interconnection between rings. The two interconnected rings being in

- the same network element or
- in different network elements.

The SNCP and MS-SPRing behave as described in ITU-T Recommendation G.841. The MS-SPRing is either a STM-256, STM-64 or a STM-16 2-Fiber MS-SPRing. The SNCP ring is either a

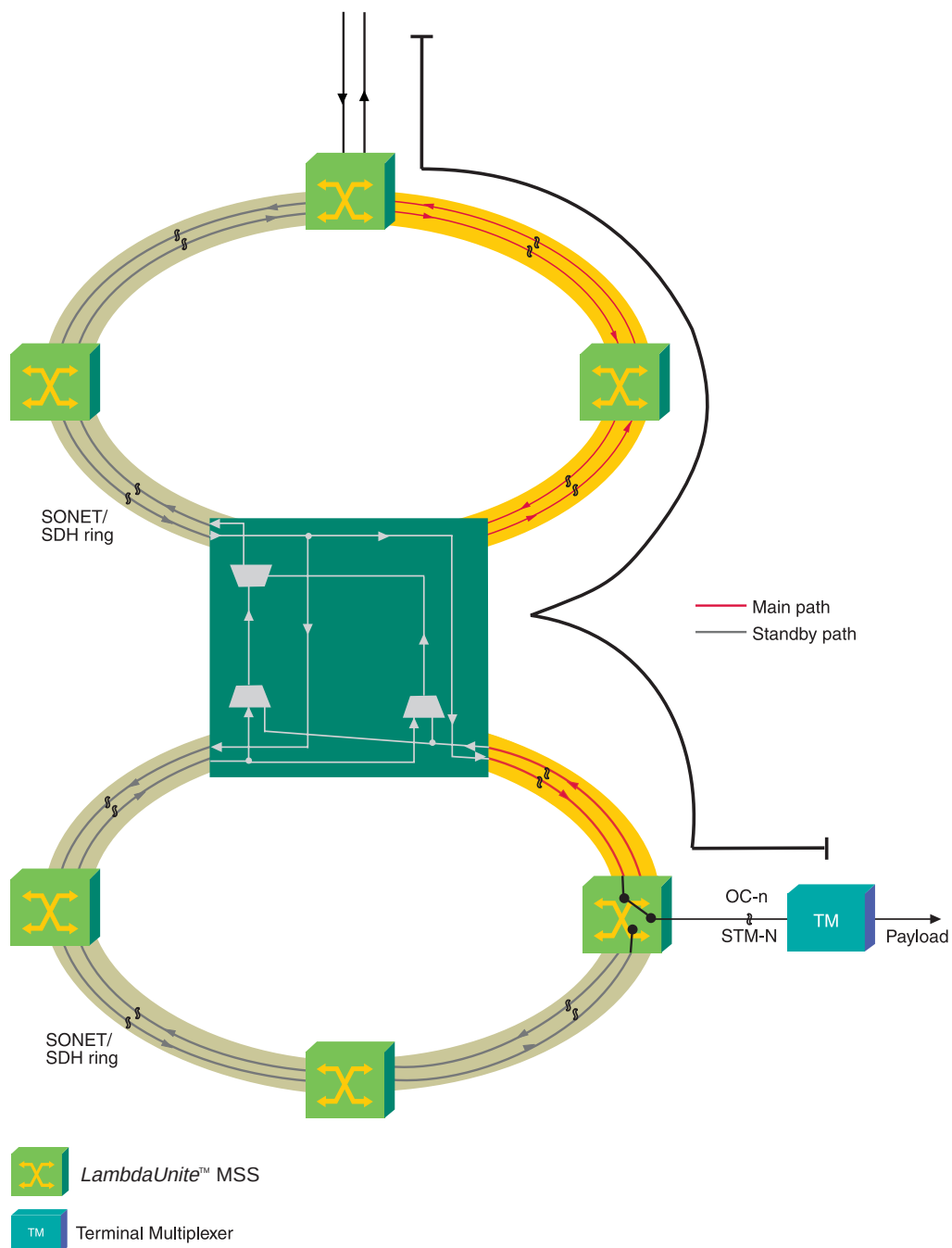
STM-256, STM-64, a STM-16, a STM-4 or an optical STM-1 SNCP ring.

The following combinations of ring interworking between a MS-SPRing and a SNCP ring are supported:

- STM-256 MS-SPRing with either STM-64 or STM-16 or STM-4 or optical STM-1 SNCP ring.
- STM-64 MS-SPRing with either STM-64 or STM-16 or STM-4 or optical STM-1 SNCP ring.
- STM-16 MS-SPRing with either STM-64 or STM-16 or STM-4 or optical STM-1 SNCP ring.
- STM-64 MS-SPRing with STM-64 SNCP ring, with both rings in separate nodes.

Both MS-SPRing/BLSR and SNCP/UPSR ring support VC-3, VC-4, VC-4-4c and VC-4-16c, VC-4-64c, STS-1, STS-3, STS-12, STS-48, STS-192, signal rates. The interconnection between rings can be done at any of these rates. The ring interworking does not require inter-ring signalling. Ring interconnection may occur among multiple rings.

Functional Details The following figure shows in more detail the interworking between the two rings (one MS-SPRing and one SNCP ring) in different network elements.



MS-SPRing Nodes

The MS-SPRing nodes support the Drop-and-Continue method, i.e.

- in one direction, the traffic is extracted from a working channel on the ring (Drop), and transmitted towards the opposite side on the ring (Continue);
- in the other direction, the signal is selected from either a traffic entering the ring (Add), or a channel from one side on the ring (Continue), and it is transmitted towards the opposite side on the ring.

The selector is called ring interworking service selector. The interconnecting node providing the Drop-and-Continue function for a tributary is called the primary node for this tributary.

The Continue traffic is only carried over the working bandwidth between the primary and secondary nodes, i.e. the channel assignment (timeslot) on the multiplex section used between the primary and secondary nodes is the same as that used between the primary and terminating nodes. The Drop-and-Continue on the protection bandwidth is not supported in this release.

The ring interworking service selector in the primary node is used to protect against ring interconnection failures. It protects at path level, based on path defects detection. It supports the SNC/N protection type only, and operates in either the revertive or the non-revertive mode. By default, it operates in the revertive mode, with a Wait-to-Restore time of 5 minutes. In other words, the ring interworking service selector shall behaves just like any other path selector.

The service selector in the primary node can be operated by the user.

The ring interworking service selector in the primary node behaves independently of the MS-SPRing scheme. Though these two protection mechanisms (i.e. path protection and MS-SPRing) are cascaded back-to-front in a primary node, they do not interfere since they do not protect at the same level. Therefore it is required to support a hold-off time for the service selector in order to avoid a double protection (hence a double transmission hit) in some failure scenarios (like a line failure between the primary and secondary nodes). The default hold-off time is 100 ms.

The hold-off time to the ring interworking service selector is also required to avoid propagation of switching from one ring to the other (e.g. a path protection switch in the SNCP ring leading to a service selector switch at the primary node in the other ring).

An interconnecting node failure is protected at Multiplex Section level by the standard MS-SPRing scheme.

The two interconnecting nodes (i.e. the primary and secondary nodes) within the MS-SPRing do not need to be adjacent.

SNCP Ring Nodes

The SNCP Ring nodes support the Drop-and-Continue method. Note that the connections for this Drop-and-Continue method differ from that used in a MS-SPRing interconnecting node (primary node). For each direction of transmission in the SNCP ring, the signal is dual-fed from the terminating (source) node around both sides of the ring. When each of the dual-fed signals hits an interconnection node, it is dropped at that node and continued onto the other interconnection node using drop-and-continue. Thus, each interconnection node can select from two signals sent on a different way around the ring. The output of the selector in each interconnection node is then transmitted to the other ring (MS-SPRing). In the other direction, the signal coming from the other ring (MS-SPRing) is transmitted towards the terminating (sink) node, away from the other interconnection node. Finally, the terminating (sink) node makes the selection between the two signals from the two directions around the ring. Due to the symmetry of this scheme, the two interconnecting nodes are completely equivalent.

The path selector in the interconnecting node supports the SNC/N protection type only, and operates in either the revertive or the non-revertive mode. By default, it operates in the revertive mode, with a Wait-to-Restore time of 5 minutes. In other words, the ring interworking service selector behaves just like any other path selector.

The path selector in the interconnecting node can be operated by the user.

A hold-off time to the path selector avoids propagation of switching (i.e. one protection switch leading to another). The default hold-off time is 100 ms.

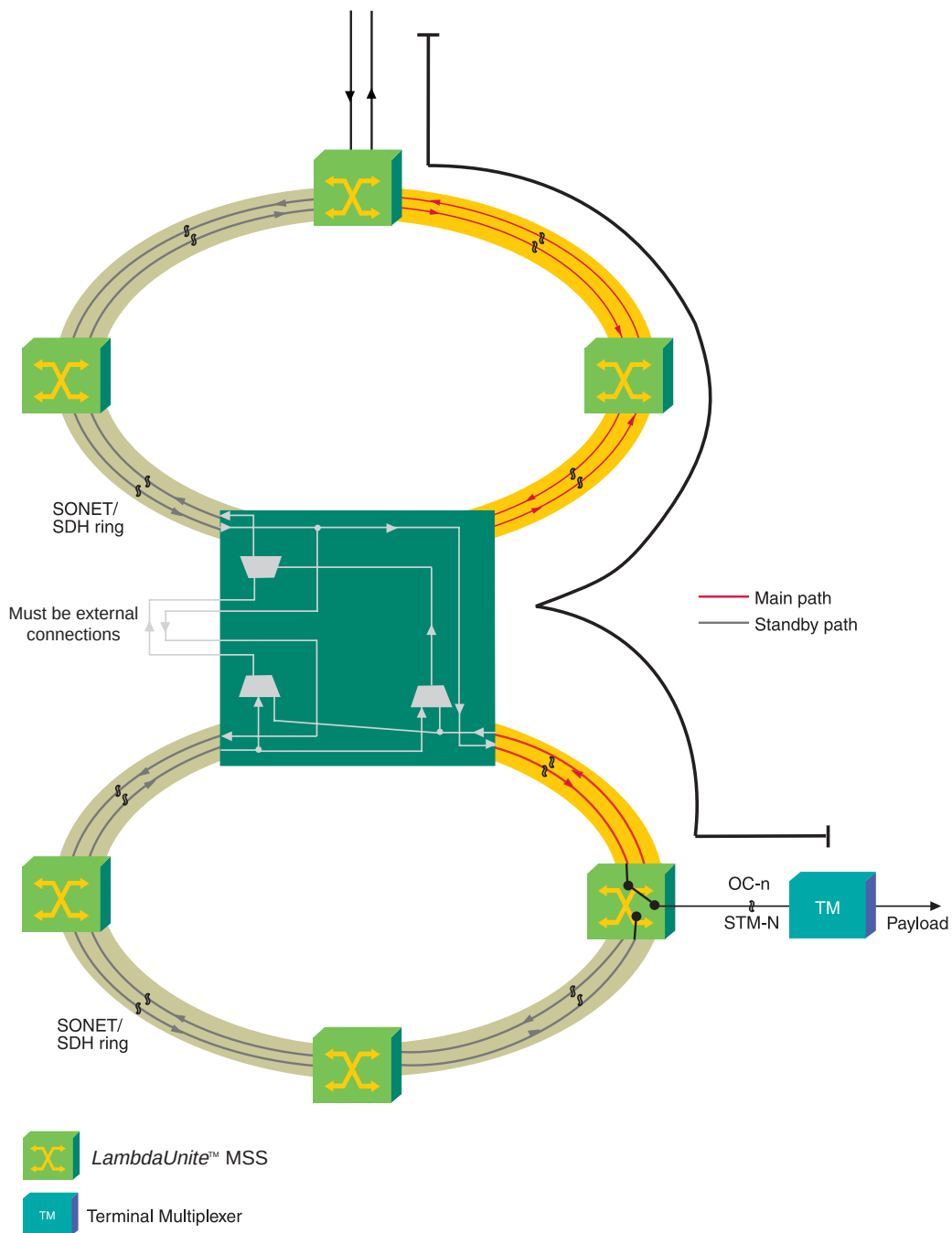
The two interconnecting nodes within the SNCP ring do not need to be adjacent.

Both rings in the same NE

The ring interworking between a MS-SPRing and a SNCP ring is supported with both rings in different NEs or with both rings in the same NE.

For this latter case, the recommended method is to connect the circuits in this limited category through an additional pair of optical ports and fibers, as if between separate NEs. One pair of unprotected optical ports could be used for all such circuits in the NE unless the number of these circuits requires additional capacity.

A bidirectional VC-3/VC-4/VC-4-Nc circuit, which is interconnected between a MS-SPRing and a SNCP Ring, is depicted in the following figure, according to this feature restriction.



□

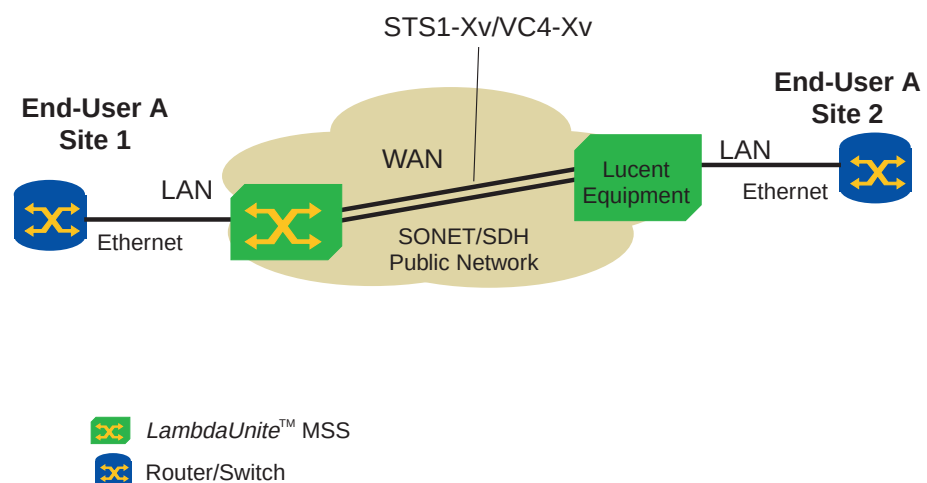
Gigabit Ethernet Interface

Overview *LambdaUnite*[™] MSS supports a Gigabit Ethernet interface. The GE1/SX4 interface conforms to the standards outlined in IEEE 802.3/IEEE 802.1Q, and supports the 1000BASE-SX protocol.

Gigabit Ethernet is mapped in up to 21 virtually concatenated STS-1 or in up to 7 virtually concatenated VC-4. 10GbE is mapped into one contiguous concatenated STS-192c or VC4-64c. Value proposition is mainly the more cost efficient solution than connecting the routers via OC-48 (STM-16) or OC-192 (STM-64) due to cheaper interface costs compared to OC/STM ports and due to higher metro/back bone fiber utilization in case of GbE with virtual concatenation compared to mapping GbE directly.

Capabilities The GE1/SX4 interface supported by *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.

Mode of operation *LambdaUnite* MSS operates in point-to-point mode. The point-to-point application is used to interconnect two sites of a customer, each of which has a LAN interface. Another application is the interconnection of two service provider routers that have Ethernet interfaces. The service offered by a point-to-point LAN connection can be compared with a leased-line. Some dedicated SONET/ SDH bandwidth is allocated to the connection between both end-points. The virtual concatenation mapping allows the operator to assign the proper amount of SONET/SDH bandwidth: “Right-sized Pipes”. The Ethernet frames from the Gigabit Ethernet LAN ports are transported over the SONET/SDH network using virtual concatenation: STS1-Xv (X=1..21) or VC4-Yv (Y=1..7). The user can provision the capacity (X or Y) of the WAN ports to allow flexible allocation of SONET/SDH network capacity for Ethernet transport. Two basic modes of operation are distinguished for point-to-point applications: repeater mode and bridge mode.



Repeater Mode The simplest form of Ethernet transport is to transparently forward all frames on the WAN that are transmitted by the end-user via the LAN; this mode is called repeater mode (also referred to as promiscuous mode or no-tag mode). In this mode minimal provisioning is necessary. Full transparency can only be obtained when sufficient bandwidth is allocated on the WAN ($X=21$ or $Y=7$). Packet loss may occur in scenarios where less bandwidth is allocated on the WAN. To prevent such packet loss one can enable flow-control over the LAN interface towards the end-user. The difference between a hub or repeater in the sense of IEEE802.3 and the repeater mode described here is two-fold: first the repeater mode will operate in store-and-forward mode; secondly, flow-control frames are not transparently forwarded, but interpreted.

VLAN tagging mode In the VLAN (Virtual Local Area Network) tagging mode frames are processed according IEEE802.1D bridging and uses IEEE802.1Q VLANs. In a point-to-point application the main functions are MAC address learning, VLAN filtering and priority queuing. MAC address learning helps prevent that frames are forwarded over the WAN link while the destination is local. VLAN filtering helps in preventing forwarding unwanted or unnecessary VLANs of the WAN link. Priority queueing allows the operator to support service differentiation: high priority tagged frames are always forwarded before low priority tagged frames. In case of a low capacity WAN link low priority tagged frames are more likely to be dropped during congestion. Another important application for bridge mode is when the remote WAN to LAN bridge is a multi-point or LAN trunk node on the network.

Media Access Control (MAC)

Configuration and operation of the Learning Process and the Filtering Database such that, for a given set of VLANs, if an individual MAC Address is learned in one VLAN, that learned information is used in forward-ing decisions taken for that address relative to all other VLANs in the given set.

The GE1/SX4 card maintains 9 MAC addresses for each LAN, WAN and the CPU. The MAC addresses need to be world wide unique and are programmed at the factory. Only the first of 9 sequential addresses is stored in the SEEPROM of each GE1 card. The 9 MAC addresses are assigned through a fixed binding to the 9 MACs under software

control: MAC1-MAC4 for LAN port 1 till 4, MAC5-MAC8 for WAN port 1 till 4, MAC9 for the CPU.

Priority Queuing

When a GbE port is in IEEE VLAN tagging mode it offers some "service differentiation". Individual Ethernet frames are treated differently depending on the user priority field in the IEEE VLAN tag. The GbE card implements two transmit queues per port. Ethernet frames with a user priority of 4, 5, 6 or 7 are maintained in the high priority queue, the other frames in the low priority queue.

When an Ethernet frame is to be transmitted, the card will always serve the high priority queue first (strict priority scheduling).

For example, first assume a full rate SONET/SDH capacity (e.g.: 1000 Mbit/s over VC-4-7v). Because the GbE port and the SDH capacity are equal, the two queues can always be served in time and the end user should not observe any packet loss or special behavior depending on the user priority. In a second scenario the operator allocates lower SONET/SDH capacity for GbE transport, say 300 Mbit/s. Ethernet frames will be dropped depending on the offered mix of frames with high or low user priority. Assume 500 Mbit/s is offered on average of which 100 Mbit/s is high priority frames and 400 Mbit/s is low priority frames. Since only 300 Mbit/s is available the end user will observe that all of high priority frames are transported successfully and only 200 Mbit/s of low priority frames. If the amount of high priority frames is higher than the allocated SONET/SDH bandwidth then all low priority frames are dropped. This behavior can be compared to the general data networking engineering rule that in a priority aware network the percentage of high priority traffic must be low enough to not impede the behavior of priority queueing.

Flow Control

The priority queueing also interacts with flow control. The flow control effectively only operates on the high priority queue. This means that the GbE card will not signal **Pause on** if the internal queues are filled with low priority frames; otherwise it could potentially halt transmission of high priority frames.

The operator can use the parameter **Default user priority** on *WaveStar*[®] CIT to support various priority queueing schemes:

- If the operator wants to create the above described priority queueing service and the end user equipment supports IEEE VLAN tagged frames only, or a mix of IEEE VLAN tagged and untagged frames, then the default user priority must be set to **Low**.
- If the end user equipment only supports untagged Ethernet frames, all are queued in the same queue according to what was provisioned on EMS for the default user priority. Priority queueing is not available.
- If the operator does not want to support priority queueing then the default user priority must be set to **High**: all frames are queued in the same queue independent of tagged or untagged and independent of the user priority field of the VLAN tagged frames.

Link Aggregation Application

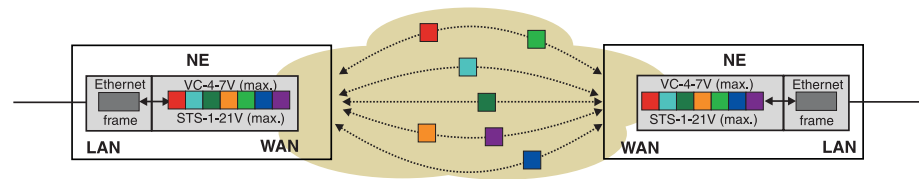
In point-to-point applications the end-user may want to use link aggregation (LAG) between the end-user equipment to create a transport capacity of more than 1 Gb/s. Two or more GbE links are bundled to create a larger capacity transport pipe. The external routers can use the LAG protocol to set up and maintain the bundled LAN ports. UNITE is not involved in the protocol itself but is fully transparent for the protocol, especially the LAG protocol PDUs.

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.

Link Capacity Adjustment Scheme

Link Capacity Adjustment Scheme (LCAS) is an extension to virtual concatenation that allows dynamic changes in the number of STS-1/VC-4 channels per connection. In case channels are added or removed by management actions this will happen without losing any customer traffic. LCAS allows a bandwidth service with scalable throughput in normal operation mode. In case of failure the connection will not be dropped completely only the affected STS-1s/VC-4s. The remaining channels will continue carrying the customer traffic. The implemented link capacity adjustment system (LCAS) provides automatic decrease of bandwidth in case of link failure and reestablishment after link recovery.

Interworking

LambdaUnite MSS supports interworking on WAN port side with the following Network elements in a point-to-point application:

- *LambdaUnite* MSS
- DMX
- *WaveStar*TDM10G
- ADM 16/1
- ADM 16/1c

Interworking with non-Lucent equipment via the WAN interface is only possible in repeater mode, without VLAN tagging.



Facility loopback

Overview Facility loopbacks are loopbacks switched on whole ports. They make it possible to verify the correct system operation and may facilitate troubleshooting of problems.

There are two types of facility loopbacks:

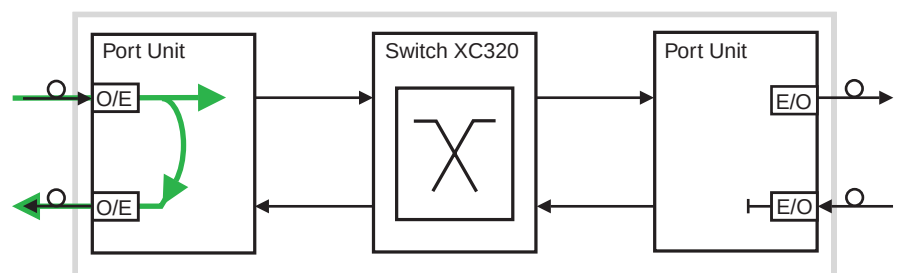
- **Near-side facility loopbacks**
The signal on the input port is looped to the corresponding output port with transpassing as few NE components as possible. Near-side facility loopbacks can be switched on all out-of-service optical interface ports.
- **Far-side facility loopbacks**
The transmission signal to the output port in the NE is looped back to the corresponding input port with passing through as many equipment components as possible. Far-side facility loopbacks can be switched on all out-of-service optical interface ports as well as on 1-Gbit/s Ethernet ports.

Near-side facility loopbacks

Near-side facility loopbacks can be used to test the correct cabling between two network elements including the involved interface ports.

Functional principle

The following schematical diagram depicts the functional principle of near-side facility loopbacks.



The incoming signal at the input port is, after optical-to-electrical conversion, entirely looped back to the output port.

Near-side facility loopbacks are characterized as follows:

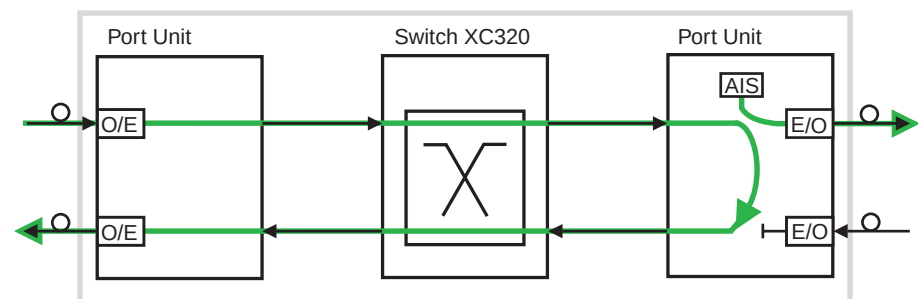
- Near-side facility loopbacks are transparent, the signal transmitted in the downstream direction is not changed.
- The signal transmitted in the original (downstream) direction is different from the signal looped back. Particular Section/RS and Line/MS Overhead bytes, such as those used for frame alignment (A1, A2) or bit error monitoring (B1, B2) for example, are not looped back but processed. The Path Overhead (POH) and the payload signal, however, are looped back unchanged.
- The incoming signal in the upstream direction is terminated during the loopback.

Far-side facility loopbacks

Far-side facility loopbacks can be used to test signal paths through a network element.

Functional principle

The following schematical diagram depicts the functional principle of far-side facility loopbacks.



Far-side facility loopbacks are characterized as follows:

- Far-side facility loopbacks are non-transparent, the signal transmitted in the original (downstream) direction is different from the signal looped back. Line AIS (SONET) or MS-AIS (SDH) respectively is inserted into the outgoing signal in the downstream direction during the loopback.
- The signal is not changed before it is looped back.
- The incoming signal in the upstream direction is terminated during the loopback.

Configuration Rules

Consider the following configuration rules to set a facility loopback:

- When a facility loopback is set, no line timing references can be assigned.
- When a line timing reference is assigned, no facility loopbacks can be set
- Before a facility loopback can be set the port must be set out-of-service.
- An MSP/APS group can only be provisioned successfully when no line timing reference is assigned to the protection port of the 1+1 MSP/APS group.
- A 4-fiber MS-SPRing/BLSR group can only be provisioned successfully when no line timing reference is assigned to the protection port of the spans of the 4-fiber MS-SPRing/BLSR group (East/West protection port).



Protection configurations

Overview This section describes the shelf configuration guidelines that have to be observed for the following protection mechanisms:

- 4-fiber MS-SPRing/BLSR
- 4-fiber MS-SPRing Transoceanic Protocol
- 2-fiber MS-SPRing/BLSR
- 1+1 MSP/1+1 APS.

MS-SPRing/BLSR The MS-SPRing/BLSR related STM-16/OC-48, STM-64/OC-192 and STM-256/OC768 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 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	19-14
Impact of configuration changes on performance monitoring	19-20



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

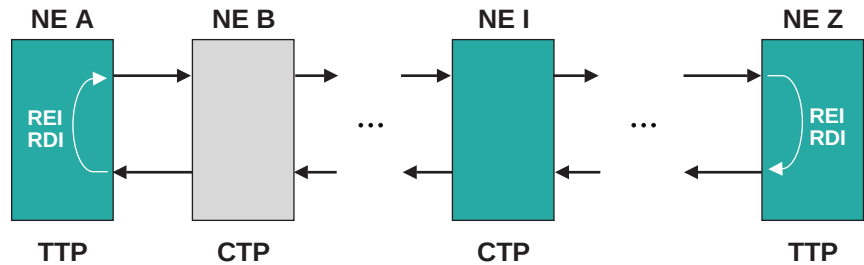
In principle, two kinds of performance monitoring can be distinguished:

- 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).

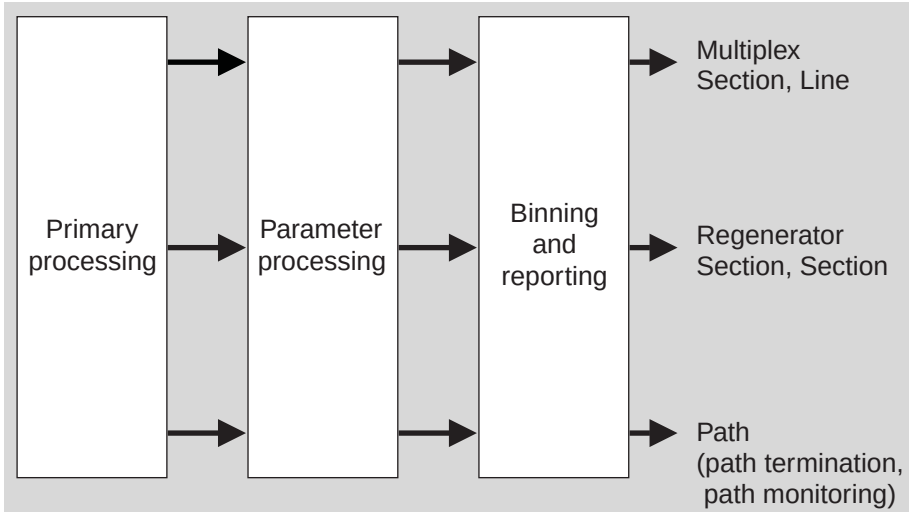
SDH performance monitoring

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. 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. 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 [“Performance parameters” \(19-6\)](#) and [“SDH/SONET far-end performance parameters” \(19-8\)](#).

Binning and reporting

In the binning and reporting phase, the performance parameters obtained during the parameter processing are stored in accumulation registers (or “bins”) over 15-minutes and 24-hours observation periods.

For each performance monitoring point (cf. [“Performance measurements” \(19-6\)](#)), 32 recent (or history) bins for 15-minutes measurements and one recent bin for 24-hours measurements are stored in the NE.

□

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 monitoring points for near-end and/or far-end performance monitoring. 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 (“pipe mode”), 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 up to 48 performance monitoring processes per monitoring direction (near end, far end).

Performance parameters These performance parameters are supported by the *LambdaUnite*[™] MSS systems:

- [“SDH/SONET near-end performance parameters” \(19-7\)](#)
- [“SDH/SONET far-end performance parameters” \(19-8\)](#)
- [“Ethernet performance parameters” \(19-9\)](#)

SDH/SONET near-end performance parameters

These are the SDH/SONET near-end performance parameters supported by the *LambdaUnite* MSS systems:

SDH/SONET near-end performance parameters	SDH	SONET
<i>Errored Seconds (ES)</i> 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. The ES counter is not incremented during a period of unavailability (cf. Unavailable Seconds).	X	X
<i>Severely Errored Seconds (SES)</i> A near-end SES 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. The SES counter is not incremented during a period of unavailability (cf. Unavailable Seconds).	X	X
<i>Background Block Errors (BBE)</i> The BBE count is the accumulated number of block errors not occurring as part of a severely errored second.	X	–
<i>Code Violations (CV)</i> The CV count is the SONET equivalent to the SDH BBE count.	–	X
<i>Unavailable Seconds (UAS)</i> Near-end UAS 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 (UAP) . 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. The ES and SES counters are not incremented during a period of unavailability.	X	X
<i>Loss of Signal Seconds (LOSS)</i> A loss of signal second is a second in which a loss of signal condition has been detected in the incoming signal.	–	X
<i>Severely Errored Framing Seconds (SEFS)</i> An SEFS is a second in which frame alignment has temporarily been lost (out-of-frame (OOF) condition).	–	X
<i>Failure count (FC)</i> The near-end FC is incremented each second in which a near-end defect (not RDI) has been detected in the incoming signal.	–	X

SDH/SONET near-end performance parameters	SDH	SONET
AIS Seconds (AISS) An AISS 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

SDH/SONET far-end performance parameters

These are the SDH/SONET far-end performance parameters supported by the *LambdaUnite* MSS systems:

Far-end performance parameter ¹	SDH	SONET
Errored Seconds (ES) A far-end ES 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. ² Far-end errored seconds are not declared when other defects than RDI are present at the near end. The ES counter is not incremented during a period of unavailability (cf. Unavailable Seconds).	X	X
Severely Errored Seconds (SES) A far-end SES 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. ² The SES counter is not incremented during a period of unavailability (cf. Unavailable Seconds).	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) The CV count is the SONET equivalent to the SDH BBE count.	–	X
Unavailable Seconds (UAS) Far-end UAS 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 the unavailability period (UAP) . 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. The ES and SES counters are not incremented during a period of unavailability.	X	X

Far-end performance parameter ¹	SDH	SONET
Failure Count (FC) The far-end FC is incremented each second in which an RDI defect has been detected in the incoming signal.	–	X

Notes:

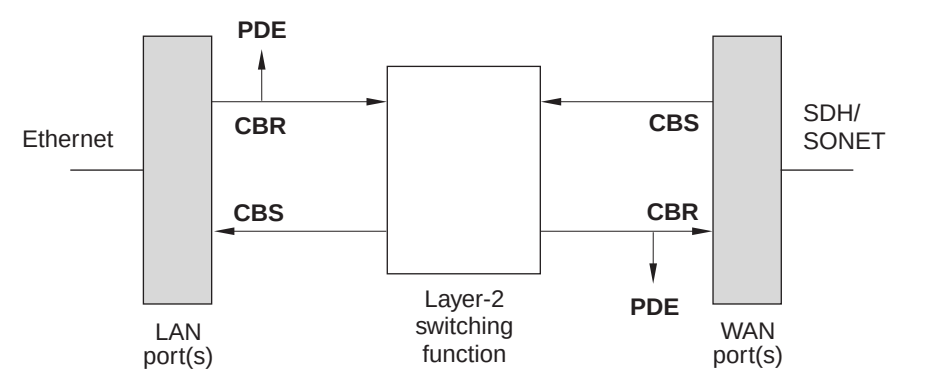
1. The far-end performance information is ***not evaluated*** during the presence of near-end defects. The corresponding counter values remain unchanged.
2. The number of block errors or bit errors at the far end is indicated at the near end by means of the Remote Error Indication (REI). The presence 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)”.
3. All OP10 circuit packs report an REI value that is approximately 4% too low. This impacts far-end performance monitoring of the NE that receives an input signal from an OP10.

Ethernet performance parameters

For the VC-4 or STS-1 termination points connected to a WAN port (VC-4-Xv or STS-1-Yv port, VCG port), the “normal” SDH/SONET performance monitoring can be activated. The same counters that apply for VC-4 or STS-1 termination points on any other port also apply to the VC-4 or STS-1 termination points on a WAN port.

In addition to the standard SDH/SONET performance parameters for WAN ports, the following Ethernet performance parameters, which apply both to LAN ports (Ethernet ports) and WAN ports are supported by the *LambdaUnite* MSS systems.

The following figure illustrates the location of the measurement points for the Ethernet performance parameters, the subsequent table describes the meaning of these parameters.



Ethernet performance parameters
Total number of bytes received (CBR) The CBR counter indicates the number of bytes in layer-2 (datalink layer) packets received within one second that are marked to be below the committed information rate.
Total number of bytes sent (CBS) The CBS counter indicates the number of bytes in layer-2 (datalink layer) packets transmitted within one second that are marked as being “committed”.
Total number of errored packets dropped (PDE) The PDE counter indicates the number of layer-2 (datalink layer) frames received within one second that are dropped because of errors.

Notes:

1. The CBS and CBR counters are rather traffic monitoring counters than performance monitoring counters, as they monitor the traffic load in the network. The PDE counter is a real performance monitoring counter as it gives an indication about the performance of the network.
2. Because of the difference in units, bytes versus packets, the counters cannot be correlated with each other.
3. The PDE counter for dropped packets considers only packets dropped due to errors, it does not include packets dropped due to congestion.

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:

- SDH Regenerator Section performance monitoring
 - **Regenerator Section Near End SES Threshold**
- SONET Section performance monitoring
 - **Section Near End SES Threshold**
- SDH Multiplex Section performance monitoring
 - **Multiplex Section Near End SES Threshold**
 - **Multiplex Section Far End SES Threshold**
- SONET Line performance monitoring
 - **Line Section Near End SES Threshold**
 - **Line Section Far End SES Threshold**
- SDH or SONET path performance monitoring
 - **Higher-order Path Near-end SES Threshold**
 - **Higher-order Path Far-end SES Threshold**

Default values

For SDH performance monitoring, the default value of the SES declaration threshold is 15% of the number of blocks per second for the MS layer, and 30% for the other layers.

For SONET performance monitoring, the default value of the SES declaration threshold is reflecting the number of code violations (CV) that are expected to be counted assuming that the bit error distribution over time is according to the Poisson law, with an average bit error ratio of 10^{-6} .

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

Parameter	Regenerator Section	Multiplex Section	Path
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

Ethernet performance parameters

The following overview shows the available Ethernet performance parameters and their association to LAN ports (Ethernet ports) and

WAN ports (VC-4-Xv or STS-1-Yv ports, VCG ports):

Parameter	LAN port	WAN port
CBR	CBR	CBR
CBS	CBS	CBS
PDE	PDE	PDE



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. 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 Time	
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” (19-15) • “SDH Multiplex Section” (19-16) • “SDH path” (19-16) • “SONET Section” (19-17) • “SONET Line” (19-17) • “SONET path” (19-18) • “Ethernet” (19-18) Please also refer to “Performance parameters” (19-6).

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” \(19-19\)](#).

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” \(19-19\)](#).

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” \(19-19\)](#).

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)

Parameter	Description
VC-N-UAS	SDH path - Near-end Unavailable Seconds (UAS)
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. For further information on the validity flag, please refer to [“Validity flag” \(19-19\)](#).

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” \(19-19\)](#).

Parameter	Description
CVL	Code Violations (CV) - Line (near end)

Parameter	Description
ESL	Errorred Seconds (ES) - Line (near end)
SESL	Severely Errorred Seconds (SES) - Line (near end)
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	Errorred Seconds (ES) - Line, Far End
SES-LFE	Severely Errorred 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” \(19-19\)](#).

Parameter	Description
CVP	Code Violations (CV) - Path (near end)
ESP	Errorred Seconds (ES) - Path (near end)
SESP	Severely Errorred 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	Errorred Seconds (ES) - Path, Far End
SES-PFE	Severely Errorred Seconds (SES) - Path, Far End
UAS-PFE	Unavailable Seconds (UAS) - Path, Far End

Ethernet The following are the parameters of the Ethernet 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” \(19-19\)](#).

Parameter	Description
CBR	Total number of bytes received (at a LAN port or WAN port respectively)
CBS	Total number of bytes sent (at a LAN port or WAN port respectively)
PDE	Total number of errored packets dropped (at a LAN port or WAN port respectively)

Notes:

1. Please also refer to [“Ethernet performance parameters” \(19-9\)](#).

Validity flag The validity flag shows the validity of the register (“bin”) 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, validity flag = “0”) for the current 15-minutes or 24-hours bin 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

Deletion of performance 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 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.

Performance monitoring history data

Performance monitoring history bins will only be deleted for those monitoring points related to a circuit pack which was explicitly deleted (deprovisioned).

In the case of

- disabling performance monitoring points manually, or
- changing the interface standard of VCG ports, or
- creating a 1+1 MSP/APS protection group

the related performance monitoring points will be deleted but the history bins for those monitoring points might still be visible (retrievable) for up to eight hours in the case of 15-minutes measurements and for up to one day in the case of 24-hours measurements.

Therefore, ignore performance monitoring history data belonging to a date and time outside the current activation period of individual performance monitoring points.

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 if provisioned on the correct granularity (STS-1 granularity is recommended).

**XC320 equipment
protection switching**

All performance monitoring event processing as well as binning and reporting is performed on the active XC320 switch unit.

On an XC320 switch unit, performance monitoring data is stored in the current bin and one recent bin. Both XC320 switch units 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
Software download for upgrade purposes	20-4



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 *Navis*[®] Optical EMS or the *WaveStar*[®] CIT. Activating (“installing”) a newly downloaded software version changes the current/previous assignment automatically.

Preparing a *CompactFlash* card When initially delivered, the *CompactFlash* card is empty. *WaveStar* CIT can be used to copy the initial software generic from the CD-ROM to the *CompactFlash* card (refer to [“Performing an initial software download using the CIT” \(10-2\)](#)).



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 *WaveStar*® 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 (*CompactFlash*™ card) associated with *WaveStar* CIT.

The software is initially delivered to the customer on a CD-ROM. The *CompactFlash* card is initially empty. The software generic has to be copied from the CD-ROM to the empty *CompactFlash* card via *WaveStar* CIT (refer to [“Performing an initial software download using the CIT” \(10-2\)](#)). Afterwards, the *CompactFlash* card is inserted into the NE.

□

Software download for upgrade purposes

Overview 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.

Software upgrading concepts *LambdaUnite™* MSS network elements support the download of software generics over DCC, OSI LAN or TCP/IP. For downloading of software generics via TCP/IP a FT-TD gateway is required (refer to [“FT-TD Gateway” \(14-22\)](#)).

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 directly via a LAN network is approx. 10 minutes, indirectly via LAN/DCC network less than 60 minutes.

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.

Download sources Software download can be performed from/via the following:

- **CIT**

To be used if the NE, to which the generic is to be downloaded, is connected to the *WaveStar* CIT via DCC or OSI LAN.

Refer to [“Remote download of software generics via CIT” \(20-5\)](#)

.

- **FTTD**

To be used if the OS, from which the generic is to be downloaded, is connected to the NE via TCP/IP using a [“FT-TD Gateway” \(14-22\)](#).

Refer to [“Remote download of software generics via FTTD” \(20-5\)](#).

- **“FTAM” (14-20)**

Refer to [“Remote download of software generics using FTAM” \(20-7\)](#).

Remote download of software generics via CIT

The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to software download:

Option	Meaning
Name	the name of the directory where the generic is currently stored.
Size	the size of the software in bytes. Possible values are: the integers from 0...999,999,999, inclusive.
Type	the file type. Possible values are NE Generic , NE Data , or Directory .
Modified	the date and time at which the file was last modified.
Source directory path	specifies the source directory path, where the generic is saved.
From, [Src]:	complete description of the location, path and file name where the SW is being transferred from.

Remote download of software generics via FTTD

The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to software

download:

Option	Meaning
The FTTD tab	
Profile	This field allows you to retrieve any FTAM information stored via a profile. This profile is stored locally on the CIT. Selecting a profile causes the required FTAM fields to be pre-populated with the stored information. If you do not select a profile, the fields are not pre-populated.
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI, IDI, DFI, Org, Res, RD, Area, Sys, and Sel). Refer to “NSAP address format” (14-24). Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
The FTP tab	
Server IP	The IP Address of the OS (specified as four subfields, each separated from the next by a period). Either this field or the IP Name field is required.
Server name	The IP Name of the OS.
Server port	The IP port. Optional field. The default value is 21.
User name	User name for the OS (if needed).
User password	Password for the user name. Only valid if the user entered a user name.
Common fields	
Source directory path	specifies the file/directory path on the OS, Required field.
From, [Src]:	complete description of the location, path and file name where the SW is being transferred from.

Remote download of software generics using FTAM

The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to software download using FTAM:

Option	Meaning
Profile	This field allows you to retrieve any FTAM information stored via a profile. This profile is stored locally on the CIT. Selecting a profile causes the required FTAM fields to be pre-populated with the stored information. If you do not select a profile, the fields are not pre-populated.
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI , IDI , DFI , Org , Res , RD , Area , Sys , and Sel). Refer to “NSAP address format” (14-24) . Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
Source directory path	In this field specify the file/directory path, where the generic is saved. Required field.
From, [Src]:	complete description of the location, path and file name where the SW is being transferred from.





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
Backup database	21-3
Restore database	21-6



Configuration backup and restoration

Overview 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.

LambdaUnite™ MSS network elements support database backup and restoration over DCC, OSI LAN or TCP/IP. For database backup and restoration via TCP/IP a FT-TD gateway is required (refer to [“FT-TD Gateway” \(14-22\)](#)).

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.
- If they are not identical the NE changes to maintenance condition.

Then the operator has two opportunities:

- perform an restore using the correct backup data
- accepting the “wrong” data base by simply exiting maintenance condition.

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, if the actual NE settings relevant for transmission are different from the settings stored in the backup database.



Backup database

Overview Database backup can be performed to/via the following:

- **CIT**
To be used if the NE, for which the database backup has to be performed, is connected directly to the *WaveStar*® CIT.
- **FTTD**
To be used if the NE, for which the database backup has to be performed, is connected to the *WaveStar* CIT via TCP/IP using a [“FT-TD Gateway” \(14-22\)](#).
Refer to [“Backup database via FTTD” \(21-3\)](#).
- **“FTAM” (14-20)**
Refer to [“Backup database using FTAM” \(21-5\)](#).

Backup database directly to *WaveStar* CIT

The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database backup:

Option	Meaning
Name	the name of the directory where the generic is currently stored.
Size	the size of the software in bytes. Possible values are: the integers from 0...999,999,999, inclusive.
Type	the file type. Possible values are NE Generic , NE Data , or Directory .
Modified	the date and time at which the file was last modified.
Destination directory path	specifies the Destination directory path, where the database is to be saved.
To, [Dst]:	complete description of location, path and directory name where the data is being transferred to.

Backup database via FTTD

The following configuration option (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database

backup:

Option	Meaning
The FTTD tab	
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI, IDI, DFI, Org, Res, RD, Area, Sys, and Sel). Refer to “NSAP address format” (14-24). Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
The FTP tab	
Profile	This field allows you to retrieve any FTP information stored via a profile. This profile is stored locally on the CIT. Selecting a profile causes the required FTP fields to be pre-populated with the stored information. If you do not select a profile, the fields are not pre-populated.
Server IP	The IP Address of the OS (specified as four subfields, each separated from the next by a period). Either this field or the IP Name field is required.
Server name	The IP Name of the OS.
Server port	The IP port. Optional field. The default value is 21.
User name	User name for the OS (if needed).
User password	Password for the user name. Only valid if the user entered a user name.
Common fields	
Destination directory path	specifies the file/directory path on the OS, Required field.
To, [Dst]:	complete description of location, path and directory name where the data is being transferred to.

Backup database using FTAM

The following configuration option (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database backup:

Option	Meaning
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI, IDI, DFI, Org, Res, RD, Area, Sys, and Sel). Refer to “NSAP address format” (14-24). Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
Destination directory path	In this field specify the file/directory path, where the database is to be saved. Required field.
To, [Dst]:	complete description of location, path and directory name where the data is being transferred to.



Restore database

Overview Database restore can be performed from/via the following:

- **CIT**
To be used if the NE, for which the database restore has to be performed, is connected directly to the *WaveStar*® CIT.
- **FTTD**
To be used if the NE, for which the database restore has to be performed, is connected to the *WaveStar* CIT via TCP/IP using a FT-TD gateway (refer to [“FT-TD Gateway” \(14-22\)](#)).
Refer to [“Restore database via FTTD” \(21-7\)](#).
- **FTAM**
(refer to [“FTAM” \(14-20\)](#)).
Refer to [“Restore database using FTAM” \(21-8\)](#).

Restore database directly from *WaveStar* CIT

The following configuration options (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database restore:

Option	Meaning
Name	the name of the directory where the backup is currently stored.
Size	the size of the software in bytes. Possible values are: the integers from 0...999,999,999, inclusive.
Type	the file type. Possible values are NE Generic , NE Data , or Directory .
Modified	the date and time at which the file was last modified.
Source directory path	specifies the Source directory path, where the database is to be saved.
From, [Src]:	complete description of location, path and directory name where the data is being transferred from.

Restore database via FTTD

The following configuration option (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database restore:

Option	Meaning
The FTTD tab	
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI, IDI, DFI, Org, Res, RD, Area, Sys, and Sel). Refer to “NSAP address format” (14-24). Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
The FTP tab	
Profile	This field allows you to retrieve any FTP information stored via a profile. This profile is stored locally on the CIT. Selecting a profile causes the required FTP fields to be pre-populated with the stored information. If you do not select a profile, the fields are not pre-populated.
Server IP	The IP Address of the OS (specified as four subfields, each separated from the next by a period). Either this field or the IP Name field is required.
Server name	The IP Name of the OS.
Server port	The IP port. Optional field. The default value is 21.
User name	User name for the OS (if needed).
User password	Password for the user name. Only valid if the user entered a user name.
Common fields	
Source directory path	specifies the file/directory path on the OS, Required field.
From, [Src]:	complete description of location, path and directory name where the data is being transferred from.

Restore database using FTAM

The following configuration option (the designations refer to the corresponding *WaveStar* CIT windows) exist with regard to database restore:

Option	Meaning
PSEL	The PSEL address (not required).
SSEL	The SSEL address (not required).
TSEL	The TSEL address (not required).
NSAP Address	The NSAP address, broken down into subfields (AFI, IDI, DFI, Org, Res, RD, Area, Sys, and Sel). Refer to “NSAP address format” (14-24). Required field. The <i>WaveStar</i> CIT displays the entire NSAP as a read-only field, generated by the subfields the user enters.
Source directory path	In this field specify the file/directory path, where the database backup is saved. Required field.
From, [Src]:	complete description of location, path and directory name where the data is being transferred from.





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.:

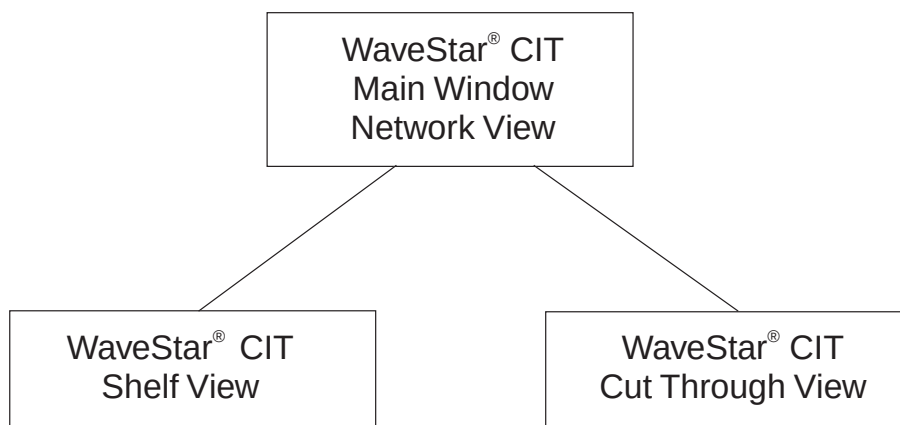
- how to log into and log out from the *WaveStar* CIT
- how to log into and log out from network elements
- the layout and the structure of the three different series of windows
 - *WaveStar* CIT main window and its menus and submenus
 - *WaveStar* CIT System View window and its menus and submenus
 - *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.

Interaction with network elements *WaveStar* CIT provides two possibilities to interact with a network element:

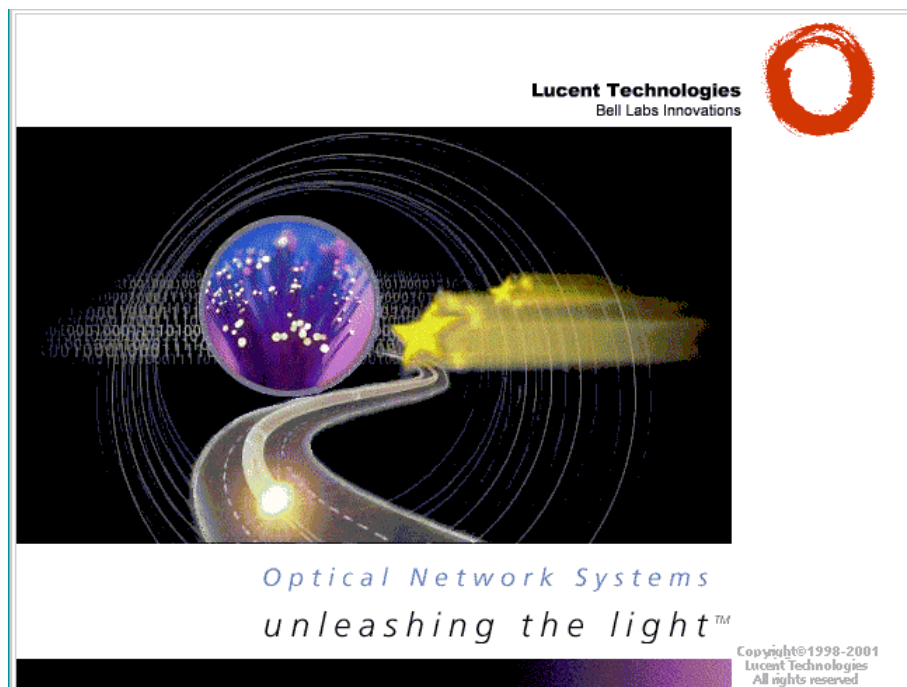
- *WaveStar* CIT System View: This is the shelf view of the network element.
- *WaveStar* CIT Cut-Through View: here, you can execute TL1 commands on a one-at-a-time basis or in a series/script.

The following figure illustrates the general *WaveStar* CIT concept.



The structure of this chapter follows the *WaveStar* CIT concept.

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

<u>Basic WaveStar CIT procedures</u>	<u>22-5</u>
<u>Installing the WaveStar CIT</u>	<u>22-6</u>
<u>WaveStar CIT login/logout procedure</u>	<u>22-9</u>
<u>Connecting/disconnecting the WaveStar CIT to/from the NE</u>	<u>22-11</u>
<u>Concepts for connecting the WaveStar CIT to the NE</u>	<u>22-12</u>
<u>Network element selection and login</u>	<u>22-16</u>
<u>Logout from NE(s)</u>	<u>22-27</u>
<u>WaveStar CIT main window</u>	<u>22-29</u>
<u>Elements of the WaveStar CIT user interface</u>	<u>22-30</u>
<u>Tool bar of the WaveStar CIT</u>	<u>22-32</u>
<u>NE connection types menu</u>	<u>22-34</u>

<u>Standard window components</u>	<u>22-36</u>
<u>Selection windows</u>	<u>22-41</u>
<u>General window handling</u>	<u>22-45</u>
<u>General pushbuttons</u>	<u>22-48</u>
<u>Basic operations</u>	<u>22-50</u>
<u>Administering NE views</u>	<u>22-51</u>
<u>Overview of the menu structure</u>	<u>22-55</u>
<u>System view</u>	<u>22-57</u>
<u>Shelf view</u>	<u>22-58</u>
<u>The ring map</u>	<u>22-68</u>
<u>Graphical view of the ring map</u>	<u>22-70</u>
<u>Overview of the shelf-view menu structure</u>	<u>22-72</u>
<u>Reports and log files</u>	<u>22-80</u>
<u>View rolling events</u>	<u>22-81</u>
<u>Cut Through view</u>	<u>22-82</u>
<u>Entering the Cut Through view</u>	<u>22-83</u>
<u>Interactive – Execute TL1 single commands</u>	<u>22-85</u>
<u>Interactive – Manage a listbox file</u>	<u>22-87</u>
<u>Working with script files</u>	<u>22-88</u>
<u>Working with logs</u>	<u>22-90</u>



Basic WaveStar® CIT procedures

Overview

Purpose The purpose of this section is to describe the installation procedures of the *WaveStar* CIT application software on a PC and how to log into and log out from the *WaveStar* CIT.

Main window 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.

Contents

Installing the WaveStar CIT	22-6
WaveStar CIT login/logout procedure	22-9



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
 - 500 MB of free hard-disk drive space
 - CD-ROM drive (16X recommended)
 - *CompactFlash*™ card
 - SVGA monitor set to 800x600 resolution or greater, with 256 colors (1024x768, 16 million colors recommended)
 - 10/100BaseT LAN interface, installed and working
 - *Adobe*® *Acrobat*® *Reader*® for *Windows*® (version 3.01 or later)
 - Removable hard-disk drive (optional; required only for system backup).
 - *Microsoft*® *Windows NT*® 4.0 with Service Pack 5 or *Microsoft Windows* 2000 operating system

Important!

Microsoft Windows 2000 does not clean up drivers properly after you have removed or exchanged network cards, causing critical network services to fail. This can cause a failure in WaveStar CIT starting after installation or the user may be unable to select the appropriate card from the list during installation.

The performance of the user interface can be enhanced by using a higher performance personal computer. An unshielded crossed Ethernet LAN cable (10/100BaseT) with 4-wire RJ-45 connectors is used for connecting the WaveStar CIT to the NE.

Required web browser For the User Assistance functionality of the WaveStar CIT application a weblication is used that displays information in HTML. Therefore the off-the-shelf browsers Netscape 4.05 (or higher) or Internet Explorer 4.02 (or higher) are recommended. The browser to be used must be set the default browser on the personal computer on which the WaveStar CIT is running.

Important! It is important to have the right version of the *URL.DLL* installed (V.4.70.1215). With recommended IE version, the DLL is provided automatically. However, for Netscape, the is not provided but can be downloaded from Netscape supported site: <http://www.ufaq.org/downloads.html>

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 <i>WaveStar</i> CIT CD Browser appears.
	autorun starts	no action is required. Result: The <i>WaveStar</i> 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



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 ...	THEN ...
	it is the first WaveStar CIT installation on the respective PC,	log into WaveStar CIT with User Id: "LUC01" or "LUC02" and Password: "LUC+01" or "LUC+02".
	a previous WaveStar CIT version has already been installed on the respective PC,	log into WaveStar 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 needed configure the basic DCN parameters for the WaveStar CIT.

Reference:

Refer to "[Configuring the basic DCN parameters for the WaveStar CIT](#)" (3-11).

5	IF ...	THEN ...
	it is the first WaveStar CIT session,	proceed to Step 6 .
	it is not the first WaveStar CIT session,	Stop! End of Task.

-
- 6 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
.....



Connecting/disconnecting the WaveStar® CIT to/from the NE

Overview

Purpose The purpose of this section is to describe how the WaveStar CIT can be connected to an NE and how you can establish a connection to the NE on the WaveStar CIT.

Additionally it is described how to logout from NE(s).

Contents

Concepts for connecting the WaveStar CIT to the NE	22-12
Network element selection and login	22-16
Logout from NE(s)	22-27



Concepts for connecting the WaveStar® CIT to the NE

Ways of connecting the WaveStar CIT to a network element

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.
- Remote Access via TCP/IP.

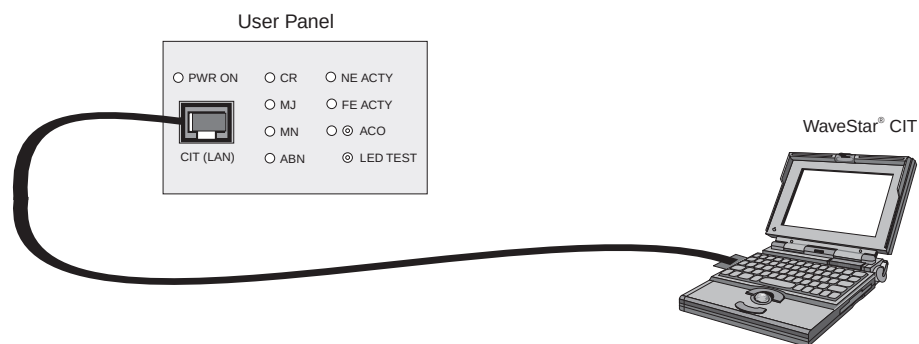
Direct LAN access (point-to-point)

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 (10/100BaseT) with 4-wire RJ-45 connectors is used for this connection.

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.

For wiring details, refer to the LambdaUnite MSS Installation Manual.

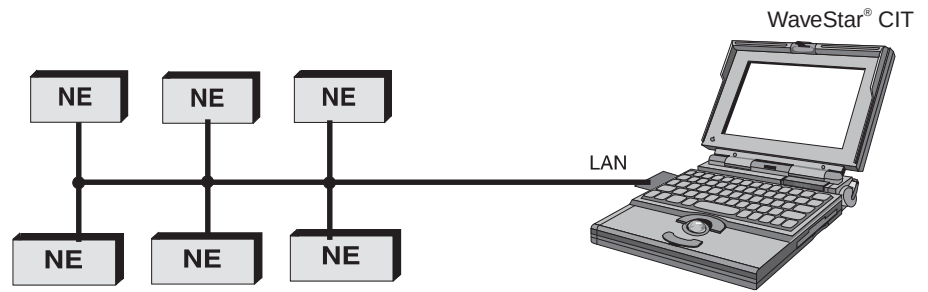
The following figure illustrates the Direct LAN Access (Point-to-Point).



**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 10/100BaseT Ethernet interfaces on 4-wire RJ-45 connectors.

The following figure illustrates the WaveStar CIT LAN Access (Network).



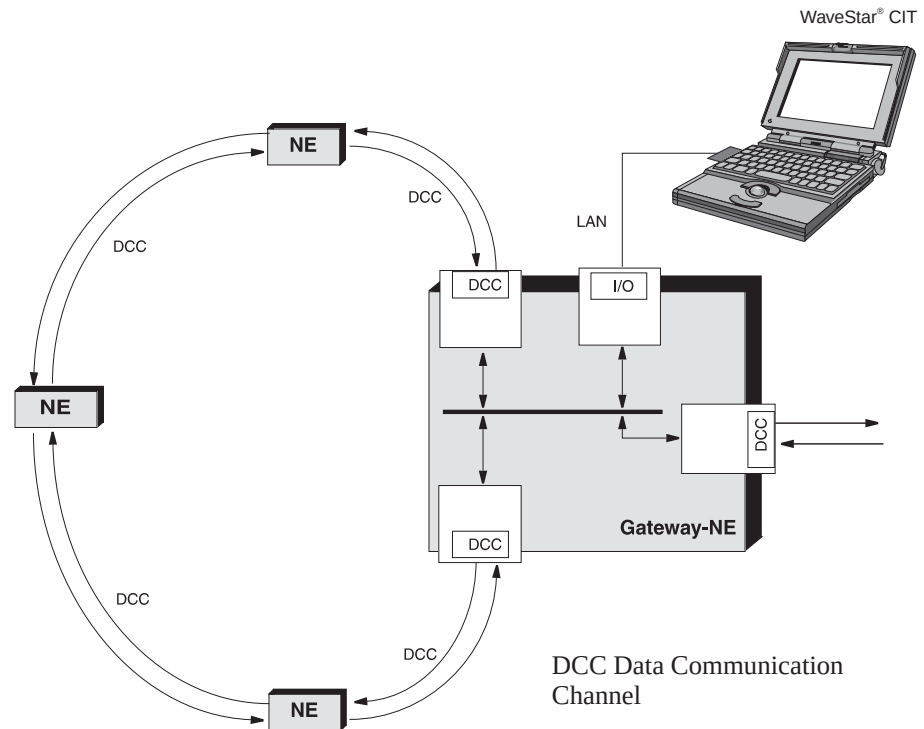
LAN Local Area Network

Important! *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.*

**WaveStar CIT access via
Data Communication
Channel (DCC)**

WaveStar CIT access to remote NEs can easily be done via the Data Communication 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 Communication Channel.



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 access via TCP/IP

The WaveStar CIT can be connected to NEs via TCP/IP or via TCP/IP on a gateway NE.

NEs that are linked to the CIT via TCP/IP or via TCP/IP on a gateway NE will not automatically appear in the Network Map in the Network View screen.

Before establishing a connection to an NE according to this connection type, an entry in the WaveStar CIT address list has to be created, containing the TID and the TCP/IP address for the NE. After that a separate view has to be created for the NE.

The procedure to be used for this special case is clearly described in [“Network element selection and login using the address list” \(22-23\)](#).

WaveStar CIT address list

For systems which do not support TARP ([“TARP” \(14-38\)](#)) for Name/Address resolution or are connected via TCP/IP (directly or via TCP/IP on a gateway NE), it is necessary to provide a mechanism to manually enter a list of TID/NSAP pairs and if necessary the according TCP/IP addresses.

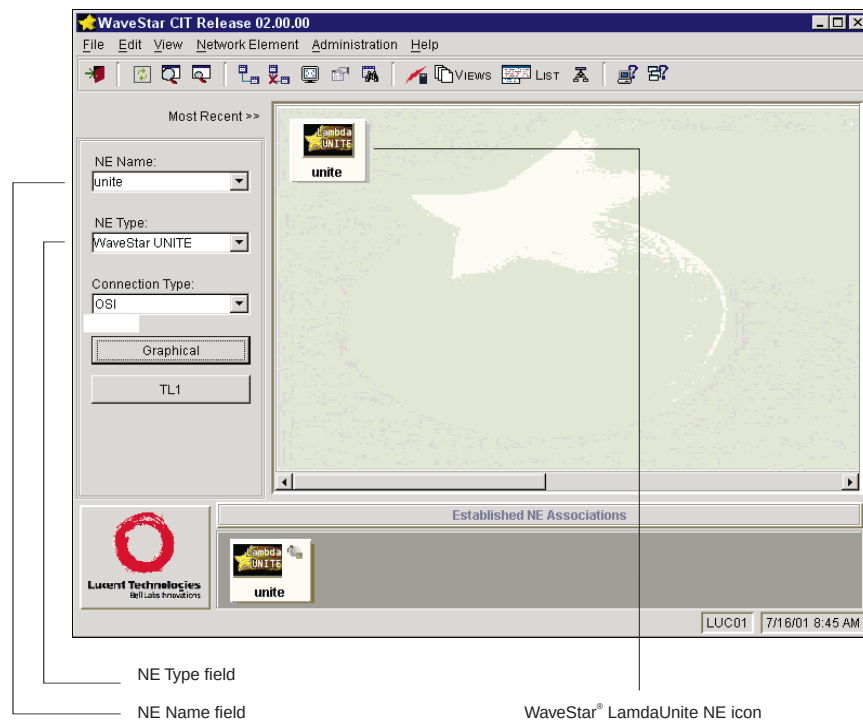
For creating and entering NEs in the CIT address list refer to [“Network element selection and login using the address list” \(22-23\)](#).



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”.



The procedure for establishing an NE connection on the WaveStar CIT depends on the type of connection between the WaveStar CIT and the NE (refer to [“Concepts for connecting the WaveStar CIT to the NE” \(22-12\)](#)). The following procedures can be used to establish an NE connection:

- [“Network element selection and login using the NE Name box” \(22-19\)](#)

This procedure is recommended to be used, if the WaveStar CIT is connected to the NE

- directly via the user panel of the NE (IP or OSI), or
- remotely via an OSI connection, if the network elements support TARP (refer to [“TARP” \(14-38\)](#)) for Name/Address resolution.

For a remote login, connect the WaveStar CIT to any network element that is part of the sub-network containing the remote NE. For this sub-network a Data Communication Network (DCN) has to be established. Please refer to [“Configuring the data communication network \(high level\)” \(3-6\)](#) to configuring the DCN.

- remotely via a GNE (WaveStar CIT connected to the user panel of the GNE).
- [“Network element selection and login using the “Graphical System View”” \(22-21\)](#)

This procedure is recommended to be used, if the WaveStar CIT is connected to the NE

- directly via the user panel of the NE (IP or OSI),
- remotely via an OSI connection, if the network elements support TARP (refer to [“TARP” \(14-38\)](#)) for Name/Address resolution,

For a remote login, connect the WaveStar CIT to any network element that is part of the sub-network containing the remote NE. For this sub-network a Data Communication Network (DCN) has to be established. Please refer to [“Configuring the data communication network \(high level\)” \(3-6\)](#) to configuring the DCN.

- directly via TCP/IP (WaveStar CIT connected to the user panel of the NE),

Before establishing a connection to an NE according to this connection type, an entry in the WaveStar CIT address list has to be created, containing the TID and the TCP/IP address for the NE. After that a separate view has to be created for the NE.

The procedure to be used for this special case is clearly described in [“Network element selection and login using the address list” \(22-23\)](#).

- via an OSI connection, if the network element does not support TARP (refer to [“TARP” \(14-38\)](#)) for Name/Address resolution,

Before establishing a connection to an NE according to this connection type, an entry in the WaveStar CIT address list has to be created, containing the TID, the TCP/IP and the NSAPs address for the NE. After that a separate view has to be created for the NE.

The procedure to be used for this special case is clearly described in [“Network element selection and login using the address list” \(22-23\)](#).

- remotely via TCP/IP on a gateway NE.
Before establishing a connection to an NE according to this connection type, an entry in the WaveStar CIT address list has to be created, containing the TID and the TCP/IP address for the NE and the definition that the NE has to be used as TCP/IP gateway. After that a separate view has to be created for the NE.

The procedure to be used for this special case is clearly described in [“Network element selection and login using the address list” \(22-23\)](#).

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

1. log into the WaveStar CIT, and

Required equipment

The following equipment is required to perform this task:

- WaveStar CIT

Prerequisites for NEs to be connected via TCP/IP (directly or via TCP/IP gateway)

Prior to performing this task, the following preconditions have to be fulfilled for the NE:

- the NE must have an TCP/IP address,
- if necessary, the **TCP/IP Gateway Host List** has to be provisioned for the NE (refer to [“Configuring a NE as T-TD Gateway” \(3-39\)](#)),
- if necessary, the **TCP/IP Gateway Control** has to be enabled for the NE (refer to [“Configuring a NE as T-TD Gateway” \(3-39\)](#)),
- the **LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),

- the **IP LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)),
- the **OSI LAN Status** of the connection has to be enabled for the NE (refer to [“Configuring the basic DCN parameters for an NE” \(3-28\)](#)).

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.

Network element selection and login using the NE Name box

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 the used **NE Type**.
- 3 Select the **Connection Type** to be used.

IF	THEN
the WaveStar CIT is connected to the NE via OSI connection (directly or remotely)	select OSI and click Graphical . Result: The WaveStar CIT password is now being used for a login attempt to the NE. Reference: Continue with Step 6 .
the WaveStar CIT is connected to the NE directly via TCP/IP.	select TCP/IP and click Graphical . Result: The TCP/IP Configure window is displayed. Reference: Continue with Step 5 .

IF	THEN
remotely via a GNE (WaveStar CIT connected to the user panel of the GNE),	select TCP/IP and click Graphical . Result: The TCP/IP Configure window is displayed. Reference: Continue with Step 4 .

-
- 4 In the **TCP/IP Configure** window enter the TCP/IP address and the port for the GNE and click **OK**.

Result:

The WaveStar CIT password is now being used for a login attempt to the NE.

Reference:

Continue with [Step 6](#).

-
- 5 In the **TCP/IP Configure** window enter the TCP/IP address and the port for the NE and click **OK**.

Result:

The WaveStar CIT password is now being used for a login attempt to the NE.

Reference:

Continue with [Step 6](#).

-
- 6 If this password is accepted, no extra login window for the NE will appear. In this case, continue with [Step 9](#).

-
- 7 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”.

-
- 8 Click **OK** to connect.

-
- 9 Click **OK** to the legal notice.

Result:

The **System View** window appears for the selected NE.

-
- 10** 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” \(2-25\)](#) and [“Changing super user IDs” \(2-22\)](#).

END OF STEPS

**Network element selection
and login using the
“Graphical System View”**

In order to log into the NE, proceed as follows:

-
- 1** In the NE Connection Type Selection pull down menu (refer to [“Elements of the main window” \(22-31\)](#)), select the view type corresponding to type of connection you want to establish to the NE (refer to [“NE connection types” \(22-34\)](#)).

IF	THEN
you want to establish a connection to an NE which is directly connected via the user panel of the NE,	select CIT OSI Neighbors from View Type Selection pull down menu.
you want to establish a connection from the WaveStar CIT to an NE, which is connected to the WaveStar CIT together with other NEs via a Local Area Network (LAN) (refer to “WaveStar CIT LAN access (network)” (22-13)),	select CIT OSI Neighbors from View Type Selection pull down menu.

IF	THEN
you want to establish a connection to an NE which is not connected as described before,	continue with “Network element selection and login using the address list” (22-23) .

Result:

The NE views defined for the NEs which have connections defined for that connection type will be shown on the NE Icons view on the right of the window.

.....

- 2 Log into the NE by double clicking on the respective icon in the NE view.

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 5](#).
-

- 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” \(2-25\)](#) and
[“Changing super user IDs” \(2-22\)](#).

END OF STEPS

**Network element selection
and login using the
address list**

In order to log into the NE, proceed as follows:

- 1 Enter the NE in the address list.

Reference:

Refer to [“Administering the address list at the WaveStar CIT” \(3-19\)](#).

- 2 Create a new view for the NE.

Reference:

Refer to [“Administering NE views” \(22-51\)](#).

- 3 Select the added NE (that you added in the address list) and bring it in the new made view.

Reference:

Refer to [“Administering NE views” \(22-51\)](#).

- 4 In the WaveStar CIT main window use the NE Connection Type Selection pull down menu (refer to [“Elements of the main window” \(22-31\)](#)) to select the view type corresponding to the connection type you want to establish to the NE.

- 5 Select the new created view.

- 6 Log into the NE according to the type of connection you want to establish to the NE.

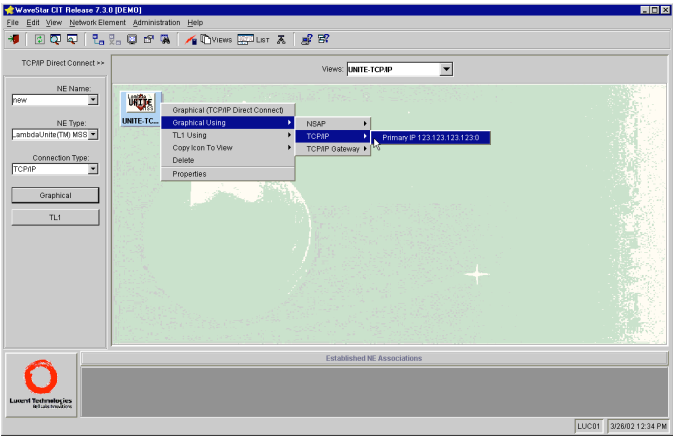
IF	THEN
you want to establish a connection of the connection type TCP/IP Direct Connect ,	Continue with Step 7 .
you want to establish a connection of the connection type TCP/IP Gateway ,	Continue with Step 8 .
you want to establish a connection of the connection type OSI Provisioned ,	Continue with Step 9 .

- 7 Right-click on the NE icon and select **Graphical Using → TCP/IP → Primary IP <IP address>**.

Result:

The WaveStar CIT password is now being used for a login attempt to the NE.

Example:



Reference:

Continue with [Step 10](#).

-
- 8 Right-click on the NE icon and select **Graphical Using** → **TCP/IP Gateway** →

Result:

The WaveStar CIT password is now being used for a login attempt to the NE.

Reference:

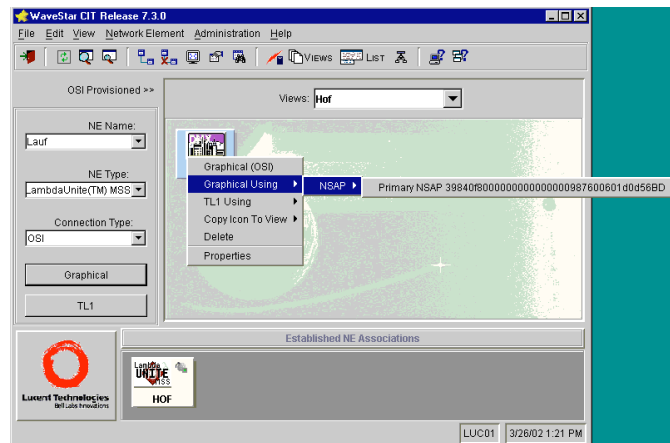
Continue with [Step 10](#).

-
- 9 Right-click on the NE icon and select **Graphical Using** → **NSAP** → **Primary NSAP <NSAP address>**.

Result:

The WaveStar CIT password is now being used for a login attempt to the NE.

Example:



Reference:

Continue with [Step 10](#).

-
- 10 If this password is accepted, no extra login window for the NE will appear. In this case, continue with [Step 12](#).
-
- 11 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”.

.....

- 12** Click **OK** to connect.
-

- 13** Click **OK** to the legal notice.

Result:

The **System View** window appears for the selected NE.

.....

- 14** 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” \(2-25\)](#) and
[“Changing super user IDs” \(2-22\)](#).

END OF STEPS

.....



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** push-button.

E N D O F S T E P S



WaveStar® CIT main window

Overview

Purpose This chapter provides information you should know before performing specific tasks, e.g.:

- 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	22-30
Tool bar of the <i>WaveStar</i> CIT	22-32
NE connection types menu	22-34
Standard window components	22-36
Selection windows	22-41
General window handling	22-45
General pushbuttons	22-48
Basic operations	22-50
Administering NE views	22-51
Overview of the menu structure	22-55

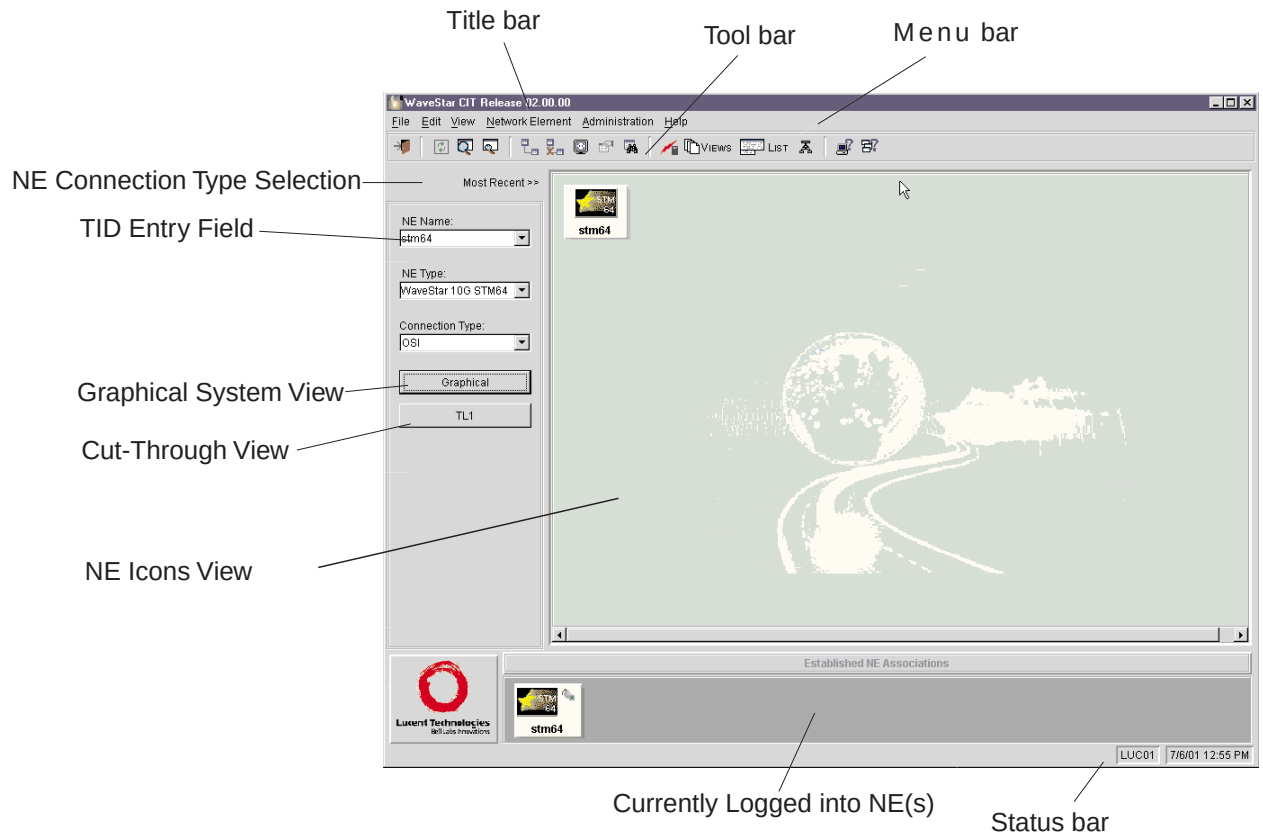


Elements of the WaveStar® CIT user interface

- 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.
 - NE icons view

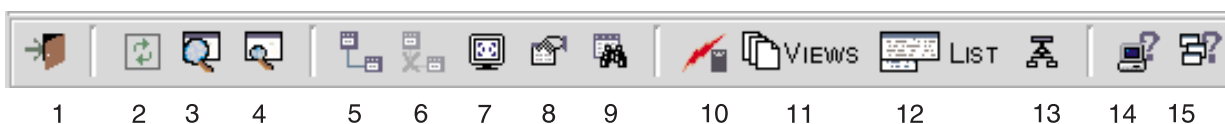
The following figure illustrates the WaveStar CIT main window.



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 OSI View Ctrl+R
3	Large icon view	View/Large Icons
4	Small icon view	View/Small Icons
5	Connect to NE	Network Element/Graphical
6	Disconnect from NE	Network Element/Disconnect from NE
7	Cut-Through view	Network Element/TL1
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.

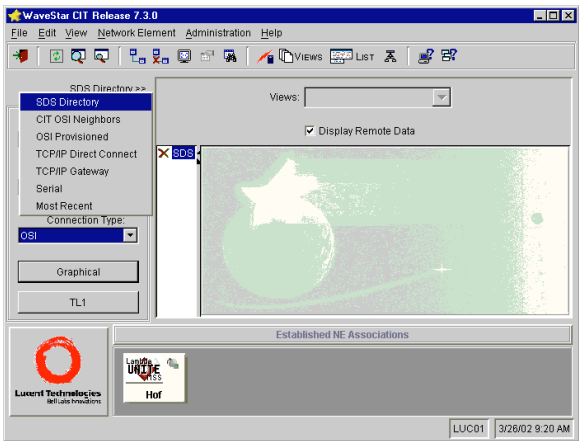
Moreover, the **Toolbar** tab in the **Preferences** window allows you to change the above described standard setting of the toolbar icons. Also, the toolbar can be re-arranged to another location on the screen by using the **Toolbar Location** group box.



NE connection types menu

Overview The NE connection types menu provides push-button access to different NE views. When a connection type is selected, the NE views and NEs which have connections defined for that type will be shown on the NE Icons view.

Example The following figure gives an example for selecting NE connection type menus:



NE connection types The NE connection types are as follows:

NE connection types	Description
SDS Directory	Not used for <i>LambdaUnite™</i> MSS.
CIT OSI Neighbors	The icons for the NEs which are the OSI neighbors of the NE to which the <i>WaveStar®</i> CIT is connected (via the user panel) are displayed.
OSI Provisioned	The icons for the NEs which have connections defined for the connection type OSI Provisioned are displayed.
TCP/IP Direct Connect	The icons for the NEs which have connections defined for the connection type TCP/IP Direct Connect are displayed.
TCP/IP Gateway	The icons for the NEs which have connections defined for the connection type TCP/IP Gateway are displayed.

NE connection types	Description
Serial	The icons for the NEs which have connections defined for the connection type Serial are displayed.
Most Recent	Displays graphical icons for the last up to 25 distinct NEs to which this user has established a GUI connection. If there are fewer than 25 distinct NEs to which this user has connected, this list will be shortened.

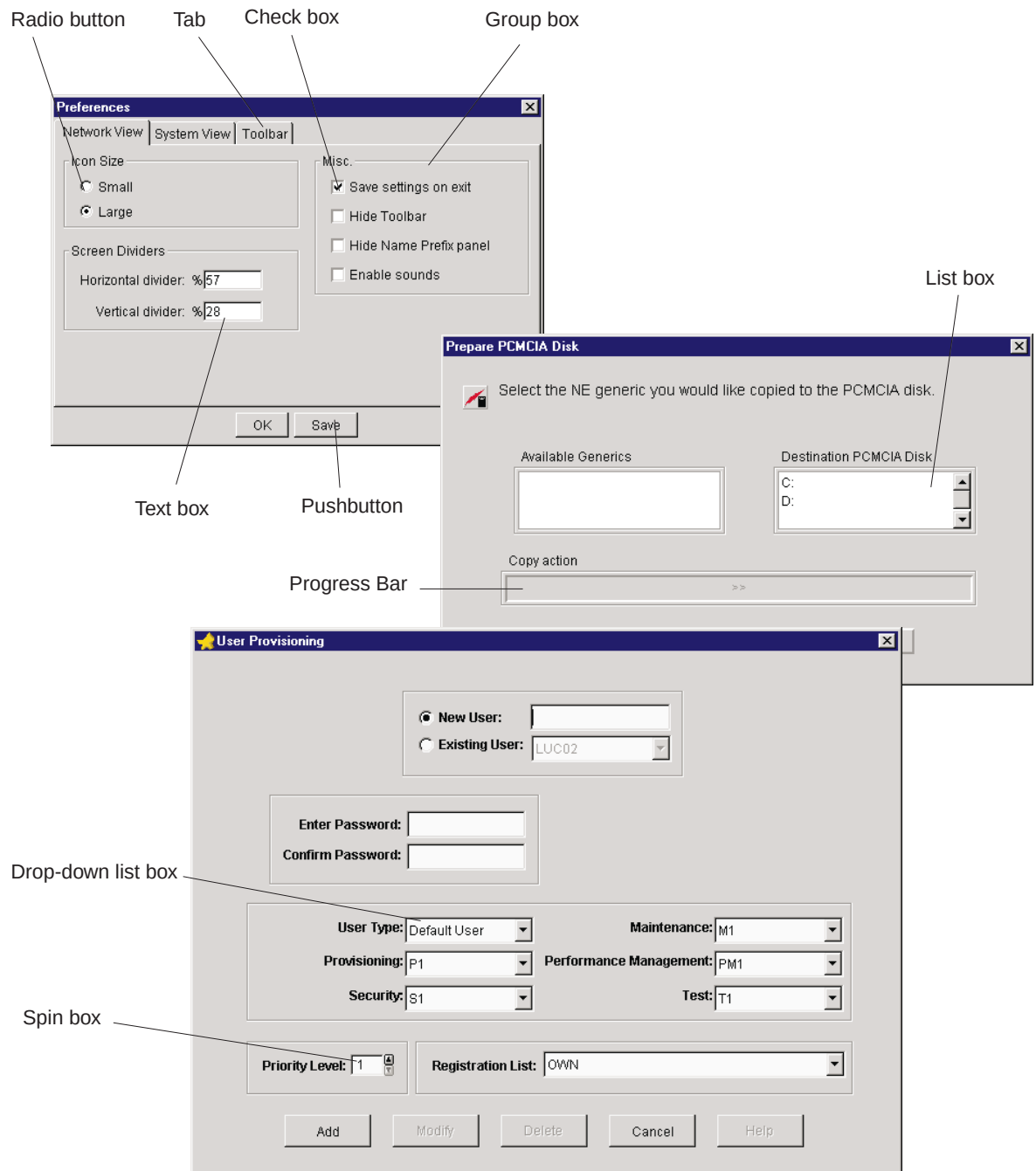
Reference How to administer NE view types is described under [“Administering NE views” \(22-51\)](#).



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.



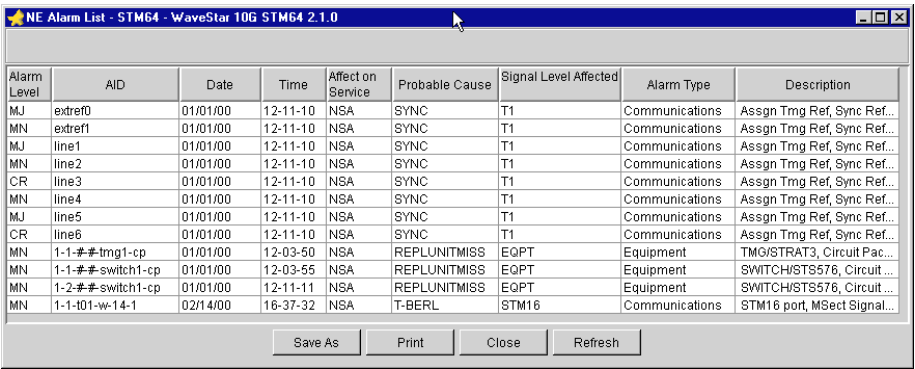
Functions of the window elements

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	Assign Tmg Ref, Sync Ref...
MN	extref1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
MJ	line1	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
MN	line2	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
CR	line3	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
MN	line4	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
MJ	line5	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
CR	line6	01/01/00	12-11-10	NSA	SYNC	T1	Communications	Assign Tmg Ref, Sync Ref...
MN	1-1-#-lmg1-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	1-1-101-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".



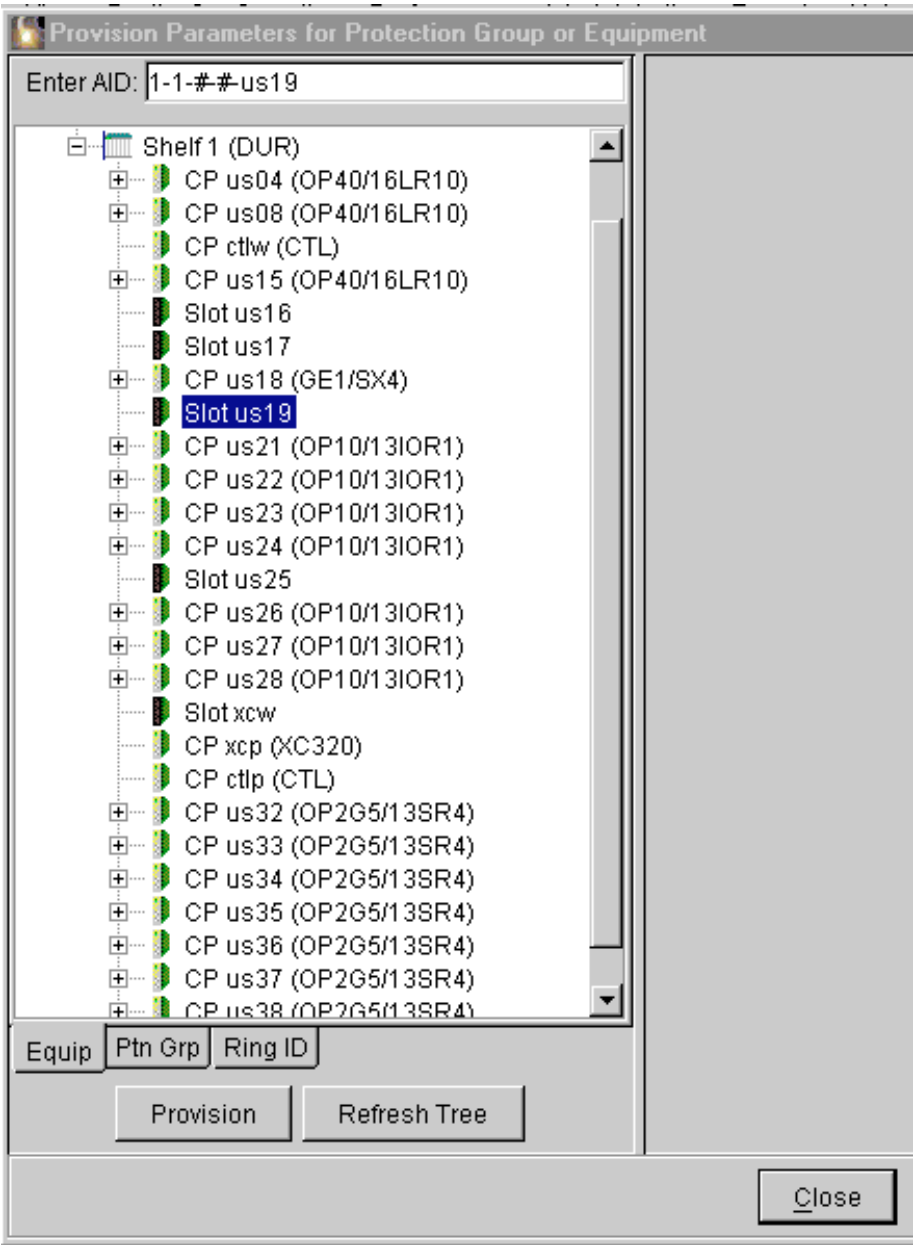
Selection windows

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 (**Equip**)
- Protection Group (**Ptn Grp**)
- Ring IDs (**Ring ID**)
- Path Protection Group (**Path Ptn**).

Window layout The following figure shows an example of a selection window.



The *Equipment* tab The window displays information on the inserted circuit packs, ports and tributaries.

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” (18-13) .
The <i>Path Ptn. Grp</i> tab	The tab Path Ptn. Grp. is similar to the tab Equipment . Any named path protection group established on the system can be selected on this tab. For further information on protection, please refer to “Protection mechanisms” (18-13) .
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” (15-9))
Specifying a component, a termination point, etc.	There are two methods to specify/identify a particular component (shelf, slot, circuit pack, port, etc.), 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” (15-9)).
Directory tree	You can make multiple selections browsing through the directory tree until finally selecting the desired item. 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.
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

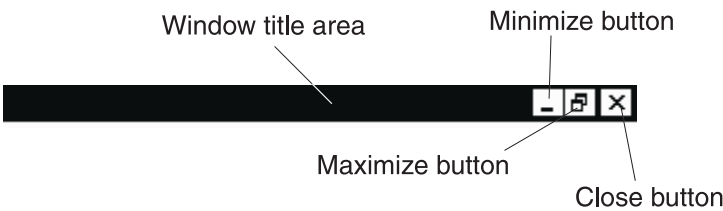
It depends on the outer window type which selection in a selection window is valid and which is invalid. A valid selection can be recognized by means of the **Select** or **Provision** pushbutton at the bottom of the selection window. If a selection in the directory tree or in the **Enter AID** field 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	THEN
you want to minimize a window,	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 Windows® operating system 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.

Designa- tion	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)**.



Administering NE views

When to use Use this procedure to add, modify or delete NE views.

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:

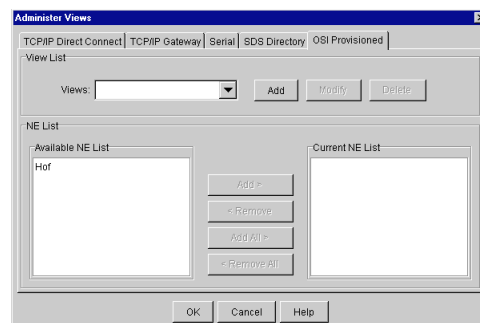
- WaveStar CIT

Instructions Complete the following steps to administer graphical views at the WaveStar CIT.

- 1 From the WaveStar CIT main menu select **Administration** → **Administer Views...**

Result:

The **Administer Views** window opens.



- 2 Choose the corresponding connection type (please refer to [“NE connection types” \(22-34\)](#)) as follows.

IF	THEN
you want to administer views of the connection type TCP/IP Direct Connect ,	in the Administer Views window select the tab TCP/IP Direct Connect .
you want to administer views of the connection type TCP/IP Gateway ,	in the Administer Views window select the tab TCP/IP Gateway .
you want to administer views of the connection type OSI Provisioned ,	in the Administer Views window select the tab OSI Provisioned. Important! The views for the following connection types are not used for <i>LambdaUnite™</i> MSS NEs. • Serial • SDS Directory

3 The NE views can be administered as follows.

IF	THEN
you want to add an NE view,	1. In the group box View List select Add. 2. In the displayed screen enter a name for the new view and click OK. 3. In the group box NE List select an NE from the Available NE List and click Add.
you want to change the name of an existing NE view,	1. select the respective entry in the group box View List and click Modify. 2. In the displayed screen enter the new name and click on OK.
you want to delete an NE view,	Select the respective entry in the group box View List and click Delete .

IF	THEN
you want to add an NE to a view,	1. In the group box View List select the view to which you want to add an NE. 2. In the group box NE List select the NE in the Available NE List and click Add.
you want to add all NEs to a view,	1. In the group box View List select the View to which you want to add all NEs. 2. In the group box NE List click on the Add All button.
you want to remove an NE from a view,	1. In the group box View List select the View from which you want to remove an NE. 2. In the group box NE List select the respective NE in the Current NE List and click Remove.
you want to remove all NEs from a view,	1. In the group box View List select the View from which you want to remove all NEs. 2. In the group box NE List click on the Remove All button.

4 Click **OK**.

Result:

The **Administer Views** window is closed.

END OF STEPS

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” (22-16)
	Login as New User...		“Administering user logins” (2-3)
	Exit		“WaveStar CIT login/logout procedure” (22-9)
Edit	Copy Icon(s) To		“Network element selection and login” (22-16)
View	Refresh OSI View		“Network element selection and login” (22-16)
	Large Icons		
	Small Icons		
	Arrange Icons	NE Name	
		NE Type	
	Preferences...		“Basic operations” (22-50)
Network Element	Graphical...		“Network element selection and login” (22-16)
	TL1...		“Entering the Cut Through view” (22-83)
	Disconnect from NE... (only accessible if connection to NE already established)		“Logout from NE(s)” (22-27)
	Disconnect from All NEs (only accessible if connection to NE already established)		
	FSTS(not accessible)		
	Find...		“Network element selection and login” (22-16)
	Properties... (only accessible if connection to NE already established)		

Menu function	Submenu		refer to
Administration	View CIT Administration...		“DCN protocols and services” (14-19) “NSAP address format” (14-24)
	Change Password...		“Changing user passwords” (2-25)
	Security	View User Logins...	“Displaying a list of all users logged into an NE” (2-38)
		User Provisioning...	“Creating a user login” (2-5)
		Change Superuser Login ID...	“Changing super user IDs on the WaveStar CIT” (2-23)
	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” (3-19)
	Administer Views...		“Network element selection and login” (22-16)
	Defaults...		
	Auto Router Discovery...		
	FTP Administration...		
	SDS Administration...		
Help	About WaveStar CIT...		“Basic operations” (22-50)
	Supported NEs...		



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.

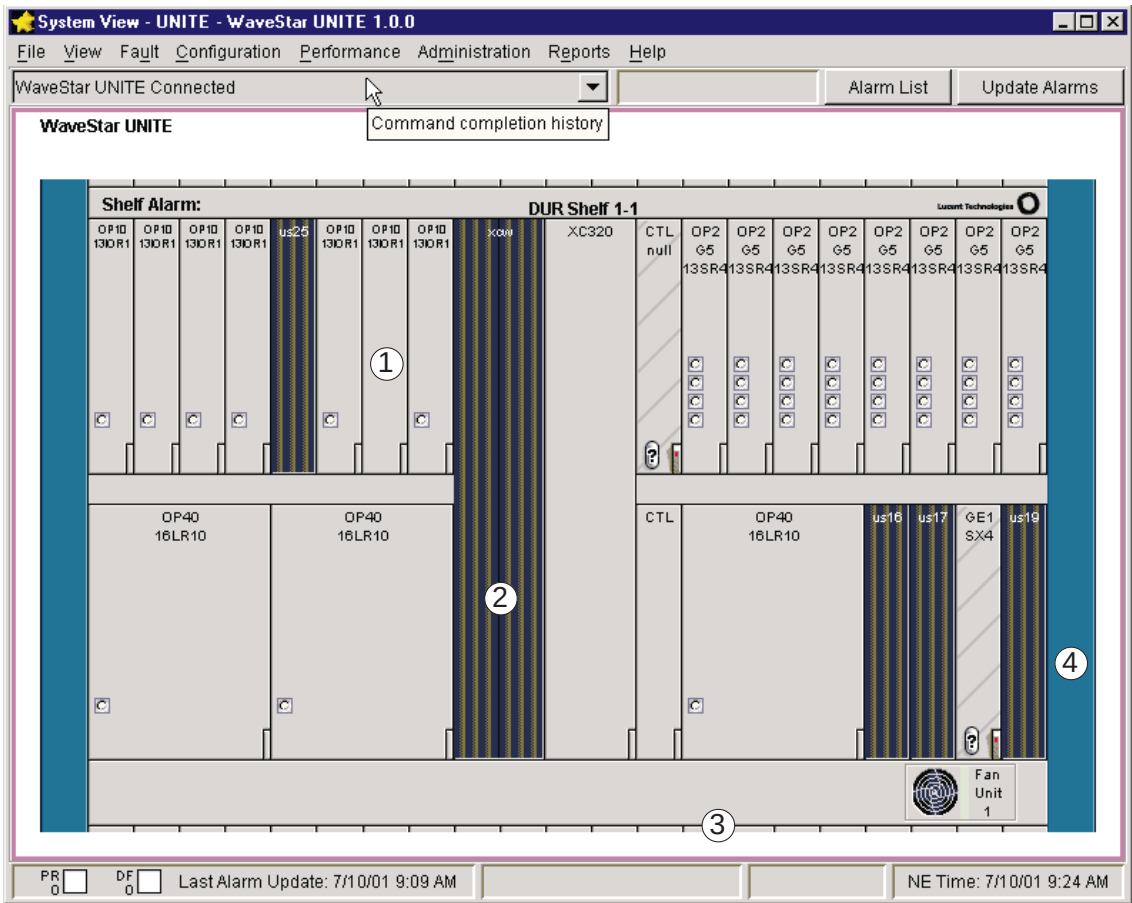
Contents

Shelf view	22-58
The ring map	22-68
Graphical view of the ring map	22-70
Overview of the shelf-view menu structure	22-72
Reports and log files	22-80
View rolling events	22-81



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
Help
- ② View Slot Details
mouse click right:

View Details
Create New Circuit Pack
Delete Circuit Pack
Provision Slot
Refresh Slot
Help
- 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
Facility Loopback
Refresh Port #
Help
- ④ View Shelf Details
mouse click right:

View Details
Provision Shelf
Refresh Shelf
Help

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” \(22-62\)](#)).
- 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” \(22-63\)](#)).
- 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” \(22-62\)](#), 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” \(22-58\)](#), 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” \(22-66\)](#)).

- A right-click on a port LED brings up a pop-up menu which provides several menu options shown in [“View Port Details window” \(22-66\)](#), 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” \(22-66\)](#)).
- 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” \(22-58\)](#), 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-#-#-08-cp
- Circuit Pack Type:** OP40/16LR10

Equipment Details

- Apparatus Code:** -
- Series Number:** -
- CLEI Code:** -
- Equipment Carrier Code:** -
- Serial Number:** -

Alarms

- Alarm Level:** Not Alarmed
- Equipment Alarm Severity Assignment Profile (unprot.):** DEFAULT
- Equipment Alarm Severity Assignment Profile (prot.):** -

At the bottom, there are four buttons: "Save As", "Refresh", "Close", and "Help". The "Save As" button is highlighted with a dashed border.



The image shows a software window titled "View Equipment Details" with a yellow star icon in the title bar. It contains two tabs: "Pack Data" and "Status", with "Status" currently selected. The "Status" tab is divided into two sections. The top section, labeled "Slot Status", displays three status indicators: "Slot Alarm Level: Not Alarmed", "Holder Status: Valid", and "Equipment Alarm Severity Assignment Profile: DEFAULT". The bottom section, labeled "Pack Status", displays "Operational Status: Enabled". At the bottom of the window, there are four buttons: "Save As", "Refresh", "Close", and "Help".

View Equipment Details

Pack Data | **Status**

Slot Status

Slot Alarm Level: Not Alarmed

Holder Status: Valid

Equipment Alarm Severity Assignment Profile: DEFAULT

Pack Status

Operational Status: Enabled

Save As Refresh Close Help

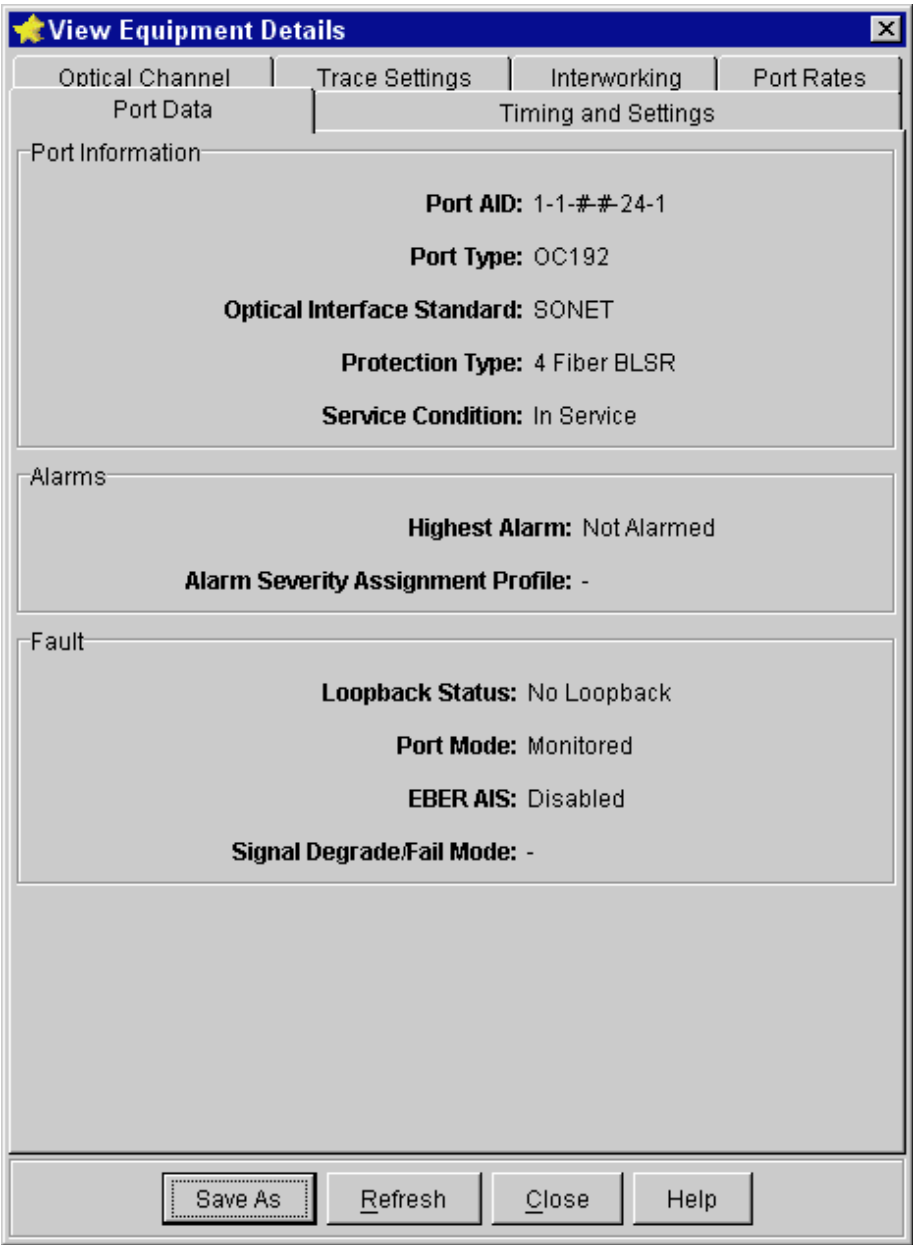
View Slot Details window The following figure illustrates the **View Slot Details** window.

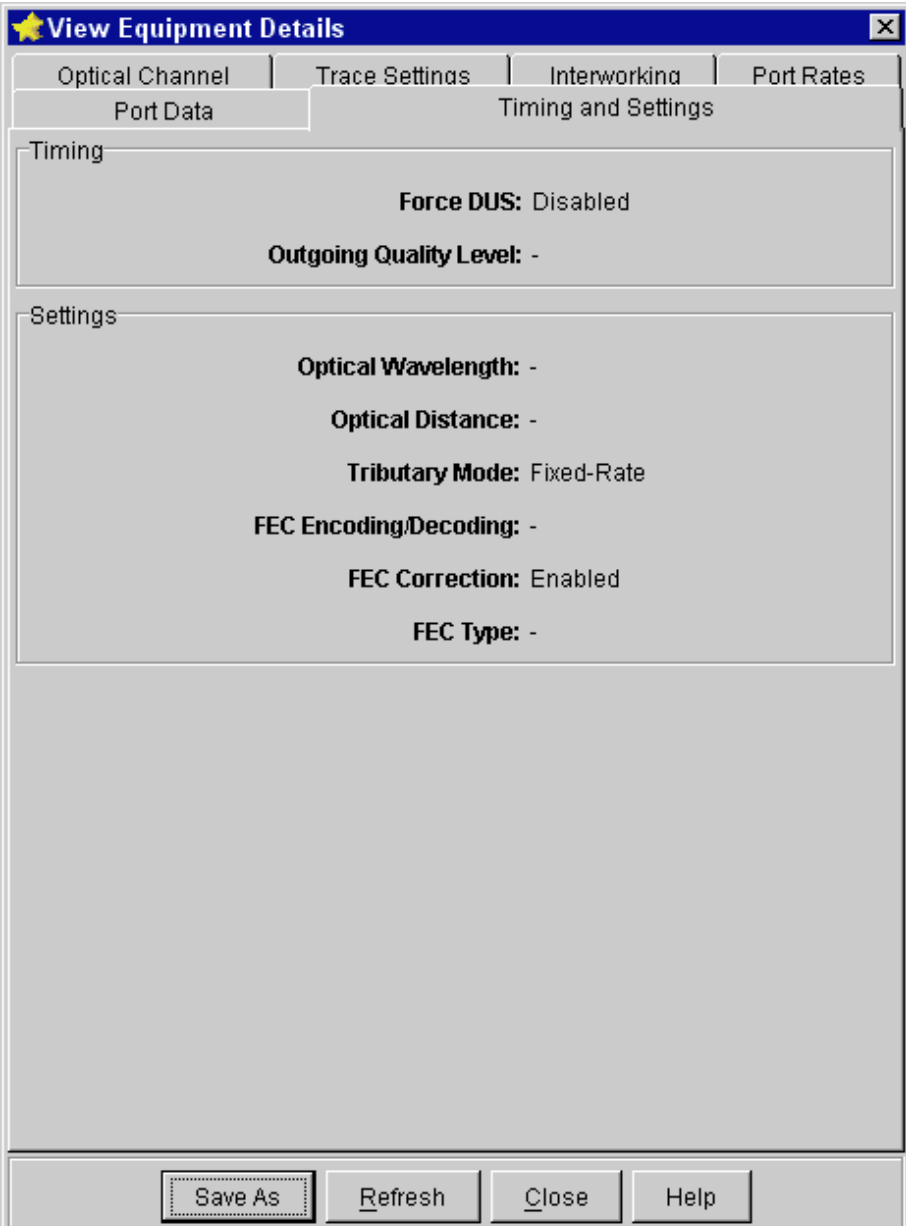
The screenshot shows a window titled "View Equipment Details" with a yellow star icon and a close button. The window is divided into four main sections:

- Slot Information:** Displays "Slot AID: 1-1-#-#16".
- Equipment:** Displays "Acceptable Pack Types: OP2G5/13SR4, OP10/13IOR1" and "Equipment Alarm Severity Assignment Profile: DEFAULT".
- Status:** Displays "Alarm Level: Not Alarmed" and "Slot Holder Status: Valid".
- Pack Data/Equipment Details:** Displays "Apparatus Code: -", "Series Number: -", "CLEI Code: -", "Equipment Carrier Code: -", and "Serial Number: -".

At the bottom of the window, there are four buttons: "Save As", "Refresh", "Close", and "Help".

View Port Details window The following figures illustrate the **View Port Details** window.





The image shows a software window titled "View Equipment Details" with a yellow star icon and a close button. It contains several tabs: "Optical Channel", "Trace Settings", "Interworking", "Port Rates", "Port Data", and "Timing and Settings". The "Timing and Settings" tab is active. Inside this tab, there are two sections: "Timing" and "Settings". The "Timing" section contains "Force DUS: Disabled" and "Outgoing Quality Level: -". The "Settings" section contains "Optical Wavelength: -", "Optical Distance: -", "Tributary Mode: Fixed-Rate", "FEC Encoding/Decoding: -", "FEC Correction: Enabled", and "FEC Type: -". At the bottom of the window are four buttons: "Save As", "Refresh", "Close", and "Help".

View Equipment Details

Optical Channel | Trace Settings | Interworking | Port Rates

Port Data | Timing and Settings

Timing

Force DUS: Disabled

Outgoing Quality Level: -

Settings

Optical Wavelength: -

Optical Distance: -

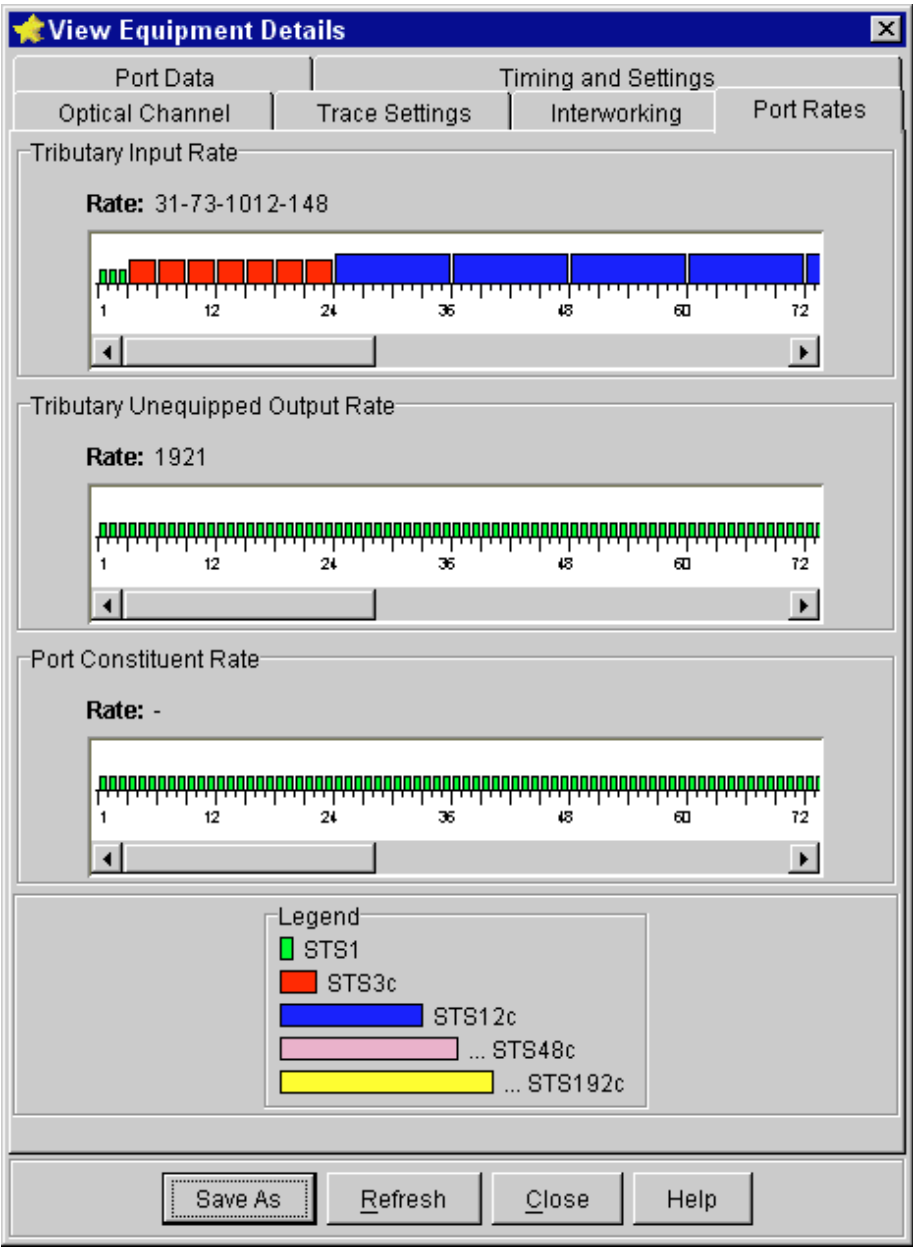
Tributary Mode: Fixed-Rate

FEC Encoding/Decoding: -

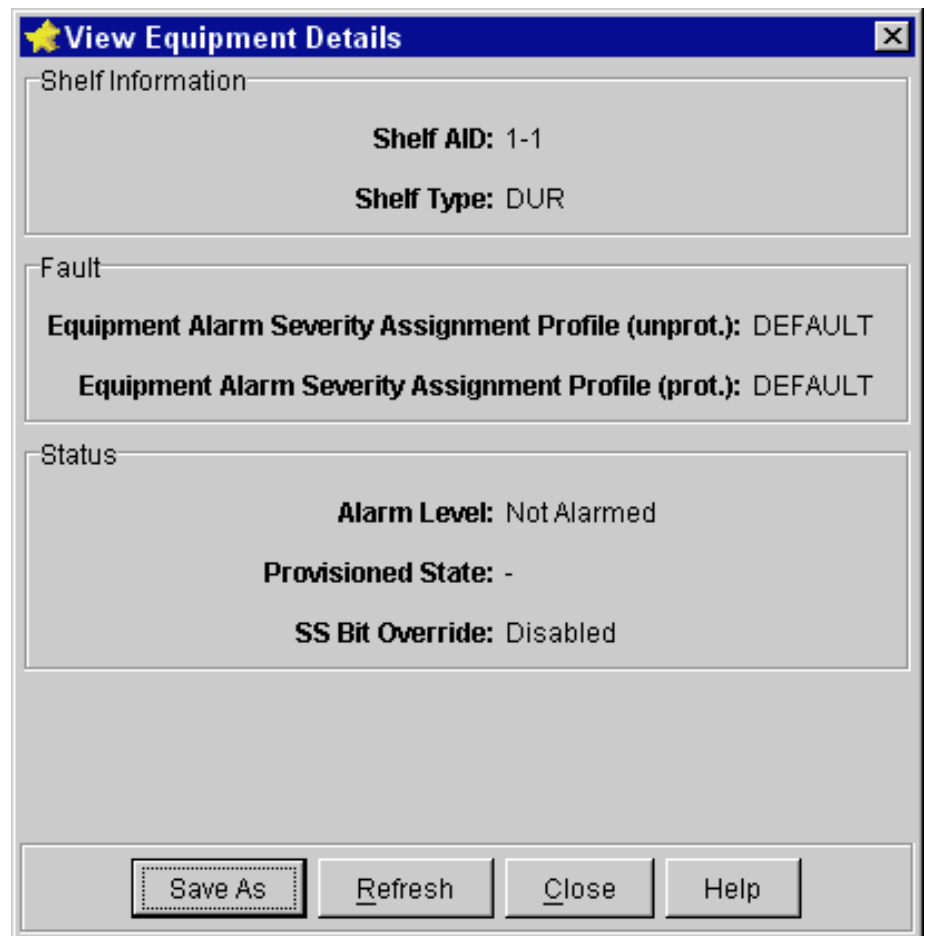
FEC Correction: Enabled

FEC Type: -

Save As | Refresh | Close | Help



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

Important! If a BLSR/MS-SPRing is composed of *LambdaUnite*[™] NEs together with other LUCENT products (e.g. BWB), link information is partly missing in the ring map for these products (i.e. the port information building the link). For that case the **Ring Map** in a multi product ring must be requested from an *LambdaUnite* node of this ring.

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 AID	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 AID	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).

Column	Description/Behavior
Network Entity 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 of the ring map

Overview 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.

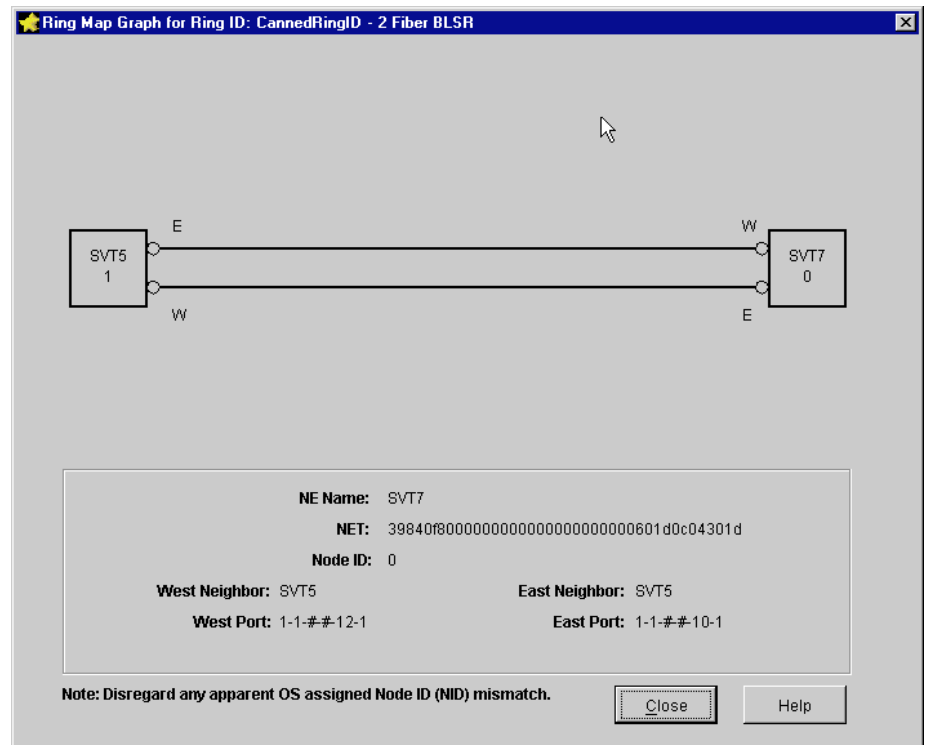
The data displayed at the bottom of the window for the selected NE are:

<i>Field ...</i>	<i>Displays...</i>
NE Name	the TID (target identifier) of this ring node NE
Network Entity Title	the network entity title for this ring node NE (network element).
Node ID	the ring address of this ring node NE. Possible values are the integers from 0-15, inclusive.
West Neighbor	the name of the NE immediately to the west of this NE.
East Neighbor	the name of the NE immediately to the east of this NE.
West Port	the west port AID (access identifier) on this node.
East Port	the east port AID (access identifier) on this node.

Authorization level You must have at least an M2, S2 or P1 authorization level to access this window.

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” (22-90)
	Disable TL1 Logging ...		
	Set/Change TL1 Logging File		
	NE Disconnect		“WaveStar CIT login/logout procedure” (22-9)

Menu function		Submenu	please refer to
View	Preferences		“Shelf view” (22-58)
	View Equipment Details...		
	View Rolling Events		“View rolling events” (22-81)
	Rings	Ring Map...	“The ring map” (22-68)
	Protection...		“Protection mechanisms” (18-13)
	View Alarms	View Alarm Severity Assignment Profile...	Chapter 5, “Alarm management”
		View Alarm Configuration...	
	Cross Connections...		“Parameters of the window “View Cross Connections”” (7-6)
	Loopback...		Chapter 5, “Alarm management”
	DCC Terminations...		Chapter 14, “Management communication setup concepts”
	Misc. Discretes...		“Configuring Miscellaneous Discrete Outputs” (4-115) “Configuring Miscellaneous Discrete Inputs” (5-48)
	Intershelf Bandwidth Utilization...		(not applicable for this release)
	Timing/Sync		“Viewing the timing configuration” (6-3)
	Software Generic...		Chapter 20, “Software upgrade concepts”
	NE Data...		Chapter 21, “Database backup concepts”
Refresh Equipment...		“Shelf view” (22-58)	
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...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	Alarm Severity Assignment Profile User List...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	Protection Switch...		Chapter 15, “Equipment provisioning concepts”
	Enter/Exit Maintenance Condition...	Enter Maintenance Condition...	Chapter 5, “Alarm management”
Exit Maintenance Condition...			

Menu function		Submenu	please refer to
	Inhibit/Allow Autonomous Message Reporting...	Current Session...	“Enabling or disabling autonomous alarm forwarding ” (5-46)
	Operate Output Misc. Discretes...		
	Analysis	Facility Loopback...	AMTCG (Alarm Messages and Trouble Clearing Guide)
		Cross-Connect Loopback...	
		Facility Failure States... (not accessible)	
		Equipment Failure States... (not accessible)	
		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...	Chapter 17, “Timing provisioning concepts”
		Switch Timing Reference Switch...	
		Output Timing Reference Switch...	

Menu function		Submenu	please refer to
Configuration	Provision...		“WaveStar CIT methods to perform provisioning” (15-4)
	Create New	Circuit Pack...	“Provisioning of new components” (15-6)
		Protection Group...	
	Exchange Circuit Pack...		
	Delete...		“Provisioning of new components” (15-6)
	Misc. Discretes...		“Configuring Miscellaneous Discrete Outputs” (4-115) “Configuring Miscellaneous Discrete Inputs” (5-48)
	DCC Terminations...		“Configuring data communication channels” (3-57)
	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 ASAP for a Shelf...	
	Software	Remote Backup...	Chapter 21, “Database backup concepts”
		Remote Restore...	AMTCG (Alarm Messages and Trouble Clearing Guide)
		Copy NVM...	
		Download Software...	
		Chapter 20, “Software upgrade concepts”	
Activate Software...			FTP Browser...

Menu function		Submenu	please refer to
Performance	Reports	SONET Section...	“Retrieving performance monitoring reports” (9-11)
		SONET Line...	
		SONET Path...	
		DS3 Line...	
		(not accessible)	
		DS3 Path...	
		(not accessible)	
		SDH Regenerator Section	
		SDH Multiplex Section	
		SDH Path	
		SDH UAT	
		(not accessible)	
		Ethernet	
	Initialize Registers...(not accessible)		
	View PM Ports...		“Retrieving performance monitoring settings for individual ports or tributaries” (9-5)
	Provision Ports...		“Enabling or disabling performance monitoring data collection” (9-2)

Menu function		Submenu	please refer to
Administration	Change Password...		“Changing user passwords” (2-25)
	Change Notifications		“Modifying a user’s own notification list” (2-31)
	Security	View User Logins...	“Displaying login information for an NE” (2-40)
		View Logged-In Users...	“Displaying a list of all users logged into an NE” (2-38)
		Disable User Login...	“Administering user logins” (2-3)
		Enable User Login...	
		Logout NE User...	“Logging out NE users” (2-17)
		User Provisioning...	“Administering user logins” (2-3)
		Security Provisioning...	“Provision global security parameters” (2-35)
	View NE Administration...		Chapter 3, “Management communication setup”
	View MAC Addresses...		“NSAP address fields” (14-25)
	Set Date and Time...		
	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 and log files” (22-80)
		Shelf...	
		Pack...	
		Port...	
		VCG...	
		Trib...	
		Misc. Discretes...	
	Status Lists	Shelf...	
		Pack...	
		Port...	
		Trib...	
	Cross-Connection List...		
	NE Alarm List...		
	NE Alarm Log...		
	Alarm Severity Assignment Profile User List...		
	NE Protection Switch Activity Log...		
	BLSR Protection Switch List...		
	NE Notification Log...		
Help	About This Network Element...		“Basic operations” (22-50)
	Help		Opens the alphabetical index for the task related online help.
	Library		Opens the online library.
	Description		Opens the alphabetical index for the screen specific online help.
	Support		Opens the technical support page for the LambdaUnite™ MSS.



Reports and log files

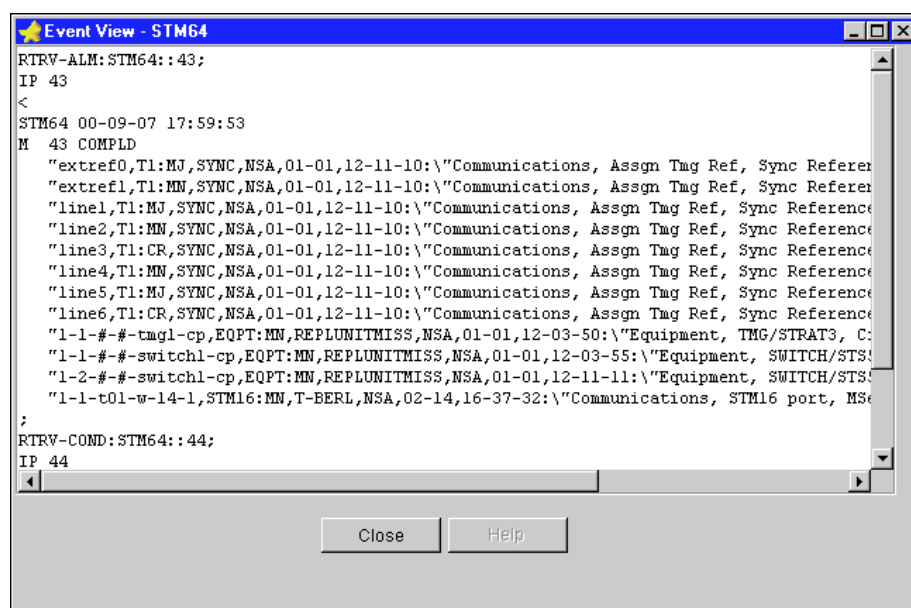
Overview	<i>WaveStar</i> ® CIT allows you to generate reports and log files of the NE equipment configuration, switched cross-connections, alarm lists, etc. via the Reports menu item.
Report formats	The reports and log files are formatted as tables and can be saved to a specified file (ASCII format) and/or can be sent as e-mail and/or to a printer. 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
Storage location	The user can decide where he wants to store the reports and log files on the CIT PC.
Report and log file forwarding	All reports and log files can be forwarded using any e-mail application implemented on the CIT PC.



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*

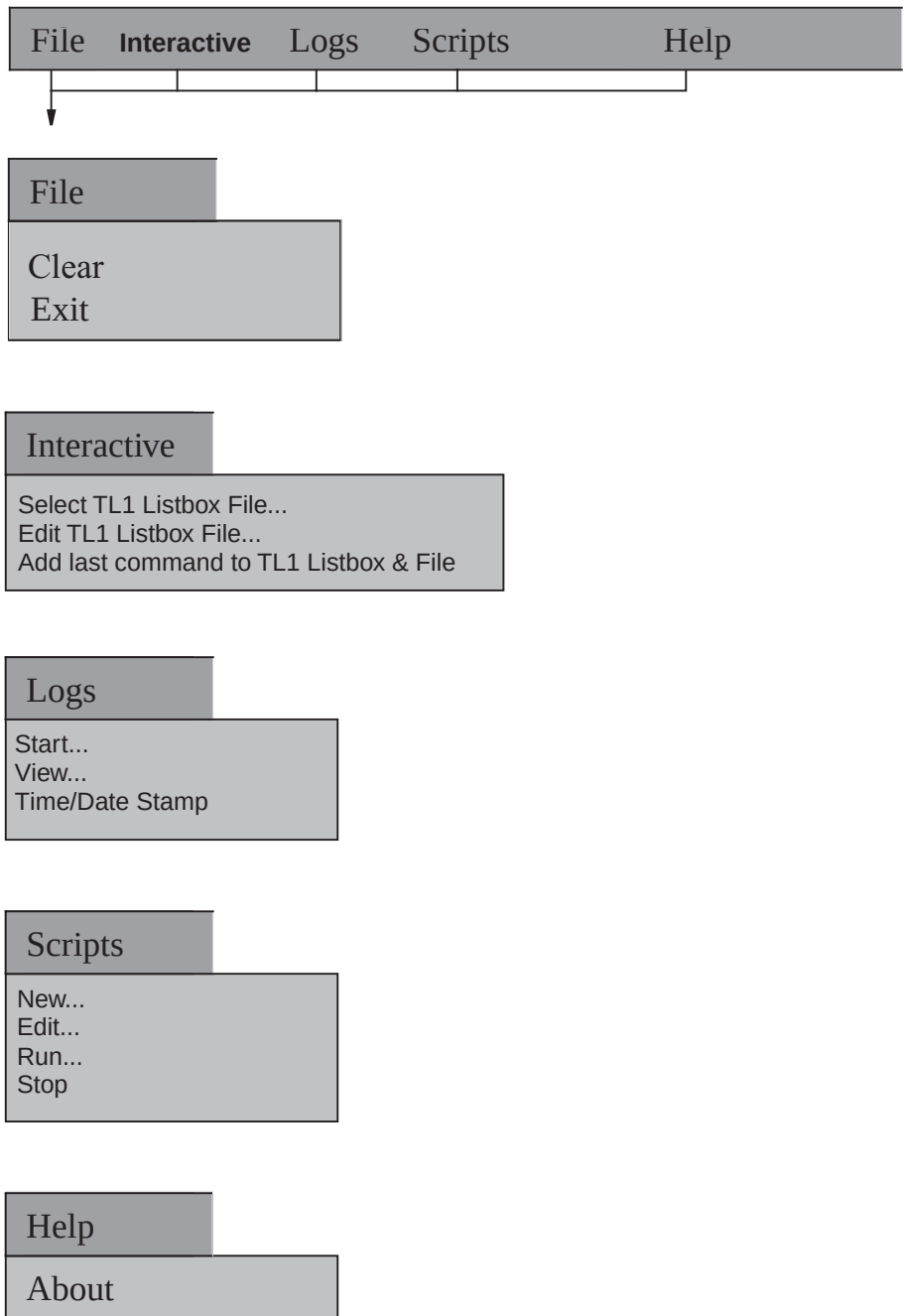
Contents

Entering the Cut Through view	22-83
Interactive – Execute TL1 single commands	22-85
Interactive – Manage a listbox file	22-87
Working with script files	22-88
Working with logs	22-90



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” (22-87)
Logs	see “Working with logs” (22-90)
Scripts	see “Working with script files” (22-88)
Help	see “Basic operations” (22-50)

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 Left-click on the **TL1** 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.

- 3 Click **OK**.

Result:

The **Cut Through** window appears.

- 4 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.

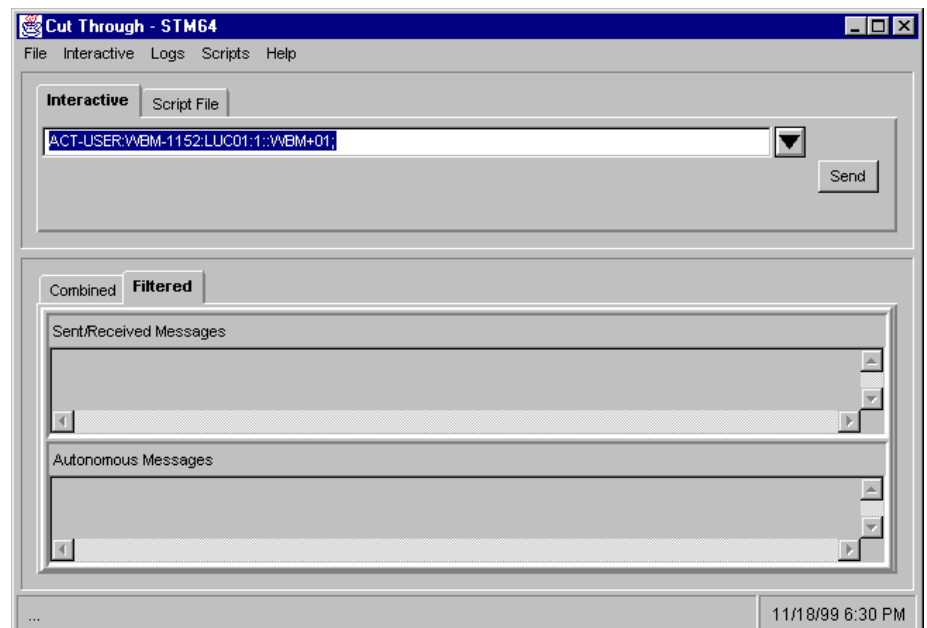
END OF STEPS



Interactive – Execute TL1 single commands

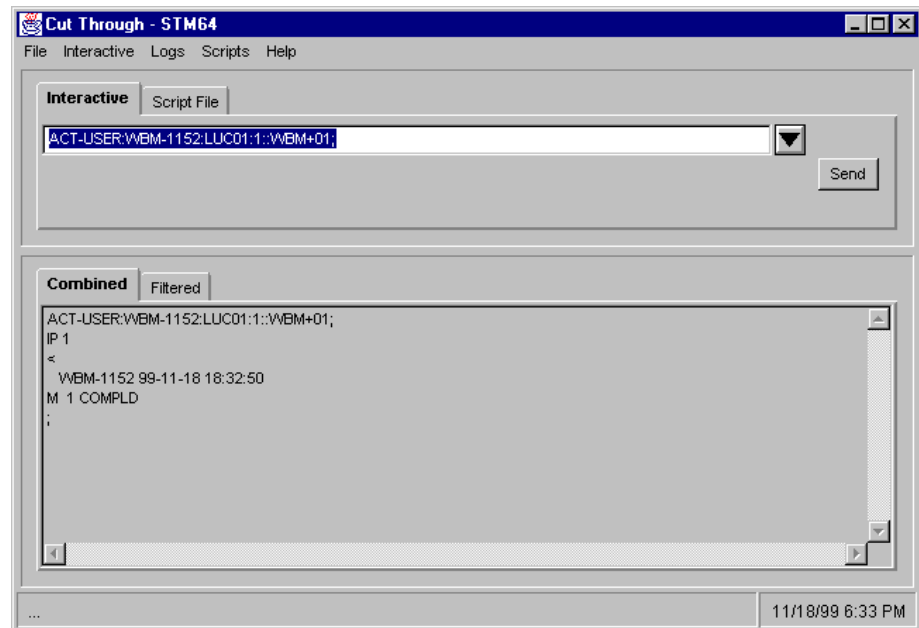
Two methods You can execute single TL1 commands on an interactive basis. There are two methods:

- 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” \(22-87\)](#)):
 - 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\ct\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

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 *WaveStar* 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 Telegraph and Telephone Consultative Committee.

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

LO

Low Order

Location

An identifier for a specific circuit pack, interface module, interface port, or communications link.

Lockout of Protection

The *WaveStar* 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, *WaveStar* 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 *WaveStar* 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 *WaveStar* 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 *WaveStar* 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 Message

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

Numerics

- 1-way cross-connection, [7-20](#)
- 1-way path-protection, [7-20](#)
- 1-way path protection, [7-67](#)
- 1-way cross-connection, [18-4](#)
- 1-way path protected cross-connection, [18-4](#)
- 2-way cross-connection, [7-20](#)
- 2F-Multiplex Section Shared Protection Ring (MS-SPRing), [7-57](#)
- 2F-Bidirectional Line-Switched Ring (BLSR), [7-57](#)
- 2-way cross-connection, [18-4](#)
- 4F-Multiplex Section Shared Protection Ring (MS-SPRing), [7-60](#)
- 4F-Bidirectional Line-Switched Ring (BLSR), [7-60](#)

-
- A** ABN LED, [16-41](#)
- Abnormal conditions, [16-41](#)

- Access identifier, [15-9](#)
- Access identifier (AID)
 - Overview of AIDs, [15-10](#)
- Access Identifiers (AID), [18-8](#)
- Access privileges, [13-10](#)
- Access privileges; User access privileges, [13-3](#)
- Acknowledged Information Transfer Service (AITS), [14-34](#)
- ACO
 - button, [16-42](#)
- ACO button, [16-42](#)
- ACO LED, [16-41](#)
- Activity LED, [16-46](#), [16-49](#)
- Adaptive-rate tributary operation, [19-6](#), [19-21](#)
- Address List Overflow, [16-28](#)
- ADDROV
 - See: Address List Overflow
- ADM-16/1, [14-31](#)
- Affect-on-service attribute, [16-24](#)
- AFI Authority and Format Identifier, [14-25](#)

- AID, [15-9](#)
- AIS Seconds (AISS), [19-8](#)
- AIS-L
 - See: Alarm Indication Signal
- AIS-P
 - See: Alarm Indication Signal
- Alarm, [16-6](#)
- Alarm acknowledgment, [16-42](#)
- Alarm category, [5-10](#), [5-17](#)
- Alarm cut-off, [16-42](#)
- Alarm format, [5-3](#), [5-4](#), [16-11](#), [16-13](#)
- Alarm history, [5-12](#), [5-12](#)
- Alarm Indication Signal
 - AIS-L, [16-33](#)
 - AIS-P, [16-32](#)
- Alarm indicators, [16-20](#)
- Alarm LEDs, [16-41](#)
- Alarm level, [5-8](#), [5-14](#)
- Alarm list, [5-6](#)
- Alarm log, [5-12](#), [13-19](#), [13-20](#)
- Alarm notification, [5-46](#), [16-5](#), [16-23](#)

Alarm notifications
(ALARMS), [13-15](#)

Alarm presentation formats,
[16-10](#)

Alarm severities, [16-42](#)

 SDH format, [16-11](#),
 [16-13](#)

 SONET format, [16-11](#),
 [16-13](#)

Alarm severity, [16-23](#)

Alarm Severity Assignment
Profile (ASAP), [4-39](#),
[4-44](#), [5-24](#), [5-27](#), [5-29](#),
[5-31](#), [5-34](#), [5-36](#), [7-40](#),
[7-43](#), [7-56](#)

Alarm severity assignment
profile (ASAP), [7-99](#)

Alarm Severity Assignment
Profile (ASAP), [15-15](#),
[15-16](#), [15-17](#), [16-10](#),
[16-13](#), [16-26](#)

 ASAP name, [5-27](#),
 [16-34](#)

 ASAP types, [16-27](#)

 Automatic Protection
 Switch, [16-28](#)

 Basic ASAP variants,
 [16-26](#)

 Data Communications
 Network, [16-28](#)

 Default ASAP, [5-36](#)

 DEFAULT ASAP, [16-28](#)

 Environmental
 (Miscellaneous
 Discrete), [5-48](#), [16-29](#)

 Equipment unprotected,
 [16-29](#)

 Equipment with
 Protection State
 Dependence, [16-30](#)

Ethernet, [16-31](#)

Maximum number of
ASAPs, [16-34](#)

MS-SPRing and
Bilateral Switched
Ring Protection
Switch, [16-31](#)

Non-reporting ASAP,
[5-29](#), [5-36](#)

Path MSA/NIM related,
[16-32](#)

Path Termination, [16-32](#)

SDH/SONET ports,
[16-33](#)

Sub-Network
Connection Protection
and Unidirectional
Path Switched Ring,
[16-33](#)

System Timing, [16-34](#)

Alarm signalling, [16-18](#)

Alarm status, [7-36](#), [7-39](#),
[7-42](#)

Alarm status display, [5-6](#),
[5-11](#), [16-20](#)

Alarm test, [16-44](#)

Alarm type
See: Alarm category

Anomaly, [16-4](#)

Antistatic covers, [1-26](#)

APSC
See: Inconsistent APS
Codes

Area address, [3-6](#), [3-14](#),
[3-14](#), [3-28](#), [3-35](#), [3-68](#),
[3-69](#), [14-25](#), [14-28](#), [14-37](#)

Area identifier, [14-6](#), [14-25](#)

ASAP
See: Alarm Severity
Assignment Profile

ASAP Alarm Severity
Assignment Profile, [15-16](#)

Audible alarms, [5-3](#), [5-4](#)

Authority and Format
Identifier (AFI), [14-25](#)

Authorization level, [13-3](#),
[13-10](#)

Auto-Learn NSAP function,
[3-14](#)

Automatic Protection
Switch, [15-6](#)

Automatic Protection
Switch (APS), [18-19](#)

Automatic Protection
Switching (APS), [7-35](#),
[7-35](#), [7-36](#), [7-37](#), [7-54](#),
[7-93](#), [8-3](#), [18-13](#)

Autonomous alarm
forwarding, [5-46](#), [16-23](#)

Autoprovisioning, [15-2](#)

.....

B B1 byte, [18-49](#), [19-4](#)

B2 byte, [18-49](#)

B2 bytes, [19-4](#)

B3 byte, [19-4](#)

Background Block Errors
(BBE), [19-7](#)

Background Block Errors
(BBE), [19-8](#)

Backplane Read Failure,
[16-29](#)

Backup Database

 CIT, [21-3](#)

 FTAM, [21-3](#)

 FTTD, [21-3](#)

Barred-hand symbol, [1-20](#)

Basic configuration
parameters, [4-5](#), [4-7](#)

BCH-2 algorithm, [16-38](#)

Bell symbol, [16-21](#)

Bidirectional
cross-connection, [18-4](#)

Bidirectional Line
Switched Ring, [7-20](#), [15-6](#)

Bidirectional Line
Switched Ring (BLSR),
[18-13](#)

Bidirectional Line
Switched Rings (BLSR),
[18-21](#)

Bidirectional
Line-Switched Ring
(BLSR), [7-39](#), [7-42](#), [7-93](#),
[8-7](#), [8-11](#)

BIP
See: Bit-interleaved parity

Bit error monitoring, [4-61](#),
[5-42](#), [18-49](#)

Bit errors, [19-4](#)

Bit-interleaved parity
(BIP), [19-4](#)

BKUPMEMO
See: NVM Shortage

BKUPMEMP
See: IDE Flash Card
Access Fail

Block errors, [19-4](#)

Blocking, [16-5](#)

BLSR, [7-20](#), [7-57](#), [7-60](#),
[18-21](#)

BPEF
See: Backplane Read
Failure

Bridging a
cross-connection, [7-28](#)

C CBR
See: Total number of
bytes received

CBS
See: Total number of
bytes sent

Central office alarm
facility, [16-51](#)

Change your password,
[2-23](#), [2-26](#), [2-28](#)

Characters allowed in a
password, [13-8](#)

Characters allowed in a
TID, [3-3](#), [3-27](#), [14-41](#)

Characters allowed in a
user login, [13-7](#)

CICOMF
See: CICTL Comm
Failure

CICTL Comm Failure,
[16-29](#)

CICTL Failure, [16-29](#)

CICTL not Present, [16-29](#)

CICTL Powered Down,
[16-29](#)

CIF
See: CICTL Failure

CIMISS
See: CICTL not Present

CIPWRDWN
See: CICTL Powered
Down

Circuit pack alarm
indicator, [16-21](#)

Circuit Pack Clock Failure,
[16-30](#)

Circuit Pack Comm
Failure, [16-29](#)

Circuit Pack Failure, [16-30](#)

Circuit Pack not Present,
[16-30](#)

Circuit pack provisioning,
[15-6](#)

Circuit pack status
indications; Status
indications, [16-47](#), [16-47](#)

Circuit Pack Type
Mismatch, [16-30](#)

circuit packs, [15-8](#)

CIT connector, [16-42](#)

Clear Mode Switch, [6-42](#)

Clear validation time, [16-4](#)

Climatic conditions, [1-27](#)

CLNP PDU lifetime, [3-6](#),
[3-28](#), [3-35](#), [3-68](#)

Clock protection, [6-17](#)

Code violations, [19-4](#), [19-4](#)

Code Violations (CV),
[19-7](#), [19-8](#)

Collapsed nodes, [7-74](#),
[18-4](#), [18-34](#)

Color scheme, [16-21](#)

Comm Channel Failure,
[16-29](#)

CompactFlash[™] card, [20-2](#)

Compound AID, [15-10](#)

Connection types, [18-3](#)

Connectionless Network
Protocol (CLNP), [14-4](#),
[14-40](#)

Connectionless Network
Service (CLNS), [14-40](#)

Connector types, [1-15](#)

Consequent actions, [16-5](#)

Conventions, [xxiii](#)

Correlated fault cause, [16-5](#)

Correlation, [16-5](#)

Cost of a route, [14-35](#)

CPCOMF
See: Circuit Pack Comm Failure

CPDEGR
See: Unit Cooling Degraded

CPFAIL
See: Circuit Pack Failure

CPTEMP
See: Unit Temperature too High

Create new components, [15-6](#)

Creating new cross-connections, [18-8](#)

Critical alarm, [16-41](#)

Cross connection wizard, [7-90](#)

Cross-connection, [7-4](#), [7-10](#)
 Bidirectional, [18-3](#)
 Broadcast, [18-3](#)
 Unidirectional, [18-3](#)

Cross-connection level, [18-5](#)

Cross-connection wizard, [7-18](#), [7-23](#), [7-25](#), [7-28](#), [7-31](#), [7-63](#), [7-67](#), [7-71](#), [7-73](#), [18-7](#)

CSDPF
See: Protection Clock Input Fail

CSDWF
See: Worker Clock Input Fail

CTL Comm Failure, [16-29](#)

CTLCOMF
See: CTL Comm Failure customer comment form; commenting, [xxvii](#)

.....

D Danger classification, [1-4](#)

Data communcation channel (DCC), [7-59](#), [7-62](#)

Data Communication Channel (DCC), [14-2](#), [14-29](#)

Data Communication Network (DCN), [3-6](#), [14-2](#), [14-29](#)

Database changes (DBCHG), [13-15](#)

Date and time setting, [4-5](#), [4-9](#)

DCC channels, [3-60](#)

DCC controller, [14-3](#), [14-5](#), [14-28](#), [14-29](#)

DCC protection switching, [14-31](#)

DCC provisioned state, [14-31](#)

DCC termination, [14-29](#)

DCC Terminations
 Configure DCC Terminations, [3-63](#)
 DCC Termination Display, [3-61](#)

DCC-M Multiplex Section Data Communication Channel, [14-29](#), [14-31](#)

DCC-R Regenerator Section Data Communication Channel, [14-29](#)

DCCMSF
See: MS DCC failure

DCCRSF
See: RS DCC failure

DCN Provisioning Not Valid, [16-28](#)

Default K-bytes, [16-31](#)

Default user, [13-10](#)

Defect, [16-5](#)

DEG-P
See: Degraded Signal

Degraded Signal
 DEG-P, [16-32](#)
 MSDEG, [16-33](#)
 THPDEG, [16-32](#)

DFI DSP Format Identifier, [14-25](#)

Disabling of DCCs, [14-34](#)

DKB
See: Default K-bytes

Document conventions, [xxiii](#)

documentation
 numbers, [xxv](#)
 set; manuals, [xxv](#)

Domain Specific Part (DSP), [14-25](#)

Download of configuration data, [4-2](#)

Drop & Continue, [7-87](#)

Drop and continue, [18-30](#)

DSP Format Identifier (DFI), [14-25](#)

Dual Node Ring
Interworking, [7-87](#)

Dual Node Ring
Interworking (DNI), [7-67](#),
[7-73](#), [18-4](#), [18-29](#)

DUPL-RNG
See: Duplicate Ring Node

Duplicate Ring Node,
[16-31](#)

.....

E Electrostatic discharge,
[1-20](#), [1-26](#), [1-29](#), [1-34](#),
[1-40](#)

Electrostatic protection,
[1-20](#)

Enabling of DCCs, [14-33](#)

End System (ES), [14-4](#)

End System Configuration
Timer (ESCT), [3-14](#), [14-4](#)

Enter/Exit Maintenance
Condition, [3-3](#), [3-3](#)

Environmental alarms,
[16-52](#)

EQPT
See: Circuit Pack Clock
Failure

Equipment details
Backplane, [4-16](#), [4-18](#)
CI-CTL, [4-20](#), [4-22](#)
Fan, [4-36](#)
Fan unit, [4-38](#)
Power Interface, [4-32](#),
[4-34](#)
System, [4-10](#), [4-12](#)
Timing Interface, [4-28](#),
[4-30](#)
User panel, [4-24](#), [4-26](#)

Equipment details list,
[4-102](#)

Equipment list
backplane, [4-107](#)
Gigabit Ethernet port,
[4-109](#)
Miscellaneous Discretes,
[4-114](#)
pack, [4-107](#)
port, [4-109](#)
shelf, [4-108](#)
tributary, [4-113](#)
virtual concatenation
group (VCG), [4-111](#)

Equipment protection,
[4-98](#), [15-19](#)

Equipment provisioning,
[15-2](#)

Errored Seconds (ES),
[19-7](#), [19-8](#)

ES-Hellos (ESHs), [3-14](#),
[14-4](#)

ES-IS protocol, [14-4](#), [14-40](#)

ESD
See: Electrostatic
discharge

ESP
See: Electrostatic
protection

ESP bonding point, [1-20](#)

ET-PREEMPT
See: Extra Traffic
Preempted

Ethernet, [14-3](#)

Ethernet performance
monitoring, [9-8](#)

Ethernet performance
parameters, [19-9](#), [19-12](#)

Ethernet port, [19-9](#)

EXC-P
See: Excessive Bit Error
Ratio

Excessive Bit Error Ratio
EXC-P, [16-32](#)
MSEXC, [16-33](#)
THPEXC, [16-32](#)

Exchangability of circuit
packs, [4-46](#)

External timing input port,
[6-3](#), [6-5](#), [6-29](#), [6-31](#)

External timing output
port, [6-3](#), [6-20](#), [6-25](#)

Extra traffic, [18-25](#)

Extra Traffic Preempted,
[16-31](#)

.....

F Facility loopback, [8-27](#),
[18-49](#)
Status, [8-31](#)

FAILTOSW
See: Path Switch Denial

Failure, [16-5](#)

Failure count (FC), [19-7](#)

Failure Count (FC), [19-9](#)

Fan Failure, [16-29](#)

Fan Unit Comm Failure,
[16-29](#)

Fan Unit Failure, [16-29](#)

Fan Unit not Present, [16-29](#)

Fan unit power feeder,
[16-49](#)

Fan Voltage Feed A
Failure, [16-29](#)

Fan Voltage Feed B
Failure, [16-29](#)

FANF
See: Fan Failure

FANUNITCOMF
See: Fan Unit Comm Failure

FANUNITF
See: Fan Unit Failure

FANUNITMISS
See: Fan Unit not Present

Far End Signal Fail, [16-28](#)

Far-end performance parameters, [19-8](#)

Far-side facility loopback, [18-50](#)

Fault, [16-5](#)

fault
 protection switch, [4-99](#)

Fault LED, [16-46](#), [16-49](#)

Fault management, [7-99](#)

Fault management process, [16-4](#)

FDA/CDRH laser classification, [1-13](#), [1-17](#)

FDA/CDRH Regulations, [1-16](#)

FE ACTY LED, [16-41](#)

FEC
See: Forward Error Correction

FEEDAF
See: Fan Voltage Feed A Failure

FEEDBF
See: Fan Voltage Feed B Failure

FESF
See: Far End Signal Fail

File Transfer Translation Device (FTTD), [11-10](#)

File Transfer, Access and Management (FTAM), [14-20](#)

Flash disk, [20-2](#)

Flow Control, [18-46](#)

Force to Holdover, [6-42](#)

Forced switch, [4-100](#), [7-37](#), [7-40](#), [7-44](#), [7-47](#), [7-49](#)

Forced Switch, [7-93](#)

Forced switch, [8-3](#), [8-8](#), [8-10](#), [8-12](#), [8-12](#), [8-14](#), [8-14](#), [8-15](#), [8-17](#), [18-18](#)

Forced switch to holdover mode, [6-42](#)

Forward Error Correction (FEC), [4-62](#), [5-43](#), [16-37](#), [19-21](#)

Forward Error Correction – corrected (FECC), [19-8](#)

Frame alignment bytes, [18-49](#)

Free running mode, [17-3](#)

FT-TD, [14-22](#)

FTAM-FTP Gateway, [3-47](#)

FTTD
See: File Transfer Translation Device

Functional category, [13-10](#)

G Gateway network element (GNE), [14-2](#)

General user, [13-10](#)

GFP Loss of Frame, [16-31](#)

GFPLOF
See: GFP Loss of Frame

Gigabit Ethernet, [18-43](#)

GNE Gateway network element, [14-2](#)

Graphical user interface
 Elements of the ~, [22-30](#)

H Handling windows, [22-45](#)

Hazard level, [1-19](#)

Hierarchical routing, [14-6](#)

History alarms, [5-12](#)

History bin, [19-20](#)

History logs, [13-19](#)

Holdoff time, [7-76](#), [7-89](#), [7-92](#)

Holdover mode, [6-35](#), [6-38](#), [6-42](#), [17-3](#), [17-5](#), [17-7](#), [17-9](#)

I

IDE Flash Card Access Fail, [16-29](#)

IDI Initial Domain Identifier, [14-25](#)

IEC laser classification, [1-13](#), [1-17](#)

IEC Requirements, [1-16](#)

IEEE 802.3 MAC address, [3-19](#), [14-25](#)

IEEE 8023 MAC address, [14-38](#)

IMAPS
See: Improper APS Codes

Improper APS Codes, [16-31](#)

In-band FEC, [4-63](#), [5-44](#), [16-37](#), [19-21](#)

Inconsistent APS Codes, [16-31](#)

Inconsistent Ring Protection Mode, 16-31	ISO-OSI network protocols, 14-4	LED TEST button, 5-23 , 16-42 , 16-43
Initial Domain Identifier (IDI), 14-25		Level-1 Intermediate System, 14-6
Initial Domain Part (IDP), 14-25	J J0 byte, 4-69	level-2 Intermediate System, 14-6
Initial equipment provisioning, 4-4		Level-2 subdomain, 14-6
Initial software download, 20-3	L L1-LSP, 14-5	LIDMSM See: MS Protocol Version Mismatch
Initialization, 16-47	L2-LSP, 14-5	LIDRSM See: RS Protocol Version Mismatch
Insertion and removal facilities, 1-20	LAN Auto Negotiation Mismatch, 16-31	Line DCC, 14-29
Insertion of circuit packs, 16-47	LAN connectors, 14-36	Line timing, 6-13
Intermediate System (IS), 3-6 , 3-28 , 14-4	LAN I/O-Panel, 14-36	Link Aggregation (LAG), 18-47
Intermediate System Configuration Timer (ISCT), 14-4	LAN Loss of Signal, 16-31	Link Capacity Adjustment Scheme (LCAS), 18-48
Interworking, 18-6	LAN port, 19-9	Link Metric, 3-35 , 3-68
Interworking between MS-SPRing and SNCP, 7-87	LAN Router Priority, 3-35 , 3-68	Link State Protocol Data Unit (LSP), 14-5
Intraoffice LAN (IAO-LAN), 3-6 , 3-28 , 3-28 , 3-40 , 3-48 , 3-50	LAN Status, 3-8	List of current alarms, 5-6 , 5-8 , 16-21
Invisible laser radiation, 1-31 , 1-33 , 1-39	LANANM See: LAN Auto Negotiation Mismatch	List of history alarms, 5-12 , 5-14
IP address, 3-8	LANLOS See: LAN Loss of Signal	Local Communication Network (LCN), 14-2
IP LAN Status, 3-8	LAPD channels, 14-29	Local Squelch Map Conflict, 16-31
IS routing capability, 3-37	LAPD protocol, 14-3	Locked mode, 17-3
IS-Hellos (ISHs), 14-4	Laser classes, 1-13	Lockout of protection, 7-37 , 7-40 , 7-44 , 7-47 , 7-49 , 8-3 , 8-8 , 8-10 , 8-12 , 8-14 , 8-15 , 8-17
IS-IS area-divided DCN, 14-8	Laser safety instructions, 1-13	LOF See: Loss of Frame
IS-IS protocol, 14-4 , 14-5 , 14-40	Laser warning labels, 1-28 , 1-34	Logging Out NE User, 2-17
ISO-DCC NSAP address format, 14-25 , 14-25	LCN Local Communication Network, 14-2	
	LDB entry timer, 3-18	
	LDB flush timer, 3-18	
	LDB Loop detection buffer, 3-16	
	LED test, 5-23	

Login, [13-3](#)
 Network element, [22-18](#)
 LOP-P
 See: Loss of Pointer
 LOS
 See: Loss of Signal
 Loss of Alignment, [16-31](#)
 Loss of Frame, [16-33](#)
 Loss of Multiframe, [16-32](#)
 Loss of Pointer
 LOP-P, [16-32](#)
 THPLOP, [16-32](#)
 Loss of Signal, [16-33](#)
 Loss of Signal Seconds
 (LOSS), [19-7](#)
 Loss of Synchronisation,
 [16-34](#)
 Low priority traffic, [18-25](#)
 LSP database, [14-5](#)

M M0 byte, [4-65](#)
 M1 byte, [4-65](#), [4-65](#)
 MAC Address, [3-74](#)
 Maintenance condition,
 [11-10](#)
 Maintenance user, [13-10](#)
 Maintenance-oriented
 performance monitoring,
 [19-2](#)
 Major alarm, [16-41](#)
 Management interfaces for
 alarm signalling, [16-18](#)
 Manual switch, [4-100](#),
 [7-37](#), [7-40](#), [7-44](#), [7-47](#),
 [7-49](#), [8-3](#), [8-8](#), [8-10](#), [8-12](#),
 [8-12](#), [8-14](#), [8-14](#), [8-16](#),
 [8-18](#), [18-18](#)

Masking, [16-5](#)
 Master timing generator,
 [17-3](#)
 MDI
 See: Miscellaneous
 Discrete Input
 MDO
 See: Miscellaneous
 Discrete Output
 Media Acces Control
 (MAC), [18-45](#)
 Media access protocols,
 [14-3](#)
 Menu bar, [22-30](#)
 Menu structure overview,
 [22-55](#), [22-72](#)
 Menu Topic
 Cross Connection
 Wizard, [18-7](#)
 Data Communications
 — Network Layer,
 [3-37](#)
 Data Communications
 — Tarp, [3-68](#)
 Slot Provisioning, [15-16](#)
 View Current Optical
 Maintenance Signal,
 [8-26](#)
 Minor alarm, [16-41](#)
 Miscellaneous Discrete
 Input (MDI), [5-48](#), [16-52](#)
 Miscellaneous Discrete
 Input 1 ... Miscellaneous
 Discrete Input 8, [16-29](#)
 Miscellaneous Discrete
 Output (MDO), [4-115](#),
 [4-117](#), [16-52](#)

MISC_1 ... MISC_8
 See: Miscellaneous
 Discrete Input 1 ...
 Miscellaneous Discrete
 Input 8
 Modifying User ID
 Lockout parameters, [2-31](#),
 [2-33](#), [2-35](#), [2-46](#)
 MS DCC failure, [16-33](#)
 MS Protocol Version
 Mismatch, [16-33](#)
 MS-SPRing, [7-20](#), [7-57](#),
 [7-60](#), [18-21](#)
 MS-SPRing Multiplex
 Section - Shared
 Protection Ring, [14-31](#)
 MS-SPRing protection
 group, [14-31](#)
 MSDEG
 See: Degraded Signal
 MSEXC
 See: Excessive Bit Error
 Ratio
 MSSSF
 See: Server Signal Fail
 Multibit FEC, [16-37](#)
 Multiplex Section - Shared
 Protection Ring
 (MS-SPRing), [14-31](#)
 Multiplex Section Data
 Communication Channel
 (DCC-M), [14-29](#), [14-31](#)
 Multiplex Section
 Protection (MSP), [7-35](#),
 [7-35](#), [7-36](#), [7-37](#), [7-54](#),
 [7-93](#), [8-3](#), [15-6](#), [18-13](#),
 [18-19](#)

Multiplex Section Shared Protection Ring (MS-SPRing), [7-39](#), [7-42](#), [7-93](#), [8-7](#), [8-11](#), [15-6](#), [18-13](#)

2-fiber MS-SPRing, [18-21](#)

Multiplexer Section Shared Protection Ring, [7-20](#)

N Name/Address List, [3-19](#), [14-37](#)

NE ACTY LED, [16-41](#)

NE alarm list, [5-6](#)

NE alarm list; Alarm list, [16-21](#)

NE alarm log, [5-12](#)

NE Clock Failure, [16-29](#)

NE configuration data, [20-2](#)

NE name, [3-19](#), [3-28](#), [14-3](#), [14-41](#)

NE selection and login, [22-16](#)

NE software, [20-2](#)

NE User, [2-17](#)

Near-end performance parameters, [19-7](#)

Near-side facility loopback, [18-49](#)

Network Entity Title (NET), [3-69](#), [3-69](#), [14-28](#)

Network Service Access Point (NSAP), [14-24](#)

Network Service Access Point (NSAP); NSAP address, [3-28](#), [14-3](#)

NID-CONFL
See: Node ID Mismatch

Node ID Mismatch, [16-31](#)

Nominal voltage, [1-32](#)

Non-reporting ASAP, [16-35](#)

Non-revertive mode, [7-66](#), [7-70](#), [7-72](#), [7-89](#), [7-92](#), [18-20](#)

Non-volatile memory (NVM), [4-1](#)

Nonvolatile memory (NVM), [20-2](#)

Notification registration list, [13-19](#)

NSAP address, [3-14](#), [3-23](#), [3-28](#), [3-35](#), [3-37](#), [3-68](#), [14-24](#), [14-37](#)

NSAP address format, [14-25](#), [14-25](#)

NSAP Network Service Access Point, [14-24](#)

NVM Nonvolatile memory, [20-2](#)

NVM Shortage, [16-29](#)

O OCh Loss of Frame, [16-33](#)

OCHLOF
See: OCh Loss of Frame

Office alarm facility, [16-51](#)

Office alarm interfaces, [16-50](#)

One Way Path Protection, [7-48](#)

ONI Failure, [16-29](#)

ONIF
See: ONI Failure

Open Ring, [16-31](#)

Operator identifier, [14-25](#)

Optical Channel, [4-54](#), [4-57](#), [4-59](#), [4-64](#), [4-66](#), [4-68](#), [4-71](#), [16-37](#)

Optical circuit pack specifications, [1-14](#)

Optical interface standard, [4-7](#)

Optical interfaces, [18-5](#)

Optical port provisioning, [15-18](#)

Optical signal-to-noise ratio (OSNR), [16-37](#)

Organization identifier (ORG), [14-25](#)

OSI LAN Status, [3-8](#)

OSI Neighbor Map, [14-5](#)

OSI network protocol, [14-3](#)

OSI protocol stack, [14-19](#), [14-29](#)

OSI Routing Map, [14-5](#)

OSI-DCN, [14-2](#)

OSNR
See: Optical signal-to-noise ratio

Out-of-band FEC, [4-54](#), [4-57](#), [4-59](#), [4-59](#), [4-59](#), [4-63](#), [4-64](#), [4-66](#), [4-68](#), [4-71](#), [4-79](#), [5-44](#), [16-37](#), [19-21](#)

Output mode, [18-6](#)

Output timing reference, [6-18](#)

P Packaging, [1-27](#)

PAMARCH
See: Prot. Arch. Mismatch

PAMMODE
See: Prot. Arch. Mode Mismatch

PAMOPER
See: Prot. Arch. Operation Mismatch

PARARREP
See: Partitioned Area Repair

Partial Transport Capacity Loss, [16-31](#)

Partitioned Area Repair, [16-28](#)

Password, [2-5](#), [2-6](#), [13-3](#), [13-8](#)

Path protection, [18-13](#)

Path Protection Switch, [8-17](#)

Path Switch Denial, [16-33](#)

Path Switch Inhibit, [16-33](#)

Payload Defect Indication, [16-32](#)

Payload Mismatch, [16-32](#)

PDE
See: Total number of errored packets dropped

PDI-P
See: Payload Defect Indication

PDP
See: Power Distribution Panel

Performance monitoring, [19-1](#)

Performance monitoring points, [19-6](#)

Persistency check, [16-5](#)

PIEF
See: Power Interface Read Failure

PIMISS
See: Power Interface not Present

Point-to-point cross-connection, [7-20](#), [18-4](#)

Port monitoring mode, [4-57](#), [5-39](#), [16-36](#)

Port unit LED, [16-21](#)

port units, [15-8](#)

Power Distribution Panel (PDP), [1-31](#), [1-33](#), [1-39](#)

Power Interface not Present, [16-30](#)

Power Interface Read Failure, [16-30](#)

Powering-up, [16-47](#)

POWF
See: System Power Failure

PPA, [18-25](#)

PRCDRERR
See: Circuit Pack Type Mismatch

Pre-emptible, [18-25](#)

Preconditions for disabling a DCC, [3-60](#)

Preconditions for enabling a DCC, [3-60](#)

Preferences, [5-3](#)

Primary and secondary nodes, [18-30](#)

Priority level, [2-7](#)

Priority queuing, [18-46](#)

Privileged user, [13-10](#)

PROCROVLD
See: Resource Overload

Prot. Arch. Mismatch, [16-28](#)

Prot. Arch. Mode Mismatch, [16-28](#)

Prot. Arch. Operation Mismatch, [16-28](#)

Prot. Switch Byte Inappropriate, [16-28](#)

Prot. Switch Byte Unacceptable, [16-28](#)

Protection access, [18-25](#)

Protection Clock Input Fail, [16-29](#)

Protection configurations, [18-52](#)

Protection group, [7-34](#), [7-39](#), [7-42](#), [7-93](#), [15-6](#)

Protection group provisioning, [15-6](#)

Protection mechanisms, [18-13](#)

Protection section, [18-19](#)

Protection switch activity log, [13-19](#), [13-21](#)

Protection switching changes (PSCHG), [13-15](#)

protection, timing, [17-5](#)

Protocol stacks, [14-20](#)

PROVINVAL
See: DCN Provisioning Not Valid

provision
circuit pack, [15-17](#)

provisioning, timing, [17-6](#)

PSBINAPPR
See: Prot. Switch Byte Inappropriate

PSBUNACC
See: Prot. Switch Byte Unacceptable

PSI
See: Path Switch Inhibit

Pushbutton, [22-48](#)

PWR ON LED, [16-41](#),
[16-43](#)

Q Q-LAN, [14-2](#)

Quality-of-service-oriented
performance monitoring,
[19-2](#)

- R** Rack alarm facility, [16-50](#)
Rack alarm interface, [16-50](#)
Raise validation time, [16-4](#)
RD Routing Domain, [14-25](#)
RDI
See: Remote Defect
Indication
Reed-Solomon code, [16-38](#)
reference signals, [17-5](#)
Refresh button, [5-11](#), [5-18](#)
Regenerator Section Data
Communication Channel
(DCC-R), [14-29](#)
REI
See: Remote Error
Indication
Remote Defect Indication,
[19-8](#)
RFI-L, [16-33](#)
RFI-P, [16-32](#)
THPRDI, [16-32](#)
Remote Error Indication,
[19-8](#)
Remote Error Indication
(REI), [19-4](#), [19-4](#)
Remote Failure Indication,
[19-8](#)
Repeater Mode, [18-45](#)
-

REPLUNITMISS

See: Circuit Pack not
Present

Reports only (user), [13-10](#)

Reserved portion of the
NSAP, [14-25](#)

Resource Overload
PROCROVLD, [16-29](#)

Restore Database

CIT, [21-6](#)

FTAM, [21-6](#)

FTTD, [21-6](#)

Revertive mode, [7-66](#),
[7-70](#), [7-72](#), [7-89](#), [7-92](#)

RFI
See: Remote Failure
Indication

RFI-L
See: Remote Defect
Indication

RFI-P
See: Remote Defect
Indication

Ring Discovery in
Progress, [16-31](#)

Ring Incomplete, [16-31](#)

Ring map, [8-7](#), [8-11](#)

Ring Protection Switch
Suspended, [16-31](#)

Ring-to-Ring SNCP, [7-90](#)

Ring-to-ring SNCP, [18-5](#)

Ring-to-ring UPSR/SNCP,
[18-16](#)

RNG-DSCVY
See: Ring Discovery in
Progress

RNG-INC
See: Ring Incomplete

RNG-IRPM

See: Inconsistent Ring
Protection Mode

RNG-OPEN
See: Open Ring

RNG-PSS
See: Ring Protection
Switch Suspended

RNG-URT
See: Unknown Ring Type

Rolling a cross-connection,
[7-25](#)

Routing Domain (RD),
[14-25](#)

Routing Information Base
(RIB), [14-5](#)

Routing metric, [14-35](#)

Routing table, [14-38](#)

Routing tables, [14-5](#)

RS DCC failure, [16-33](#)

RS Protocol Version
Mismatch, [16-33](#)

RS(255,239), [16-38](#)

RSTIM
See: Trace Identifier
Mismatch

- S** SA bit Location, [6-5](#)
Safety of laser products,
[1-16](#), [1-16](#)
SCM
See: Switch Channel
Mismatch
SDH management network,
[14-2](#)
SDH performance
monitoring, [19-4](#), [19-4](#)
SDH performance
parameters, [19-11](#)
-

SDH tributary AIDs, [5-19](#)

SDH tributary numbering format, [16-15](#)

Section DCC, [14-29](#)

Section trace identifier, [4-69](#)

Security administrator, [13-4](#)

Security database, [13-3](#), [13-5](#)

Selector, [14-25](#)

Self healing rings, [18-22](#)

Self-test, [16-47](#)

Sequence Number Mismatch, [16-32](#)

Server Signal Fail

- MSSSF, [16-33](#)
- SSF-P, [16-32](#)
- THPSSF, [16-32](#)
- VCGSSF, [16-31](#)

SES declaration threshold, [9-2](#), [19-10](#)

Severely Errored Framing Seconds (SEFS), [19-7](#)

Severely Errored Seconds (SES), [19-7](#), [19-8](#)

Shelf, [15-7](#)

Shelf layout, [15-7](#)

Shelf parameters, [4-14](#)

Shelf provisioning, [15-15](#)

Shortest path first algorithm, [14-4](#), [14-6](#), [14-35](#)

Signal Degrade, [7-37](#), [7-37](#), [7-47](#), [7-49](#)

Signal Fail, [7-37](#), [7-37](#), [7-47](#), [7-49](#)

Signal Fail (SF) condition, [16-5](#)

Signal Rate Mismatch, [16-32](#)

Single-ring UPSR/SNCP, [18-15](#)

Sink End Failure of Protocol, [16-31](#)

Slave timing generator, [17-3](#)

Slot provisioning, [15-16](#)

SNCP, [7-20](#)

Software download, [14-20](#), [16-47](#), [20-4](#)

SONET performance monitoring, [19-4](#), [19-4](#)

SONET performance parameters, [19-12](#)

SONET tributary numbering format, [16-15](#)

Source End Failure of Protocol, [16-31](#)

SQMAP-CONFL

- See: Local Squelch Map Conflict

SRM-P

- See: Signal Rate Mismatch

SS Bit Override, [4-15](#)

SSF-P

- See: Server Signal Fail

SSM

- See: Synchronization Status Message

Standards Compliance, [1-16](#)

State changes, [16-23](#)

State changes (STCHG), [13-15](#)

Static routing table, [14-38](#)

Static routing table;

- Routing table, [3-3](#), [3-19](#), [3-20](#), [14-37](#)

Station alarm interface, [16-51](#)

Status bar, [22-30](#)

Status indications, [16-47](#)

Strong FEC, [16-37](#)

Sub-Network Connection Protection, [7-20](#)

Sub-Network Connection Protection (SNCP), [7-4](#), [7-10](#), [7-46](#), [7-63](#), [7-67](#), [7-90](#), [8-15](#), [18-4](#), [18-13](#), [18-14](#)

Subsystem, [16-9](#)

Super user, [13-10](#), [13-10](#)

Switch Channel Mismatch, [16-28](#)

Switch circuit pack, [4-100](#)

Switch request, [4-98](#), [7-36](#)

Switch request state, [7-37](#), [7-40](#), [7-44](#), [7-47](#), [7-49](#)

Switching an MSP, [8-3](#)

Switching APS, [8-3](#)

SYNCCLK

- See: NE Clock Failure

Synchronization Status Marker (SSM), [17-6](#)

Synchronization Status Message (SSM), [6-5](#), [6-8](#)

SYNCLOSS

- See: Loss of Synchronisation

SYNCRF

- See: Timing Reference Failure

SYNCT4OUT
 See: T4 quality
 insufficient

SYSCOMF
 See: Comm Channel
 Failure

System controller, [20-2](#)

System identifier, [14-25](#)

System Power Failure,
[16-30](#)

System reset, [3-3](#)

System Synch
 Characteristics, [4-7](#)

System timing, [6-3](#), [6-17](#),
[6-17](#), [6-39](#)

System timing reference,
[6-17](#), [6-18](#)

T T-TD Gateway, [3-39](#), [3-50](#)

T4 quality insufficient,
[16-34](#)

Target identifier (TID), [3-3](#),
[3-28](#), [14-3](#), [14-37](#), [14-41](#)

Target Identifier (TID),
[18-11](#)

TARP Data Cache (TDC),
[14-38](#)

TARP manual adjacencies;
 Manual adjacencies, [3-69](#),
[14-40](#)

TARP originator
 functionality, [14-38](#)

TARP PDU lifetime, [14-38](#)

TARP PDU types, [14-39](#)

TARP propagation
 functionality, [3-65](#)

TARP responder
 functionality, [3-65](#), [14-38](#)

TCP/IP Gateway, [3-47](#)

TCP/IP gateway, [11-10](#)

THPDEG
 See: Degraded Signal

THPEXC
 See: Excessive Bit Error
 Ratio

THPLOP
 See: Loss of Pointer

THPPLM
 See: Payload Mismatch

THPRDI
 See: Remote Defect
 Indication

THPSSF
 See: Server Signal Fail

THPTIM
 See: Trace Identifier
 Mismatch

THPUNEQ
 See: Unequipped

TI Mismatch, [16-29](#)

TID Address Resolution
 Protocol (TARP), [14-25](#),
[14-37](#), [14-38](#)

TID to NSAP address
 translation; Name to
 address translation, [14-37](#)

TID/NSAP address pair,
[3-23](#)

TIM-P
 See: Trace Identifier
 Mismatch

timing, [17-6](#)

Timing circuit pack, [4-100](#)

Timing configuration, [6-3](#),
[17-4](#)

Timing generator, [6-35](#),
[6-38](#), [17-3](#), [17-5](#), [17-9](#)

Timing input format, [6-5](#)

Timing marker, [17-6](#)

Timing modes, [17-3](#)

Timing protection, [17-9](#)

Timing provisioning, [17-1](#)

Timing quality, [17-5](#)

Timing reference, [6-3](#),
[6-13](#), [6-44](#), [6-47](#)

Timing Reference Failure,
[16-34](#)

Timing reference protection
 switching, [17-9](#)

Timing references, [6-33](#),
[6-36](#)

TIMM
 See: TI Mismatch

Title bar, [22-30](#)

Tool bar, [22-30](#)

Total number of bytes
 received (CBR), [19-10](#)

Total number of bytes sent
 (CBS), [19-10](#)

Total number of errored
 packets dropped (PDE),
[19-10](#)

Total Transport Capacity
 Loss, [16-31](#)

Trace Identifier Mismatch
 RSTIM, [16-33](#)
 THPTIM, [16-32](#)
 TIM-P, [16-32](#)

Traffic Squelched, [16-31](#)

Transmission interfaces,
[18-5](#)

Transoceanic protocol,
[18-25](#)

Tributary Mode Default,
[4-7](#)

Tributary numbering
format, [16-15](#)

Tributary operation mode,
[4-7](#), [4-56](#)

Tributary provisioning,
[15-18](#)

TS
See: Traffic Squelched

TXI Failure, [16-30](#)

TXInF
See: TXI Failure

U Unacknowledged
Information Transfer
Service (UITS), [14-34](#)

Unavailability period
(UAP), [19-7](#), [19-8](#)

Unavailable Seconds
(UAS), [19-7](#)

Unavailable Seconds
(UAS), [19-8](#)

Undivided DCN, [14-8](#)

UNEQ-P
See: Unequipped

Unequipped
THPUNEQ, [16-32](#)
UNEQ-P, [16-32](#)

Unidirectional Path
Switched Ring (UPSR),
[18-13](#)

Unidirectional
cross-connection, [18-4](#)

Unidirectional path
protected
cross-connection, [18-4](#)

Unidirectional Path
Switched Ring (UPSR),
[7-90](#)

Unidirectional Path
Switched Ring UPSR,
[18-5](#)

Unidirectional Path
Switched Rings (UPSR),
[18-14](#)

Unidirectional
Path-Switched Ring
(UPSR), [7-4](#), [7-10](#), [7-46](#),
[8-15](#)

Unit Cooling Degraded,
[16-29](#)

Unit Temperature too High,
[16-30](#)

Unknown Ring Type, [16-31](#)

UPCOMF
See: User Panel Comm
Failure

Update Alarms button,
[5-11](#), [5-18](#), [16-20](#)

Updating the alarm list,
[5-11](#), [5-18](#)

UPMISS
See: User Panel not
Present

UPSR, [7-20](#)

User interface
Elements of the ~,
[22-30](#)

User login, [2-1](#), [2-3](#), [2-5](#),
[2-6](#), [13-7](#), [13-7](#)

User panel, [5-23](#)

User panel alarm LEDs,
[16-42](#)

User Panel Comm Failure,
[16-29](#)

User Panel not Present,
[16-29](#)

User privilege code, [13-10](#)

User privilege codes, [2-7](#)

User provisioning, [2-5](#), [2-6](#),
[2-17](#)

User type, [2-7](#)

User types, [13-10](#)

User types; Predefined user
types, [13-10](#)

User-Network Side MSect
Failure, [3-57](#)

User-Network Side RSect
Failure, [3-57](#)

V Validation, [16-5](#)

VCG port, [19-9](#)

VCG tributary parameters,
[7-99](#)

VCGFOPR
See: Sink End Failure of
Protocol

VCGFOPT
See: Source End Failure
of Protocol

VCGLOA
See: Loss of Alignment

VCGLOPC
See: Partial Transport
Capacity Loss

VCGLOTC
See: Total Transport
Capacity Loss

VCGSSF
See: Server Signal Fail

VCLOM
See: Loss of Multiframe

VCSQM
See: Sequence Number
Mismatch

view

software generic, [10-15](#)

View preferences, [5-3](#)

Virtual concatenation,
[18-47](#)

Virtual Local Area
Network, [18-45](#)

VLAN tagging, [18-45](#)

-
- W** Wait-to-restore time
(WTR), [6-17](#), [7-40](#), [7-44](#),
[7-47](#), [7-49](#), [17-10](#)
- WAN port, [19-9](#)
- WaveStar*® CIT NE Alarm
List, [5-6](#), [5-8](#)
- WaveStar* CIT NE Alarm
Log, [5-12](#), [5-14](#)
- WaveStar* CIT System View
window size, [5-3](#), [5-4](#)
- Window handling, [22-45](#)
- Worker Clock Input Fail,
[16-29](#)
- Working port, [3-61](#)
- Working section, [18-19](#)
-

- X** XC320 equipment
protection, [15-19](#)

