



Lucent Optical Management System (OMS)

Release 6.1

Provisioning Guide for *LambdaUnite*[®] MSS, Release 9.1

365-312-876R9.1
CC109646869
Issue 1
July 2007

Alcatel-Lucent - Proprietary

This document contains proprietary information of Alcatel-Lucent and is not to be disclosed or used except in accordance with applicable agreements.

Copyright © 2007 Alcatel-Lucent
Unpublished and Not for Publication
All Rights Reserved

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2007 Alcatel-Lucent. All Rights Reserved.

Contents

About this information product

Purpose	xv
Safety information	xv
Conventions used	xv
Orientation aids	xvi
Related information	xvii
Document support	xix
Technical support	xix
How to order	xix
How to comment	xix

1 Safety

Overview	1-1
Structure of hazard statements	1-3
Basic safety aspects	1-5
Symbols used in hazard statements	1-7

2 Security administration tasks

Overview	2-1
To retrieve the current user's security information	2-2
To retrieve user security information	2-5
To modify the current user's security information	2-9

	To modify user security information	2-12
	To modify the current user's password	2-16
	To terminate user sessions	2-18
	To create new users	2-20
	To delete users	2-23
3	Management communication setup concepts	
	Overview	3-1
	Basic DCN principles	3-2
	DCN configurations	3-5
	DCN configuration guidelines	3-9
	DCN protocols and services	3-10
	NSAP address structure	3-12
	Data communication channels (DCC)	3-14
	LAN access	3-17
	Name-to-address translation	3-18
	OMS-to-NE connections concepts	3-19
	NE CIT Cut-Through Concepts	3-21
	Orderwire and user bytes	3-23
4	Management communication setup tasks	
	Overview	4-1
	Tasks related to OMS-to-NE connections	
	To view a list of OMS-to-NE connections	4-3
	To add an OMS-to-NE connection	4-4
	To modify an OMS-to-NE connection	4-9
	To deactivate an OMS-to-NE connection	4-13
	To activate an OMS-to-NE connection	4-15

To delete an OMS-to-NE connection	4-17
To delete an NE	4-19
To display the communication state of an NE	4-21
Tasks related to DCC	
To retrieve DCC related parameters	4-23
To modify DCC related parameters	4-26
To retrieve DCC/EOW status information for a port	4-28
To modify DCC/EOW status information for a port	4-30
To view a list of transparent DCC cross-connections	4-32
To add a transparent DCC cross-connection	4-34
To delete a transparent DCC cross-connection	4-36
Tasks related to system provisioning	
To view NE date and time	4-38
To modify NE date and time	4-40
Tasks related to OMS-to-NE CIT Cut-Through	
Command Files for the NE CIT Cut-Through	4-42
Install the NE CIT	4-44
Launch the NE CIT away from the Default Location	4-46
Configure the java.policy File for NE CIT Cut-Through	4-48
Work with Command Files to Invoke the NE CIT Cut-Through	4-50
Troubleshoot the NE CIT	4-51
5	Equipment provisioning concepts
Overview	5-1
System configurations	
Network element configurations	5-2
Pluggable optical interface modules	5-12

Overview of replaceable units	5-19
NE hardware components and their identifiers	5-25
Port types	5-26
Miscellaneous discrete inputs and outputs	5-30
Equipment protection	
CTL equipment protection (duplex control)	5-32
XC equipment protection	5-37
STM-1E equipment protection	5-40
DS3/EC-1 equipment protection	5-47
LOXC equipment protection	5-55
6 Equipment provisioning tasks	
Overview	6-1
Provisioning of slots and SFP modules	
To view a list of slots	6-3
Port provisioning	
To view a list of physical ports	6-4
To view a list of logical ports	6-5
To view a list of loopback-enabled ports	6-6
To provision or deprovision a loopback on a port	6-7
To modify the parameters of a physical or logical port	6-9
Parameters for SDH/SONET/PDH ports	6-11
Parameters for Ethernet ports	6-26
Parameters for VCG ports	6-30
Provisioning of NE event controls	
To inhibit the forwarding of autonomous messages	6-38
To allow the forwarding of autonomous messages	6-40

Provisioning of MDIs and MDOs

To retrieve the MDO configuration 6-42

To set the MDO configuration 6-44

To switch on an MDO 6-46

To switch off an MDO 6-48

To retrieve the MDO state 6-50

To retrieve the MDI configuration 6-52

To set the MDI configuration 6-54

Equipment protection

To retrieve equipment protection group information 6-56

To add an equipment protection group 6-59

To operate an equipment protection group 6-61

To release an equipment protection group 6-63

To delete an equipment protection group 6-65

7 ONNS

Overview 7-1

ONNS Concepts 7-3

ONNS Network Element Management 7-6

ONNS Port Parameters Provisioning 7-8

ONNS Multiplex Section Connection Provisioning Concepts 7-11

ONNS Service Connection Provisioning Concepts 7-13

ONNS MxN Service Group Connection Provisioning Concepts 7-19

Association of MxN Connections with Controlled Planes 7-23

ONNS Infrastructure Connection Provisioning Concepts 7-24

Modify Route Concepts for ONNS 7-26

Graphical Layout for ONNS 7-28

ONNS Database Synchronization	7-30
Filter ONNS NEs on the Network Map	7-32
Provision ASTN NE Port Parameters	7-33
Provision an ONNS Multiplex Section Connection	7-35
Modify ASTN NE Port Parameters for Multiplex Section Connections	7-41
View ONNS Connection Groups	7-43
View/Query ONNS ASTN Capacity Utilization	7-44
View ONNS Associated MxN Connection List	7-46
Associate a Tandem Connection to a Controlled Plane	7-47
Provision an ONNS Controlled Plane Service Connection	7-48
Provision an ONNS Mixed Plane Service Connection	7-56
Provision an OUC Connection for In Effect Steps	7-64
Add an ONNS MxN Service Group Network Connection	7-72
Add an ONNS MxN Working Connection to an Existing MxN Connection Group	7-79
Modify the Route of (Rearrange) an ONNS In Effect Connection	7-85
Delete Group for an ONNS MxN Connection Group	7-90
DB Delete Group for an ONNS MxN Connection Group	7-91
Cancel Group for an ONNS MxN Connection Group	7-92
Provision an ENNI ONNS Controlled Plane Service Connection	7-93
View ENNI Associated ASTN Connection List	7-100
Perform a Partial Database Synchronization for Network Connections	7-101

8 Timing provisioning concepts

Overview	8-1
NE timing – general functional overview	8-2
Timing interfaces	8-6
Timing references	8-9
Timing link switches	8-12

	The internal timing generator	8-18
	Timing quality	8-20
	Timing protection	8-21
	Synchronization characteristics – external timing inputs	8-23
	Synchronization characteristics – external timing outputs	8-25
	Synchronization characteristics – assigned timing references	8-30
	Synchronization characteristics – system timing	8-35
9	Timing provisioning tasks	
	Overview	9-1
	To retrieve synchronization information	9-2
	To set the synchronization - assigned timing reference	9-7
	To set the synchronization - external timing input	9-9
	To set the synchronization - external timing output	9-11
	To set the synchronization - system timing	9-14
	To release the synchronization switch (REF)	9-16
	To release the synchronization switch (MOD)	9-18
	To operate the synchronization switch (MOD)	9-20
	To release the synchronization switch (OUTREF)	9-22
	To operate the synchronization switch (REF)	9-24
	To operate the synchronization switch (OUTREF)	9-26
10	Traffic provisioning concepts	
	Overview	10-1
	SDH/SONET traffic provisioning concepts	
	Cross-connections	10-2
	Lower-order cross-connections (LOXC)	10-8
	Path protection (SNCP/UPSR)	10-13

Line protection (MSP/APS)	10-15
Ring protection (MS-SPRing/BLSR)	10-17
Dual node interworking / Dual ring interworking (DNI/RNI)	10-22
Ethernet traffic provisioning concepts	
<i>TransLAN</i> [®] Ethernet over SDH implementation	10-23
Virtual concatenation	10-25
Virtual LAN	10-27
Tagging schemes	10-29
Spanning tree protocol	10-30
Link path through	10-32
11 Traffic provisioning tasks	
Overview	11-1
Provisioning of cross-connections	
To view all cross-connections	11-4
To view lower-order cross-connections	11-8
To view higher-order cross-connections	11-12
To add an uncorrelated lower-order cross-connection	11-16
To create a 1-Way conversion cross-connection	11-19
To create a 2-Way conversion cross-connection	11-23
To add an uncorrelated higher-order cross-connection	11-27
To modify a lower-order cross-connection's topology	11-30
To modify a higher-order cross-connection's topology	11-34
To modify a cross-connection's parameters	11-38
To change a higher-order cross-connection from ONNS to traditional mode	11-41
To roll the input of a lower-order cross-connection from one tributary port to another	11-43
To roll the input of a higher-order cross-connection from one tributary port to another	11-46

To delete a cross-connection	11-49
To retrieve ONNS to UPSR/SNCP constructs	11-52
To add an ONNS to UPSR/SNCP construct	11-54
To delete an ONNS to UPSR/SNCP construct	11-56
Provisioning of path protection groups (SNCP, UPSR)	
To view a list of path protection groups (SNCP, UPSR)	11-58
To modify a path protection group (SNCP, UPSR)	11-60
To operate a path protection group switch (SNCP, UPSR)	11-62
To operate an SNCP VC-4 protection group switch on constituent members	11-64
Provisioning of MSP protection groups	
To view a list of 1+1 or 1x1 MSP protection groups	11-66
To add a 1+1 MSP protection group	11-67
To add a 1x1 MSP protection group	11-69
To modify a 1+1 or 1x1 MSP protection group	11-71
To delete a 1+1 or 1x1 MSP protection group	11-73
To operate an MSP protection switch	11-75
Provisioning of APS protection groups	
To view a list of 1+1 or 1x1 APS protection groups	11-77
To add a 1+1 APS protection group	11-78
To add a 1x1 APS protection group	11-80
To modify a 1+1 or 1x1 APS protection group	11-82
To delete a 1+1 or 1x1 APS protection group	11-84
To operate an APS protection switch	11-86
Provisioning of MS-SPRing protection groups	
To view a list of 2-fiber MS-SPRing protection groups	11-88
To add a 2-fiber MS-SPRing protection group	11-89

	To modify a 2-fiber MS-SPRing protection group	11-91
	To delete a 2-fiber MS-SPRing protection group	11-93
	To operate a 2-fiber MS-SPRing protection switch	11-95
	To view a list of 4-fiber MS-SPRing protection groups	11-97
	To add a 4-fiber MS-SPRing protection group	11-98
	To modify a 4-fiber MS-SPRing protection group	11-100
	To delete a 4-fiber MS-SPRing protection group	11-102
	To operate a 4-fiber MS-SPRing protection switch	11-104
	Provisioning of BLSR protection groups	
	To view a list of 2-fiber BLSR protection groups	11-106
	To add a 2-fiber BLSR protection group	11-107
	To modify a 2-fiber BLSR protection group	11-109
	To delete a 2-fiber BLSR protection group	11-111
	To operate a 2-fiber BLSR protection switch	11-113
	To view a list of 4-fiber BLSR protection groups	11-115
	To add a 4-fiber BLSR protection group	11-116
	To modify a 4-fiber BLSR protection group	11-118
	To delete a 4-fiber BLSR protection group	11-120
	To operate a 4-fiber BLSR protection switch	11-122
12	Software and NE database management concepts	
	Overview	12-1
	Functionality description	12-2
	Software upgrade	12-5
13	Software and NE database management tasks	
	Overview	13-1

Tasks related to NE generics

To view a list of NE generics stored on the management system 13-3

To add an NE generic to the management system 13-4

To delete an NE generic from the management system 13-5

To transfer an NE generic from the management system to an NE 13-6

To schedule the transfer of an NE generic from the management system to an NE 13-8

To view a list of in-progress transfers of NE generics 13-11

To abort an in-progress NE generic transfer 13-12

To view a list of NE generics stored on an NE 13-15

To activate an NE generic on an NE 13-17

To commit an NE generic on an NE 13-20

To revert an NE generic on an NE 13-22

To schedule NE generic activation 13-24

Tasks related to NE databases

To view a list of NE database versions stored on the management system 13-28

To view a list of NE database versions stored on an NE 13-31

To back up NE database versions onto the management system 13-32

To schedule the backup of an NE database version onto the management system 13-37

To restore an NE database version from the management system to an NE 13-39

Glossary

Index

About this information product

Purpose

This information product provides information specific to the *LambdaUnite*[®] MSS network element managed with Lucent Optical Management System (OMS). It is designed to cover mainly the Lucent OMS tasks that are traditionally related to the element management level.

Safety information

This information product contains hazard statements for your safety. Hazard statements are given at points where safety consequences to personnel, equipment, and operation may exist. Failure to follow these statements may result in serious consequences.

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 and numbering conventions are identical. 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, and so on

- 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)
- Examples for file names and system path information:
 - *console*
 - */usr/local/bin/*
- Examples for 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, press a single key or a number of keys in sequence.

Abbreviations

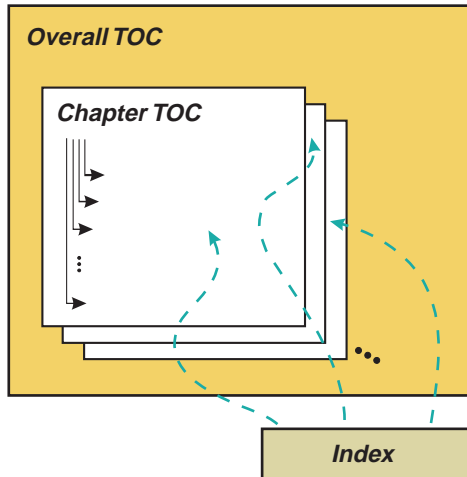
Abbreviations used in this document can be found in the “Glossary” unless it can be assumed that the reader is familiar with the abbreviation.

Orientation aids

This document contains the following orientation aids:

- *Overall TOC*
- *Chapter TOCs*
- *Index*

The following graphic depicts the principle structure of this document:



Overall TOC

The overall table of contents (TOC) provides a structural overview of the entire document. It lists the content of each chapter and the associated page number where the respective information can be found.

The overall table of contents can be found after the legal page, before the “About this information product” preface.

Chapter TOCs

Each chapter contains a table of contents (TOC) in its “Overview” section. The scope of each chapter TOC is limited to the corresponding chapter. As in the overall TOC, page numbers indicate where the respective information can be found.

Index

This manual also contains an alphabetical index, which can be found at the end of the document, after the “Glossary”.

The index helps users to find specific information quickly by providing an alphabetical list of key words with associated page numbers.

Related information

The manuals related to *LambdaUnite*[®] MSS are shown in the following table:

Document title	Document code
<i>LambdaUnite</i> [®] MSS Applications and Planning Guide Presents a detailed overview of the system, describes its applications, gives planning requirements, engineering rules, ordering information, and technical specifications.	109646802 (365-374-176R9.1)

Document title	Document code
<p>LambdaUnite® <i>MSS User Operations Guide</i></p> <p>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 ITM-CIT.</p>	<p>109646828 (365-374-177R9.1)</p>
<p>LambdaUnite® <i>MSS Alarm Messages and Trouble Clearing Guide</i></p> <p>Gives detailed information on each possible alarm message. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.</p>	<p>109646810 (365-374-178R9.1)</p>
<p>LambdaUnite® <i>MSS Installation Guide</i></p> <p>A step-by-step guide to system installation and set up. It also includes information needed for pre-installation site planning and post-installation acceptance testing.</p>	<p>109646844 (365-374-179R9.1)</p>
<p>LambdaUnite® <i>MSS Operations System Engineering Guide (TL1 Reference Manual)</i></p> <p>A reference for all TL1 commands which can be used to operate the network element. The manual gives an introduction to the concept of the TL1 commands and instructs how to use them.</p>	<p>109646836 (365-374-180R9.1)</p>
<p><i>Documentation CD-ROM LambdaUnite® MSS (all manuals on a CD-ROM)</i></p>	<p>109646851 (365-374-181R9.1)</p>
<p><i>Documentation CD-ROM LambdaUnite® MSS Software Release Description</i></p>	<p>This document is delivered with the NE software.</p>
<p>LambdaUnite® <i>MSS Engineering and Ordering Information</i></p>	<p>Drawing ED8C948-10</p>
<p>LambdaUnite® <i>MSS Interconnect and Circuit Information</i></p>	<p>Drawing ED8C948-20</p>

The documentation set related to Lucent OMS is shown in the following table:

Document title	Document code
<p>Lucent OMS Getting Started Guide</p> <p>Instructs new users how to use Lucent OMS. This document contains a glossary of terms.</p>	<p>365-315-145R5.0.2</p>
<p>Lucent OMS Connection Management Guide</p> <p>Instructs users how to use Lucent OMS to provision and manage network connections.</p>	<p>365-315-150R5.0.2</p>
<p>Lucent OMS Network Element Management Guide</p> <p>Instructs users how to use Lucent OMS to provision and manage network elements.</p>	<p>365-315-146R5.0.2</p>
<p>Lucent OMS Ethernet Management Guide</p> <p>Instructs users on how to use the Ethernet Management feature to provision and manage Ethernet connections in a network.</p>	<p>365-315-147R5.0.2</p>
<p>Lucent OMS Service Assurance Guide</p> <p>Instructs users on how to manage and interpret fault information collected from the network.</p>	<p>365-315-148R5.0.2</p>

Document title	Document code
Lucent OMS Administration Guide Instructs users on how to administer and maintain Lucent OMS and the network.	365-315-149R5.0.2

In addition, it is highly recommended to consult the TransLAN[®] *Ethernet SDH Transport Solution Applications and Planning Guide*, 365-377-003 (109637223) when planning to use *LambdaUnite*[®] MSS for Ethernet applications.

These documents and drawings can be ordered at or downloaded from the [Customer Information Center \(CIC\)](#) (<http://www.cic.lucent.com/>) or via your Local Customer Support.

Document support

The document support telephone numbers are:

- 1 630 713 5000 (for all countries)
- 1 888 727 3615 (for the continental United States)

Technical support

For technical support, contact your local customer support team. Reach them [via the web](#) (<https://support.lucent.com/>) or the telephone number listed under the [Technical Assistance Center menu](#) (<http://www.lucent.com/contact/>).

How to order

The order number of this document is 365-312-876R9.1 (issue 1).

How to comment

To comment on this information product, go to the [Online Comment Form](#) (<http://www.lucent-info.com/comments/enus/>) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Safety

Overview

Purpose

The aim of this chapter on safety is to provide users of *LambdaUnite*[®] MSS systems with the basic safety information.

In addition, the *LambdaUnite*[®] *MSS Release 9.1 Safety Guide*, 365-374-159 contains all the relevant information and safety guidelines to safeguard against personal injury in a large number of languages. Furthermore, the *Safety Guide* may be useful to prevent material damage to the equipment. The *Safety Guide* must be read by the responsible technical personnel before carrying out relevant work on the system. The valid version of that 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
- Sharp edges

Contents

Structure of hazard statements	1-3
Basic safety aspects	1-5
Symbols used in hazard statements	1-7



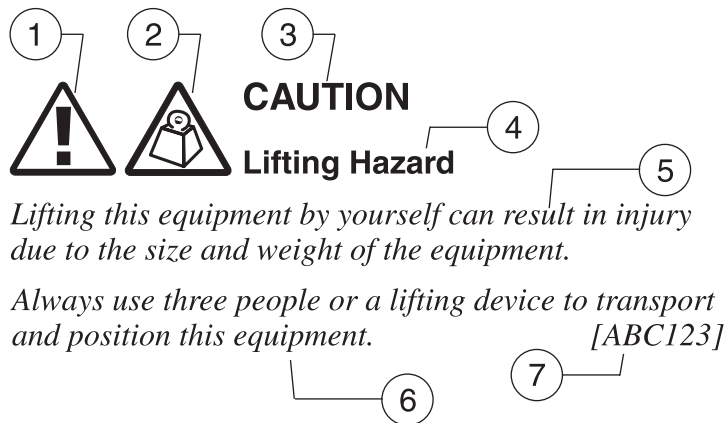
Structure of hazard statements

Overview

Hazard statements describe the safety risks relevant while performing tasks on Alcatel-Lucent products during deployment and/or use. Failure to avoid the hazards may have serious consequences.

General structure

Hazard statements include the following structural elements:



Item	Structure element	Purpose
1	Personal-injury symbol	Indicates the potential for personal injury (optional)
2	Hazard-type symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard
4	Hazard type	Describes the source of the risk of damage or injury
5	Damage statement	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the hazard statement (optional)

Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an imminently hazardous situation (high risk) which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation (medium risk) which, if not avoided, could result in death or serious injury.
CAUTION	<p><i>When used with the personal injury symbol:</i></p> <p>Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in personal injury.</p> <p><i>When used without the personal injury symbol:</i></p> <p>Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in property damage, such as service interruption or damage to equipment or other materials.</p>



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 authorized 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 Alcatel-Lucent personnel or by expert personnel authorized by Alcatel-Lucent.
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 (CD, DVD, floppy disks, streamer tapes, ...).

Summary of important safety instructions

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

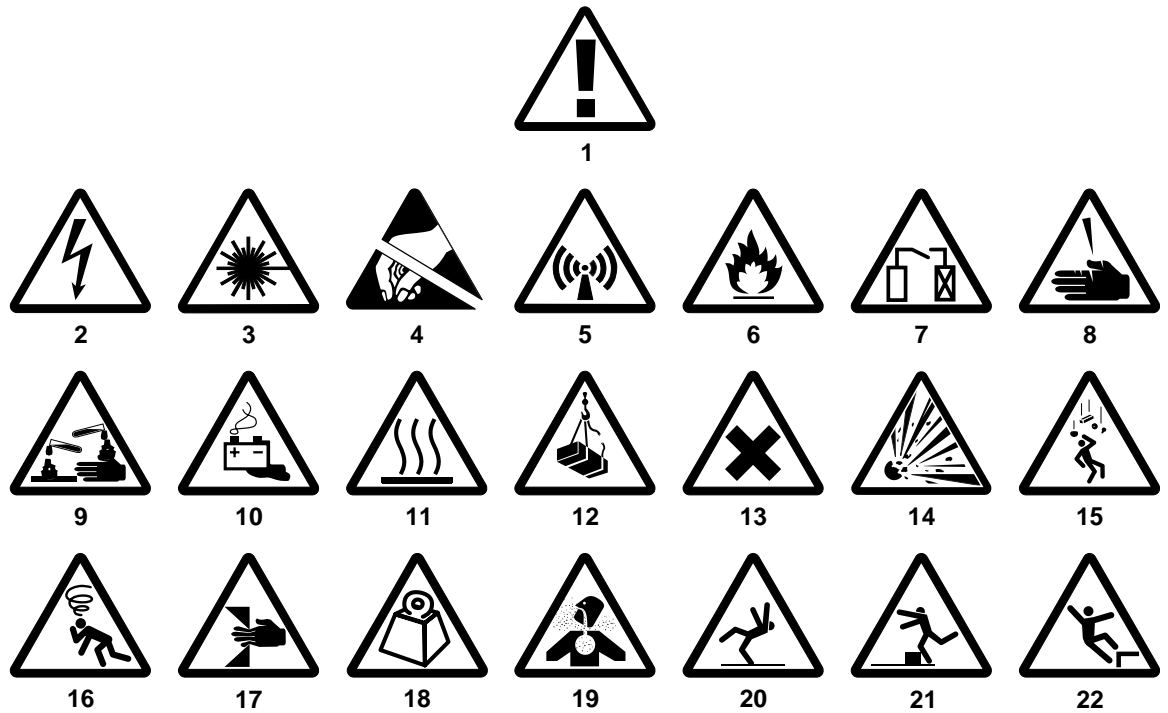
- This equipment is to be installed only in *Restricted Access Areas* in business and customer premises.
Applications in accordance with Articles 110-16, 110-17 and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other installations exempt from the enforcement of the National Electrical Code 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.
- 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-cut parts that could result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.



Symbols used in hazard statements

Symbol table

The following symbols are defined for hazard statements:



Legend:

1	Personal injury symbol	12	Heavy overhead load
2	Electric shock	13	Noxious substance
3	Hazard of laser radiation	14	Explosion hazard
4	Components sensitive to electrostatic discharge (ESD)	15	Falling object hazard
5	Electromagnetic radiation	16	Risk of suffocation
6	Flammable material / risk of fire	17	Pinch hazard
7	Service disruption hazard	18	Lifting hazard, heavy object
8	Laceration hazard	19	Inhalation hazard
9	Corrosive substance	20	Slip hazard
10	Hazard caused by batteries	21	Trip hazard
11	Hot surface	22	Hazard of falling



2 Security administration tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to security and user (login) administration.

Contents

To retrieve the current user's security information	2-2
To retrieve user security information	2-5
To modify the current user's security information	2-9
To modify user security information	2-12
To modify the current user's password	2-16
To terminate user sessions	2-18
To create new users	2-20
To delete users	2-23



To retrieve the current user's security information

When to use

Use this task to view security information for the current user (current login) on a network element. The information is related to the NE primary login used when the OMS-to-NE connection has been set up.

Related information

For a more detailed explanation, please refer to the description of the RTRV-USER command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Retrieve User**.
 5. Click **Go**.

Result: The **Retrieve User** page is displayed.

- 3 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

1. uid – User ID
User ID whose security parameters are displayed. the NE primary login used when the OMS-to-NE connection has been set up.
2. page – Password Aging Interval
This parameter specifies the period in days after which the user has to change the password of their account.
Type: integer
Range: 0 - password aging function is disabled, 7-999 [days]
Default: 90
3. screen – Message Screening
This parameter specifies what output messages are associated with the *uid*. This parameter is omitted if the user has none of these values. Any combination of these values may be displayed using ampersand (&)
Range:
 - DBCHG
Data Base Change notifications: changes in creation of entities, in user provisionable parameters, in deletion of entities will be reported (data base changes).
File Transfer In-progress notifications: The user will receive REPT DBCHG and REPT EVT FXFR messages.
The value DBCHG shall always be used together with the value STCHG.
 - STCHG
State Change notifications – report changes in user non-provisionable parameters (state changes). The user will receive REPT DBCHG messages.
The value STCHG shall always be used together with the value DBCHG.
 - PSCHG
Protection switch notifications – report protection switch changes. User will receive REPT EVT and REPT SW messages.
 - ALARMS
Alarm notifications. The user will receive REPT ALM ENV, REPT ALM, and REPT EVT messages.
 - ONNS
ONNS Notifications. Database and state changes associated with entities managed by ONNS application and only issued when *xcsetup* = NN. The related ONNS TL1 notifications are REPT PTHCHG, REPT PTHEVT, REPT NNCHG, REPT NNEVT.

- SECURITY: Security event notifications
 - OWN
Responses to own commands. The user will receive no other notifications.
 - NA
Not applicable. For users with uidclass=MEMADMIN only this value is allowed. The notification behavior is controlled in this case by the user class. If the value NA is applied for users of other user classes, then the value has the same effect as DBCHG.
4. tmtout – Inactivity Timeout Period
If there are no messages between the user and the NE over the Timeout Period, the session is logged off. A value of 0 disables the timeout function.
 5. uidclass – UID Class
This is the user class of a *uid*.
Type: alphanumeric value set
Range:
 - 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.
 - MEMADMIN – User class for memory administration users. All users of this class share the same atag counter for autonomous messages and are allowed to execute the command RTRV-AO.
 6. upc – User Privilege Code List
This parameter specifies the user privilege code UCFC/UCAL pair assigned to a user. If a user tries to operate a command with a privilege code higher than assigned to the user for the category of the command, the command will be denied.
Type: alphanumeric string. Also allowed is '&' for concatenation.
Range: Pi, Mi, Ti, Si, PMi, Di where “i” is an integer ranging from 0 to 5, with i=0 implying that there is no authorization for the functional category. Note: S0 is not allowed.
Default: P1&M1&T1&S1&PM1

END OF STEPS



To retrieve user security information

When to use

Use this task to view security information for one or all users (logins) on a network element.

Related information

For a more detailed explanation, please refer to the description of the RTRV-USER-SECU command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Retrieve User Security**.
 5. Click **Go**.

Result: The **Retrieve User Security** page is displayed.

- 3 In the **User identifier** field, enter a login (user) name. To retrieve information for all logins (users), leave the field empty.

- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

6 The output parameters for this function are:

1. uid – user ID

User ID whose security parameters are to be retrieved. the NE primary login used when the OMS-to-NE connection has been set up.

2. alw_login – allow login

This parameter displays the enable/disable state of a User ID.

A User ID can be automatically disabled by the system when the time specified by parameter *usrage* expires or via the ED-USER-SECU command. A User ID can be enabled via the ED-USER-SECU command.

If a User ID is disabled, logins with that User ID are denied.

3. initobs – initialization observability

This parameter allows the system to accept commands before it has completed initialization.

4. page – password aging interval

This parameter specifies the period in days after which the user has to change the password of their account.

Type: integer

Range: 0 - password aging function is disabled, 7-999 [days]

Default: 90

5. screen – message screening

This parameter specifies what output messages are associated with the *uid*. This parameter is omitted if the user has none of these values. Any combination of these values may be specified using ampersand (&)

Range:

- DBCHG

Data base change notifications: changes in creation of entities, in user provisionable parameters, in deletion of entities will be reported (data base changes).

File transfer in-progress notifications: The user will receive REPT DBCHG and REPT EVT FXFR messages.

The value DBCHG shall always be used together with the value STCHG.

- STCHG

State change notifications – report changes in user non-provisionable parameters (state changes). The user will receive REPT DBCHG messages.

The value STCHG shall always be used together with the value DBCHG.

- PSCHG

Protection switch notifications – report protection switch changes. User will receive REPT EVT and REPT SW messages.

- ALARMS
Alarm notifications. The user will receive REPT ALM ENV, REPT ALM, and REPT EVT messages.
- ONNS
ONNS notifications. Database and state changes associated with entities managed by ONNS application and only issued when *xcsetup* = NN. The related ONNS TL1 notifications are REPT PTHCHG, REPT PTHEVT, REPT NNCHG, REPT NNEVT.
- SECURITY: Security event notifications
- OWN
Responses to own commands. The user will receive no other notifications.
- NA
Not applicable. For users with uidclass=MEMADMIN only this value is allowed. The notification behavior is controlled in this case by the user class. If the value NA is applied for users of other user classes, then the value has the same effect as DBCHG.

6. tmtout – inactivity timeout period
If there are no messages between the user and the NE over the Timeout Period, the session is logged off. A value of 0 disables the timeout function.
7. ucpl – user community priority level
This value is always set to 1.
8. uidclass – UID class
This is the user class of a *uid*.
Type: alphanumeric value set
Range:
 - 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.
 - MEMADMIN – User class for memory administration users. All users of this class share the same atag counter for autonomous messages and are allowed to execute the command RTRV-AO.
9. upc – user privilege code list
This parameter specifies the user privilege code UCFC/UCAL pair assigned to a user. If a user tries to operate a command with a privilege code higher than assigned to the user for the category of the command, the command will be denied.
Type: alphanumeric string. Also allowed is '&' for concatenation.
Range: Pi, Mi, Ti, Si, PMi, Di where “i” is an integer ranging from 0 to 5, with i=0 implying that there is no authorization for the functional category. Note: S0 is not allowed.
Default: P1&M1&T1&S1&PM1

END OF STEPS



To modify the current user's security information

When to use

Use this task to modify security information for the current user (the current login) on a network element. The information is related to the NE primary login used when the OMS-to-NE connection has been set up.

Related information

For a more detailed explanation, please refer to the description of the ED-USER command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Edit User**.
 5. Click **Go**.

Result: The **Edit User** page is displayed.

- 3 In the **Message screening** field, enter an alphanumeric string composed of a list of values from the list below. To enter more than one value, concatenate using the '&' symbol.

Range:

- **DBCHG**
Data Base Change notifications: changes in creation of entities, in user provisionable parameters, in deletion of entities will be reported (data base changes).
File Transfer In-progress notifications: The user will receive REPT DBCHG and REPT EVT FXFR messages.
The value DBCHG shall always be used together with the value STCHG.
- **STCHG**
State Change notifications – report changes in user non-provisionable parameters (state changes). The user will receive REPT DBCHG messages.
The value STCHG shall always be used together with the value DBCHG.
- **PSCHG**
Protection switch notifications – report protection switch changes. User will receive REPT EVT and REPT SW messages.
- **ALARMS**
Alarm notifications. The user will receive REPT ALM ENV, REPT ALM, and REPT EVT messages.
- **ONNS**
ONNS Notifications. Database and state changes associated with entities managed by ONNS application and only issued when *xcsetup* = NN. The related ONNS TL1 notifications are REPT PTHCHG, REPT PTHEVT, REPT NNCHG, REPT NNEVT.
- **SECURITY: Security event notifications**
- **OWN**
Responses to own commands. The user will receive no other notifications.
- **NA**
Not applicable. For users with uidclass=MEMADMIN only this value is allowed. The notification behavior is controlled in this case by the user class. If the value NA is applied for users of other user classes, then the value has the same effect as DBCHG.

4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To modify user security information

When to use

Use this task to modify security information for the users (logins) on a network element.

Related information

For a more detailed explanation, please refer to the description of the ED-USER-SECU command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Edit User Security**.
 5. Click **Go**.

Result: The **Edit User Security** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **Current user identifier** – the login (user) for which the security settings should be modified.
Range: 1 to 10 characters
 - **New password identifier** – specifies the new password ID for the addressed login. This is an optional parameter and in the absence of a value the default is the current value.
Range: 6 to 10 legal characters. Valid passwords consist of at least two non-alphabetic characters with at least one special character. The special character can be one of the required non-alpha characters. For example, TEST1+ is a valid password. The first character of a password must be a letter.
 - **User privilege code list** – specifies the user privilege code UCFC/UCAL pair assigned to a user. Multiple UCFC/UCALs can be specified using single ampersands (&). If a user tries to operate a command with a privilege code higher than assigned to the user for the category of the command the command will be denied.
Range: Pi , Mi , Ti , Si , PMi , Di where i is an integer ranging from 0 to 5, with $i = 0$ implying that there is no authorization for the functional category. S0 is not allowed.
 - **Allow login** – specifies the enable/disable state of a User ID.
A User ID can be automatically disabled by the system or via the ED-USER-SECU command. A User ID can be enabled via the ED-USER-SECU command.
If a User ID is disabled, logins with that User ID are denied.
Range:
 - YES: User ID is enabled
 - NO: User ID is disabled
 - **New user identifier** – allows to rename the 2 predefined super-users. It cannot be used to rename a non-super-user login. .
Range: 1 to 10 characters
The *uid* ALL is not allowed in any combination of upper or lower cases.
 - **Password aging interval (days)** – specifies the period in days after which the user has to change the password of their account. If the value is set to 0 then the password aging function is disabled.
Range: 0, 7 to 999 [days]
 - **Message screening** – enter an alphanumeric string composed of a list of values from the list below. To enter more than one value, concatenate using the '&' symbol.
Range:
 - DBCHG

Data Base Change notifications: changes in creation of entities, in user provisionable parameters, in deletion of entities will be reported (data base changes).

File Transfer In-progress notifications: The user will receive REPT DBCHG and REPT EVT FXFR messages.

The value DBCHG shall always be used together with the value STCHG.

– STCHG

State Change notifications – report changes in user non-provisionable parameters (state changes). The user will receive REPT DBCHG messages.

The value STCHG shall always be used together with the value DBCHG.

– PSCHG

Protection switch notifications – report protection switch changes. User will receive REPT EVT and REPT SW messages.

– ALARMS

Alarm notifications. The user will receive REPT ALM ENV, REPT ALM, and REPT EVT messages.

– ONNS

ONNS Notifications. Database and state changes associated with entities managed by ONNS application and only issued when *xcsetup* = NN. The related ONNS TL1 notifications are REPT PTHCHG, REPT PTHEVT, REPT NNCHG, REPT NNEVT.

– SECURITY: Security event notifications

– OWN

Responses to own commands. The user will receive no other notifications.

– NA

Not applicable. For users with uidclass=MEMADMIN only this value is allowed. The notification behavior is controlled in this case by the user class. If the value NA is applied for users of other user classes, then the value has the same effect as DBCHG.

- **Inactivity timeout period (min)** – if there are no messages between the user and the NE for the time specified, the session is logged off. A value of 0 disables the timeout function.

Range: 0 – 999 [minutes]

- **User identifier class** – specifies the user class.

Range:

- *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.

- *Memory Administration User* – User class for memory administration users. All users of this class share the same atag counter for autonomous messages and are allowed to execute the command RTRV-AO.

-
- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To modify the current user's password

When to use

Use this task to modify the current user's password (which is the current login on a network element). The information is related to the NE primary login used when the OMS-to-NE connection has been set up.

Related information

For a more detailed explanation, please refer to the description of the ED-PID command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Edit Password Identifier**.
 5. Click **Go**.

Result: The **Edit Password Identifier** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **Old password identifier** – specifies the password ID for the addressed login. This is an optional parameter and in the absence of a value the default is the current value.
Range: 6 to 10 legal characters. Valid passwords consist of at least two non-alphabetic characters with at least one special character. The special character can be one of the required non-alpha characters. For example, TEST1+ is a valid password. The first character of a password must be a letter.
 - **New password identifier** – specifies the password ID for the addressed login. This is an optional parameter and in the absence of a value the default is the current value.
Range: 6 to 10 legal characters. Valid passwords consist of at least two non-alphabetic characters with at least one special character. The special character can be one of the required non-alpha characters. For example, TEST1+ is a valid password. The first character of a password must be a letter.
-

- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To terminate user sessions

When to use

Use this task to terminate all login sessions of a particular user or all users within the NE.

Related information

For a more detailed explanation, please refer to the description of the CANC-USER-SECU command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Cancel User Security**.
 5. Click **Go**.

Result: The **Cancel User Security** page is displayed.

- 3 In the **User identifier** field, enter the login (user) for which the session should be terminated. To terminate all user's session, leave the field empty. Only privileged users can log out other users.
-

- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.
-

- 5 Click **Submit**.
-

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To create new users

When to use

Use this task to create new logins (users) and the related security information on a network element.

Related information

For a more detailed explanation, please refer to the description of the ENT-USER-SECU command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Users**.
4. In the **Function** field, select **Enter User Security**.
5. Click **Go**.

Result: The **Enter User Security** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **User identifier** – the new login (user) name.
Range: 1 to 10 characters
- **Password identifier** – specifies the password ID for the addressed login. This is an optional parameter and in the absence of a value the default is the current value.
Range: 6 to 10 legal characters. Valid passwords consist of at least two non-alphabetic characters with at least one special character. The special character can be one of the required non-alpha characters. For example, TEST1+ is a valid password. The first character of a password must be a letter.

- **User privilege code list** – specifies the user privilege code UCFC/UCAL pair assigned to a user. Multiple UCFC/UCALs can be specified using single ampersands (&). If a user tries to operate a command with a privilege code higher than assigned to the user for the category of the command the command will be denied.
Range: Pi, Mi, Ti, Si, PMi, Di where i is an integer ranging from 0 to 5, with $i = 0$ implying that there is no authorization for the functional category. S0 is not allowed.
- **Password aging interval (days)** – specifies the period in days after which the user has to change the password of their account. If the value is set to 0 then the password aging function is disabled.
Range: 0, 7 to 999 [days]
- **Message screening** – enter an alphanumeric string composed of a list of values from the list below. To enter more than one value, concatenate using the '&' symbol.
Range:
 - DBCHG
Data Base Change notifications: changes in creation of entities, in user provisionable parameters, in deletion of entities will be reported (data base changes).
File Transfer In-progress notifications: The user will receive REPT DBCHG and REPT EVT FXFR messages.
The value DBCHG shall always be used together with the value STCHG.
 - STCHG
State Change notifications – report changes in user non-provisionable parameters (state changes). The user will receive REPT DBCHG messages.
The value STCHG shall always be used together with the value DBCHG.
 - PSCHG
Protection switch notifications – report protection switch changes. User will receive REPT EVT and REPT SW messages.
 - ALARMS
Alarm notifications. The user will receive REPT ALM ENV, REPT ALM, and REPT EVT messages.
 - ONNS
ONNS Notifications. Database and state changes associated with entities managed by ONNS application and only issued when *xcsetup* = NN. The related ONNS TL1 notifications are REPT PTHCHG, REPT PTHEVT, REPT NNCHG, REPT NNEVT.
 - SECURITY: Security event notifications
 - ALL
All notifications.
This value can be used in input direction as a short-hand notation for DBCHG&STCHG&PSCHG&ALARMS&ONNS&SECURITY

- OWN (default)
Responses to own commands. The user will receive no other notifications.
- NA
Not applicable. For users with uidclass=MEMADMIN only this value is allowed. The notification behavior is controlled in this case by the user class. If the value NA is applied for users of other user classes, then the value has the same effect as DBCHG.
- **Inactivity timeout period (min)** – if there are no messages between the user and the NE for the time specified, the session is logged off. A value of 0 disables the timeout function.
Range: 0 – 999 [minutes]
- **User identifier class** – specifies the user class.
 - *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.
 - *Memory administration user* – user class for memory administration users. All users of this class share the same *atag* counter for autonomous messages and are allowed to execute the command RTRV-A0.

4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To delete users

When to use

Use this task to delete a particular user (login) within the NE.

Related information

For a more detailed explanation, please refer to the description of the DLT-USER-SECU command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Users**.
 4. In the **Function** field, select **Delete User Security**.
 5. Click **Go**.

Result: The **Delete User Security** page is displayed.

- 3 In the **User identifier** field, enter the login (user) to be deleted.

- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



3 Management communication setup concepts

Overview

Purpose

This chapter presents concept information related to management communication setup on *LambdaUnite*® MSS network elements using Lucent OMS.

Contents

Basic DCN principles	3-2
DCN configurations	3-5
DCN configuration guidelines	3-9
DCN protocols and services	3-10
NSAP address structure	3-12
Data communication channels (DCC)	3-14
LAN access	3-17
Name-to-address translation	3-18
OMS-to-NE connections concepts	3-19
NE CIT Cut-Through Concepts	3-21
Orderwire and user bytes	3-23



Basic DCN principles

Purpose

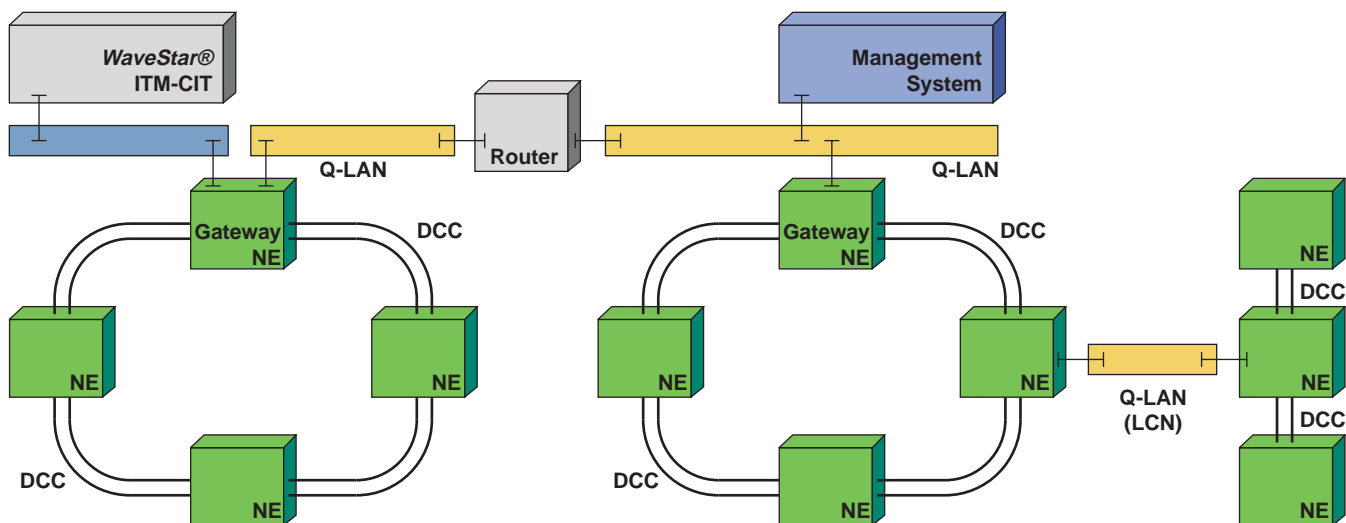
A *data communication network (DCN)* is used for the exchange of management data. This section provides an overview of the data communication network and describes the type of communication between the nodes in the network and the protocols used.

SDH/SONET management network

The SDH/SONET management network is an overlay of the transmission network. The management system (for example Lucent OMS) and the network elements (NEs) together are the nodes of this network. The 10/100BASE-T interface and *data communication channel (DCC)* provide the physical connection between the nodes.

DCN physical components

The figure below illustrates a data communication network (DCN) as defined by the Open Systems Interconnection (OSI) model. This figure refers to the physical components and connections in the DCN. It does not give information about the logical configuration of the DCN.



The figure shows three LANs and a number of DCC channels in an SDH/SONET transmission network with point-to-point configuration and two rings connected to a management system, for example Lucent OMS. The management system is connected to the transmission network via *gateway network elements (GNE)* by the LAN. The network elements are connected to each other by DCC channels.

Local Communications Network (LCN)

In the case where there is no DCC connectivity between nodes, a *local communications network (LCN)* can be used to connect the nodes to each other. See the LCN on the right side of the figure.

“NE” versus “Node”

Network elements can be identified by their *target identifier (TID)*, that is their NE name (“NE name” and “TID” are used synonymously throughout this manual), 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

A network element can consist of multiple OSI nodes (OSI node1 to OSI node8). 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 node1, which is the only node to offer the 7 layer OSI services to all application parts. Only node1 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 communication protocols

Communication protocols used in the data communication network (DCN) between the nodes include:

- Ethernet (on the 10BASE-T) LAPD (on the DCC channels)
- OSI network protocol (DCN wide)

The OSI network protocol (OSI-DCN) is used for routing management data between nodes in the DCN.

ISO-OSI network protocol

The network protocol used between nodes is the ISO-OSI network protocol (ISO/IEC 8648). According to this protocol a node in the network can behave as an end system (ES) or as an intermediate system (IS), sometimes called a router.

End systems (ES)

Nodes behaving as *end systems (ES)* perform no forwarding of data packets. They communicate with each other on an end-to-end basis via intermediate systems.

Intermediate systems (IS)

Intermediate systems (IS) are used for routing data between nodes and (sub) networks. The *end system to intermediate system (ES-IS) protocol* is responsible for the exchange of data between an end system and intermediate system. A network element can act both as an end system as well as an intermediate system. However, a Lucent OMS, for example, can only act as end system.

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. *LambdaUnite*[®] MSS products make use of the ES-IS protocol acc. to ISO 9542.

IS-IS protocol

The *intermediate system to intermediate system (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 this information base is used for the routing of management data packets in the DCN by the intermediate systems.

Routing information base and LSPs

Each RIB comprises a number of tables. These tables contain information on *network service access point (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 protocol data units (LSP)*.

The LSPs contain the information on the NSAP addresses of nodes used in the tables of the RIBs.

Management protocol: TL1

The management of *LambdaUnite*[®] MSS products is based on the use of the *transaction language 1 (TL1)*, defined by Telcordia Technologies, formerly Bellcore, standards on the OSI application layer.

□

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 is 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 algorithm.

Hierarchical routing definition

In hierarchical routing, the DCN addressing domain is divided into a number of areas. Each area is assigned a unique identifier. The value of the area identifier of each node's NSAP address is set according to the area the node is part of.

Level 1, level 2 definition

Each area contains a number of:

- End systems
- First level (level 1) intermediate systems
- Second level (level 2) intermediate systems

Level 1 intermediate systems provide interconnectivity between nodes within the same area. Level 2 intermediate systems provide interconnectivity between nodes belonging to different areas.

Level 2 subdomain

The complete set of level 2 intermediate systems is also referred to as the level 2 subdomain. All areas in a network are connected via the level 2 subdomain.

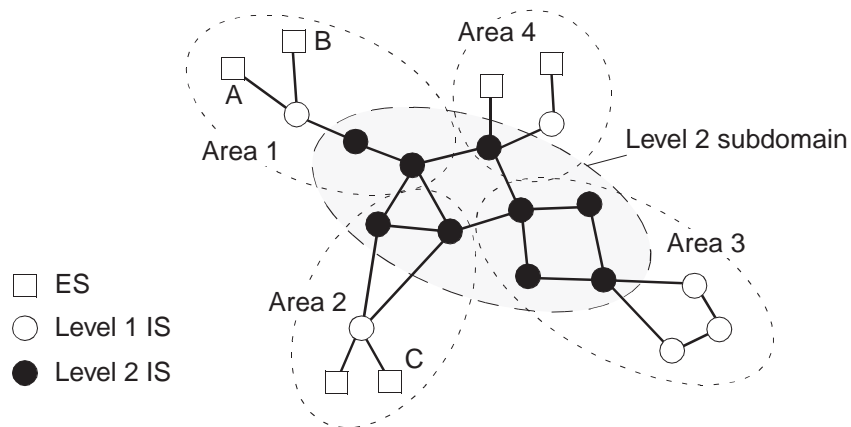
Area-divisioning of a DCN

Partitioning is configuration of the DCN in such a way that the exchange of LSPs between intermediate systems is limited.

When networks are partitioned into areas, the RIB database(s) in the systems are much smaller and hence the routing overhead is significantly reduced. Intermediate systems in an area only exchange information (LSPs) on nodes with other systems in their own area. Information on other areas is exchanged by level 2 intermediate systems only and maintained by the level 2 intermediate systems of the area.

In this way, the data management load 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 figure below illustrates how a network can be partitioned into areas, connected by level 2 intermediate systems. Each area has at least one level 2 intermediate system assigned and can have a number of level 1 intermediate systems and end systems.



Routing management data

The following scenario describes routing management data in a divisioned network. Suppose a node A wants to send messages to another node. If this node is in its own area (determined by the area ID part in the area address field), the messages from A to this particular node (B) are routed directly using the level 1 intermediate system (see previous figure).

Alternatively, if the required destination is in a different area (C), the messages are sent to a second, higher level (level 2) intermediate system. This intermediate system routes the messages coming from node A to other level 2 intermediate systems until they reach a level 2 intermediate system attached to the destination area of C. From there it is routed within the area using level 1 intermediate systems to node C.

Notice that in both of the above cases the ES-ES communication between nodes in the same or in different areas is still possible.

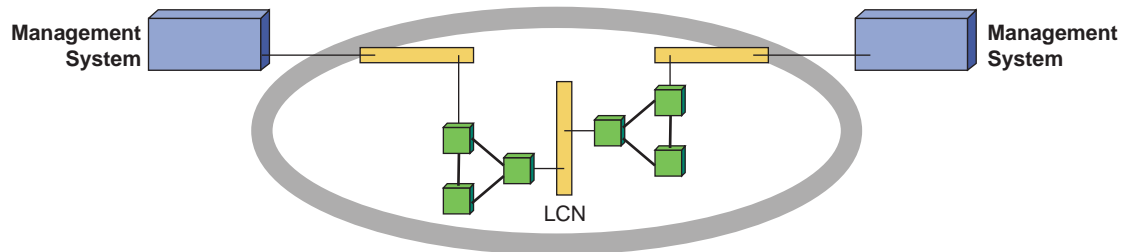
OSI-DCN networks types

In general, the OSI-DCN network can be classified in three types:

- Undivided
- IS-IS clustered
- IS-IS area divided network

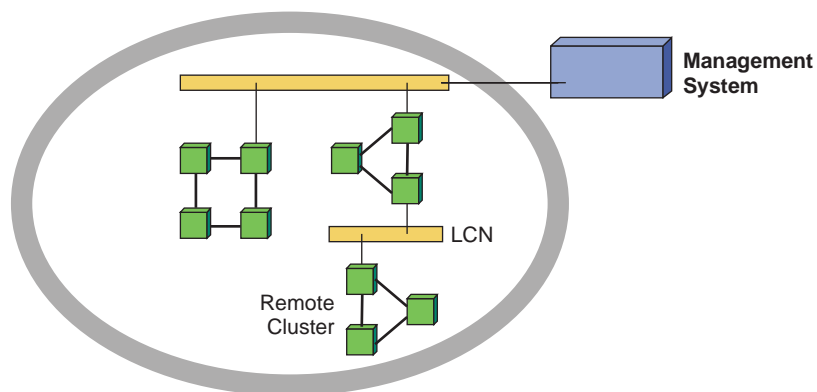
Undivided network definition

An undivided network consists of a single routing domain. There is no division between the nodes at the 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 Lucent OMS 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 of the network.



IS-IS clustered DCN

In order to avoid the decrease of performance, the exchange of LSPs over a certain port can be disabled in some nodes. A node can exchange LSPs over its DCC or LAN (10BASE-T) ports. The exchange of LSPs over the DCC channel can be disabled. However, this also prevents the exchange of management data over this port and prevents the use of this DCC port for re-routing in case of a failure of another port.



Disabling exchange of LSPs

Another option is to disable the exchange of LSPs over the LAN (10BASE-T) port. This can be done by choosing the IS to have a NO-IS-IS port. This node is also referred to as a NO-IS-IS (gateway) node. If this is done for all intermediate systems on a LAN, the LAN becomes a NO-IS-IS LAN. In NO-IS-IS LANs, the IS-IS protocol

is not run on the 10BASE-T. This prevents the exchange of LSPs between intermediate systems on a 10BASE-T. This results in a network which comprises several clusters of nodes. Between the clusters there is no IS-IS traffic.

ES-ES communication

Within a cluster the ES-ES, ES-IS and IS-IS communication is still possible. There is however no communication possible between nodes in different clusters. For example a ITM-CIT can be connected to a node in a cluster for maintenance activities on nodes within a cluster. However, it is then not possible to do a remote login from this node to a node of another cluster.

Management system connections

The management system connected to the 10BASE-T can still communicate with all nodes in the clusters since the ES-IS protocol on the 10BASE-T is not disabled. Important to notice is that the nodes in a remote cluster lose their association with the management system when NO-IS-IS is chosen on the gateway node of the remote cluster. It is advised to connect the management system to the 10BASE-T that connects the clusters to each other and to assign NO-IS-IS only to nodes on this LAN.

IS-IS area divided DCN

The division of the DCN in areas by introducing level 2 intermediate systems is similar to disabling the IS-IS protocol over the 10BASE-T port of nodes, as described earlier.

Similar to clustering, the exchange of level 1 LSPs between intermediate systems in different areas is prevented. However, level 2 LSPs are still exchanged between level 2 intermediate systems.

□

DCN configuration guidelines

Guidelines

Please observe the following engineering guidelines when configuring a DCN with *LambdaUnite*[®] MSS systems involved:

- A maximum of 250 nodes (NSAP addresses) is supported in an area.
Notice that a *LambdaUnite*[®] MSS network element can contain one or more *nodes*.
- A maximum of 50 areas is supported in a subnetwork.
- All nodes in an area must have the same area address.
- 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 across 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.
 - The number of level-2 ISs be about the same as the average area size.

□

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. ITM-CIT dialogues and OS messages are transmitted in these DCC bytes.

The *LambdaUnite*[®] MSS OS interface is accessed through one of the rear panel LAN connectors (10BASE-T or 100BASE-T). 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:

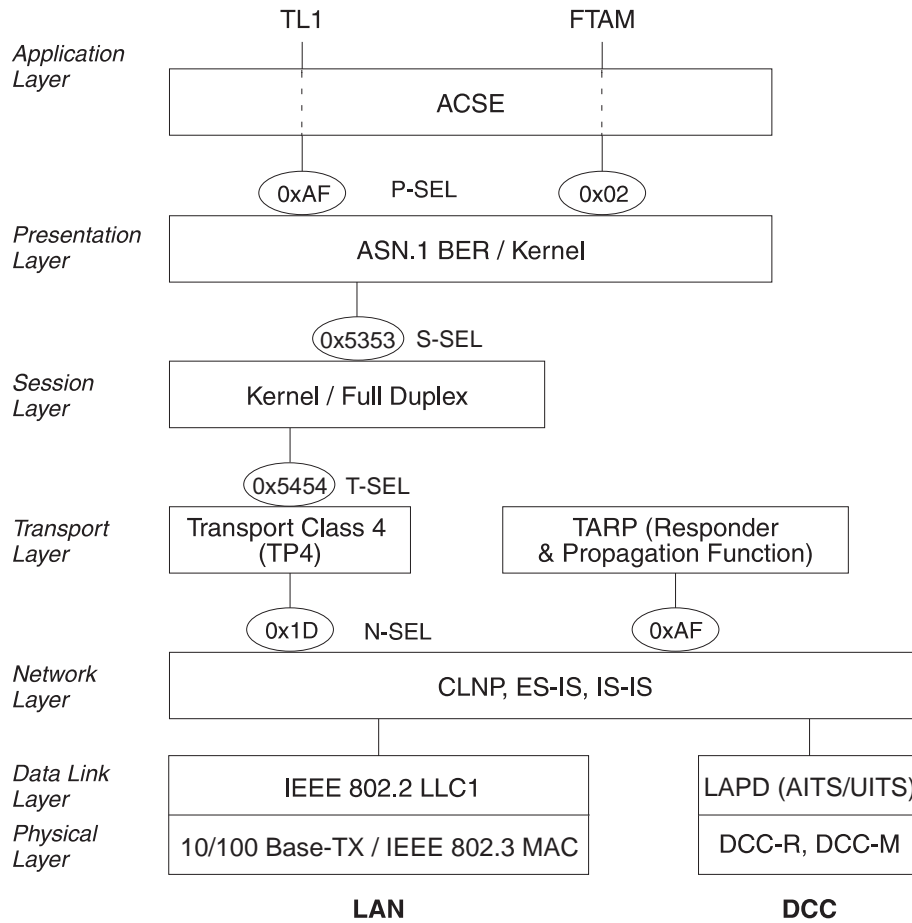
- OSI LAN/WAN
- TL1 TCP/IP (using the internal gateway function)
- FTAM protocol for software download, database backup and restore.
- FTP for software download, database backup and restore.

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.

□

NSAP address structure

NE addressing

A *LambdaUnite*[®] MSS NE that runs OSI has at least one node, which is referred to as *node1*. Additional nodes can be added, with a subset of the functionality of *node1*.

When a node acts as an intermediate system (all nodes), SEL is 0, implying that we are concerned with the *network entity title (NET)* alone. When a node acts as an end system (*node1*), which is where the network services are provided, SEL is not 0, implying we are concerned with the NSAPs.

A node is known by its unique NET. 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 TL1 messages toward the user interfaces, the NSAP for TL1 management via *node1* will be presented. For the other nodes, the NET is used.

Background

The following three NSAP structures can be distinguished:

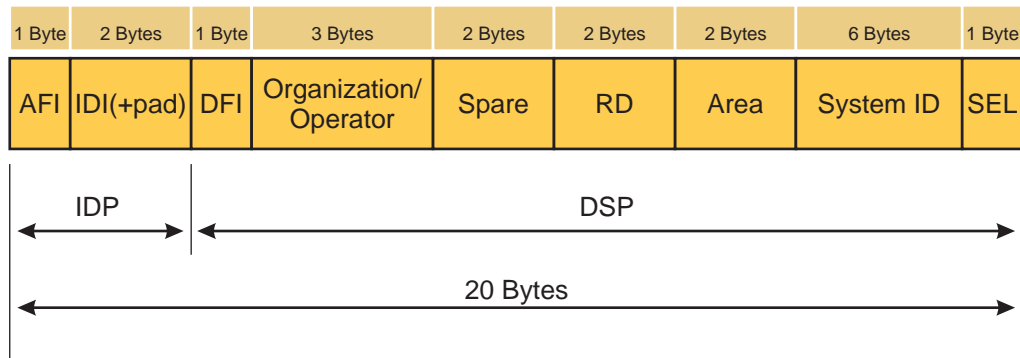
- ISO DCC NSAP address format (fixed 20-byte address structure). This format is used by most Lucent Technologies network element types in the network.
- Local Lucent Technologies NSAP address format (fixed 10-byte address structure). This format is also used by a number of Lucent Technologies network element types.
- Flexible NSAP address structure. An alternative to the previous two formats.

Although different NSAP address formats exist, preferably all nodes in a network should use the same address format.

LambdaUnite[®] MSS supports the ISO DCC NSAP address format (fixed 20-byte address structure).

Fixed 20-byte address structure

The fixed 20-byte address structure (ISO DCC NSAP address format, in accordance with ISO 8348) is shown in the following figure:



Address fields

The meaning of the NSAP address fields is described in the following table:

Field	Meaning	Description
<i>Initial domain part (IDP):</i>		
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.
IDI	Initial domain identifier specifying the country code. The designation "IDI+pad" indicates that the field is padded to its maximum length	The predefined value is 0x0000 (hex.).
<i>Domain specific part (DSP):</i>		
DFI	DSP format identifier specifying the DSP format.	The predefined value is 0x80 (hex.).
Operator	Organization or operator identifier representing the network service provider (NSP).	The predefined value is 0x000000 (hex.).
Spare	Reserved portion of the NSAP.	The predefined value is 0x0000 (hex.).
RD	Routing domain.	The predefined value is 0x0000 (hex.).
Area	Area identifier indicating the routing area to which a node belongs.	The predefined value is 0x0000 (hex.).
System ID	System identifier representing the node. The IEEE 802.3 MAC address.	A IEEE-MAC number is reserved and physically stored on every NE.
SEL	Selector field used to direct the protocol data units (PDU) to the correct destination.	The predefined value is 0x01 (hex.).



Data communication channels (DCC)

Data communication channels (DCC)

The *data communication channels (DCC)* are part of the data communication network (DCN). The channels are used to exchange management data between the management system and the network elements. The channels are also used for communication between the different network elements (for example remote logins). The DCC connection is achieved by means of layer 2 protocol High Level Data Link Control (HDLC) Frame bridging (at the data link layer level). HDLC Frame bridging always applies to two ports (labeled TTP1 and TTP2); more than two ports (that is, broadcasting) is not supported. The DCC connection is implemented via Layer bridging.

DCC channel selection

The following DCC channels exist on an STM-*n* connection:

- DCC bytes of the RSOH (bytes D1-D3) termed RS-DCC.
- DCC bytes of the MSOH (bytes D4-D12) termed MS-DCC.

Transparent DCC cross-connections

The *transparent DCC cross-connect* feature allows to transparently pass-through certain DCC channels which cannot or should not be processed by the system.

Transparent DCC cross-connections are to be used when there is a router on one side of the SDH/SONET network which uses the DCC to transport some IP-based protocol to a router on the other side of the network. This feature can be used to avoid interworking with equipment from a different vendor in a common routing domain.

The transparent DCC cross-connection path is transparent. This means that no processing at all will be done as the data travels along the path. Therefore, the entire transparent DCC cross-connection path counts as a single hop for the network elements at the ends of the path.

The transparent DCC cross-connections are completely independent from the transmission cross-connections. There is no relation between the number of “normal” (terminated) DCC channels and the number of transparent DCC channels. They are taken from different pools.

Therefore, enabling a “normal” (terminated) DCC channel does not reduce the number of available transparent DCC channels, and vice versa.

For each DCC channel, transparent DCC cross-connection and traditional DCC processing on the CTL/DCF are mutually exclusive.

Functional requirements

The following functional requirements to the transparent DCC channels:

- The number of bidirectional transparent DCC channels is limited to 25.
- It is possible to use transparent DCC cross-connections for RS-DCC and MS-DCC.

Establishing transparent DCC cross-connections

Transparent DCC cross-connections are to be established by identification of the two ports of an NE that are to be cross-connected and the DCC type (RS-DCC or MS-DCC).

LAPD protocol

The LAPD protocol, which controls communication between the network elements, operates in either of the following modes:

- *Network side*
The LAPD is assigned as network. This mode complies with the standards and interoperates successfully with other LAPDs operating in user_side mode.
- *User side*
The LAPD is assigned as user. This mode complies with the standards and interoperates successfully with other LAPDs operating in network_side mode.

Please note that the DCCs work according to the master/slave principle, that is the LAPD modes of two interconnected SDH ports must be set differently. A corresponding “user-network side failure” alarm will be generated if the LAPD mode is the same at both ends of a DCC.

AIMS and UITS supported

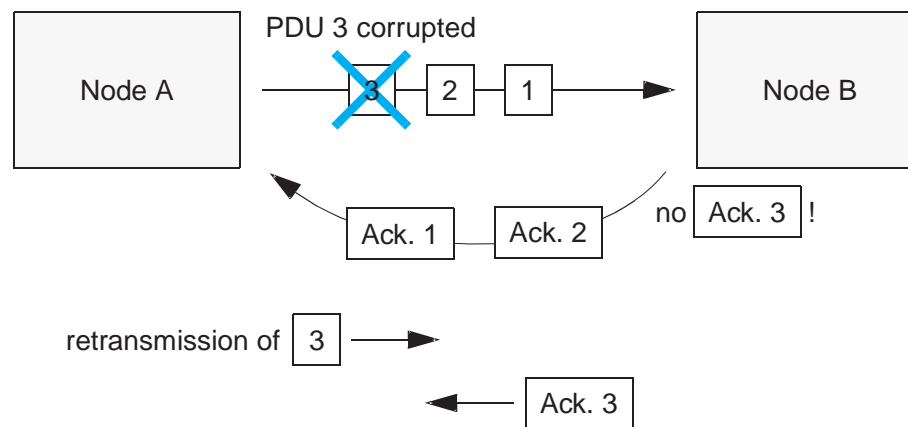
LambdaUnite[®] MSS network elements support the acknowledged information transfer service (AIMS) and the unacknowledged information transfer service (UITS) as the basis for the LAPD or LinkID protocol with the UITS mode being the default mode of operation. AIMS should only be used if required by other 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 acknowledgment PDUs are sent back from the receiver to the sender. If a PDU is lost, that is, if the sender gets no acknowledgment, the PDU is retransmitted.

Functional principle of the AIMS



DCC over 1+1 MSP protected interfaces

To support DCC communication over 1+1 MSP protected STM-*n* links, two modes of operation are defined, which can be selected independently for RS-DCC and MS-DCC

1. MSP DCC Independent Mode

In this mode the DCC channels over the working and protection STM-*n* interface operate independently from the MSP protocol and can individually be enabled/disabled. DCC protection is performed at the IS-IS protocol level.

2. MSP DCC Slave Mode

In this case the DCC information in the transmit direction is bridged over both the working and the protection part of the MSP connection. At the receive end the DCC is retrieved from the service (= active) part.

□

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 an EMS).
4. LAN4: This LAN interface is HW-prepared only. There is no protocol definition available yet.

TARP LAN storm suppression (TLSS)

TARP LAN storm suppression (TLSS) works by using enhanced propagation rules for TARP PDUs of types 1, 2 and 4, for either level-1 or level-2 IS routers. For LANs, the enhanced propagation rules result in significantly fewer TARP/CLNP messages. If N is the number of network elements on the LAN, then the number of messages launched for each propagated query (type 1 or 2 message) or autonomous notification (type 4 message) would be of order N instead of order N*N.

Network elements that implement TLSS can co-exist with network elements that do not implement TLSS. The performance improvement will of course be less when there are network elements present that do not implement TLSS.

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 ITM-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.

TID to NSAP-address translation

LambdaUnite[®] MSS offers two possible ways to accomplish the TID to NSAP-address translation:

1. A static routing table
2. The TID address resolution protocol (TARP).

To establish a management association to a remote NE, the ITM-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.

□

OMS-to-NE connections concepts

Definition: OMS-to-NE connection

An OMS-to-NE connection is the communications connection between the management system and an NE. This connection is established when the NE is added to the management system. OMS-to-NE connections exist only in the management system; the addition of an OMS-to-NE connection has no influence on an NE.

Functionality description

The management system is used to establish and manage OMS-to-NE connections. An OMS-to-NE connection is established when an NE is added to the management system. When an OMS-to-NE connection is established, the communications interface that will be used for communication from the NE to the management system is selected.

In a High Availability configuration, if any NE is manually added to the primary management system using the management system's graphical user interface, in the same way, the NE must also be manually added to the secondary management system. Similarly, any NE that is auto-discovered by the primary management system will be auto-discovered by the secondary management system.

Preconditions

A minimum subset of provisioning must be done before NEs can be added to the management system. The craft interface terminal (ITM-CIT) must be used to provision certain information when the NE is set up.

Consult the LambdaUnite® *MSS User Operations Guide* for instructions on how to provision an NE so it is ready to be managed by a management system such as Lucent OMS.

For *LambdaUnite*® MSS NEs that use OSI communications, the NSAP address of the management system must be added to the access list of the NE so the NE can communicate with the management system.

Supported communications interfaces

LambdaUnite[®] MSS supports the following types of communications interfaces:

- *OSI*: Communication occurs via a direct connection between the management system and each of the NEs.
- *TCP/IP GNE*: The management system communicates with a subnetwork of NEs through one NE that has been designated as the gateway. An NE using a communications interface of TCP/IP GNE has been designated as the *gateway NE (GNE)*, which means it is the gateway for communications between the management system and the other NEs in a network communications group. The GNE is used by the management system to communicate with all NEs in a network communications group.
- *TCP/IP RNE*: The management system communicates with a subnetwork of NEs through one NE that has been designated as the gateway. An NE using a communications interface of TCP/IP RNE is has been designated as a *remote NE (RNE)*, which means it is not the gateway for communications with the subnetwork. An RNE is an NE in a network communications group that the management system accesses through a GNE.

The management system communicates with a GNE using TCP/IP, while the managed NEs in a network communications group communicate with each other using OSI.

FTP/FTAM gateway

An FTP/FTAM gateway converts FTP, which is the file transfer protocol used in TCP/IP networks, to FTAM, which is the file transfer protocol used in OSI networks.

Every RNE and GNE must have an FTP/FTAM gateway defined because the following features of the management system utilize file transfer protocol:

- Backup NE database version
- Restore NE database version
- Download from Management System to NE

If it is not done already, the user must, either via the ITM-CIT or the management system **NE Management Functions** page, provision the NE selected as the FTP/FTAM gateway to serve that role before any file transfer activity is attempted. File transfer attempts will fail if the NE is not enabled for that role.

When adding a NE to the management system, the user must specify the FTP/FTAM gateway designations. If the NE is automatically discovered without the FTP/FTAM gateway designations, the operator can establish the designations afterwards.

Reference

For more detailed explanations related to the concepts of OMS-to-NE connections, refer to the *Lucent OMS Network Element Management Guide*.



NE CIT Cut-Through Concepts

NE CIT cut-through for a supported NE

The management system supports cut-through capabilities from the Lucent OMS PC client to the craft interface terminal (CIT) for the LambdaUnite[®] MSS NE.

NE CIT cut-through supported platforms

The use of cut-through capabilities from the Lucent OMS PC client to the NE CIT is supported on the following platforms:

- *Lucent OMS HP[®] PA RISC Server Hardware Platform*, which is commonly referred to as the Server Platform.
- *Lucent OMS HP[®] Itanium[®] Server Hardware Platform*, which is commonly referred to as the Server Platform.

The use of cut-through capabilities to the NE CIT is not supported on the “Lucent OMS PC Platform”, which is commonly referred to as the PC Platform.

Location of the NE CIT

Once installed, the LambdaUnite[®] MSS CIT software is installed in the following default directory:

C:\Program Files\Lucent Technologies\WaveStar CIT

The java.policy file for NE CIT cut-through

The property, file, and socket permissions in the java.policy file must be set so the Lucent OMS management system can access system files. Refer to the *Configure the java.policy File for NE CIT Cut-Through* task for detailed instructions.

Once the java.policy file is modified, the browser must be closed and reopened for any changes to take effect. The management system can then access the command files that are needed to invoke the cut-through to the NE CIT. These command files are explained in detail in *Command Files for the NE CIT Cut-Through* section and in the *Work with Command Files to Invoke the NE CIT Cut-Through* task.

Order of task execution for NE CIT cut-through

To support the display of the CIT from the management system pages, execute the following tasks in the order in which they follow:

1. Execute the *Install the NE CIT* task.
2. If needed, execute the *Launch the NE CIT away from the Default Location* task.
3. Execute the *Configure the java.policy File for NE CIT Cut-Through* task.

4. If needed, execute the *Work with Command Files to Invoke the NE CIT Cut-Through* task.
5. If needed, execute the *Troubleshoot the NE CIT* task.



Orderwire and user bytes

Introduction

Each *LambdaUnite*[®] MSS network element provides six user byte interfaces which can be used to access certain overhead bytes of an SDH/SONET transport signal. If desired, an external orderwire equipment can be connected to these interfaces for example.

User bytes can be provisioned by associating or disassociating an SDH/SONET port with a user byte interface.

Important! Orderwire and user byte access is supported by 155-Mbps and 10-Gbps port units (EP155, OP155, OP10) *only*.

Overhead bytes

Each SDH/SONET port supports three dedicated user bytes:

- The *E1* byte in the SDH regenerator section overhead (RSOH) or SONET section overhead (SOH), respectively, can be used as a 64-kbps orderwire channel.
- The *E2* byte in the SDH multiplex section overhead (MSOH) or SONET line overhead (LOH), respectively, can be used as a 64-kbps orderwire channel.
- The *F1* byte in the SDH regenerator section overhead (RSOH) or SONET section overhead (SOH), respectively, can be used as a 64-kbps user data channel.

Each shelf provides user-provisionable access to up to six of these bytes from among the provisioned SDH/SONET ports in the shelf.

User byte interfaces

The six user byte interfaces are available on the CI-CTL (connection interface of the controller; accessible from the rear side of the shelf).

There are four universal interfaces which can be used as G.703 co-directional or V.11 contra-directional interfaces. Two interfaces can be used as V.11 only.

These interfaces can be used as G.703 or V.11 interfaces:

- User byte interface #1 (USERBIO1)
- User byte interface #2 (USERBIO2)
- User byte interface #3 (USERBIO3)
- User byte interface #4 (USERBIO4)

These interfaces can only be used as V.11 interfaces:

- User byte interface #5 (USERBIO5)
- User byte interface #6 (USERBIO6)

Pin assignment

The pin assignment of the user byte interfaces is described in the LambdaUnite® *MSS Installation Guide*.



4 Management communication setup tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to management communication setup and to system provisioning.

Contents

Tasks related to OMS-to-NE connections	4-3
To view a list of OMS-to-NE connections	4-3
To add an OMS-to-NE connection	4-4
To modify an OMS-to-NE connection	4-9
To deactivate an OMS-to-NE connection	4-13
To activate an OMS-to-NE connection	4-15
To delete an OMS-to-NE connection	4-17
To delete an NE	4-19
To display the communication state of an NE	4-21
Tasks related to DCC	4-23
To retrieve DCC related parameters	4-23
To modify DCC related parameters	4-26
To retrieve DCC/EOW status information for a port	4-28
To modify DCC/EOW status information for a port	4-30
To view a list of transparent DCC cross-connections	4-32
To add a transparent DCC cross-connection	4-34
To delete a transparent DCC cross-connection	4-36
Tasks related to system provisioning	4-38

To view NE date and time	4-38
To modify NE date and time	4-40
Tasks related to OMS-to-NE CIT Cut-Through	4-42
Command Files for the NE CIT Cut-Through	4-42
Install the NE CIT	4-44
Launch the NE CIT away from the Default Location	4-46
Configure the java.policy File for NE CIT Cut-Through	4-48
Work with Command Files to Invoke the NE CIT Cut-Through	4-50
Troubleshoot the NE CIT	4-51



Tasks related to OMS-to-NE connections

To view a list of OMS-to-NE connections

When to use

Use this task to view a list of OMS-to-NE connections.

Task

-
- 1 Use the object links to follow this path: **Management Network** → **OMS to NE Connections**.

Result: The **Search** section of the **OMS to NE Connections** page is displayed.

- 2 Make selections in one or more of the following fields in the **Search** section of the window:
 - In the **NE type** field, select a type of NE.
 - In the **NE name(s)** field, the **Available** table contains all NEs of the selected NE type available on the management system. The **Selected** table contains the NEs that are to be considered in the search. Click an NE and use the arrow buttons to move one or more NEs from the **Available** table to the **Selected** table, or click the double arrows to move all the NEs to the **Available** table.
 - In the **Comm type** field, select a type of communication interface between the NE and the management system.
 - In the **Net Comm Group** field select the NCG name from the drop-down list. The NCG names displayed depend on the selection in the **Comm type** field.
-

- 3 Click **Search**.

Result: The list at the bottom of the **OMS to NE Connections** page is populated with a list of the OMS-to-NE connections in the network that meet your search criteria.

END OF STEPS



To add an OMS-to-NE connection

When to use

Use this task to add an NE and establish an OMS-to-NE connection between the management system and the new NE.

Important! Indirectly managed NEs cannot be added using this task.

Before you begin

Gather the following information about the NE to be added:

- NE name
- NE type (here: *LambdaUnite*[®] MSS)
- Communications type (here: OSI or TCP/IP)
- Network communications group to which the NE will be assigned; ensure that it exists
- NSAP information or IP address of the NE, respectively

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network**. The **Network Map** is displayed. Click on the **New** tool in the toolbar and select **Network element** from the drop-down list.
 - Use the object links to follow this path: **Network Elements**. Click on the **New** tool in the toolbar.
 - Use the object links to follow this path: **Management Network** → **OMS-to-NE connections**. Click on the **New** tool in the **Search** section of the window.

Result: The **Add OMS-to-NE connection** page is displayed.

- 2 In the **NE name** field, enter a name that will be used by the management system to identify this NE. This field accepts a maximum of 20 characters. Use the *target identifier (TID)* of the NE, which was provisioned during installation of the NE as *NE name*. See the *Lucent OMS Getting Started Guide* for a list of allowable characters.

- 3 In the **NE type** field, select *LambdaUnite*[®] MSS.

-
- 4 In the **Comm type** field, select one of the following
- **OSI** – the NE in question communicates via the OSI interface
 - **TCP/IP GNE** – the NE in question communicates via the TCP/IP interface and acts as gateway NE for a subnetwork
 - **TCP/IP RNE** – the NE in question communicates via the TCP/IP interface and acts as a remote NE. That means the NE is not the gateway for communications with the subnetwork.
-

- 5 Move to the **OMS-to-NE connections details** panel by clicking the number 2 in the navigation aid or click **Next**.

Result: The **OMS-to-NE connections details** panel is displayed.

.....

6	If you add...	then...
	an OSI NE	go to Step 7 .
	a TCP/IP GNE	go to Step 8 .
	a TCP/IP RNE	go to Step 9 .

.....

- 7 Set the fields of the **OMS-to-NE connections details** panel as required:
- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
 - **NSAP address** – enter the NSAP address details of the NE in the following text fields:
 - **AFI** – the authority and format identifier specifying the NSAP address format (1 hexadecimal digit). The predefined value is 0x39 (hex.), indicating that the ISO Data Country Code (ISO-DCC) is the address format.
 - **IDI+pad** – the initial domain identifier specifying the country code, padded to its maximum length (2 hexadecimal digits).
 - **DFI** – the DSP format identifier specifying the DSP format (2 hexadecimal digits).
 - **Operator ID** – the operator or organization identifier representing the network service provider (NSP) (3 hexadecimal digits).
 - **RD** – the routing domain (2 hexadecimal digits).

- **Area** – the area identifier indicating the routing area to which a node belongs (4 hexadecimal digits).
- **System ID** – the system identifier representing the node. The IEEE 802.3 MAC address (12 hexadecimal digits).

Continue with [Step 10](#).

- 8** Set the fields of the **OMS-to-NE connections details** panel as required:
- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
 - **Primary IP address** – enter the four fields of the network element's IP address.
 - **Secondary GNE** – optionally select a secondary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **FTP/FTAM gateway** – select one of the following options:
 - **This NE does not use a FTP/FTAM gateway**
 - **This NE is a FTP/FTAM gateway.** If this option is selected, provide the controller #1 NSAP address.
 - **This NE uses the following FTP/FTAM gateway.** If this option is selected, choose one of the FTP/FTAM gateway NEs from the drop-down list provided.

Continue with [Step 10](#).

- 9** Set the fields of the **OMS-to-NE connections details** panel as required:
- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
 - **Primary GNE** – select the primary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **Secondary GNE** – optionally select a secondary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **FTP/FTAM gateway** – select one of the following options:
 - **This NE does not use a FTP/FTAM gateway**
 - **This NE uses the following FTP/FTAM gateway.** If this option is selected, choose one of the FTP/FTAM gateway NEs from the drop-down list provided.

- 10** Click **Next**.
-

Result: The **OMS to NE connections security information** panel is displayed.

- 11 Set the fields of the **OMS-to-NE security information** panel as required:
- **NE primary login** – enter the primary login (user) of the NE for establishing association. This must be a valid login ID in the NE.
 - **NE primary password** – enter the primary password of the NE for establishing association.
 - **Retype NE primary password** – reenter the primary password of the NE.
 - **NE secondary login** – optionally enter the secondary login (user) of the NE for establishing association. This must be a valid login ID in the NE.
 - **NE secondary password** – optionally enter the secondary password of the NE for establishing association.
 - **Retype NE secondary password** – optionally reenter the secondary password of the NE.

Click **Next**.

Result: The **OMS-to-NE connection summary** panel is displayed.

- 12 Review the summary for this OMS-to-NE connection.

Do one of the following:

- If you wish to return to a panel to change a selection, either click the panel number on the navigation aid, or click **Edit** for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step.
- If the selections are all correct, click **Submit** to complete the addition of the OMS-to-NE connection.

Result: A confirmation is issued in the **Message** section of the **OMS-to-NE connection summary** page, the NE is added to the management system and a communications connection is established between the management system and the new NE.

The addition of an NE to the management system initiates a full database synchronization. The NE is automatically added to the **Network Map**. The NE is added to the remaining pages of the management system after a refresh is executed.

If the OMS-to-NE connection being added is a GNE, a message is displayed: “The system will be unable to perform most management functions until the full database synchronization with the NE is completed. Do you want to activate the automatic database synchronization after the NE is added?”. The user can choose “Yes” or “No”. If the user chooses “Yes”, the system initiates a full database synchronization after the OMS-to-NE connection is successfully added. If the user chooses “No”, the system does not initiate a full database synchronization after the OMS-to-NE connection is successfully added.

Initially, the color of the NE icon will be magenta, which indicates a loss of communications. Once the NE addition is complete, the color of the NE icon will change to green, indicating *normal* status, or another color that indicates the presence of an alarm.

END OF STEPS



To modify an OMS-to-NE connection

When to use

Use this task to modify an OMS-to-NE connection.

Important! Changing OMS-to-NE connection details may result in a loss of association. Incorrect values for the parameters may result in the NE becoming unmanageable.

Task

- 1 Use the object links to follow this path: **Management Network** → **OMS-to-NE Connections**.

Result: The **Search** section of the **OMS-to-NE Connections** page is displayed.

- 2 Make selections in one or more of the following fields in the **Search** section of the window:
 - In the **NE type** field, select a type of NE.
 - In the **NE name(s)** field, the **Available** table contains all NEs of the selected NE type available on the management system. The **Selected** table contains the NEs that are to be considered in the search. Click an NE and use the arrow buttons to move one or more NEs from the **Available** table to the **Selected** table, or click the double arrows to move all the NEs to the **Available** table.
 - In the **Comm Type** field, select a type of communication interface between the NE and the management system.
 - In the **Net Comm Grp** field select the NCG name from the drop-down list. The NCG names displayed depend on the selection in the **Comm Type** field.
-

- 3 Click **Search**.

Result: The list at the bottom of the **OMS-to-NE Connections** page is populated with a list of the OMS-to-NE connections in the network that meet your search criteria.

- 4 The **NE name** column of the table lists the names of the OMS-to-NE connections. The name in this column is a hyperlink.

Do one of the following:

- Click the name of the OMS-to-NE connection you wish to view.
- Click the radio button next to the OMS-to-NE connection you wish to modify. From the **Go** menu, select **Modify** and click **Go**.

Result: The **OMS-to-NE connections general information** page is displayed.

- 5** On the **OMS-to-NE connections general information** panel, no modifications are possible if you want to modify an OSI NE or a TCP/IP GNE.

If you want to modify a TCP/IP RNE to be a TCP/IP GNE, change the **Communications type**.

- 6** Move to the **OMS-to-NE connections details** panel by clicking the number 2 in the navigation aid or click **Next**.

Result: The **OMS-to-NE connections details** panel is displayed.

7	If you modify...	then...
	an OSI NE	go to Step 8 .
	a TCP/IP GNE	go to Step 9 .
	a TCP/IP RNE	go to Step 10 .

- 8** Set the fields of the **OMS-to-NE connections details** panel as required:

- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
- **NSAP address** – enter the NSAP address details of the NE in the following text fields:
 - **AFI** – the authority and format identifier specifying the NSAP address format (1 hexadecimal digit). The predefined value is 0x39 (hex.), indicating that the ISO Data Country Code (ISO-DCC) is the address format.
 - **IDI+pad** – the initial domain identifier specifying the country code, padded to its maximum length (2 hexadecimal digits).
 - **DFI** – the DSP format identifier specifying the DSP format (2 hexadecimal digits).
 - **Operator ID** – the operator or organization identifier representing the network service provider (NSP) (3 hexadecimal digits).
 - **RD** – the routing domain (2 hexadecimal digits).

- **Area** – the area identifier indicating the routing area to which a node belongs (4 hexadecimal digits).
- **System ID** – the system identifier representing the node. The IEEE 802.3 MAC address (12 hexadecimal digits).

Continue with [Step 11](#).

- 9** Set the fields of the **OMS-to-NE connections details** panel as required:
- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
 - **Primary IP address** – enter the four fields of the network element’s IP address.
 - **Secondary GNE** – optionally select a secondary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **FTP/FTAM gateway** – select one of the following options:
 - **This NE does not use a FTP/FTAM gateway**
 - **This NE is a FTP/FTAM gateway.** If this option is selected, provide the controller #1 NSAP address.
 - **This NE uses the following FTP/FTAM gateway.** If this option is selected, choose one of the FTP/FTAM gateway NEs from the drop-down list provided.

Continue with [Step 11](#).

- 10** Set the fields of the **OMS-to-NE connections details** panel as required:
- **Net Comm Grp** – select the network communications group to which the OMS-to-NE connection belongs from the drop-down list.
 - **Primary GNE** – select the primary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **Secondary GNE** – optionally select a secondary GNE to connect through from the list of all GNEs in the network communications group provided.
 - **FTP/FTAM gateway** – select one of the following options:
 - **This NE does not use a FTP/FTAM gateway**
 - **This NE uses the following FTP/FTAM gateway.** If this option is selected, choose one of the FTP/FTAM gateway NEs from the drop-down list provided.

- 11** Click **Next**.
-

Result: The **OMS to NE connections security information** panel is displayed.

12 Set the fields of the **OMS-to-NE security information** panel as required:

- **NE primary login** – enter the primary login (user) of the NE for establishing association. This must be a valid login ID in the NE.
- **NE primary password** – enter the primary password of the NE for establishing association.
- **Retype NE primary password** – reenter the primary password of the NE.
- **NE secondary login** – optionally enter the secondary login (user) of the NE for establishing association. This must be a valid login ID in the NE.
- **NE secondary password** – optionally enter the secondary password of the NE for establishing association.
- **Retype NE secondary password** – optionally reenter the secondary password of the NE.

Click **Next**.

Result: The **OMS-to-NE connection summary** panel is displayed.

13 Review the summary for this OMS-to-NE connection.

14 Do one of the following:

- If you wish to return to a panel to change a selection, either click the panel number on the navigation aid, or click **Edit** for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step
- If the selections are all correct, click **Submit** to complete the modification of the OMS-to-NE connection.

Result: A confirmation is issued in the **Message** section of the **OMS-to-NE connection summary** page, and the OMS-to-NE connection is modified.

END OF STEPS



To deactivate an OMS-to-NE connection

When to use

Use this task to deactivate the communications connection between the management system and an NE. When you deactivate an OMS-to-NE connection, the NE is not communicating with the management system.

Before you begin

In order to deactivate an OMS-to-NE connection, the NE communications status must be either **Up** (the NE is communicating with the management system) or **Down** (the NE is not communicating with the management system and the management system is attempting to regain communications).

Task

- 1 Use the object links to follow this path: **Management Network** → **OMS-to-NE Connections**.

Result: The **Search** section of the **OMS-to-NE Connections** page is displayed.

- 2 Make selections in one or more of the following fields in the **Search** section of the window:
 - In the **NE type** field, select a type of NE.
 - In the **NE name(s)** field, the **Available** table contains all NEs of the selected NE type available on the management system. The **Selected** table contains the NEs that are to be considered in the search. Click an NE and use the arrow buttons to move one or more NEs from the **Available** table to the **Selected** table, or click the double arrows to move all the NEs to the **Available** table.
 - In the **Comm Type** field, select a type of communication interface between the NE and the management system.
 - In the **Net Comm Grp** field select the NCG name from the drop-down list. The NCG names displayed depend on the selection in the **Comm Type** field.
-

- 3 Click **Search**.

Result: The list at the bottom of the **OMS-to-NE Connections** page is populated with a list of the OMS-to-NE connections in the network that meet your search criteria.

- 4 The **NE name** column of the table lists the names of the OMS-to-NE connections. Click the radio button next to the OMS-to-NE connection you wish to deactivate. From the **Go** menu, select **Deactivate** and click **Go**.

Result: A confirmation is issued in the **Message** section of the **OMS to NE connections** page, the management system logs out of the NE and sets the communications status to **Deactivated**.

To update the **OMS to NE connections** page, click the refresh button.

END OF STEPS



To activate an OMS-to-NE connection

When to use

Use this task to activate the communications connection between the management system and an NE. When you activate an OMS-to-NE connection, the NE is not communicating with the management system.

Before you begin

In order to activate an OMS-to-NE connection, the NE communication status must be **Deactivated**. The NE is not communicating with the management system because the user manually deactivated the OMS-to-NE connection.

Task

- 1 Use the object links to follow this path: **Management Network** → **OMS-to-NE Connections**.

Result: The **Search** section of the **OMS-to-NE Connections** page is displayed.

- 2 Make selections in one or more of the following fields in the **Search** section of the window:
 - In the **NE type** field, select a type of NE.
 - In the **NE name(s)** field, the **Available** table contains all NEs of the selected NE type available on the management system. The **Selected** table contains the NEs that are to be considered in the search. Click an NE and use the arrow buttons to move one or more NEs from the **Available** table to the **Selected** table, or click the double arrows to move all the NEs to the **Available** table.
 - In the **Comm Type** field, select a type of communication interface between the NE and the management system.
 - In the **Net Comm Grp** field select the NCG name from the drop-down list. The NCG names displayed depend on the selection in the **Comm Type** field.
 - 3 Click **Search**.
-

Result: The list at the bottom of the **OMS-to-NE Connections** page is populated with a list of the OMS-to-NE connections in the network that meet your search criteria.

- 4 The **NE name** column of the table lists the names of the OMS-to-NE connections. Click the radio button next to the OMS-to-NE connection you wish to activate. From the **Go** menu, select **Activate** and click **Go**.

Result: A confirmation is issued in the **Message** section of the **OMS to NE connections** page, the management system connects to the NE and sets the communications status to **Activated**.

To update the **OMS to NE connections** page, click the refresh button.

END OF STEPS



To delete an OMS-to-NE connection

When to use

Use this task to delete the communications connection between the management system and an NE. When you delete an OMS-to-NE connection, its corresponding NE is also deleted from the management system's database.

Before you begin

An NE and its corresponding OMS-to-NE connection cannot be deleted in the following situations:

1. When the NE is a GNE for a Network Communications Group, and it has RNEs assigned to it
2. When the NE has cross-connections being used in network connections. For information about how to delete a network connection, see the *Lucent OMS Connection Management Guide*.
3. When the NE is being used as an FTP/FTAM gateway
4. When a database synchronization is in progress for that NE
5. When a software download is in progress for that NE
6. If the management system cannot delete the NE from the primary network adapter
7. When a backup or restore is in progress for that NE

Task

- 1 Use the object links to follow this path: **Management Network** → **OMS-to-NE Connections**.

Result: The **Search** section of the **OMS-to-NE Connections** page is displayed.

- 2 Make selections in one or more of the following fields in the **Search** section of the window:
 - In the **NE type** field, select a type of NE.
 - In the **NE name(s)** field, the **Available** table contains all NEs of the selected NE type available on the management system. The **Selected** table contains the NEs that are to be considered in the search. Click an NE and use the arrow buttons to move one or more NEs from the **Available** table to the **Selected** table, or click the double arrows to move all the NEs to the **Available** table.

- In the **Comm Type** field, select a type of communication interface between the NE and the management system.
 - In the **Net Comm Grp** field select the NCG name from the drop-down list. The NCG names displayed depend on the selection in the **Comm Type** field.
-

3 Click **Search**.

Result: The list at the bottom of the **OMS-to-NE Connections** page is populated with a list of the OMS-to-NE connections in the network that meet your search criteria.

4 The **NE name** column of the table lists the names of the OMS-to-NE connections. Click the radio button next to the OMS-to-NE connection you wish to delete. From the **Go** menu, select **Delete** and click **Go**.

Result: A confirmation window is displayed.

5 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Network Elements** page, and the OMS-to-NE connection is deleted. The NE is automatically deleted from the **Network Map**. The NE is deleted from the remaining pages of the management system after a refresh is executed.

END OF STEPS



To delete an NE

When to use

Use this task to delete an NE from the management system's database. When you delete an NE, its corresponding OMS-to-NE connection is also deleted.

There are two methods for this task.

Before you begin

An NE and its corresponding OMS-to-NE connection cannot be deleted in the following situations:

1. When the NE is a GNE for a Network Communications Group, and it has RNEs assigned to it
2. When the NE has cross-connections being used in network connections. For information about how to delete a network connection, see the *Lucent OMS Connection Management Guide*.
3. When the NE is being used as an FTP/FTAM gateway
4. When a database synchronization is in progress for that NE
5. When a software download is in progress for that NE
6. If the management system cannot delete the NE from the primary network adapter
7. When a backup or restore is in progress for that NE

Task, method 1: from the Network Elements page

- 1 Use the object links to follow this path: **Network Elements**.

Result: The **Network Elements** page is displayed. It includes a table that lists all NEs.

- 2 The **NE name** column of the table lists the names of the NEs. Click the radio button next to the NE you wish to delete. From the **Go** menu, select **Delete** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

- 3 Click **OK**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Network Elements** page, and the NE is deleted.

If the management system finds that the NE to be deleted has cross-connections in that NE that are being used in network connections, a failure notice is displayed.

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

Task, method 2: from the Network Map

-
- 1 On the **Network Map**, right-click the ODO_AREA and select *Expand all*, then right-click the NE icon that represents the NE you wish to delete.

Result: The **Node** menu is displayed.

-
- 2 Select **Delete**.

Result: A confirmation window is displayed asking you to confirm the deletion.

-
- 3 Click **OK**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Network Map** page, and the NE is deleted.

If the management system finds that the NE to be deleted has cross-connections in that NE that are being used in network connections, a failure notice is displayed.

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



To display the communication state of an NE

Procedure

- 1 Use the object link **Network Elements**.

Result: The **Search for Network Elements** page is displayed.

- 2 The **Search for Network Elements** page allows you to search for a specific network element or a number of network element elements. Note that additional search fields are displayed by selecting the **More** button.

Depending on the expected type of search result, use one or more of the following fields to refine the search request:

- **NE name** – this is a hyperlink to the **Network Elements** pop up window, from which you may select an NE to include in your search. You can also enter the NE name in the text box. The text box includes the use of “*” as wildcard.
- **NE type** – select the type of NE from the drop down list.
- **Central office name** – this is a hyperlink to the **Central Offices** pop up window, from which you may select a central office to include in your search. You can also enter the central office name in the text box. The text box includes the use of “*” as wildcard.
- **Comms status** – select the communications status of the NE from the drop down box.
- **Activity state** – select the activity state of the NE from the drop down box.
- **Last outage time** – enter the time that the management system last experienced a loss of communications with the NE. Manually enter a date followed by a time in either the **To** or **From** text box or use the calendar function next to each text box to choose the date and time information.

Click **Search**.

Result: The lower part of the page is populated with a list of network elements that meet your search criteria.

- 3 Use the column **Comms status** to analyze the communication status of a network element.

The possible values for communications status are described in the following table:

Communications status	Definition
Up	Communications with the NE are working.
Down	Loss of communications. The management system continues to attempt to communicate with the NE.
Failed	Permanent loss of communications. The management system has stopped attempting to communicate with the NE.
Unknown	Communications status cannot be determined.
Deactivated	The NE is not communicating with the system because the OMS to NE connection was manually deactivated.
NA	Not Applicable. For Non-managed NEs and Unmanageable Devices only.

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



Tasks related to DCC

To retrieve DCC related parameters

When to use

Use this task to view DCC related parameters for an NE.

Related information

For a more detailed explanation, please refer to the description of the RTRV-FECOM command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Data Communication Networks**.
4. In the **Function** field, select **Retrieve Far End OSI Communications**.
5. Click **Go**.

Result: The **Retrieve Far End OSI Communications** page is displayed.

3 To limit the information output to a single port, enter the ID of the port in question in the **DCC port** field. To retrieve information for all ports, leave the field empty.

To further restrict the information displayed, select a value in the following fields:

- **DCC type**
 - *Line*: the information relates to the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH), respectively.
 - *Section*: the information relates to the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH), respectively.
 - **Network type** – select either *MCN* (management communication network) or *SCN* (signaling communications network).
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

1. *port* – DCC port
This parameter indicates the port AID of a circuit pack which is used together with *dcctype* to identify the DCC channel.
2. *dcctype*
This parameter indicates whether the LINE/MS or SECTION/RS DCC parameters of the *port* are reported by the command.
3. *dccprotp*
This parameter reports the protection type of the DCC channel. 0X1 means the port is not involved in a protection group or DCC protection switching is disabled. 1+1 means DCC protection switching is enabled: In these case only the active worker line is shown.
4. *dcstat*
This parameter indicates whether management communication network (MCN) communication over the DCC channel is enabled or if it is used in a transparent DCC cross-connection.
5. *lapdmode*
This parameter indicates the type of LAPD service. Modes are AITS and UITS.
6. *lapdrl*
This parameter indicates the LAPD role. This parameter is also used to determine the service for the LinkID protocol.
7. *osinode*
Assignment of a DCC channel to an MCN node in the NE. The parameter is omitted when *dcstat*=ENABLE.

8. *scn_dccstat*

This parameter indicates whether the DCC channel is used for communication over the signaling communications network (SCN) or is involved in a transparent DCC cross-connection.

9. *uni_dccstat*

Indicates whether the DCC channel is used for UNI communication.

Type: Alphanumeric value set

Range: DISABLE (default), ENABLE, TRANSPARENT

Note: Output responses with *uni_dccstat*=DISABLE will only sent when either *dccstat*=ENABLE or *scn_dccstat*=ENABLE.

END OF STEPS



To modify DCC related parameters

When to use

Use this task to modify DCC related parameters for an NE.

Related information

For a more detailed explanation, please refer to the description of the ENT-FECOM command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Data Communication Network**.
4. In the **Function** field, select **Enter Far End OSI Communications**.
5. Click **Go**.

Result: The **Enter Far End OSI Communications** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Port** – the port AID of a circuit pack which is used together with *dcctype* to identify the DCC channel. You may copy the ID of the port from the **Port** page to fill this field.
- **DCC type**
 - *Line*: the modification relates to the DCC using the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH) of the port, respectively
 - *Section*: the modification relates to the DCC using the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH) of the port.

- **DCC stat** – indicates whether communication over the DCC channel is enabled or disabled. Select either *Enable* or *Disable*.
 - **LAPD mode** – indicates the type of LAPD service. Select either *AIMS* (acknowledged information transfer service) or *UITS* (unacknowledged information transfer service).
 - **LAPD role** – indicates the LAPD role. Select either *User side* or *Network side*.
 - **OSI node** – assigns a DCC channel to a management communication network (MCN) node in the NE. Possible values are:
 - *osinode1 (LAN1, 2, or 3)*
 - *osinode2 (LAN2 or LAN3) to osinode8 (LAN2 or LAN3)*
 - *scnnode (LAN2 or LAN3)*
 - **Unidirectional DCC over SCN** – indicates whether the DCC channel is used for communication over the signaling communications network (SCN). Select either *Enable* or *Disable*.
 - **Unidirectional DCC** – indicates whether the DCC channel is used for UNI communication. Select either *Enable* or *Disable*.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To retrieve DCC/EOW status information for a port

When to use

Use this task to retrieve DCC/EOW status information for a single port or a number of ports.

Related information

For a more detailed explanation, please refer to the description of the RTRV-OW command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Network Elements**.
 4. In the **Function** field, select **Retrieve Orderwire and User Bytes**.
 5. Click **Go**.

Result: The **Retrieve Orderwire and User Bytes** page is displayed.

- 3 Use the field **Access identifier** to specify for which user byte the output is to be retrieved. Possible values are *1-1-ubio1* to *1-1-ubio6* for the six user byte interfaces which can be used to access certain overhead bytes of an SDH/SONET transport signal. To retrieve information for all userbytes, use the value *1-1-ubioall*.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

1. aid – access identifier
Indicates the overhead access port for which the following information is displayed.
2. intfctype – interface type
This parameter indicates which electrical interface standard of the overhead access port is used.
 - *G703* – electrical interface according to G.703
 - *V11* – electrical interface according to V.11.
3. ohbyte – overhead byte
Indicates which of the overhead bytes is used:
 - E1 and F1 in the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH), respectively
 - E2 in the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH), respectively
4. portaid
Shows the optical port (of an OPn) with which the overhead access port (given by the output parameter aid) is associated.
The value *NOCONNECT* is used to indicate that the port given by portaid is not associated to the overhead access port given by the parameter aid.

END OF STEPS



To modify DCC/EOW status information for a port

When to use

Use this task to modify DCC/EOW status information for a port.

Related information

For a more detailed explanation, please refer to the description of the SET-0W command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Network Elements**.
4. In the **Function** field, select **Set Orderwire and User Bytes**.
5. Click **Go**.

Result: The **Set Orderwire and User Bytes** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Access identifier** – specify the overhead access port to be used for association (or removing the association).
Type: UserBytePortAID.
Range: *1-1-ubio1* to *1-1-ubio6*
Note: The value *ubioall* is not allowed.
- **Interface Type** – specify the electrical interface according to either *G.703* or *V.11* as selectable.
Note: The overhead access ports *ubio1* to *ubio4* are configurable with both “G.703” or “V.11”, *ubio5* and *ubio6* are fixed to “V.11”.

- **Overhead-Byte** – specifies which of the overhead bytes is used:
 - *E1* and *F1* in the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH), respectively
 - *E2* in the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH), respectively.
 - **Port Identifier** – specifies the optical/electrical port (of an OPn/EPn) of the userbyte to which the overhead access port is associated. You may copy the ID of the port in question from the **Port** page to fill the field.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To view a list of transparent DCC cross-connections

When to use

Use this task to view a list of transparent DCC cross-connections for a selected NE.

Related information

For a more detailed explanation, please refer to the description of the RTRV-CRS-FECOM command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Data Communication Network**.
 4. In the **Function** field, select **Retrieve Transparent DCC Cross Connection**.
 5. Click **Go**.

Result: The **Retrieve Transparent DCC Cross Connection** page is displayed.

- 3 If you want to retrieve information related to a specific port of the NE, enter a port ID in the **DCC port** field. To retrieve information for all ports of the NE, leave the field empty.

If you want to restrict the information to a specific type of DCC cross-connection, select the type (either *Line* or *Section*) in the **DCC type** field. To retrieve information for all types of DCC cross-connections, leave the field empty.

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

- 5 If a *transparent DCC cross-connection* exists the output parameters for this function are:
1. port_aid1 – DCC port 1
This parameter indicates the first optical port AID of an OPn circuit pack which is used together with dcctype to identify the DCC channel which is involved in a transparent DCC cross-connection.
 2. port_aid2 – DCC port 2
This parameter indicates the second optical port AID of an OPn circuit pack which is used together with dcctype to identify the DCC channel which is involved in a transparent DCC cross-connection.
 3. dcctype
 - *LINE/MS*: the information relates to the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH), respectively.
 - *SECTION/RS*: the information relates to the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH), respectively.otherwise only the completion report **COMPLD** returns.

END OF STEPS



To add a transparent DCC cross-connection

When to use

Use this task to add a transparent DCC cross-connection between two port overheads in a selected NE.

Related information

For a more detailed explanation, please refer to the description of the ENT-CRS-FECOM command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Data Communication Networks**.
 4. In the **Function** field, select **Enter Transparent DCC Cross Connection**.
 5. Click **Go**.

Result: The **Enter Transparent DCC Cross Connection** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **DCC port 1** – indicates the first optical port AID of an OPn circuit pack which is used together with dctype to identify the DCC channel which is involved in a transparent DCC cross-connection. You may copy the ID of the port in question from the **Port** page to fill the field.
 - **DCC port 2** – indicates the second optical port AID of an OPn circuit pack which is used together with dctype to identify the DCC channel which is involved in a transparent DCC cross-connection. You may copy the ID of the port in question from the **Port** page to fill the field.

- **DCC type**
 - *Line*: the transparent DCC cross-connection is to be established via the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH) of the port, respectively.
 - *Section*: the transparent DCC cross-connection is to be established via the DCC using the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH) of the port, respectively.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To delete a transparent DCC cross-connection

When to use

Use this task to delete a transparent DCC cross-connection.

Related information

For a more detailed explanation, please refer to the description of the DLT-CRS-FECOM command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 To get information about the transparent DCC cross-connections in place, refer to task [“To view a list of transparent DCC cross-connections”](#) (p. 4-32).

If you already have the necessary data, do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Data Communication Networks**.
4. In the **Function** field, select **Delete Transparent DCC Cross Connection**.
5. Click **Go**.

Result: The **Delete Transparent DCC Cross Connection** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **DCC port 1** – indicates the first optical port AID of an OPn circuit pack which is used together with *dcctype* to identify the DCC channel which is involved in a transparent DCC cross-connection. You may copy the ID of the port in question from the **Port** page to fill the field.
 - **DCC port 2** – indicates the second optical port AID of an OPn circuit pack which is used together with *dcctype* to identify the DCC channel which is involved in a transparent DCC cross-connection. You may copy the ID of the port in question from the **Port** page to fill the field.
 - **DCC type**
 - *Line*: the DCC cross-connection has been established via the DCC using the SDH multiplex section overhead (MSOH) or the SONET line overhead (LOH) of the port, respectively.
 - *Section*: the DCC cross-connection has been established via the SDH regenerator section overhead (RSOH) or the SONET section overhead (SOH) of the port, respectively.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



Tasks related to system provisioning

To view NE date and time

When to use

Use this task to view the NE date and time.

Related information

For a more detailed explanation, please refer to the description of the RTRV-HDR command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Network Elements**.
 4. In the **Function** field, select **Retrieve Header**.
 5. Click **Go**.

Result: The **Retrieve Header** page is displayed.

- 3 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function. The response includes the current date and time.

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



To modify NE date and time

When to use

Use this task to modify the NE date and time. Note that when the date is changed in a way that a performance monitoring period is crossed, than one history bin will be lost.

Related information

For a more detailed explanation, please refer to the description of the ED-DAT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Network Elements**.
 4. In the **Function** field, select **Edit Date and Time**.
 5. Click **Go**.

Result: The **Edit Date and Time** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **Date** – specifies the current date as YY-MM-DD. If the parameter *time* is not specified, the current value is not changed, but then *date* must be specified. Range: YY-MM-DD, with YY between 00 and 99, MM between 01 and 12, DD between 01 and 31.
 - **Time** – specifies the current time of day as HH-MM-SS. If the parameter *date* is not specified, the current value is not changed, but then *time* must be specified. Range: HH-MM-SS, with HH between 00 and 23, MM between 00 and 59, SS between 00 and 59.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function. Note that the response does not show the modified date and time.

5 To verify that date and time meet are correct, follow the instructions in [“To view NE date and time”](#) (p. 4-38).

END OF STEPS



Tasks related to OMS-to-NE CIT Cut-Through

Command Files for the NE CIT Cut-Through

The command files

Once the `java.policy` file has been modified so the management system can access system files, the management system PC client then uses the following files to invoke the cut-through to the NE CIT:

- `cutthru.txt` file
- `cutthru_UNIE_CIT.bat` file
- `LaunchUniteGUI.bat` file

`cutthru.txt` file

The `cutthru.txt` file, which is a text file, allows users to specify the configuration parameters that the Lucent OMS GUI cut-through software uses. Comments in this file describe the purpose and format of each configuration parameter.

If the CIT is to be launched from its default directory, this file is irrelevant and does not have to be used or edited.

If the CIT is to be launched from another directory, the following parameters must be specified in the `cutthru.txt` file:

- `CITDRIVE`
- `CITROOT`

In addition, the `NAIP` or `NAHOST` parameters for each TNA server, particularly for distributed TNA servers, must be specified

The path to this file is as follows:

- `C:\cutthru.txt`

`cutthru_UNIE_CIT.bat` file

The `cutthru_UNIE_CIT.bat` is a batch file that Lucent OMS automatically generates to incorporate execution from the launching directory. Users do not have to alter the content of this file. However, when the CIT software is moved to a new location, users must delete this file so the new file reflecting the new location is automatically regenerated.

The path to this file is as follows:

- `C:\cutthru_UNIE_CIT.bat`

LaunchUniteGUI.bat file

The **LaunchUniteGUI.bat** file is a text file that is used to invoke the CIT to pass parameters that are needed to communicate with the target NE.

If the CIT software does not contain this file, it can be obtained from the Lucent OMS host at the following URL:

- **<https://<OMS host IP address>/CITDATA>**

The **LaunchUniteGUI.bat** file must be put at the root directory of the CIT software. If the CIT software is moved to another location, this file must also be moved.



Install the NE CIT

When to use

Along with the NE CIT documentation, use this task to install the NE craft interface terminal (CIT).

Related information

See the following topic in this document:

- *NE CIT Cut-Through Concepts*

Before you begin

You cannot successfully complete this task unless you have the following:

1. The NE CIT documentation that fully explains how to install the CIT
2. The media on which the CIT software is installed

Task

Complete the following steps to install the NE CIT.

- 1 Insert the CD-ROM.

The default directory for the LambdaUnite® MSS CIT is the following:

- **C:\Program Files\Lucent Technologies\WaveStar CIT**
-

- 2 Select the **setup.exe** file by clicking or double clicking.

Result: The **setup.exe** file prompts you to complete the installation.

- 3 When setup.exe prompts you to complete the installation, make the following selections:

- Choose to Disable Wavestar CIT logins.
- Choose to install the client software at the default directory.
- Choose not to connect the server via OSI.

If the CIT software has installed successfully, you are done with this task. If the CIT software has not installed successfully, go to Step 4.

- 4** If the CIT software does not contain the launch file (**LaunchUniteGUI.bat**), go to the following link to get the launch file:

- **<https://<your OMS host IP address>/CITDATA>**

END OF STEPS



Launch the NE CIT away from the Default Location

When to use

Use this task to launch the NE craft interface terminal (CIT) away from its default location to another location.

Important! We recommend that the NE CIT cut-through is installed in the default directory because it requires the minimal manual configuration. However, if you need to move the software to another location, or even to an external disk, you need to follow the steps in this task.

The software can be installed from the following locations:

- From a location other than the default location; see *Install the NE CIT* for details.
- On the default location, then moved to a new location.

The new root directory always includes a subdirectory named WaveStar CIT for the installation case, but may not for the move case.

Related information

See the following topic in this document:

- *NE CIT Cut-Through Concepts*

Before you begin

Follow the order of task execution that is specified in *Order of task execution for NE CIT cut-through*.

Task

Complete the following steps to launch the NE craft interface terminal (CIT) away from its default location to another location..

-
- 1 In the c: directory, delete the **cutthru_UNITE_CIT.bat** if this file exists. (This file will be regenerated automatically once the NE CIT is moved to its new location.)
-

- 2 Edit the **C:cutthru.txt** file to specify the new location through the two variables below:
CITDRIVE<\t>UNITE<\t><new drive>
CITROOT<\t>UNITE<\t><new root dir>

If the file does not exist, create one. Note that the delimiter between words is one <\t>, which is one tab character.

Example 1: To install the CIT software to the f drive, directory **Install Here**, the CIT can be launched from the following:

f:\Install Here\WaveStar CIT

Set:

CITDRIVE UNITE f CITROOT UNIT \Install Here\WaveStar CIT\
.....

Example 2: To move the CIT software to the f drive, directory **Move Here**, the CIT can be launched from the following:

f:\Move Here

Set:

CITDRIVE UNITE f CITROOT UNIT \Move Here\
.....

- 3** If the CIT software does not contain the launch file **LaunchUniteGUI.bat**, go to the following link to get the launch file:

<https://<your OMS host IP address>/CITDATA>
.....

- 4** Update the **java.policy** file to include the appropriate file permission. Refer to the *Configure the java.policy File for NE CIT Cut-Through* task.

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

Configure the java.policy File for NE CIT Cut-Through

When to use

Use this task to configure the **java.policy** file for a cut-through to the NE CIT.

Related information

See the following topic in this document:

- *NE CIT Cut-Through Concepts*

Before you begin

The entries that you are to add to the **java.policy** file allow the management system GUI to create and run batch files that are to used for a subtending NE CIT.

Task

Complete the following steps to configure the **java.policy** file for an NE CIT cut-through.

-
- 1 At your PC, navigate to this path to access the **java.policy** file.

C:\ProgramFiles\Java\j2re<version>\lib\security\java.policy

Result: The directory is changed.

-
- 2 Using Wordpad, access the **java.policy** file and add the following lines to the bottom of the file:

```
grant { permission java.util.PropertyPermission "user.name", "read";
  permission java.io.FilePermission "c:\\cutthru.txt","read,write,execute";
  permission java.io.FilePermission "c:\\cutthru_UNITE_CIT.bat","read, write,execute";
  permission java.io.FilePermission "c:\\ProgramFiles\\LucentTechnologies\\WaveStarCIT\\LaunchUniteGUI.bat","read,write,execute";
  permission java.net.SocketPermission "<TNA hostname>","resolve";
  permission java.net.SocketPermission "<TNA hostname>:9099","connect";
```

Important! Note that the reserved port is 9099.

If the CIT software is moved away from the default directory, you must update this file to reflect the new disk drive and the path of the launching file (for example: **LaunchUniteGUI.bat**).

If Lucent OMS manages NEs with multiple TNA servers, you must grant socket permission to each TNA server; meaning, you must repeat the two `java.net.SocketPermission` lines for each TNA server.

-
- 3 Use the editor's **save** command to save the lines that you have just added.

Result: The changes made to the **java.policy** file are saved.

-
- 4 Close and reopen the browser so the changes that you have made to the **java.policy** file take effect.

Result: The changes have been made to the **java.policy** file have now taken effect.

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



Work with Command Files to Invoke the NE CIT Cut-Through

When to use

Use this task to work with the management system command files that are used to invoke the cut-through to the NE CIT.

Related information

See the following topic in this document:

- *EMS Concepts*
- *Command Files for the NE CIT Cut-Through*

Before you begin

Follow the order of task execution that is specified in *OMS Administration Guide*.

Task

Complete the following steps to work with the management system command files that are used to involve the cut-through to the NE CIT.

1 Use Wordpad to edit the **C:\cutthru.txt** file. Refer to *cutthru.txt file* for details. Save your changes.

2 If the CIT software has been moved to a new location, if necessary, delete the **C:\cutthru_UNIE_CIT.bat** file. Refer to *cutthru_UNIE_CIT.bat file* for details.

3 If the CIT software does not contain the **LaunchUniteGUI.bat** file, obtain this file from the Lucent OMS host at the following URL:

https://<OMS host IP address>/CITDATA

Put the **LaunchUniteGUI.bat** file in the root directory of the CIT software.

If the CIT software has been moved to a new location, move the **LaunchUniteGUI.bat** file. Refer to *Launch file (LaunchUniteGUI.bat) file* for details.

END OF STEPS



Troubleshoot the NE CIT

When to use

Use this task to troubleshoot the NE CIT.

Related information

See the following topic in this document:

- *NE CIT Cut-Through Concepts*

Before you begin

Follow the order of task execution that is specified in *Order of task execution for NE CIT cut-through*.

Task

Complete the following steps to move the NE craft interface terminal (CIT) from its default location to another location.

- 1 Enable the debugging flag.

In the **C:\cutthru.txt** configuration file, set the debug parameter to the value **true**, which enables low level tracing of the cut-through operations for all subsequent cut-through requests from the Lucent OMS GUI. The debug output for this tracing can be seen on the java console, which can be accessed from the IE tools menu item (**Tools >Sun Java Console**). Debugging is enabled on the very next GUI cut-through request from a pull down menu.

If the java console does not display when it is invoked from the IE toolbar, enable the console in the java plugin. The Plug-In configuration program can be access from the Windows Start Button:

Start->Control Panel-> Java [Plugin]

Configuring the console depends on the java plugin configuration. To enable the plug in, select the show option on the console configuration option. You must restart your browser session once the java plugin configuration is changed.

Note: After this debugging is completed, disable the console in order to maximize the speed of IE. To disable the console, set the console configuration parameter to **Do not start console**.

- 2 Try to launch the NE CIT manually.

To launch a Lucent OMS NE CIT manually, invoke the corresponding launch batch file directly from MS-DOS command prompt. Each batch file requires specification of input parameters.

Launch an MS-DOS command prompt window from the Start button menus items:

Start Button > Programs > Accessories > Command Prompt or Start Button-Programs > Command Pro

To invoke UNITE CIT directly, enter the following:

```
cd c: cd \Program Files\Lucent Technologies\WaveStar CIT
  LaunchUniteGUI.bat LaunchUniteGUI.bat <TNA IP address> 3099 <NE name>
<NE login> < NE password>
```

-
- 3 Verify the parameter values that are specified in the **c:cutthru.txt** file.

If the CIT GUI launches, but it cannot connect to the TNA, verify or reset the NAIP or NAHOST parameter and retry the launch.

If the CIT software is moved away from the default directory, verify or reset the CITHOST and CITROOT parameters.

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



5 Equipment provisioning concepts

Overview

Purpose

This chapter presents concept information related to equipment provisioning on *LambdaUnite*® MSS network elements using Lucent OMS.

Contents

System configurations	5-2
Network element configurations	5-2
Pluggable optical interface modules	5-12
Overview of replaceable units	5-19
NE hardware components and their identifiers	5-25
Port types	5-26
Miscellaneous discrete inputs and outputs	5-30
Equipment protection	5-32
CTL equipment protection (duplex control)	5-32
XC equipment protection	5-37
STM-1E equipment protection	5-40
DS3/EC-1 equipment protection	5-47
LOXC equipment protection	5-55



System configurations

Network element configurations

Supported LXC configurations

These LXC configurations are supported:

- LXC with a max. switching capacity of 160 Gbps
- LXC with a max. switching capacity of 320 Gbps
- LXC with a max. switching capacity of 640 Gbps
- LXC supporting ONNS applications

All these configurations can be realized by using a dual unit row (DUR) shelf.

DUR shelf

A DUR shelf can be equipped from the front as well as from the rear side.

A DUR shelf is designed such that optical interfaces can be accessed from the front while electrical interfaces can be accessed from the rear side.

Available slots on the front side

The following illustration shows the available circuit pack slots on the front side of a DUR shelf.

										User panel 40											
Universal slot 21	Universal slot 22	Universal slot 23	Universal slot 24	Universal slot 25	Universal slot 26	Universal slot 27	Universal slot 28				CTL (P) slot 31	Universal slot 32	Universal slot 33	Universal slot 34	Universal slot 35	Universal slot 36	Universal slot 37	Universal slot 38	Universal slot 39		
Universal slot 1	Universal slot 2	Universal slot 3	Universal slot 4	Universal slot 5	Universal slot 6	Universal slot 7	Universal slot 8	XC (W) slot 9	XC (P) slot 10	CTL (W) slot 11	Universal slot 12	Universal slot 13	Universal slot 14	Universal slot 15	Universal slot 16	Universal slot 17	Universal slot 18	Universal slot 19			

front view

A DUR shelf provides the following circuit pack slots on the front side:

- 2 dedicated slots for CTL (slots 11 and 31, “W” = worker, “P” = protection).
- 2 dedicated slots for XC cross-connection and timing units (slots 9 and 10, “W” = worker, “P” = protection).
- 32 “universal slots” for port units (slots 1-8, 12-19, 21-28, and 32-39).
- 1 dedicated slot for the user panel (slot 40).

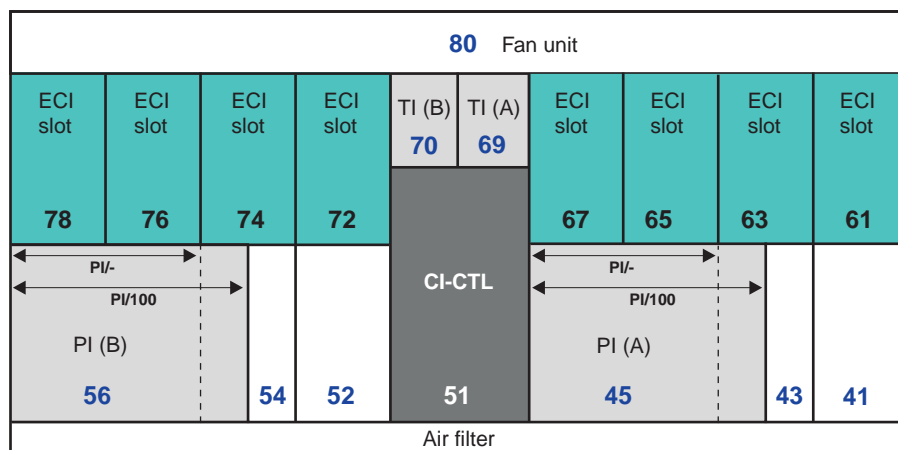
Slots		Slot equipage
1...8 12...19 21...28 32...39	Universal slots ¹	<p>Universal slots can be used for any mix of port units:²</p> <ul style="list-style-type: none"> • Electrical DS3 (45 Mbps, plesiochronous) or EC-1 (51 Mbps, synchronous) port units (EP51...)³ For the EP51 port units, there are dedicated slots for the electrical connection interfaces (ECI) on the rear side of the shelf. • Electrical 155-Mbps (STM-1E) port units (EP155...)³ For the EP155 port units, there are dedicated slots for the electrical connection interfaces (ECI) on the rear side of the shelf. • Optical 155-Mbps port units (OP155...) • 622-Mbps port units (OP622...) • 2.5-Gbps port units (OP2G5...) • 10-Gbps port units (OP10...) • 1-Gigabit Ethernet interface (GE1) • 10-Gigabit Ethernet WANPHY interface (realized on an OP10 port unit) <p><i>Lower order cross-connection units (LOXC):</i></p> <p>The slots 4, 17, 18, 19, 37, and 39 can be used for lower order cross-connection units, depending on the maximum switching capacity of the system and the type of LOXC.</p>
9	XC (W) slot	<p>Cross-connection and timing unit (XC) – worker (W).⁴</p> <p>This XC is paired with the XC in the protection slot in a 1+1 non-revertive protection mode configuration. Furthermore, the XC contains the timing generator function for the NE.</p>
10	XC (P) slot	<p>Cross-connection and timing unit (XC) – protection (P).⁴</p> <p>This XC is paired with the XC in the worker slot in a 1+1 non-revertive protection mode configuration. Furthermore, the XC contains the timing generator function for the NE.</p>
11	CTL (W) slot	<p>Controller (CTL) – worker (W).⁴</p> <p>Controller including the non-volatile memory (NVM, <i>CompactFlash</i>[®] card). After initial system startup (power on), this Controller takes on the active role.</p>
31	CTL (P) slot	<p>Controller (CTL) – protection (P).⁴</p> <p>Optionally, a second Controller can be equipped for CTL equipment protection (duplex control). After initial system startup (power on), this Controller takes on the standby role.</p>
40		User panel
The slots 20, 29, and 30 do <i>not</i> exist.		

Notes:

1. Slots for port units are called “universal slots”. The transmission capacity of a port unit in a universal slot can be up to 20 Gbps per slot.
2. If not stated otherwise, each port unit occupies one universal slot,.
3. The electrical port units (EP...) can only be used in the universal slots in the *upper row* of the shelf (slots 21 ... 28, and 32 ... 39), and in a shelf of type DUR/2.
4. The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role.

Available slots on the rear side

The following illustration shows the available slots on the rear side of a DUR shelf.



rear view

A DUR shelf provides the following slots on the rear side:

- One dedicated slot for the connection interface of the Controller (CI-CTL).
- Two dedicated slots for timing interfaces (TI A and TI B).
- Two dedicated slots for power interfaces (PI A and PI B).
- Eight dedicated slots for electrical connection interfaces (ECI).
- One dedicated slot for the fan unit.

Slots	Slot equipage
41	– (reserved for future applications)
43	– (reserved for future applications)
45	Power interface (PI A) The PI/100 variant of the power interface requires a wider slot than the PI/- variant.

Slots	Slot equipage
51	Connection interface of the Controller (CI-CTL)
52	– (reserved for future applications)
54	– (reserved for future applications)
56	Power interface (PI B) The PI/100 variant of the power interface requires a wider slot than the PI-variant.
61...67	Electrical connection interfaces (ECI). Grouping of the slots <ul style="list-style-type: none"> • when EP51 is used: 61 and 65, or 63; the respective ECI is 4 slots wide; • when EP155 is used: 61, 63, 65, 67 the respective ECI is 2 slots wide.
69	Timing interface (TI A)
70	Timing interface (TI B)
72...78	Electrical connection interfaces (ECI). Grouping of the slots <ul style="list-style-type: none"> • when EP51 is used: 72 and 76, or 74; the respective ECI is 4 slots wide; • when EP155 is used: 72, 74, 76, 78; the respective ECI is 2 slots wide.
80	Fan unit

General configuration rules and guidelines

Observe the following general rules and guidelines with regard to the shelf configuration. Take *all* these rules and guidelines into consideration as the ordering in the list does not necessarily reflect the order of importance.

1. Use the configurator tool to verify if a certain subrack equipage is permitted.
For example: Do not install a GE1 port unit in the lower row of the subrack below an OP10 port unit in the upper row. This rule applies to all supported OP10 versions except the OP10/1.3IOR1.
2. Ensure that both power feeders are operating. If this is not possible due to maintenance operations, and if the system configuration consumes more than 2200 W, ensure that the power battery is in “charging mode” (also known as “floating mode”). Do not perform maintenance operations on the power feeder while the power plant is in “battery mode”, that is, while the voltage at the system power interface (PI) is less than 49 V.
3. Never operate a *LambdaUnite*[®] MSS system without a fan unit for more than *two* (2) minutes to avoid overheating of the system.
Leaving the fan unit out of operation for more than two minutes may cause the respective network element to fail.
4. Do not operate a network element without a CI-CTL, as the initialization/re-initialization of the CTL may fail when no CI-CTL is present.

5. *Do not* insert circuit packs simultaneously. When several circuit packs have to be inserted, they should be inserted one after the other, with intervals of at least one second.
6. Cover unequipped slots and OM sockets with blank front plates or OM socket covers to guarantee proper cooling, airflow, and EMC behavior. Do not leave unequipped slots uncovered for more than *ten* (10) minutes to avoid overheating of the system. Disregarding this warning could cause the system to fail and voids warranty. Blank front plates are available as orderable items (cf. LambdaUnite® *MSS Installation Guide*). Parent boards for optical modules are shipped with the OM sockets covered.
The cooling of the LambdaUnite® MSS system relies on sufficient airflow. Uncovered slots or OM sockets prevent an adequate cooling because LambdaUnite® MSS systems make use of the stack effect.
7. To avoid damaging the blank front plates, ensure that the maximum upward and downward displacement of the latches does not exceed 5 mm.
8. To avoid damage to the NE database stored on the CompactFlash® card, it is of great importance to follow a *special procedure for removing the Controller (CTL)* from its slot. Proceed as follows:
 - a. Open the latches of the CTL to be replaced. *Do not immediately remove the CTL from its slot at that time.*
The green activity LED on the faceplate of the CTL starts flashing.
 - b. Wait until the green activity LED has stopped flashing (about five seconds).
 - c. Remove the CTL from its slot.
9. Please note that, if you insert a circuit pack into a universal slot, which is neither (auto-)provisioned nor preprovisioned, and you *do not close the latches* of the circuit pack, then *no* alarm will be reported to indicate that communication between this circuit pack and other circuit packs of the system will not be possible.

Specific configuration rules and guidelines

Specific configuration rules and guidelines apply depending on the maximum switching capacity of a LambdaUnite® MSS system and on the desired application.

Maximum switching capacity

A LambdaUnite® MSS system can be configured for different values of the maximum cross-connect capacity (**Maximum Switch Capacity**):

LXC160	<p>The maximum switch capacity of the system is 160 Gbps (3072 × 3072 VC-3/STS-1; 1024 × 1024 VC4).</p> <p>This is the default value after a <i>new NE installation</i> with Release 4.0 (or higher) NE software and an empty database.</p>
---------------	---

LXC320	The maximum switch capacity of the system is 320 Gbps (6144 × 6144 VC-3/STS-1; 2048 × 2048 VC4). This is the default value after an <i>upgrade from a previous NE software release</i> to Release 4.0 (or higher) NE software.
LXC640	The maximum switch capacity of the system is 640 Gbps (12288 × 12288 VC-3/STS-1; 4096 × 4096 VC4).

Important! The maximum switch capacity is independent of the type of cross-connection and timing unit used. However, the shelf equipage concerning the cross-connection and timing units depends on the maximum switch capacity.

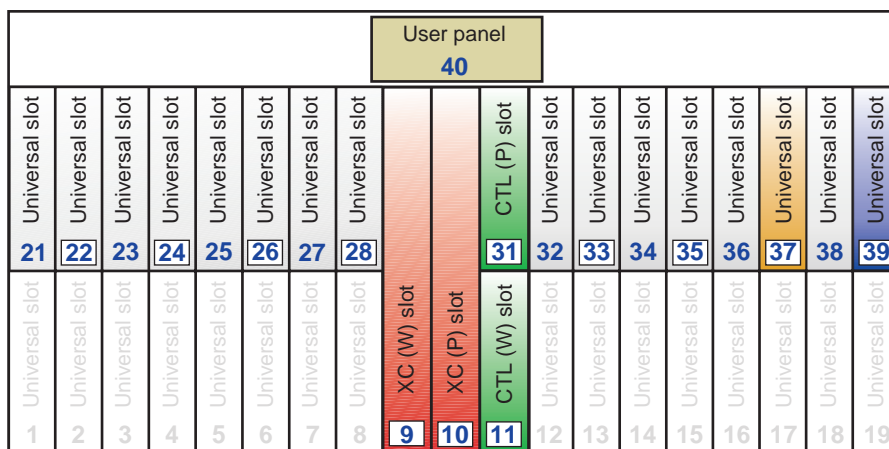
LXC with a max. switching capacity of 160 Gbps

These rules and guidelines apply when the **Maximum Switch Capacity** of the system is set to **LXC160**:

1. The maximum switching capacity of the system is 160 Gbps (3072 × 3072 VC-3/STS-1; 1024 × 1024 VC4).
2. Each type of cross-connection and timing unit (XC160, XC320, XC640) can be provisioned in slot 9 and slot 10. However, the maximum switching capacity that can be used is 160 Gbps, and the slot equipage rules as described above apply independent of which cross-connection and timing unit is used.
3. Port units can only be used in the upper row of the DUR shelf, that is, in the universal slots 21 ... 28 and 32 ... 39.
When a port unit is installed in any of the remaining universal slots, then the green activity LED of that port unit will be flashing, and a Circuit Pack Type Mismatch alarm will be reported. An attempt to preprovision a port unit for any of these slots will be denied.
Cover all unequipped slots with blank front plates.
4. Port units with a transmission capacity of 20 Gbps (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules) can only be used in the universal slots 22, 24, 26, 28, 33, 35, 37, and 39. The slot left to a slot where such a port unit is installed has to remain unequipped, that is, cannot be used for other applications. Please also refer to the diagram subsequent to this list.
5. Lower order cross-connection units of type LOXC/1 can be used in the universal slots 37 (worker slot) and 39 (protection slot). The slot left to an LOXC/1 has to remain unequipped, that is, cannot be used for other applications.
Lower order cross-connection units of type LOXC40G2S/1 *cannot* be used in a system with a maximum switching capacity of 160 Gbps. However, the universal slot pairs 36/37 and 38/39 *can* be used for lower order cross-connection units of type LOXC40G2S/1 (2 slots wide) after the system has been upgraded to a maximum switching capacity of 640 Gbps (XC in-service upgrade XC160 → XC640).

Lower order cross-connection units of type LOXC40G3S/1 cannot be used in a system with a maximum switching capacity of 160 Gbps. However, the universal slots 2/3/4 and 17/18/19 can be used for lower order cross-connection units of type LOXC40G3S/1 (3 slots wide) after the system has been upgraded to a maximum switching capacity of 320 Gbps (XC in-service upgrade XC160 @ XC320).

6. XC160 cross-connection and timing units support ONNS applications.
7. Lucent recommends to use *two* XC160 cross-connection and timing units. Thus, both the cross-connect as well as the timing function are automatically 1+1 equipment protected. However, an LXC configuration with a single, but unprotected XC160 cross-connection and timing unit is also possible.



front view

LXC with a max. switching capacity of 320 Gbps

These rules and guidelines apply when the **Maximum Switch Capacity** of the system is set to **LXC320**:

1. The maximum switching capacity of the system is 320 Gbps (6144 × 6144 VC-3/STS-1; 2048 × 2048 VC4).
2. Only XC320 or XC640 cross-connection and timing units can be provisioned in slot 9 and slot 10. However, the maximum switching capacity that can be used is 320 Gbps, and the slot equipage rules as described above apply independent of whether an XC320 or XC640 is used.

When an XC160 cross-connection and timing unit is installed in slot 9 or slot 10, then the green activity LED of that XC160 will be flashing, and a Circuit Pack Type Mismatch alarm will be reported.

3. Port units can be used in *all* universal slots.
However, port units with a transmission capacity of 20 Gbps (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules) can only be used in the universal slots 2, 4, 6, 8, 13, 15, 17, 19, 22, 24, 26, 28, 33, 35, 37, and 39. The slot left to a slot where a 20-Gbps port unit is installed has to remain unequipped, that is, cannot be used for other applications. Please also refer to the diagram subsequent to this list.
Cover all unequipped slots with blank front plates.
4. Lower order cross-connection units of type LOXC/1 can be used in the universal slots 4, 17, 19, 37, and 39.
The slots 4, 17 and 37 are worker slots. The slots 19 and 39 are protection slots. If the worker LOXC/1 is installed either in slot 4 or in slot 17, then the protection LOXC/1 must be installed in slot 19. If the worker LOXC/1 is installed in slot 37, then the protection LOXC/1 must be installed in slot 39. The slot left to an LOXC/1 has to remain unequipped, that is, cannot be used for other applications.
Lower order cross-connection units of type LOXC40G2S/1 *cannot* be used in a system with a maximum switching capacity of 320 Gbps. However, the universal slot pairs 3/4, 18/19, 36/37 and 38/39 *can* be used for lower order cross-connection units of type LOXC40G2S/1 (2 slots wide) after the system has been upgraded to a maximum switching capacity of 640 Gbps (XC in-service upgrade XC320 → XC640).
Lower order cross-connection units of type LOXC40G3S/1 cannot be used in a system with a maximum switching capacity of 160 Gbps. However, the universal slots 2/3/4 and 17/18/19 can be used for lower order cross-connection units of type LOXC40G3S/1 (3 slots wide) after the system has been upgraded to a maximum switching capacity of 320 Gbps (XC in-service upgrade XC160 ® XC320).
Please note that *at most one LOXC equipment protection group may exist, that is, at most one worker slot can be used in combination with one protection slot.*
5. Only the XC320/B variant of the XC320 cross-connection and timing units supports ONNS applications.
6. Lucent recommends to use *two* XC320 cross-connection and timing units. Thus, both the cross-connect as well as the timing function are automatically 1+1 equipment protected. However, an LXC configuration with a single, but unprotected XC320 cross-connection and timing unit is also possible.

Pluggable optical interface modules

Port units with optical interface modules

LambdaUnite[®] MSS supports optical port units consisting of a parent board which can be equipped with field-replaceable optical interface modules.

An optical module is a replaceable unit with a receiver and transmitter function providing the optical port. *LambdaUnite*[®] MSS optical interface modules are “hot pluggable” (field-replaceable), i.e. the interface modules can be inserted or removed while the parent board is in operation, without affecting the service of other interface modules on the same parent board.

The following parent boards with field-replacable optical interface modules are supported:

Parent board	Available optical interface modules	Remark
OPLB/PAR8	OM155/1.3IR1	The OPLB/PAR8 parent board can be equipped with up to 8 optical interface modules (ports), each having a transmission capacity of either 155 Mbps or 622 Mbps. Mixing of ports with different reaches is supported on a single parent board. However, mixing of ports with different bit rates is <i>not</i> supported.
	OM155/1.3LR1	
	OM155/1.5LR1	
	OM622/1.3IR1	
	OM622/1.3LR1	
	OM622/1.5LR1	
OP2G5D/PAR8	OM2G5/1.3SR1	The OP2G5D/PAR8 parent board can be equipped with up to 8 optical interface modules (ports), each having a transmission capacity of 2.5 Gbps. Thus, the transmission capacity of a fully equipped OP2G5D/PAR8 port unit is <i>20 Gbps</i> . Therefore, specific configuration rules need to be observed, please refer to “ Specific configuration rules and guidelines ” (p. 5-6). Mixing of ports with different reaches and/or different wavelengths is supported on a single parent board.
	OM2G5/1.3LR1	
	OM2G5/1.5LR1	
	OM2G5/CL47S1, OM2G5/CL49S1, ... OM2G5/CL61S1	
	OM2G5/CL47L1, OM2G5/CL49L1, ... OM2G5/CL61L1	

Parent board	Available optical interface modules	Remark
OP2G5/PAR4	OM2G5/1.3SR1	<p>The OP2G5/PAR4 parent board can be equipped with up to 4 optical interface modules (ports), each having a transmission capacity of 2.5 Gbps.</p> <p>Mixing of ports with different reaches and/or different wavelengths is supported on a single parent board.</p>
	OM2G5/1.3LR1	
	OM2G5/1.5LR1	
	OM2G5/CL47S1, OM2G5/CL49S1, ... OM2G5/CL61S1	
	OM2G5/CL47L1, OM2G5/CL49L1, ... OM2G5/CL61L1	
OPT2G5/PAR3	OM2G5/1.3SR1	<p>The OPT2G5/PAR3 transparency parent board can be equipped with up to 3 optical interface modules (ports), each having a transmission capacity of 2.5 Gbps.</p> <p>Mixing of ports with different reaches and/or different wavelengths is supported on a single parent board.</p>
	OM2G5/1.3LR1	
	OM2G5/1.5LR1	
	OM2G5/CL47S1, OM2G5/CL49S1, ... OM2G5/CL61S1	
	OM2G5/CL47L1, OM2G5/CL49L1, ... OM2G5/CL61L1	
OP10/PAR1XFP	OMX10/10KM1	<p>The OP10/PAR1XFP parent board can be equipped with an optical XFP interface module with a transmission capacity of 10 Gbps. Thus, the transmission capacity of a fully equipped OP10D/PAR2 port unit is 20 Gbps. Therefore, specific configuration rules need to be observed, please refer to “Specific configuration rules and guidelines” (p. 5-6).</p>
	OMX10/40KM1	
	OMX10/ 80KM1	
OP10D/PAR2	OM10/1.3IOR1	<p>The OP10D/PAR2 parent board can be equipped with up to 2 optical interface modules (ports), each having a transmission capacity of 10 Gbps. Thus, the transmission capacity of a fully equipped OP10D/PAR2 port unit is 20 Gbps. Therefore, specific configuration rules need to be observed, please refer to “Specific configuration rules and guidelines” (p. 5-6).</p> <p>Mixing of ports with different reaches and/or different wavelengths is supported on a single parent board.</p>
	OM10/1.5IR1	
	OM10/1.5LR1	
OP10D/PAR2XFP	OMX10/10KM1	<p>The OP10D/PAR2XFP parent board can be equipped with up to 2 XFP optical interface modules (ports), each having a transmission capacity of 10 Gbps. Thus, the transmission capacity of a fully equipped OP10D/PAR2XFP port unit is 20 Gbps. Therefore, specific configuration rules need to be observed, please refer to “Specific configuration rules and guidelines” (p. 5-6).</p> <p>Mixing of ports with different reaches and/or different wavelengths is supported on a single parent board.</p>
	OMX10/40KM1	
	OMX10/ 80KM1	

Parent board	Available optical interface modules	Remark
GE10PL1/1A8	OMGE1/SX1	The GE10PL1/1A8 is a high density private line unit for Gigabit Ethernet applications. The parent board can optionally be equipped with either one 10-Gbps or eight 1-Gbps optical interface modules (ports).
	OMGE1/LX1	
	OMGE1/ZX1	
	OMX10/10KM1	
	OMX10/40KM1	
	OMX10/ 80KM1	

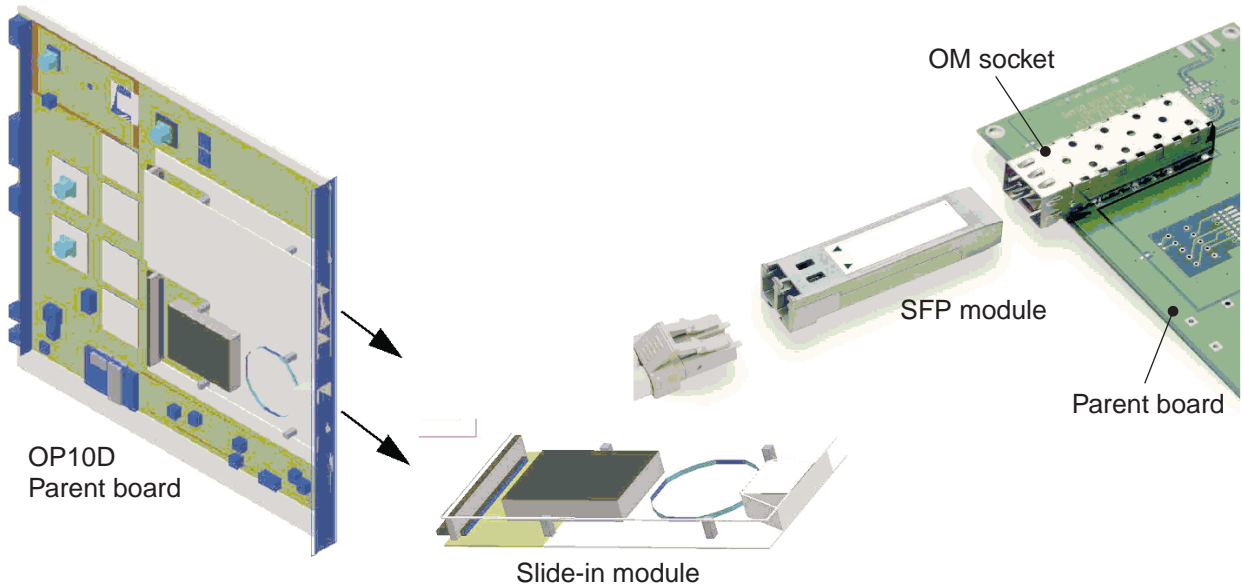
The major advantage of these optical port units is that the optical interface modules (ports) can be added, exchanged, or removed in the field without requiring special tools, and without impacting the operation of the remaining ports. Thus, the transmission capacity of a *LambdaUnite*[®] MSS system can easily be adapted. It is possible to leave the receptacles of optical modules (OM sockets) unequipped as long as the transmission capacity of these ports is not needed.

Important! Cover unequipped slots and OM sockets with blank front plates or OM socket covers to guarantee proper cooling, airflow and EMC behavior. Do not leave unequipped slots uncovered for more than *ten* (10) minutes to avoid overheating of the system. Disregarding this warning could cause the system to fail and voids warranty. Blank front plates are available as orderable items (cf. *LambdaUnite*[®] *MSS Installation Guide*). Parent boards for optical modules are shipped with the OM sockets covered.

Types of optical interface modules

For *LambdaUnite*[®] MSS systems, the following types of optical interface modules can be used:

- For the 10-Gbps optical interface modules, these types of optical interface modules are available:
 - Slide-in modules with a Alcatel-Lucent proprietary design
 - 10 Gigabit Small Form-factor Pluggable (XFP) modules
- For the 155-Mbps, 622-Mbps and 2.5-Gbps optical interface modules, standardized Small Form-factor Pluggable (SFP) modules are used which comply to the SFP MSA standard of the SFF Committee.



Available modules

The available optical interface modules are basically characterized by their bit rate, wavelength and reach.

155 Mbps

The following optical interface modules with a bit rate of 155 Mbps are available:

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OM155/1.3IR1 (SFP)	OM155A184	STM-1/OC-3	1310 nm	15 km
OM155/1.3LR1 (SFP)	OM155A183	STM-1/OC-3	1310 nm	40 km
OM155/1.5LR1 (SFP)	OM155A185	STM-1/OC-3	1550 nm	80 km

622 Mbps

The following optical interface modules with a bit rate of 622 Mbps are available:

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OM622/1.3IR1 (SFP)	OM622A182	STM-4/OC-12	1310 nm	15 km
OM622/1.3LR1 (SFP)	OM622A181	STM-4/OC-12	1310 nm	40 km
OM622/1.5LR1 (SFP)	OM622A180	STM-4/OC-12	1550 nm	80 km

1 Gbps (Gigabit Ethernet)

The following optical interface modules are available for Gigabit Ethernet applications:

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OMGE1/SX1 (SFP, 1000BASE-SX)	OMSX1	1 Gbps (1 GbE)	850 nm	550 m
OMGE1/LX1 (SFP, 1000BASE-LX)	OMLX1	1 Gbps (1 GbE)	1310 nm	10 km
OMGE1/ZX1 (SFP, 1000BASE-ZX)	OMZX1	1 Gbps (1 GbE)	1550 nm	70 km

2.5 Gbps

The following optical interface modules with a bit rate of 2.5 Gbps are available:

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OM2G5/1.3SR1 (SFP)	OM2G5A12	STM-16/OC-48	1310 nm	2 km
OM2G5/1.3LR1 (SFP)	OM2G5A203	STM-16/OC-48	1310 nm	40 km
OM2G5/1.5LR1 (SFP)	OM2G5A204	STM-16/OC-48	1550 nm	80 km
OM2G5/CL47S1 (CWDM SFP)	2CL47S1	STM-16/OC-48	1471 nm	40 km
OM2G5/CL49S1 (CWDM SFP)	2CL49S1	STM-16/OC-48	1491 nm	40 km
OM2G5/CL51S1 (CWDM SFP)	2CL51S1	STM-16/OC-48	1511 nm	40 km
OM2G5/CL53S1 (CWDM SFP)	2CL53S1	STM-16/OC-48	1531 nm	40 km
OM2G5/CL55S1 (CWDM SFP)	2CL55S1	STM-16/OC-48	1551 nm	40 km
OM2G5/CL57S1 (CWDM SFP)	2CL57S1	STM-16/OC-48	1571 nm	40 km
OM2G5/CL59S1 (CWDM SFP)	2CL59S1	STM-16/OC-48	1591 nm	40 km
OM2G5/CL61S1 (CWDM SFP)	2CL61S1	STM-16/OC-48	1611 nm	40 km
OM2G5/CL47L1 (CWDM SFP)	2CL47L1	STM-16/OC-48	1471 nm	80 km
OM2G5/CL49L1 (CWDM SFP)	2CL49L1	STM-16/OC-48	1491 nm	80 km
OM2G5/CL51L1 (CWDM SFP)	2CL51L1	STM-16/OC-48	1511 nm	80 km

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OM2G5/CL53L1 (CWDM SFP)	2CL53L1	STM-16/OC-48	1531 nm	80 km
OM2G5/CL55L1 (CWDM SFP)	2CL55L1	STM-16/OC-48	1551 nm	80 km
OM2G5/CL57L1 (CWDM SFP)	2CL57L1	STM-16/OC-48	1571 nm	80 km
OM2G5/CL59L1 (CWDM SFP)	2CL59L1	STM-16/OC-48	1591 nm	80 km
OM2G5/CL61L1 (CWDM SFP)	2CL61L1	STM-16/OC-48	1611 nm	80 km

10 Gbps

The following optical interface modules with a bit rate of 10 Gbps are available:

Opt. interface module	Apparatus code	Bit rate	Wavelength	Reach
OM10/1.3IOR1 (Slide-in module)	OM10G7	STM-64/OC-192	1310 nm	600 m
OM10/1.5IR1 (Slide-in module)	OM10G14	STM-64/OC-192	1550 nm	40 km
OM10/1.5LR1 (Slide-in module)	OM10G6	STM-64/OC-192	1550 nm	80 km
OMX10/10KM1 (XFP, 10GBASE-LR / I-64.1)	OMX10G10	10 Gbps (10 GbE, STM-64/OC-192)	1310 nm	10 km
OMX10/40KM1 (XFP, 10GBASE-ER / S-64.2b)	OMX10G40	10 Gbps (10 GbE, STM-64/OC-192)	1550 nm	40 km
OMX10/80KM1 (XFP, 10GBASE / L-64.2)	OMX10G80	10 Gbps (10 GbE, STM-64/OC-192)	1550 nm	80 km

Notes:

- The OMX10 optical interface modules can optionally be used with a GE10PL1/1A8, OP10/PAR1XFP, or OP10D/PAR2XFP parent board.

Provisioning of optical interface modules

Optical interface modules can be auto-provisioned, pre-provisioned, provisioned, and de-provisioned, just like any other optical interface.

Preprovisioning

The desired type of optical interface module, being suitable for the corresponding port unit (parent board), can be preprovisioned for an OM socket. Afterward, exactly the preprovisioned type of optical interface module needs to be inserted into that OM socket. Otherwise an `Optical Module Type Mismatch` alarm will be reported.

Please also consider the specific rules that apply to the OPLB (see below).

Autoprovisioning

Any type of optical interface module which is suitable for the corresponding port unit (parent board) can be inserted into an empty OM socket, and thus be autoprovioned.

Please also consider the specific rules that apply to the OPLB (see below).

Provisioning

Provisioning an optical interface module is equivalent to provisioning an optical port.

Deprovisioning

Optical interface modules can either be deprovisioned explicitly by deprovisioning each module individually, or implicitly by deprovisioning the parent board.

Exchangeability

It is possible to exchange the provisioned type of an optical interface module. For example, you can exchange an optical module by another module of the *same bit rate* but *different wavelength and/or reach*.

Special case: OPLB

A special case is the OPLB parent board as it supports two different bit rates.

The following applies to the OPLB parent board:

- When for an OPLB parent board an optical module with a bit rate of either 155 or 622 Mbps is preprovisioned or present in one of the OM sockets, then only optical modules of the same bit rate can be inserted or preprovisioned for the remaining OM sockets.
- When an OPLB parent board with two or more pre-installed optical modules is inserted into a slot, and nothing has been preprovisioned, then the bit rate supported by the OPLB parent board is determined by the bit rate of the optical module in the OM socket with the lowest number. Further optical modules with the same bit rate will be autoprovioned. Already present or subsequently inserted optical modules with a different bit rate will be alarmed (`Optical Module Type Mismatch`).



Overview of replaceable units

Shelves

These types of shelves are supported:

Type	Functional name	Functional qualifier	Apparatus Code	Remarks
DUR/-	DUR	–	(none)	Dual unit row shelf for LXC configurations (without support of electrical port units)
DUR/2	DUR	2	(none)	Dual unit row shelf for LXC configurations (with support of electrical port units)
DUR/3	DUR	3	(none)	Dual unit row shelf supporting scalable packet switching and lower order cross-connection units with a higher switching capacity (LOXC40)

External system interfaces and peripheral units

These external system interfaces and peripheral units are supported:

Interface	Functional name	Functional qualifier	Apparatus Code	Remarks
TI/E1/DS1	TI	E1/DS1	(none)	Timing interface
PI/-	PI	–	(none)	Power interfaces
PI/100		100	(none)	
UPL/-	UPL	–	(none)	User panel
FU/-	FU	–	(none)	Fan unit for DUR/- and DUR/2 shelves
FU/2	FU	2	(none)	Fan unit for DUR/3 shelves
ECI/155MP8	ECI	155MP8	(none)	Electrical connection interfaces for EP155 port units
ECI/155ME8		155ME8	(none)	
ECI51/MP72	ECI51	MP72	(none)	Electrical connection interface for EP51 port units

Notes:

1. These system components are *not* listed in the acceptable circuit pack type list. As they are replaceable units the above table is included in this document for the sake of completeness.

Controllers (CTL)

These types of controllers are supported:

Circuit pack			Occupied slots	Apparatus Code	Remarks
Type	Functional name	Functional qualifier			
CTL/-	CTL	–	1	KFA1	<ul style="list-style-type: none"> 256 MByte NVM storage capacity
CTL/2	CTL	2	1	KFA531	<ul style="list-style-type: none"> 512 MByte NVM storage capacity ONNS support
CTL/3T	CTL	3T	1	KFA536	<ul style="list-style-type: none"> 1 GByte NVM storage capacity LOXC support Support of 180 DCCs
CTL/3S	CTL	3S	1	KFA537	<ul style="list-style-type: none"> 1 GByte NVM storage capacity ONNS support LOXC support Support of 180 DCCs
CTL/4T	CTL	4T	1	KFA538	Redesigned hardware, fully compatible with the CTL/-: <ul style="list-style-type: none"> 256 MByte NVM storage capacity
CTL/4S	CTL	4S	1	KFA539	Redesigned hardware, fully compatible with the CTL/2: <ul style="list-style-type: none"> 512 MByte NVM storage capacity ONNS support

Non-volatile memory

The system's non-volatile memory (NVM) is realized by means of a *CompactFlash*[®] card with IDE interface. The required size of the *CompactFlash*[®] card depends on the Controller used:

- The CTL/- Controller variant requires a *CompactFlash*[®] card with a 256-MByte NVM storage capacity.
- The CTL/2 Controller variant requires a *CompactFlash*[®] card with a 512-MByte NVM storage capacity.
- The CTL/3T Controller variant requires a *CompactFlash*[®] card with a 1-GByte NVM storage capacity.
- The CTL/3S Controller variant requires a *CompactFlash*[®] card with a 1-GByte NVM storage capacity.

- The CTL/4T Controller variant requires a *CompactFlash*[®] card with a 256-MByte NVM storage capacity.
- The CTL/4S Controller variant requires a *CompactFlash*[®] card with a 512-MByte NVM storage capacity.

Cross-connect units (XC)

These cross-connect units are supported:

Circuit pack			Occupied slots	Apparatus Code	Remarks
Type	Functional name	Functional qualifier			
XC160/-	XC160	–	1	KFD3	Cross-connection and timing unit: <ul style="list-style-type: none"> • 160-Gbps switching capacity • Suitable for ONNS applications
XC320/-	XC320	–	1	KFD1	Cross-connection and timing unit: <ul style="list-style-type: none"> • 320-Gbps switching capacity • <i>Not</i> suitable for ONNS applications
XC320/A	XC320	A	1	KFD1A	Cross-connection and timing unit: <ul style="list-style-type: none"> • 320-Gbps switching capacity • <i>Not</i> suitable for ONNS applications
XC320/B	XC320	B	1	KFD1B	Cross-connection and timing unit: <ul style="list-style-type: none"> • 320-Gbps switching capacity • Suitable for ONNS applications
XC640/-	XC640	–	1	KFD2	Cross-connection and timing unit: <ul style="list-style-type: none"> • 640-Gbps switching capacity • Suitable for ONNS applications
LOXC/1	LOXC	1	1	KFA700	Lower order cross-connection unit: <ul style="list-style-type: none"> • 15-Gbps switching capacity
LOXC40G2S/1	LOXC40G2S	1	2	KFA702	Lower order cross-connection unit: <ul style="list-style-type: none"> • 40-Gbps switching capacity Only in combination with XC640.
LOXC40G3S/1	LOXC40G3S	1	3	KFA 703	Lower order cross-connection unit: <ul style="list-style-type: none"> • 40-Gbps switching capacity Only in combination with XC320.

10-Gbps optical port units (SDH/SONET)

These 10-Gbps optical SDH/SONET port units are supported:

Circuit pack			Occupied slots	Apparatus Code	Number of ports	Remarks
Type	Functional name	Functional qualifier				
OP10/1.5LR1	OP10	1.5LR1	1	KFA6	1	–
OP10/1.3IOR1	OP10	1.3IOR1	1	KFA7	1	–
OP10/1.5IR1	OP10	1.5IR1	1	KFA14	1	–
OP10/01/800G ... OP10/80/800G	OP10	01/800G ... 40/800G	1	KFA9, KFA81 ... KFA159	1	80 port unit variants for interworking with <i>WaveStar</i> [®] (800G)
OP10/01/PWDM ... OP10/16/PWDM	OP10	01/PWDM ... 16/PWDM	1	KFA11, KFA61 ... KFA75	1	16 port unit variants for passive WDM applications (36-km reach)
OP10/17/PWDM ... OP10/32/PWDM	OP10	17/PWDM ... 32/PWDM	1	KFA515 ... KFA530	1	16 port unit variants for passive WDM applications (22-km reach)
OP10/9285XT ... OP10/8650XT	OP10	9285XT ... 8650XT	1	KFA210 ... KFA482	1	128 port unit variants for interworking with <i>LambdaExtreme</i> [™] Transport
OP10/XTTC	OP10	XTTC	1	KFA361	1	Port unit with tunable laser (C-Band) for interworking with <i>LambdaExtreme</i> [™] Transport (laser tunable from 1554.54 nm to 1568.36 nm, that is, 192.85 THz to 191.15 THz, 50-GHz spacing, 35 colors)
OP10/XTTL	OP10	XTTL	1	KFA362	1	Port unit with tunable laser (L-Band) for interworking with <i>LambdaExtreme</i> [™] Transport (laser tunable from 1568.77 nm to 1607.47 nm, that is, 191.10 THz to 186.50 THz, 50-GHz spacing, 93 colors)
OP10D/PAR2	OP10D	PAR2	1	KFA630	1 - 2	Parent board for up to 2 SFP optical interface modules
OP10D/PAR2XFP	OP10D	PAR2XFP	1	KFA632	1 - 2	Parent board for up to 2 XFP optical interface modules
OP10/PAR1XFP	OP10	PAR1XFP	1	KFA631	1	Parent board for 1 XFP optical interface module

For more detailed information (technical specifications for example), also refer to the *LambdaUnite*[®] *MSS Applications and Planning Guide*.

2.5-Gbps optical port units (SDH/SONET)

These 2.5-Gbps optical SDH/SONET port units are supported:

Circuit pack			Occupied slots	Apparatus Code	Number of ports	Remarks
Type	Functional name	Functional qualifier				
OP2G5/1.3SR4	OP2G5	1.3SR4	1	KFA12	4	–
OP2G5/1.3LR4	OP2G5	1.3LR4	1	KFA203	4	–
OP2G5/1.5LR4	OP2G5	1.5LR4	1	KFA204	4	–
OP2G5/PARENT	OP2G5	PARENT	1	KFA20	1 - 2	Parent board for up to 2 passive WDM interface modules
OM2G5/921PWDM ... OM2G5/959PWDM	OM2G5	921PWDM ... 959PWDM	–	OM2G5A921 ... OM2G5A959	1	Optical interface modules for passive WDM applications
OP2G5D/PAR8	OP2G5D	PAR8	1	KFA620	1 - 8	Parent board for up to eight pluggable optical interface modules
OP2G5/PAR4	OP2G5	PAR4	1	KFA621	1 - 4	Parent board for up to four pluggable optical interface modules
OPT2G5/PAR3	OPT2G5	PAR3	1	KFA540	1 - 3	Transparency parent board for up to three pluggable optical interface modules

For more detailed information (technical specifications for example), also refer to the LambdaUnite® *MSS Applications and Planning Guide*.

622-Mbps and 155-Mbps optical port units (SDH/SONET)

These 622-Mbps and 155-Mbps optical SDH/SONET port units are supported:

Circuit pack			Occupied slots	Apparatus Code	Number of ports	Remarks
Type	Functional name	Functional qualifier				
OP622/1.3IR16	OP622	1.3IR16	1	KFA17	16	OC-12/STM-4 port unit (622-Mbps)
OP155M/1.3IR16	OP155M	1.3IR16	1	KFA18	16	OC-3/STM-1 port unit (155-Mbps)
OPLB/PAR8	OPLB	PAR8	1	KFA180	1 - 8	Parent board for up to eight pluggable optical interface module

For more detailed information (technical specifications for example), also refer to the LambdaUnite® *MSS Applications and Planning Guide*.

Electrical port units

The following electrical port units are supported:

Circuit pack			Occupied slots	Apparatus Code	Number of ports ¹	Remarks
Type	Functional name	Functional qualifier				
EP155/EL8	EP155	EL8	1	KFA533	8	Electrical port unit (STM-1)
EP51/EL36	EP51	EL36	1	KFA535	36	Electrical port unit (DS3 or EC-1)
EP51/EL36B	EP51	EL36B	1	KFA535B	36	Electrical port unit (DS3 or EC-1)

Notes:

1. The STM-1e, DS3, or EC-1 ports respectively are located on electrical connection interfaces (ECI) which have to be installed in corresponding rear-side slots.

Gigabit Ethernet port units

These Gigabit Ethernet port units are supported:

Circuit pack			Occupied slots	Apparatus Code	Number of ports	Remarks
Type	Functional name	Functional qualifier				
GE1/SX4	GE1	SX4	1	KFA13	4	1000BASE-SX interface (short reach)
GE1/LX4	GE1	LX4	1	KFA532	4	1000BASE-LX interface (long reach)
GE10PL1/1A8	GE10PL1	1A8	1	KFA720	1 × 10GbE (XFP), <i>or</i> 8 × 1GbE (SFP)	Private Line Gigabit Ethernet unit with either 1 × 10GBASE-X or 8 × 1000BASE-X interfaces

Refer to the LambdaUnite® *MSS Applications and Planning Guide* for more detailed technical specifications.



NE hardware components and their identifiers

Reference

For a complete and up-to-date list of all hardware items with the respective comcodes, refer to the *Engineering Drawings* ED8C948-10 and ED8C948-20. You can order them in the latest version from the [Lucent's Product Documentation web site](http://www.cic.lucent.com/drawings.html) (<http://www.cic.lucent.com/drawings.html>).



Port types

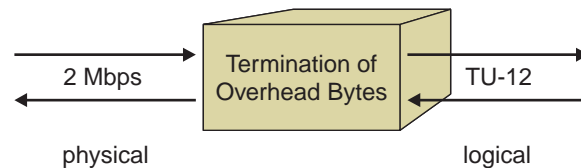
Definition of port

A port is a connectable point that can terminate a physical or logical network connection.

There are two types of ports:

- A *physical port* is a physical connection point. Transmission lines attach to physical ports.
- A *logical port* is a logical connection point within a physical connection point. At the logical port the overhead bytes are terminated: in the transmit direction overhead bytes are added, in the receive direction overhead bytes are extracted. Therefore logical ports are also called *termination points*. Logical ports are contained within physical ports. Logical ports can contain other logical ports.

An example for the principle definition of physical and logical ports is shown in the following figure:



Add and delete ports

Ports are automatically created in the management system when an NE is added to the management system or when a circuit pack is installed. Upon addition to the management system the port parameters are available for provisioning.

For logical ports, only the ones that exist on the NE and also have associated port parameters are supported in the management system. For the majority NEs, logical ports are supported only when they are involved in cross-connections.

Ports are automatically deleted from the management system when an NE is deleted from the management system or when a circuit pack is removed.

Supported ports

All ports that carry port parameters are supported by the management system. These ports include physical ports or logical ports. For logical ports, typically the ports only carry parameters after being involved in a cross-connection. However, there are cases in which logical ports have parameters even when they are not used in a cross-connection.

Supported port rates

The available port rates are shown in the following table:

Port rate	Description	Category
STM-64	Optical interface, 10 Gbps	SDH physical
OC-192	Optical interface, 10 Gbps	SONET physical
STM-16	Optical interface, 2.5 Gbps	SDH physical
OC-48	Optical interface, 2.5 Gbps	SONET physical
STM-4	Optical interface, 622 Mbps	SDH physical
OC-12	Optical interface, 622 Mbps	SONET physical
STM-1	Optical interface, 255 Mbps	SDH physical
OC-3	Optical interface, 255 Mbps	SONET physical
STM-1	Electrical interface, 255 Mbps	SDH physical
EC-1	Electrical interface, synchronous, 51.840 Mbps	SONET physical
T3	Electrical DS3 interface, plesiochronous 44.736 Mbps	SONET physical
E3	Electrical interface, 34 Mbps	SDH physical
E1	Electrical interface, 2 Mbps	SDH physical
DS1	Electrical interface, 1.5 Mbps	SDH physical
10 Gb Ethernet	Gigabit Ethernet interface	Ethernet physical
1 Gb Ethernet	Gigabit Ethernet interface	Ethernet physical
VCG	Virtual concatenation group	VCG physical
OS	Optical channel	
VC-4-64C	Virtual container concatenated	VC-4-64C logical
VC-4-16C	Virtual container concatenated	VC-4-16C logical
VC-4-4C	Virtual container concatenated	VC-4-4C logical
VC-4	Virtual container	VC-4 logical
HO-VC-3	Virtual container	HO-VC-3 logical
ODU10G	Virtual container	ODU10G

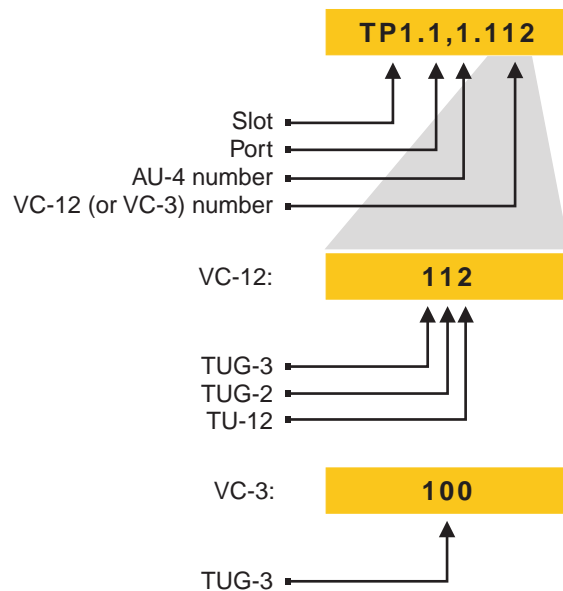
Port names

The name of the physical ports consists of two parts separated by a dot. The first part is related to the slot name, the second part is the port number within that slot.

Example: LP2.1, TP1.3

The name of the logical ports consists of the physical port name followed by the AU-4 number and for low order signals, the VC number (VC-12 or VC-3). The VC number consists of:

- The number of the TUG-3 inside the VC-4
- The number of the TUG-2 inside the TUG-3
- The TU-12 number inside the TUG-2



Port ID formats



The management system supports two port ID formats and the ability to control which format is used:

- *Native Name*: This format is the default setting.
- *ITU-T G.707 Format*: This format applies to certain logical ports.

The management system allows the user to select which format is used for port names throughout the management system. This is controlled on the **Preferences** page.

The management system also allows the user to select which format is used for port names on specific pages. This is controlled by a toggle button on the **Add Connection**, **Graphical Layout**, and **Ports** pages.

The two states of the **Port ID Format** button are shown in the following table:

Button state	Port ID format
	Native name
	ITU-T G.707

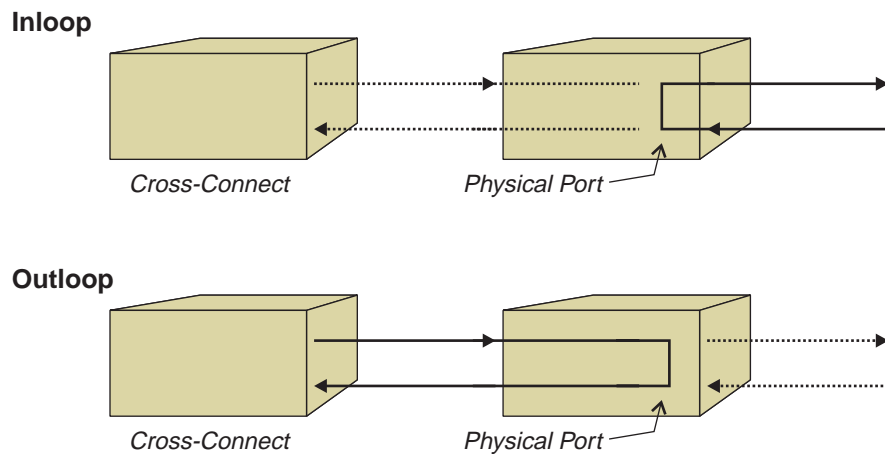
Test loops

An incoming test loop (inloop) can be set on the 1.5 Mbps, 2 Mbps, 34 Mbps, and 45 Mbps ports. The input signal is directly routed back to its corresponding output without altering the signal format. This loop can be used to test the connectors. Only one inloop can be set at the same time.

An outgoing test loop (outloop) can be set on the 1.5 Mbps, 2 Mbps, 34 Mbps, and 45 Mbps ports. The output signal is directly routed back to its corresponding input without altering the signal format. This loop can be used to test how the signal passes through the system.

If a test loop is enabled, the *abnormal* state is activated. After disabling the test loop the cross-connections that existed before setting the test loop are restored.

Test loops for physical ports of tributary port units are shown in the following figure:



□

Miscellaneous discrete inputs and outputs

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 ITM-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 is to 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-condition 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.

Transient behavior 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.

Reference

Refer to “[Provisioning of MDIs and MDOs](#)” (p. 6-42) for detailed tasks related to MDI and MDO provisioning.

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.

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}). They 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} . They are ESD safe up to 2 kV.

□

Equipment protection

CTL equipment protection (duplex control)

Introduction

Optionally, a 1+1 equipment protection of the system and DCC control functions (SCF, DCF) can be realized by adding a redundant Controller to a *LambdaUnite*[®] MSS system. Thus the reliability of the control functions can be increased.

Simplex control vs. Duplex control

In a simplex control configuration (one single, unprotected Controller), a defective Controller leads to a loss of management communication to the affected network element (NE), and may also lead to a loss of management communication to other NEs.

Operations interfaces, such as the user panel, office alarm indicators or Miscellaneous Discrete Inputs/Outputs (MDI/MDO) for example become unavailable as well. Furthermore, some other system functions (for example XC equipment protection, BLSR/MS-SPRing internal management communication, ONNS, or event logging) are stopped.

The only way to regain the control in such a case is to replace the defective Controller.

In a duplex control configuration, the redundant (standby) Controller can take over the full control functionality in case of a defect of the active Controller, and thus automatically restore the control.

In addition, maintenance action can be executed more easily if the Controller which needs to be temporarily removed has been switched into the standby role first.

To summarize, the major functions of duplex control are:

- Automatic restoration of control in case of a defective active Controller.
- Manual switching between both Controllers for maintenance reasons.
- Seamless CTL hardware upgrade.

Static and dynamic role in a protection

The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role in a protection.

Preconditions for duplex control

Duplex control can only be activated if:

- the currently installed NE software release supports duplex control, and
- a CTL equipment protection group exists (i.e. two Controllers are equipped).

The *LambdaUnite*[®] MSS NE software release 3.0 is the first NE software generic that supports both simplex control and duplex control (depending on the shelf equipage). NE software releases prior to the release 3.0 do *not* support duplex control but only simplex control.

Controller variants

These Controller variants exist:

- CTL/- with a 256-MByte NVM storage capacity (*CompactFlash*[®] card).
- CTL/2 with a 512-MByte NVM storage capacity (*CompactFlash*[®] card).
- CTL/3T with a 1-GByte NVM storage capacity (*CompactFlash*[®] card).
- CTL/3S with a 1-GByte NVM storage capacity (*CompactFlash*[®] card).
- CTL/4T with a 256-MByte NVM storage capacity (*CompactFlash*[®] card), redesigned hardware, fully compatible with the CTL/-.
- CTL/4S with a 512-MByte NVM storage capacity (*CompactFlash*[®] card), redesigned hardware, fully compatible with the CTL/2.

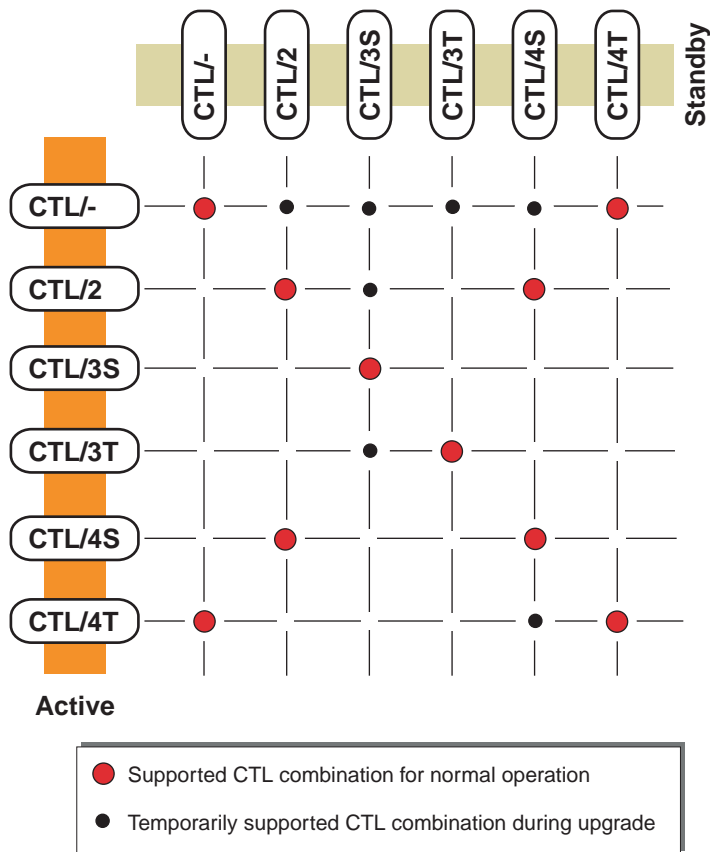
The CTL/3 variants offer enhanced DCC capabilities (support of 180 DCCs) and a greater NVM storage capacity in comparison with the other Controller variants.

The CTL/2, CTL/3S, and CTL/4S support ONNS applications while the CTL/-, CTL/3T, and CTL/4T do not.

The use of a Controller of type CTL/3S or CTL/3T is required to support lower order cross-connection units (LOXC).

It is *not permitted* to permanently operate a *LambdaUnite*[®] MSS system in a mixed Controller configuration for duplex control unless the CTL combination is explicitly supported. Otherwise, a mixed Controller configuration is only temporarily possible during an upgrade.

The following diagram shows the supported CTL combinations:



Important! Although ONNS applications are in principle possible in a simplex control configuration, it is strongly recommended to operate the system in duplex control mode for ONNS applications.

Creation of a CTL protection group

A CTL equipment protection group is created automatically when a second Controller is plugged in or preprovisioned.

All duplex control related functionality is only operational if a CTL protection group exists.

Important! Please observe the following rules:

1. Do not remove or reset the standby (inactive) CTL while a software download or database restoration is in progress. Otherwise, the software download or database restoration will be aborted.
2. Do not open the latches of both CTLs at the same time because this would lead to the recovery of the master CTL to be blocked for approx. 15 minutes after closing the latch again.

In case you have mistakenly opened both CTLs at the same time, close both latches again and wait the 15 minutes in which the system is blocked.

Deletion of a CTL protection group

A CTL equipment protection group is deleted automatically when one of the two Controllers is deprovisioned (plugged out).

Important! As the default alarm severity of the Duplex Control not Present alarm is “Not reported”, *no* alarm will be reported when the standby Controller is removed unless you explicitly change the alarm severity to a value other than “Not reported”.

Mode of operation

The CTL equipment protection operates in 1+1 non-revertive mode.

Only one of the two Controllers can be active at a time, the redundant Controller operates in a so-called “warm standby” mode.

The non-volatile memories (NVMs) on both Controllers are synchronized during a synchronization process. Once the initial NVM synchronization process has finished, all NVM-related operations (configuration and status updates of the NVM) are performed synchronously. Thus, both Controllers share the same configuration and status information (for example alarm supervision).

The standby Controller takes over the functionality of the previously active Controller as soon as an autonomous or manual switch request is present (see switching criteria).

Active/standby role and slot assignment

In the case that two error free Controllers are present in the system, one takes on the active role and the other one the standby role. The decision is made by intercommunication between the two Controllers. A successful protection switch leads to a swap of both roles.

There is no strict assignment between the CTL worker or protection slot (slot 11: worker, slot 31: protection) and the active or standby role of the respective Controller. In general, the active role assignment depends on the previous history.

The Controller which first becomes operational after a reset takes on the active role. If both Controllers recover at the same time, for example after a system reset or an initial system startup, then the Controller in the worker slot takes on the active role, and the Controller in the protection slot takes on the standby role.

Switching criteria

Besides an autonomous protection switch in the case of an equipment failure condition of the currently active Controller, also user-initiated switch requests are possible.

The following list summarizes the possible switch requests (autonomous and user-initiated):

- Autonomous protection switch in the case of an equipment failure condition (e.g. hardware defect, or removal of the currently active Controller)
- **Manual To Working**
Manual protection switch to the Controller in the CTL worker slot (slot 11)
- **Manual To Protection**
Manual protection switch to the Controller in the CTL protection slot (slot 31)
- **Clear**
Manual clearing of a previously performed protection switch

Important! A protection switch from the currently active to the standby Controller is only possible if the standby Controller is in a position to take over the active role. This is the reason why no provision is made for forced protection switches.

Furthermore, instead of using the manual switch commands, it is rather recommended to provoke an autonomous protection switch (by removing the active CTL) for triggering an intentional CTL equipment protection switch.

Alarm signaling after a CTL protection switch

After a CTL protection switch, all currently present alarms are redetected and reported again. As a consequence the alarm signaling is as follows:

- All currently present alarms, including those that were previously acknowledged by means of the ACO button on the user panel, will be signaled again by the user panel LEDs and the office alarm interfaces.
- In the **NE Alarm List**, the same alarms are listed as before the CTL protection switch. They are, however, marked with a new timestamp.
- In the **NE Alarm Log**, alarms may appear twice, but with different timestamps, without a clear notification between the two log entries.

□

XC equipment protection

Introduction

An active XC cross-connection and timing unit (XC160, XC320, or XC640) can be protected by a standby unit. Both the cross-connection function as well as the timing function are protected on this way and form a single protection object. The equipment protection process is fully performed by a central process in the Controller (CTL).

Support of ONNS applications

Only the XC160, XC320/B, and XC640 support ONNS applications. Especially when the ONNS functionality is used, it is recommended to operate the cross-connection and timing units in a 1+1 equipment protected configuration.

Static and dynamic role in a protection

The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role in a protection.

Creation

An XC equipment protection group is created automatically if

- the second cross-connection and timing unit is inserted into the shelf, or
- the two slots for the working and the protection cross-connection and timing unit are preprovisioned, or
- one of the two slots is autoprovisioned and the other one is preprovisioned.

Mode of operation

An XC equipment protection operates in 1+1 non-revertive mode.

Hot standby

The standby cross-connection and timing unit works in the so-called hot-standby mode, which means both cross-connection and timing units work in parallel. The whole configuration of the XC cross-connection and timing unit 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 unit	Active switch request	Denied switch request
Worker	Forced Switch	Force To Protection
Protection	Forced Switch	Force To Working
Worker	Equipment Failed	Manual To Working
Protection	Equipment Failed	Manual To Working
Worker	Equipment Failed	Manual To Protection
Protection	Equipment Failed	Manual To Protection
Worker	Manual Switch	Manual To Protection
Protection	Manual Switch	Manual To Working
Worker	Forced Switch	Manual To Working
Protection	Forced Switch	Manual To Working
Worker	Forced Switch	Manual To Protection
Protection	Forced Switch	Manual To Protection

Furthermore, a forced switch to the standby side will be denied if ...

- ... the standby XC is only preprovisioned but not yet installed in its slot.
- ... the latches of the standby XC are open.
- ... the standby XC has been removed from its slot.

Deletion

An XC equipment protection group is deleted automatically, if one of the two cross-connection and timing units is removed, and the respective slot is deprovisioned, or if a preprovisioned slot is deprovisioned.

Important XC equipment protection switching details

Please observe these functional details with respect to XC 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 cross-connection and timing unit is inserted into the system (i.e. when the latches are closed) it enters a warming-up state for several minutes. During this warming-up state the system timing quality level is explicitly set to DNU/DUS (Do not use for synchronization). If an equipment protection switch occurs during the warming-up period of the standby unit 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 approx. 15 minutes after the insertion of a standby cross-connection and timing unit before performing a manual or forced equipment protection switch.
3. On a cross-connection and timing unit, performance monitoring data is stored in the current bin and one recent bin. Both cross-connection and timing 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 XC equipment protection switch. Thus, an XC equipment protection switch may result in loss of performance monitoring data, depending on the time the standby unit was plugged into the system.
Prior to an (intentional) XC equipment protection switch the standby unit should have been present in the system for a full 24-hours binning period. Otherwise, performance monitoring data may be lost.
4. In rare cases, provisioning or deprovisioning of port units may cause an XC equipment protection switch.

In-service hardware upgrades

These in-service hardware upgrades of cross-connection and timing units (in protected and unprotected configurations) are supported:

From ...	to ...
XC160/-	XC320/-, XC320/A, XC320/B, or XC640/-
XC320/- or XC320/A	XC320/B
XC320/-, XC320/A or XC320/B	XC640/-

Please note that a downgrade of the cross-connection and timing units (i.e. reducing the switch capacity of the system) is *not* possible, because it is not possible to decrease the **Maximum Switch Capacity** parameter.

□

STM-1E equipment protection

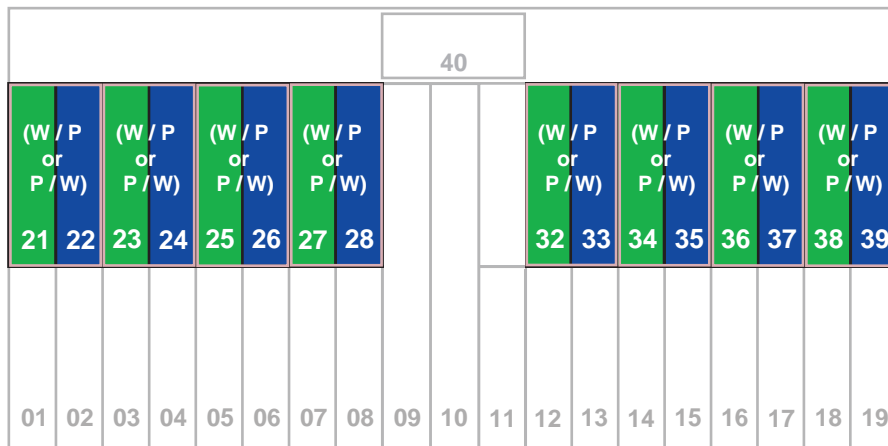
Introduction

LambdaUnite[®] MSS systems support electrical STM-1 interfaces (STM-1E) in unprotected as well as protected configurations.

To accomplish STM-1E transmission (with or without 1+1 equipment protection), EP155 port units can be used in combination with electrical connection interfaces (ECI).

EP155 slot assignment

EP155 port units have to be installed in the upper row of the DUR shelf.



In an STM-1E equipment protection configuration, the EP155 worker (W) and protection (P) port units are adjacently inserted as pairs, as shown in the preceding figure. The worker port unit can be flexibly configured on the right hand side or on the left hand side of the protection port unit.

Worker and protection role

These rules apply concerning the worker and protection role assignment:

- The worker role can be assigned flexibly to either of the two EP155 port units of an STM-1E equipment protection group as long as there are no cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned for any of the two EP155 port units.
- Only one of the two EP155 port units of an STM-1E equipment protection group may have cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned. This EP155 port unit can take on the worker role.
- If both EP155 port units of an STM-1E equipment protection group have cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned, then none of these two port units can take on the worker role. In that situation, all these provisionings need to be removed for at least one of the two EP155 port units.

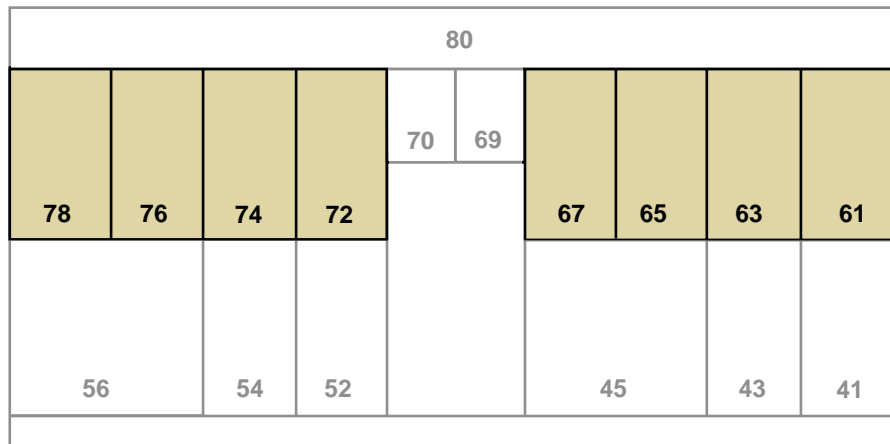
Electrical connection interfaces

The STM-1E input and output ports are located on the electrical connection interfaces.

There are two types of electrical connection interfaces:

ECI/155ME8	16-ports variant for <i>unprotected configurations only</i> (see “ Specific STM-1E configuration aspects ” (p. 5-43)).
ECI/155MP8	8-ports variant for <i>protected and unprotected configurations</i> (see “ Specific STM-1E configuration aspects ” (p. 5-43)).

The electrical connection interfaces have to be installed in the rear-side slots 61, 63, 65, 67, 72, 74, 76, and 78.



Important! The electrical connection interfaces and their inventory data are only accessible when at least one EP155 port unit is installed in the corresponding front-side slot pair.

Association between EP155 and ECI slots

The association between two adjacent EP155s and the a rear-side electrical connection interface (ECI) is as follows:

EP155 slot pair	ECI slot
21/22	61
23/24	63
25/26	65
27/28	67
32/33	72
34/35	74
36/37	76
38/39	78

STM-1E equipment protection groups

Up to 8 STM-1E equipment protection groups can exist per shelf.

Each STM-1E equipment protection group is formed by two adjacent EP155s in combination with a rear-side ECI, as listed in [“Association between EP155 and ECI slots”](#) (p. 5-42).

Please also refer to [“Specific STM-1E configuration aspects”](#) (p. 5-43).

Mode of operation

The STM-1E equipment protection operates in 1+1 non-revertive mode.

Creating an STM-1E equipment protection group

STM-1E equipment protection groups need to be created *manually*.

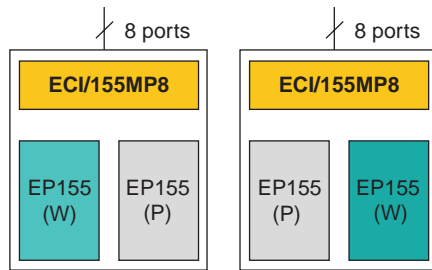
Static and dynamic role in a protection

The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role in a protection.

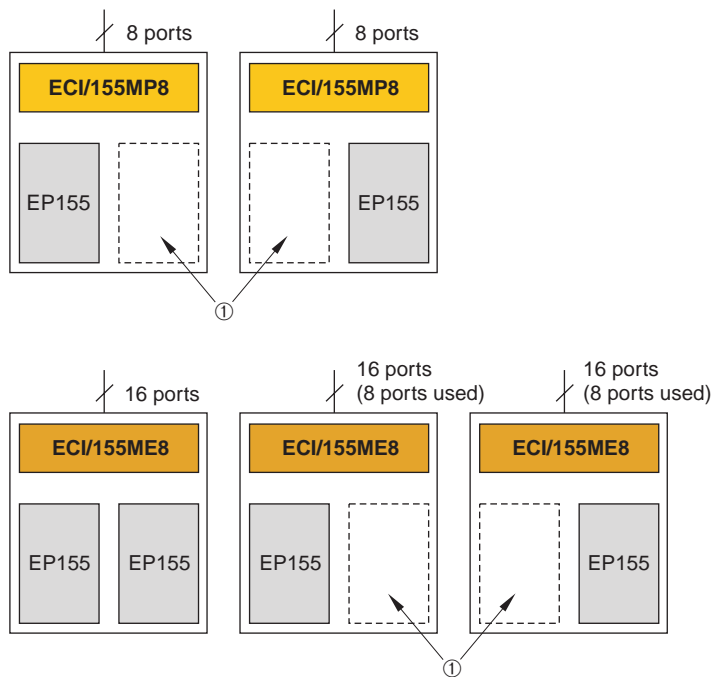
Specific STM-1E configuration aspects

These are the supported combinations of EP155 port units with electrical connection interfaces:

Protected



Unprotected



Legend:

- 1 These slots may be empty, or equipped with an optical SDH/SONET or Gigabit Ethernet port unit, but *not* with an EP51 or EP155 port unit.

Important! When installing EP155 port units without having an ECI installed, unexpected ECI Comm Failure and Loss of Signal alarms may be reported. Therefore, always *first install the ECI before installing the EP155* port units!

STM-1E protected configuration

There is one dedicated configuration for STM-1E equipment protection:

- Two EP155 port units in a universal slot pair as listed in “[Association between EP155 and ECI slots](#)” (p. 5-42), and an ECI/155MP8 electrical connection interface in the corresponding ECI slot.

STM-1E unprotected configurations

There are five possible unprotected configurations:

- One EP155 port unit in either of the two slots of a universal slot pair as listed in “[Association between EP155 and ECI slots](#)” (p. 5-42), and either of the two possible electrical connection interfaces (ECI/155MP8 or ECI/155ME8) in the corresponding ECI slot (→ four possible combinations).
- Two EP155 port units in a universal slot pair as listed in “[Association between EP155 and ECI slots](#)” (p. 5-42), and an ECI/155ME8 electrical connection interface in the corresponding ECI slot. This is the only configuration where 16 STM-1E ports are available.

Configuration changes

These configuration changes are possible without impacting the service:

- ECI/155ME8 with 1 × EP155 → ECI/155ME8 with 2 × EP155.
This configuration change can be achieved by adding the second EP155.
- ECI/155ME8 with 1 × EP155 and empty adjacent slot → ECI/155ME8 with 1 × EP155 and an optical SDH/SONET or Gigabit Ethernet port unit in the adjacent slot.
This configuration change can be achieved by adding the optical SDH/SONET or Gigabit Ethernet port unit.
- ECI/155MP8 with 1 × EP155 → ECI/155MP8 with 2 × EP155.
This configuration change can be achieved by adding the second EP155. In this case, you also need to create the STM-1E equipment protection group.
- ECI/155MP8 with 1 × EP155 and empty adjacent slot → ECI/155MP8 with 1 × EP155 and an optical SDH/SONET or Gigabit Ethernet port unit in the adjacent slot.
This configuration change can be achieved by adding the optical SDH/SONET or Gigabit Ethernet port unit.

Furthermore, observe these rules concerning configuration changes:

- If you want to convert an unprotected configuration with two EP155s (ECI/155ME8 with 2 × EP155) into a protected configuration (ECI/155MP8 with 2 × EP155), then:
 1. Delete all cross-connections, DCC terminations, orderwire and user byte assignments etc. for the EP155 port unit in the protection slot.
 2. Remove and deprovision both EP155 port units.
 3. Replace the ECI/155ME8 by an ECI/155MP8.

4. Re-install the EP155 port units.
 5. Create the STM-1E equipment protection group. Creating an STM-1E equipment protection group is not possible as long as both EP155 port units have cross-connections, DCC terminations, orderwire and user byte assignments etc. assigned.
- If you want to convert a protected configuration (ECI/155MP8 with 2 × EP155) into an unprotected configuration with two EP155s (ECI/155ME8 with 2 × EP155), then:
 1. Delete all cross-connections, DCC terminations, orderwire and user byte assignments etc.
 2. delete the STM-1E equipment protection group.
 3. Remove and deprovision both EP155 port units.
 4. Replace the ECI/155MP8 by an ECI/155ME8.
 5. Re-install the EP155 port units.



DS3/EC-1 equipment protection

Introduction

LambdaUnite® MSS systems support electrical DS3 and EC-1 interfaces in unprotected as well as protected configurations.

To accomplish DS3 or EC-1 transmission (with or without 1+1 equipment protection), EP51 port units are used in combination with ECI51 electrical connection interfaces.

Each port of an EP51 port unit can separately be configured for the transport of one of the following signals:

DS3	Plesiochronous 44.736 Mbps (SONET)
EC-1	Synchronous 51.840 Mbps (SONET)

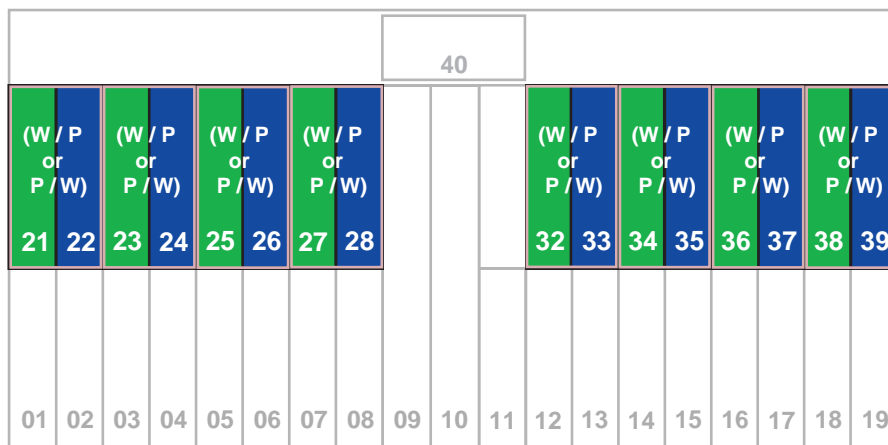
An EP51 port unit can be operated in a mixed configuration with DS3 and EC-1 on different ports.

Important! No traffic will be possible via a DS3/EC-1 port of an EP51 port unit if a signal of the wrong type is applied. When a DS3 signal is applied to a port in EC-1 mode then a Loss of Frame alarm will be reported. However, no specific alarm will be reported when an EC-1 signal is applied to a port in DS3 mode.

Therefore, always *ensure to apply a signal of the correct type* to a DS3/EC-1 port on an EP51 port unit, i.e. a signal in compliance with the port configuration (EC-1 signals to ports in EC-1 mode, DS3 signals to ports in DS3 mode).

EP51 slot assignment

EP51 port units can be inserted only in the upper row of the DUR shelf.



In a DS3/EC-1 equipment protection configuration, the EP51 worker (W) and protection (P) port units are adjacently inserted as pairs, as shown in the preceding figure. The worker port unit can be flexibly configured on the right hand side or on the left hand side of the protection port unit.

Worker and protection role

These rules apply concerning the worker and protection role assignment:

- The worker role can be assigned flexibly to either of the two EP51 port units of an DS3/EC-1 equipment protection group as long as there are no cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned for any of the two EP51 port units.
- Only one of the two EP51 port units of an DS3/EC-1 equipment protection group may have cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned. This EP51 port unit can take on the worker role.
- If both EP51 port units of an DS3/EC-1 equipment protection group have cross-connections, timing reference assignments, transmission protection schemes, DCN or orderwire connections, facility or cross-connection loopbacks, or transparent DCC connections provisioned, then none of these two port units can take on the worker role. In that situation, all these provisionings need to be removed for at least one of the two EP51 port units.

Electrical connection interfaces

The DS3/EC-1 input and output ports are located on the ECI51/MP72 electrical connection interfaces.

The ECI51/MP72 electrical connection interfaces must be installed in the rear-side slot pairs 61/63, 63/65, 65/67, 72/74, 74/76, or 76/78.

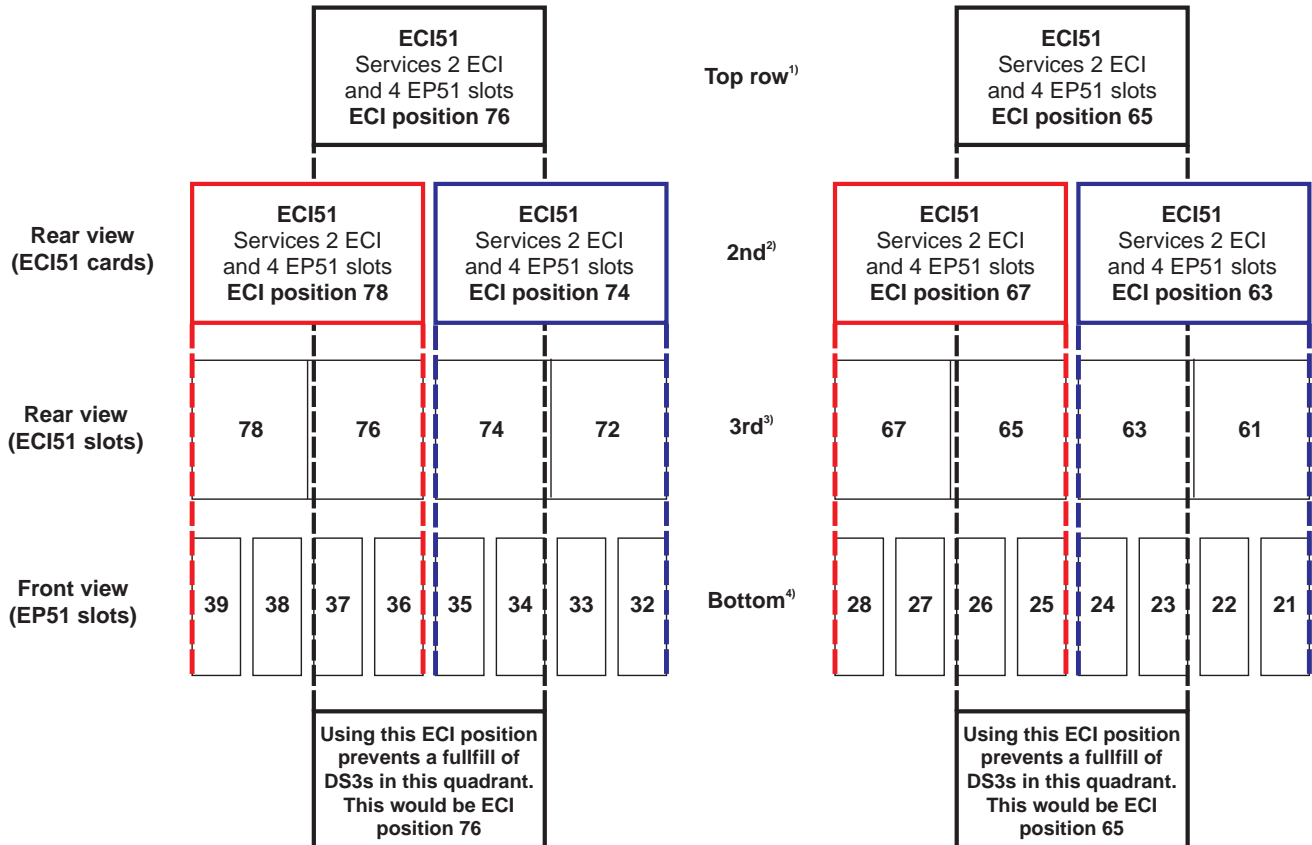
Important! The electrical connection interfaces and their inventory data are only accessible if at least one EP51 port unit is installed in the corresponding front-side slot.

EP51/ECI51 slot assignments

The association between the slots for the EP51s and the rear-side electrical connection interface (ECI51) slots is as follows:

EP51 slots	ECI51 slots	ECI51 position
21 ... 24	61/63	63
25 ... 28	65/67	67

EP51 slots	ECI51 slots	ECI51 position
32 ... 35	72/74	74
36 ... 39	76/78	78
23 ... 26	63/65	65
34 ... 37	74/76	76



¹⁾ Top row represents ECI51 cards (DS3 paddle boards) that could be installed in positions 65 and/or 76 on the third row.
²⁾ Second row represents ECI51 cards (DS3 paddle boards) that could be installed in positions 63, 67, 74, and/or 78.
³⁾ Third row represents ECI51 slots on the rear of the LambdaUnite[®] shelf where ECI51 cards (DS3 paddle boards) can be installed.
⁴⁾ Bottom row represents the channel slots on the front of the LambdaUnite[®] shelf and are shown under the ECI51 slots that serve them.

NOTE:
 If ECI51 position 65 is used, positions 63 and 67 are not available. If ECI51 position 76 is used, positions 74 and 78 are not available.

DS3/EC-1 equipment protection groups

Up to 8 DS3/EC-1 equipment protection groups can be set up per shelf.

Each DS3/EC-1 equipment protection group is formed by two adjacent EP51s, cf. “EP51 slot assignment” (p. 5-47), in combination with half a rear-side ECI51, as listed in the preceding table “EP51/ECI51 slot assignments” (p. 5-48).

Please also refer to “Specific EP51 configuration aspects” (p. 5-50).

Mode of operation

The DS3/EC-1 equipment protection operates in 1+1 non-revertive mode.

Creating a DS3/EC-1 equipment protection group

DS3/EC-1 equipment protection groups need to be created *manually*.

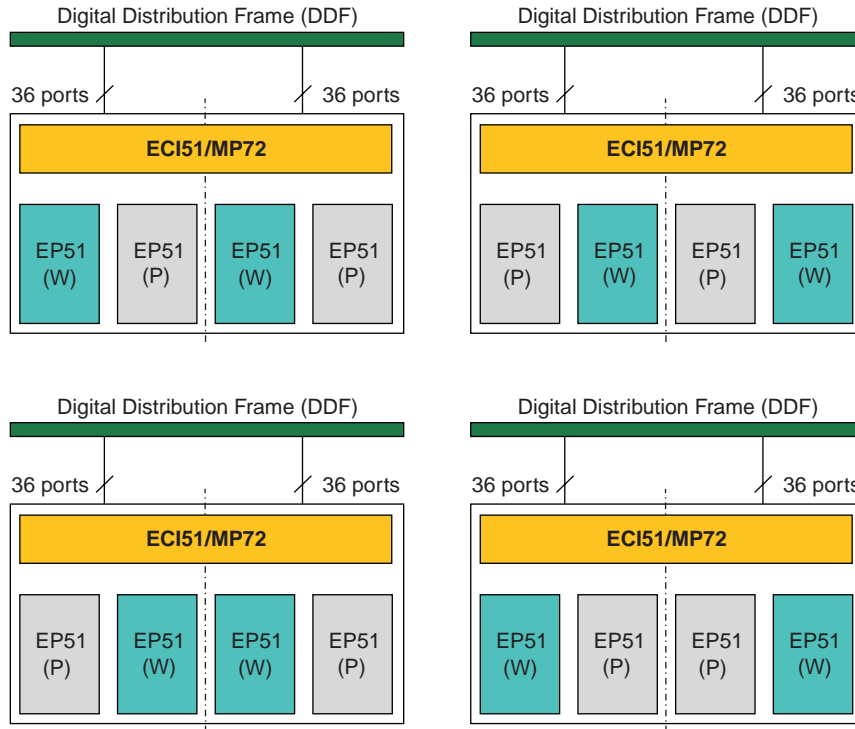
Static and dynamic role in a protection

The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role in a protection.

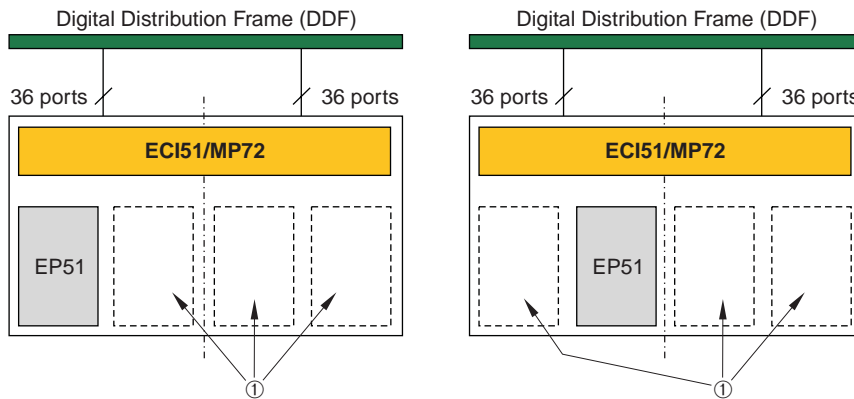
Specific EP51 configuration aspects

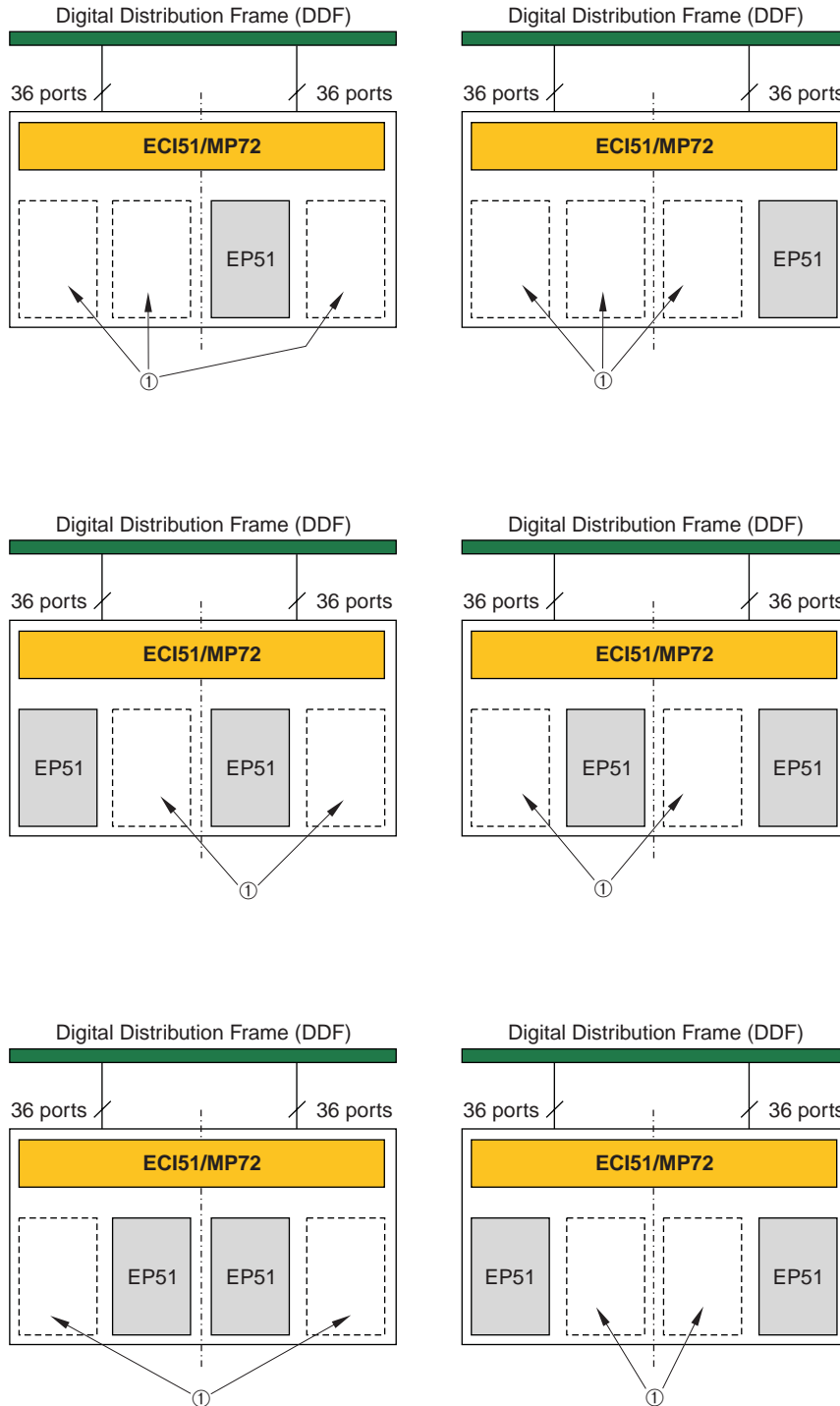
There is no restriction regarding the allocation of the worker and protection EP51 port units within the protection slot pair as long as the rules concerning the worker and protection role assignment as listed in “EP51 slot assignment” (p. 5-47) are observed.

Therefore all combinations of EP51 port units with ECI51 electrical connection interfaces are supported for protected configurations:



For unprotected configurations the following combinations of EP51 port units with ECI51 electrical connection interfaces are supported:

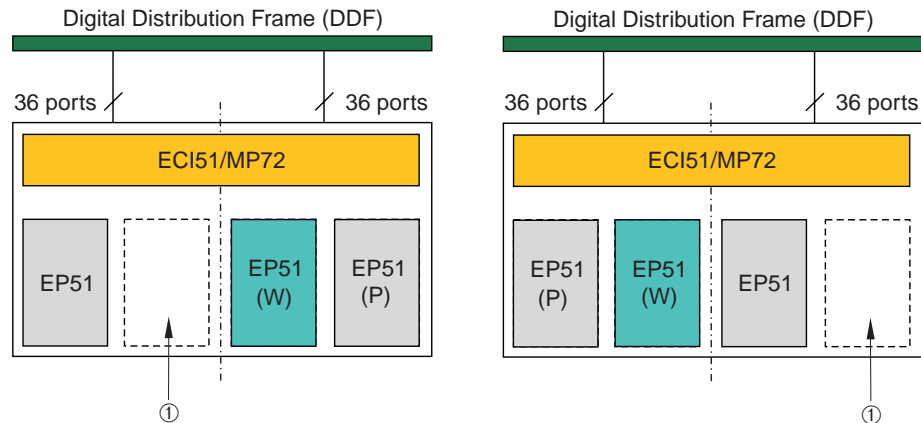




Legend:

- 1 These slots may be empty, or equipped with an optical SDH/SONET or Gigabit Ethernet port unit, but *not* with an EP51 or EP155 port unit.

Any mix of protected and unprotected configurations is possible, maintaining the pair pattern of the EP51 protection slot pairs, as displayed in “EP51 slot assignment” (p. 5-47). The following figure shows examples for mixed configurations:



Legend:

- 1 These slots may be empty, or equipped with an optical SDH/SONET or Gigabit Ethernet port unit, but *not* with an EP51 or EP155 port unit.

Important!

1. *Do not* use two EP51 port units in adjacent slots with an ECI51 installed but without having a DS3/EC-1 equipment protection group created. Such an unsupported configuration may lead to a loss of traffic.
2. When installing EP51 port units without having an ECI51 installed, unexpected ECI Comm Failure and Loss of Signal alarms may be reported. Therefore, always *first install the ECI51 before installing the EP51* port units!

DS3/EC-1 protected configurations

Protected DS3 configurations can be set up as follows:

- Two EP51 port units in a universal slot pair as listed in “EP51 slot assignment” (p. 5-47), and an ECI51 in the corresponding ECI slot (half of its capacity used), cf. “EP51/ECI51 slot assignments” (p. 5-48).

DS3/EC-1 unprotected configurations

Unprotected DS3 configurations can be set up as follows:

- One EP51 port unit in one of the two slots of a universal slot pair as listed in “EP51 slot assignment” (p. 5-47), and an ECI51 in the corresponding ECI slot (half of its capacity used), cf. “EP51/ECI51 slot assignments” (p. 5-48).

Configuration changes

These configuration changes are possible without impacting the service:

- Half an ECI51 with 1 × EP51 (unprotected) → ECI51 with 2 × EP51 (protected).
This configuration change can be achieved by adding the second EP51 in the respective protection pair slot, cf. “EP51 slot assignment” (p. 5-47), and creating the DS3/EC-1 equipment protection group
- Half an ECI51 with 1 × EP51 and empty adjacent slot → ECI51 with 1 × EP51 and an optical SDH/SONET or Gigabit Ethernet port unit in the adjacent slot.
This configuration change can be achieved by adding the optical SDH/SONET or Gigabit Ethernet port unit.

Note that the maximum number of active DS3/EC-1 ports per *LambdaUnite*[®] MSS NE is 288 (4 ECI51 with 72 ports each, 8 EP51 with 36 ports each), regardless if protected or not.



LOXC equipment protection

Terminology

“LOXC” is the collective term for lower order cross-connection units (LOXC/1, LOXC40G2S/1, LOXC40G3S/1).

“LOXC40” is the collective term for lower order cross-connection units with a switching capacity of 40 Gbps (LOXC40G2S/1, LOXC40G3S/1).

Lower order cross-connections

LambdaUnite[®] MSS systems support switching of lower order cross-connections.

Lower order tributaries cannot be terminated within the *LambdaUnite*[®] MSS system, but are embedded in substructured higher order transport signals which need to be terminated before the embedded lower order signals can be cross-connected.

In the input direction, the higher order transport signals are terminated before the contained lower order tributaries are cross-connected. In the output direction, the lower order signals are integrated into the substructure of a newly generated higher order transport signal.

Lower order cross-connections can be unidirectional or bidirectional.

Signal rates

These types of lower order tributaries are supported:

- VT1.5 (SONET)
- VC-12 (SDH)
- VC-3 (SDH)

These types of substructured higher order transport signals are supported:

- STS-1 (SONET), carrying VT1.5 signals
- VC-4 (SDH), carrying VC-3 or VC-12 signals, or a mix of VC-3 and VC-12

Hardware prerequisites

The usage of a lower order cross-connection unit (LOXC) in combination with a Controller of type CTL/3S or CTL/3T is required.

Important! An LOXC can support either SONET or SDH traffic.

Equipment protection groups may be configured for both the LOXC as well as the Controller.

LOXC switching capacity

When an LOXC is inserted into a permissible slot (see “[Specific LOXC equipage rules](#)” (p. 5-56)), then it becomes autoprovisioned with a switching capacity of 0 Gbps.

Important! You can activate at most *one* LOXC by explicitly setting the switching capacity to 15 Gbps or 40 Gbps, respectively. A second LOXC automatically may get a switching capacity of 15 Gbps or 40 Gbps assigned when it is included in an LOXC equipment protection group as the protection unit. However, only *one* LOXC may be active at a time.

LOXC equipment protection

Please also refer to “[Specific LOXC equipage rules](#)” (p. 5-56).

Mode of operation

The LOXC equipment protection operates in 1+1 non-revertive mode.

Activating of an LOXC

In order to activate an LOXC, its lower order switching capacity must be set to a value different from 0.

Creating an LOXC equipment protection group

LOXC equipment protection groups need to be created *manually*.

Static and dynamic role in a protection

The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role in a protection.

LOXC in-service upgrade

Please note that no LOXC in-service upgrade is supported in the present software release.

Specific LOXC equipage rules

LOXC lower order cross-connection units must be installed in dedicated universal slots or slot combinations. Moreover, which universal slots or slot combinations support the lower order cross-connection functionality also depends on the maximum switching capacity of the system.

These are the supported slot combinations for the usage of lower order cross-connection units ((W): worker; (P): protection):

Max. switching capacity		Slot assignment		
		LOXC (W)	LOXC (P)	Remarks and additional equipage guidelines
LXC160		37	39	The slots 36 and 38 must remain empty.
LXC320	Option 1 ⁽¹⁾	4	19	The slots 3 and 18 must remain empty. Bear in mind, that the slots 2 and 17 may be required at a later date in case an in-service upgrade is planned towards LOXC units which occupy 3 slots.
	Option 2	17	19	Alternative equipage if slot 4 is occupied. The slots 16 and 18 must remain empty.
	Option 3 ⁽²⁾	37	39	The slots 36 and 38 must remain empty.
LXC640	Option 1 ⁽¹⁾	4	19	Bear in mind, that the slots 3 and 18 may be required at a later date in case an in-service upgrade is planned towards LOXC units which occupy 2 slots.
	Option 2 ⁽³⁾	17	19	Bear in mind, that the slots 16 and 18 may be required at a later date in case an in-service upgrade is planned towards LOXC units which occupy 2 slots.
	Option 3 ⁽⁴⁾	18	19	–
	Option 4 ⁽⁵⁾	37	39	Bear in mind, that the slots 36 and 38 may be required at a later date in case an in-service upgrade is planned towards LOXC units which occupy 2 slots.

Notes:

- Option 1 is the preferred option.
- LXC320, option 3, is the preferred option for a seamless upgrade from LXC160 to LXC320.
- LXC640, option 2, is the preferred option for a seamless upgrade from LXC320 to LXC640.
- LXC640, option 3, is the preferred option for maximized automatic I/O slot usage by *Telcordia*[®] Technologies.
- LXC640, option 4, is the preferred option for a seamless upgrade from LXC160 to LXC640.

Important! There may be at most *one active* LOXC. A second LOXC may be configured for protection purposes. This implies that at most one LOXC equipment protection group may exist.

The following figures serve to visualize the permissible LOXC slot positions (W: worker, P: protection), depending on the system's maximum switching capacity:

LXC160:

								User panel 40											
										(W) (P)									
Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	XC (W) slot	XC (P) slot	CTL (W) slot	CTL (P) slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot		
21	22	23	24	25	26	27	28	9	10	11	31	32	33	34	35	36	37	38	39
Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	XC (W) slot	XC (P) slot	CTL (W) slot	CTL (P) slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot
1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19

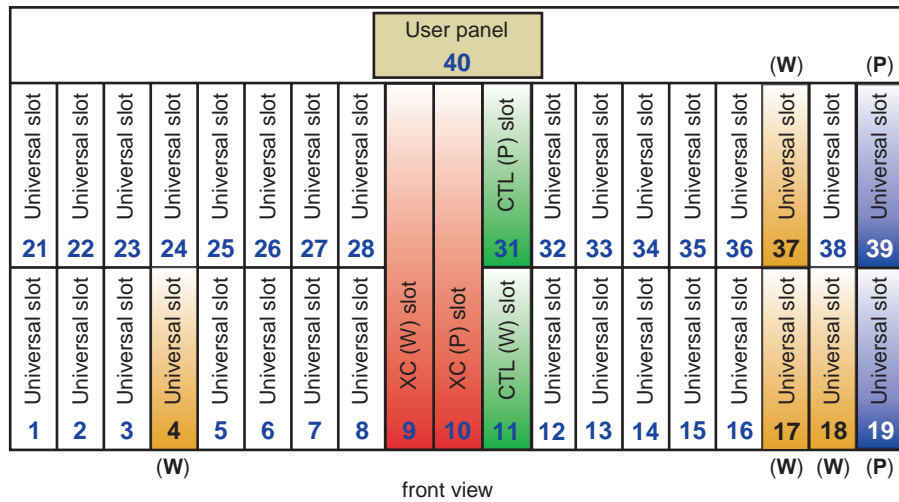
front view

LXC320:

								User panel 40											
										(W) (P)									
Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	XC (W) slot	XC (P) slot	CTL (W) slot	CTL (P) slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot
21	22	23	24	25	26	27	28	9	10	11	31	32	33	34	35	36	37	38	39
Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	XC (W) slot	XC (P) slot	CTL (W) slot	CTL (P) slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot	Universal slot
1	2	3	4	5	6	7	8	9	10	11		12	13	14	15	16	17	18	19
(W)														(W) (P)					

front view

LXC640:



Preconditions for creating an LOXC equipment protection group

Before an LOXC equipment protection group can be created, the following preconditions must *all* be fulfilled:

- At least one cross-connection and timing unit (XC) is provisioned.
- The potential worker LOXC
 - has been provisioned,
 - is not yet involved in an LOXC equipment protection group, and
 - has already been activated (switching capacity is 15 Gbps or 40 Gbps).
- The potential protection LOXC
 - has been provisioned, and
 - has a switching capacity of 0 Gbps (i.e. is currently inactive).

Switch requests

Besides an autonomous protection switch in the case of an equipment failure condition of the currently active LOXC, also user-initiated switch requests are possible.

The following list summarizes the possible switch requests (autonomous and user-initiated):

- Autonomous protection switch in the case of an equipment failure condition (e.g. hardware defect, or removal of the currently active LOXC)
- **Manual To Working**
Manual protection switch to the LOXC in the worker slot.
- **Manual To Protection**
Manual protection switch to the LOXC in the protection slot.

- **Forced To Working**
Forced protection switch to the LOXC in the worker slot.
- **Forced To Protection**
Forced protection switch to the LOXC in the protection slot.
- **Clear**
Manual clearing of a previously performed protection switch.

Important LOXC equipment protection switching details

Please observe these functional details with respect to LOXC equipment protection switching:

1. Note that a manual or forced LOXC equipment protection switch causes short traffic hits even if the destination LOXC works properly.
The traffic is interrupted for a few milliseconds. B3 errors are detected. No alarm will be raised.



6 Equipment provisioning tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to equipment provisioning.

Contents

Provisioning of slots and SFP modules	6-3
To view a list of slots	6-3
Port provisioning	6-4
To view a list of physical ports	6-4
To view a list of logical ports	6-5
To view a list of loopback-enabled ports	6-6
To provision or deprovision a loopback on a port	6-7
To modify the parameters of a physical or logical port	6-9
Parameters for SDH/SONET/PDH ports	6-11
Parameters for Ethernet ports	6-26
Parameters for VCG ports	6-30
Provisioning of NE event controls	6-38
To inhibit the forwarding of autonomous messages	6-38
To allow the forwarding of autonomous messages	6-40
Provisioning of MDIs and MDOs	6-42
To retrieve the MDO configuration	6-42
To set the MDO configuration	6-44
To switch on an MDO	6-46

To switch off an MDO	6-48
To retrieve the MDO state	6-50
To retrieve the MDI configuration	6-52
To set the MDI configuration	6-54
Equipment protection	6-56
To retrieve equipment protection group information	6-56
To add an equipment protection group	6-59
To operate an equipment protection group	6-61
To release an equipment protection group	6-63
To delete an equipment protection group	6-65



Provisioning of slots and SFP modules

To view a list of slots

When to use

Use this task to view a list of slot information for a selected NE.

Task

- 1 Use the object links to follow this path: **Network Elements** → **Equipment**.

Result: The **Search for Equipment** page is displayed.

- 2 Do the following:

1. In the **NE type** field, select a type of NE.
2. In the **NE name** field, select the name of the target NE.
3. In the **Equipment type** field, select **Slot/Circuit pack**.
4. For the **Search by** field, select the option **Equipment ID**.
5. Leave the **Equipment ID** field empty.
6. Click **Search**.

Result: The **Equipment - Slots/Circuit Packs** page is displayed. It includes a list of slots for the selected NE.

END OF STEPS



Port provisioning

To view a list of physical ports

When to use

Use this task to view a list of physical ports.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network**. The **Network Map** is displayed. Right-click an NE icon. From the resulting **Node** menu, select **Network Element** → **Ports**.
 - Use the object links to follow this path: **Network Elements** → **Ports**.
Result: The **Search for Ports** page is displayed.
-

- 2 Complete the following steps to begin to specify the criteria for your search.
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of an NE (if not already present).
 3. In the **Port type** field, select **Physical**.
-

3	If...	then...
	you want the search to return a single port,	in the Search by field, select Port ID . In the Port ID field, enter the port ID. Click Search .
	you want the search to return a list of multiple ports,	in the Search by field, select Port list . Select a Port rate and/or a Slot / Circuit Pack . Click Search .

Result: The list at the bottom of the **Ports** page is populated with a list of ports in the NE that meet your search criteria.

END OF STEPS



To view a list of logical ports

When to use

Use this task to view a list of logical ports.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network**. The **Network Map** is displayed. Right-click an NE icon. From the resulting **Node** menu, select **Network Element** → **Ports**.
 - Use the object links to follow this path: **Network Elements** → **Ports**.

Result: The **Search for Ports** page is displayed.

- 2 Complete the following steps to begin to specify the criteria for your search.
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of an NE (if not already present).
 3. In the **Port type** field, select **Logical**.

3 If...	then...
you want the search to return a single port,	in the Search by field, select Port ID . In the Port ID field, enter the port ID. Click Search .
you want the search to return a list of multiple ports,	in the Search by field, select Port list . Select a Port rate , a Parent port rate , and a Slot / Circuit Pack . Click Search .

Result: The list at the bottom of the **Ports** page is populated with a list of ports in the NE that meet your search criteria.

END OF STEPS



To view a list of loopback-enabled ports

When to use

Use this task to view a list of loopback-enabled ports.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network**. The **Network Map** is displayed. Right-click an NE icon. From the resulting **Node** menu, select **Network Elements** → **Ports**.
 - Use the object links to follow this path: **Network Elements** → **Ports**.
- Result:** The **Ports** page is displayed.
-

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE.
2. In the **NE name** field, enter the name of the NE from the drop-down menu.
3. In the **Search by** field, click the radio button **Port list**.
4. In the **Port type** field, click the radio button **Physical**.
5. Make a selection in the **Port rate** and the **Slot / Circuit pack** fields.
Note: If the “Slot / Circuit pack” field is not selectable, change the selection of the **Port rate** and try again.
6. In the **Filter by** field, click the check-box next to **Loopback provisioned**.
7. Click **Search**.

Result: The **Ports** panel is populated at the bottom containing a list of records that meet your search criteria.

If the list is empty, no loopbacks are provisioned.

END OF STEPS



To provision or deprovision a loopback on a port

When to use

Use this task to provision or deprovision a loopback on a port.



CAUTION

Service-disruption hazard

Provisioning a loopback may result in a disruption of traffic, timing, and the possible loss of DCN connections.

Before you begin

Loopback is supported only on physical ports.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network**. The **Network Map** is displayed. Right-click an NE icon. From the resulting **Node** menu, select **Network Element** → **Ports**.
 - Use the object links to follow this path: **Network Elements** → **Ports**.

Result: The **Search for Ports** page is displayed.

- 2 Complete the following steps to begin to specify the criteria for your search.
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of an NE (if not already present).
 3. In the **Port type** field, select **Physical**.

3 If...	then...
you want the search to return a single port,	in the Search by field, select Port ID . In the Port ID field, enter the port ID. Click Search .
you want the search to return a list of multiple ports,	in the Search by field, select Port list . Select a Port rate , a Parent port rate , and a Slot / Circuit Pack . Click Search .

Result: The list at the bottom of the **Ports** page is populated with a list of ports in the NE that meet your search criteria.

- 4 The **Native name** column of the table lists the names of the ports. Click the radio button next to the port on which you wish to provision loopback.
-

- 5 From the **Go** menu, select **Provision loopback** and click **Go**.

Result: The **Loopback Provisioning** page is displayed.

- 6 In the **Loopback type** field, click the radio button in either of the following fields:

- **Inloop Loopback**
- **Outloop Loopback**

Result: The **Operation** field changes to **Provision** or **Deprovision**, depending on your selection, and whether an inloop loopback or outloop loopback is provisioned on the port.

- 7 In the **Operation** field, select **Provision** or **Deprovision** and click **Submit**.

Important! The NE will reject loopback creation if the port is in service.

Result: A confirmation window is displayed asking you to confirm the provisioning or deprovisioning.

- 8 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the page, and the loopback is provisioned or deprovisioned on the port.

END OF STEPS



To modify the parameters of a physical or logical port

When to use

Use this task to modify the parameters of a port.



CAUTION

Service-disruption hazard

Modification of port parameters may be traffic affecting.

Before starting to modify port parameters, make sure that the port is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path).

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network**. The **Network Map** is displayed. Right-click an NE icon. From the resulting **Node** menu, select **Network Element** → **Ports**.
 - Use the object links to follow this path: **Network Elements** → **Ports**.

Result: The **Ports** page is displayed.
- 2 Complete the following steps to begin to specify the criteria for your search.
 1. In the **NE type** field, select a type of NE.
 2. In the **NE name** field, select the name of an NE.
 3. In the **Port type** field, select **Physical** or **Logical**, respectively, depending on the type of port you want to modify.

3	If...	then...
	you want the search to return a single port,	in the Search by field, select Port ID . In the Port ID field, enter the port ID. Click Search .
	you want the search to return a list of multiple ports,	in the Search by field, select Port list . Select a Port rate , a Parent port rate , and a Slot / Circuit Pack . Click Search .

Result: The list at the bottom of the **Ports** page is populated with a list of ports in the NE that meet your search criteria.

- 4 The **Native name** column of the table lists the names of the ports. Each name is a hyperlink.

Do one of the following:

- Click the name of the port you wish to modify.
- Click the radio button next to the port you wish to modify. From the Go menu, select **View/modify port parameters** and click **Go**.

Result: The **View/modify port** page is displayed.

- 5 Change the entries or selections for any modifiable port parameters.

Detailed information about the parameters to be modified and the possible values is provided in the following sections:

- [“Parameters for SDH/SONET/PDH ports”](#) (p. 6-11).
 - [“Parameters for Ethernet ports”](#) (p. 6-26).
 - [“Parameters for VCG ports”](#) (p. 6-30).
-

- 6 Click **Submit**.

Result: A confirmation window is displayed asking you to confirm the modification.

- 7 Click **Yes**.

Result: The port parameters are modified, and a confirmation is issued in the **Messages** panel. The **Job Updates** page is displayed and reports the status of the modification of the port parameters.

END OF STEPS



Parameters for SDH/SONET/PDH ports

Introduction

This section lists the parameters that can be modified for SDH, SONET, or PDH ports. Note that not all parameters and possible values apply to all port types, plug-in units, and network element configurations.

For a number of parameters, the network elements can report the value *not applicable*. This value is for information purposes only, it cannot be entered.

Transmission

In the **Transmission** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Port mode	Indicates the monitoring state of the specified port.	Depending on the port rate and type the following values are possible: <ul style="list-style-type: none"> <i>on</i> – the port is being monitored. <i>auto</i> – the port is ready to transition into a monitored state, when a signal is detected. <i>off</i> – the port is not being monitored.
FEC type	Specifies the FEC type on a DWDM port of a G.709 10G OT.	<i>RS_FEC</i> – out-of-band FEC making use of an RS(255,239) reed-solomon code; <i>V_FEC</i> – Lucent-proprietary enhanced forward error correction (EFEC, also referred to as ultra forward error correction, UFEC) using an OTU2V frame structure acc. to the ITU-T Rec. G.709/Y.1331 (03/2003), appendix II.
Electrical interface type	For a port on the electrical transmission unit EP51, this parameter specifies the type of input signal the port has been provisioned for.	<i>DS3</i> , <i>ECL</i> .
Transmitted interface standard	The interface standard setting.	<i>SONET</i> , <i>SDH</i> .
Inloop/Facility loopback	The field name is a hyperlink. To create or delete a loopback, click the link and follow the task “ To provision or deprovision a loopback on a port ” (p. 6-7).	

Parameter	Function	Possible values
Outloop/Terminal loopback	The field name is a hyperlink. To create or delete a loopback, click the link and follow the task “To provision or deprovision a loopback on a port” (p. 6-7) .	
Service condition	The status of the port concerning service involvement.	<ul style="list-style-type: none">• <i>in service</i> – provisioning values for service will be accepted.• <i>out of service</i> – provisioning values for service will not be accepted.

Parameter	Function	Possible values
Tributary mode	<p>The user-provisionable attribute of tributaries of a port.</p> <p>It can be of two types:</p> <ul style="list-style-type: none"> <p>Fixed-rate tributary mode:</p> <p>In this mode, a tributary is provisioned for an expected and fixed signal rate, which is used for cross-connection rate validation. SDH ports can only be provisioned for fixed-rate operation, so a cross-connection from a tributary on an SDH port provisioned for VC-4 must be at the VC-4 rate and can contain only a VC-4 signal, not three VC-3 signals. (If $3 \times$ VC-3 did appear on the tributary input, the associated pointer processor would declare loss of pointer and path AIS would be inserted downstream.) With SONET ports provisioned for fixed-rate operation, the only allowed constituents for an STS-1, STS-3, STS-12, STS-48, or STS-192 cross-connection from a fixed-rate port are respectively STS-1, STS-3c, STS-12c, STS-48c, or STS-192c. LO cross-connections can only be switched from input ports in fixed rate tributary mode. Also within the HO VC-4 / STS-1 there is only fixed rate operation for the LO constituents.</p> <p>Adaptive-rate tributary mode (also known as “pipe mode”):</p> <p>In this mode, a tributary is not provisioned for an expected signal rate. The system identifies, and adapts to transitions in, the signal rates. With adaptive-rate tributary operation, an STS-<i>N</i> cross-connection could have a single STS-<i>N</i>c constituent signal or any mix of multiple lower-rate constituent signals (for example STS-1s and STS-3cs in an STS-12), consistent with the SONET standard. Transitions between these constituent signal rates can take place. The system adapts to the current concatenation state by auto-detection of the concatenation indicators in the signal. This “pipe mode” can only be provisioned for SONET ports.</p> 	<i>fixed, adaptive.</i>

Parameter	Function	Possible values
Tributary input signal rate	The tributary input signal rate indicates the expected tributary structure for the port in the incoming direction.	For a SONET port, a valid value is a string of the format <i>NX-NX-NX...-NX</i> , where <i>N</i> is the number of <i>X</i> s and <i>X</i> can be 1, 3, 12, 48, or 192 (representing STS1, STS3, STS12, STS48, or STS192, respectively). For an SDH port, a valid value is a string of the format <i>NX-NX-NX...-NX</i> , where <i>N</i> is the number of <i>X</i> s and <i>X</i> can be 3, 4, 4C, 16C, or 64C (representing VC3, VC4, VC4-4C, VC4-16C, or VC4-64C, respectively).
Tributary output signal rate	The tributary output signal rate indicates the expected tributary structure for the unequipped signal that will be transmitted when there are no cross connections.	For a SONET port, a valid value is a string of the format <i>NX-NX-NX...-NX</i> , where <i>N</i> is the number of <i>X</i> s and <i>X</i> can be 1, 3, 12, 48, or 192 (representing STS1, STS3, STS12, STS48, or STS192, respectively). For an SDH port, a valid value is a string of the format <i>NX-NX-NX...-NX</i> , where <i>N</i> is the number of <i>X</i> s and <i>X</i> can be 3, 4, 4C, 16C, or 64C (representing VC3, VC4, VC4-4C, VC4-16C, or VC4-64C, respectively).
Sub structure	This parameter is used to indicate whether a VC-4 (SDH) or STS-1 (SONET) CTP contains LO CTPs or not.	<i>no</i> – no substructure; <i>mansub</i> – manual substructure; <i>yes</i> – automatic substructure.
Optical channel	Indicates whether the Optical Channel (OCh) is enabled or disabled. Applies only to port units that support out-of-band FEC. The OCh needs to be enabled for out-of-band FEC	<i>enable</i> , <i>disable</i> .
Optical output enable	Enables the OT1 port of an optical port unit with tunable laser.	<i>enable</i> , <i>disable</i> .
OTN client port	Specifies if the port of an optical port unit with tunable operates as OTN client port or as SDH/SONET port.	<i>yes</i> – OTN client port; <i>no</i> – SDH/SONET port.
Outgoing Z0 byte	This parameter <i>only applies to OC-48 and lower rate SONET interfaces</i> . It indicates the configured mode of outgoing Z0 byte insertion.	Possible values are: <ul style="list-style-type: none"> <i>Fixed CChex</i> The value of the Z0 byte is CC_{hex} (hexadecimal value). <i>STS-Id</i> The value of the Z0 byte is the STS identifier (the number) of the corresponding STS frame.

Parameter	Function	Possible values
Ring A node ID	Specifies the TID of the node at which the service is added to the BLSR ring. It is required for the input of tributaries to be used by ONNS on ports of portClass=EDGE being members in BLSR/MS-SPring protection groups.	
Ring Z node ID	Specifies the TID of the node at which the service is added to the BLSR ring. It is required for the input of tributaries to be used by ONNS on ports of portClass=EDGE being members in BLSR/MS-SPring protection groups.	
Frame format	The provisioned DS3 signal format: <ul style="list-style-type: none"> • <i>C-bit parity</i> C-bit parity channelized DS3 format, which supports full P-bit parity VMR, VM, or no VM. It may also use full C-bit parity monitoring. • <i>M23</i> M23 channelized DS3 format, which supports full P-bit parity VMR, VM, or no VM. The C-bit monitoring is disabled for this format. • <i>Unframed and Clear Channel</i> P-bit parity VMR, VM, and C-bit parity monitoring is disabled. 	<i>CBIT, M23, UNFRAMEDCC.</i>
Line build out	The cable length applicable for the DS3 port.	<i>short</i> (0 to 68.5 m; 0 to 225 ft); <i>long</i> (68.5 to 137 m; 225 to 450 ft)
Unconnected output maintenance signal	Indicates whether an AIS, DS3AIS or IDLE signal is transmitted in response to an unconnected input.	<i>AIS, DS3AIS, idle.</i>
DS3 violation monitoring mode	The status of the DS3 P-bit parity violation monitoring and removal.	<i>NO-VM</i> – no violation monitoring; <i>VMR</i> – violation monitoring and removal; <i>VM</i> – violation monitoring.
PDI-P switching	Enables payload defect indication on path level (PDI-P) switching.	<i>enable, disable.</i>

Optics

In the **Optics** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Optical wavelength (nm)	The optical wavelength in nanometers of the signal transmitted and received at that port.	For a DWDM port of a G.709 10G OT the following values are possible: <ul style="list-style-type: none"> • 0 (undefined) • OP10/XTTC: 35 wavelengths in the BAND_C (1554.537 nm to 1568.362 nm) • OP10/XTTL: 93 wavelengths in the BAND_L (1568.773 nm to 1607.466 nm)

Supported optical wavelengths

DWDM ports of a G.709 10G OT support the following wavelength:

OP10/XTTC	OP10/XTTL
35 wavelengths in the BAND_C: 1554.537, 1554.940, 1555.343, 1555.747, 1556.151, 1556.555, 1556.959, 1557.363, 1557.768, 1558.173, 1558.578, 1558.983, 1559.389, 1559.794, 1560.200, 1560.606, 1561.013, 1561.419, 1561.828, 1562.233, 1562.640, 1563.047, 1563.455, 1563.863, 1564.271, 1564.679, 1565.087, 1565.496, 1565.905, 1566.314, 1566.723, 1567.133, 1567.542, 1567.952, 1568.362	93 wavelengths in the BAND_L: 1568.773, 1569.183, 1569.594, 1570.005, 1570.416, 1570.828, 1571.239, 1571.651, 1572.063, 1572.476, 1572.888, 1573.301, 1573.714, 1574.127, 1574.540, 1574.954, 1575.368, 1575.782, 1576.196, 1576.610, 1577.025, 1577.440, 1577.855, 1578.270, 1578.686, 1579.102, 1579.518, 1579.934, 1580.350, 1580.767, 1581.184, 1581.601, 1582.018, 1582.436, 1582.854, 1583.271, 1583.690, 1584.108, 1584.527, 1584.946, 1585.365, 1585.784, 1586.203, 1586.623, 1587.043, 1587.463, 1587.884, 1588.304, 1588.725, 1589.146, 1589.568, 1589.989, 1590.411, 1590.833, 1591.255, 1591.678, 1592.100, 1592.523, 1592.946, 1593.369, 1593.793, 1594.217, 1594.641, 1595.065, 1595.489, 1595.914, 1596.339, 1596.764, 1597.189, 1597.615, 1598.041, 1598.467, 1598.893, 1599.320, 1599.746, 1600.173, 1600.600, 1601.028, 1601.455, 1601.883, 1602.311, 1602.740, 1603.168, 1603.597, 1604.026, 1604.455, 1604.885, 1605.314, 1605.744, 1606.174, 1606.605, 1607.035, 1607.466

Trace information

In the **Trace Information** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Expected trail trace out format	Specifies the expected trail trace out format on a STM-16/OC48 port in transparent mode.	Depending on the port and signal type, a subset of the following: <ul style="list-style-type: none"> • <i>1</i>: non-specific byte – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • <i>2</i>: specific byte (1-byte string) – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). • <i>16</i>: 16-byte string – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • <i>64</i>: 64-byte string – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).
Transmitted trail trace value	If the <i>Expected trail trace out format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the expected character string is set here. The field name is a hyperlink. Click it to open a window where you can enter the desired string.	
Trail trace out mismatch detection mode	Controls the RS TIM out monitor (SDH) or the section TIM out monitor (SONET), respectively, on a STM-16/OC48 port in transparent mode.	<i>enable, disable.</i>

Parameter	Function	Possible values
Transmitted trail trace format	Selects the format of the transmitted trail trace identifier (TTI).	Depending on the port and signal type, a subset of the following: <ul style="list-style-type: none"> • <i>non-specific byte</i> – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • <i>specific byte (1-byte string)</i> – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). • <i>16-byte string</i> – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • <i>64-byte string</i> – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).
Transmitted trail trace value	If the <i>transmitted trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the transmitted character string is set here. Since the possible values depend on the setting of the <i>transmitted trace display mode</i> parameter, it is recommended to set that parameter in advance. The field name is a hyperlink. Click it to open a window where you can enter the desired string.	
Transmitted trace display mode	If the <i>transmitted trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the format of the transmitted character string is set here.	<i>ascii, hex.</i>

Parameter	Function	Possible values
Expected trail trace format	Selects the format of the expected trail trace identifier (TTI).	Depending on the port and signal type, a subset of the following: <ul style="list-style-type: none"> • <i>non-specific byte</i> – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • <i>specific byte (1-byte string)</i> – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). • <i>16-byte string</i> – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • <i>64-byte string</i> – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).
Expected trail trace value	If the <i>expected trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the transmitted character string is set here. Since the possible values depend on the setting of the <i>expected trace display mode</i> parameter, it is recommended to set that parameter in advance. The field name is a hyperlink. Click it to open a window where you can enter the desired string.	
Expected trace display mode	If the <i>expected trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the format of the expected character string is set here.	<i>ascii, hex.</i>
Accepted trace display mode	Sets the format of the accepted character string.	<i>ascii, hex.</i>
Trail trace mismatch detection mode	Controls the detection mode.	<i>enabled, disabled.</i>
Consequent action on trail trace mismatch	Enables / disables consequent action in case of a trace identifier mismatch detection. For SDH: Note that this function is only supported if the related trace read format is set to <i>16-byte string</i> .	<i>enabled, disabled.</i>
Signal label mismatch detection mode	Controls the signal label mismatch detection for VC-4 or STS-1 ports.	<i>enable, disable.</i>

Timing

In the **Timing** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
ForceDNU	<i>Force DNU</i> allows to force an S1 byte value <i>DNU</i> into an outgoing signal. When an outgoing signal is forced to carry DNU, this signal cannot be used for synchronization by another NE.	<i>enable, disable.</i>

Fault management

In the **Fault Management** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Alarm profile name	The name of a pre-defined alarm severity assignment profile (ASAP) to be used for the port in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.	1 to 24 characters.
Signal degrade/signal fail mode	Sets the preferred mode of bit error monitoring to monitor the bit error performance during transmission.	<ul style="list-style-type: none"> <i>burst</i> – this mode of bit error monitoring means that a bursty distribution of bit errors is presumed (default setting for SDH ports). <i>poisson</i> – this mode of bit error monitoring means that a random (“Poisson”) distribution of bit errors is presumed (default setting for SONET ports). Tooltip: For an STS1 on an EC1, the value is fixed to poisson. Info: For EP51 (modifier: STS)
Bursty error threshold (%)	Defines the threshold value for bursty errors. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “burst”.	Integer in the range from 0 to 50 in steps of 5.
Bursty interval (sec)	Defines the measurement interval for bursty errors. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “burst”.	Integer in the range from 2 to 10.

Parameter	Function	Possible values
REI mode	Specifies the MS remote error indication (REI) mode.	<i>Single</i> – provision is made for interworking with older equipment (only the M1 byte is used for the remote error indication). <i>Extended</i> – no provision is made for interworking with older equipment (the M0 byte and the M1 byte are used for the remote error indication).
Signal degrade threshold (10 Exp)	Sets the signal degrade threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before a Degraded Signal alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “poisson”.	Integer in the range from –5 to –9.
Signal fail threshold (10 Exp)	Sets the signal fail threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before an Excessive Bit Error Ratio alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “poisson”.	Integer in the range from –3 to –5.
Forward error correction	Depending on the port capabilities, this parameter specifies the NE to include the Forward Error Correction (FEC) information in the outgoing signal. Modifying the FEC parameters during operation may be traffic affecting. Therefore, it is recommended to configure all FEC parameters prior to putting the corresponding port unit into operation and leave them unchanged during operation.	<i>enable, disable.</i>
Forward error correction scrambling polynomial	Specifies the polynomial used by the <i>WaveWrapper</i> TM scrambler on the Optical Channel (OCh) to generate a pseudo random binary sequence (PRBS) for STM-64 and OC-192 ports. The FEC Scrambling Polynomial is of special importance for the interworking with wavelength division multiplexing (WDM) systems (such as <i>WaveStar</i> [®] OLS 1.6T or <i>LambdaXtreme</i> TM). It is relevant only if the FEC Type is Out-Band , and the Optical Channel is enabled.	Possible values are: <ul style="list-style-type: none"> $1 - x^7 + x + 1$ (acc. to ITU-T Rec. G.975) $2 - x^{16} + x^{12} + x^3 + x + 1$ (acc. to ITU-T Rec. G.709)

Performance management

In the **Performance** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
TCA reset mode	Specifies the TCA mode.	<i>TRRTR</i> – implicit reset method, also known as transient condition method, for SDH and Ethernet ports only. <i>TR</i> – explicit reset method, also known as standing condition method.
Near-end PM	Controls the near-end path performance monitoring.	<i>enable, disable.</i>
Far-end PM	Controls the far-end path performance monitoring.	<i>enable, disable.</i>
Pointer justification event PM enable	Controls the pointer justification event PM monitor.	<i>enable, disable.</i>
Incoming PM enable	Controls the DS3 incoming performance monitoring.	<i>enable, disable.</i>
Outgoing PM enable	Controls the DS3 outgoing performance monitoring.	<i>enable, disable.</i>
Far-end incoming path PM enable	Controls the incoming DS3 far-end path performance monitoring.	<i>enable, disable.</i>
Far-end outgoing path PM enable	Controls the outgoing DS3 far-end path performance monitoring.	<i>enable, disable.</i>
Incoming line PM enable	Controls the DS3 incoming line performance monitoring.	<i>enable, disable.</i>
Section/RS PM enable	Controls the performance monitoring on regenerator section level (SDH) or section level (SONET), respectively.	<i>enable, disable.</i>
Section/RS out PM enable	Controls the performance monitoring (outgoing) on STM-16 regenerator section level (SDH) or OC-48 section level (SONET), respectively, for transparent services.	<i>enable, disable.</i>
Near-end line/MS PM	Controls the near-end performance monitoring on multiplex section level (SDH) or line level (SONET), respectively.	<i>enable, disable.</i>
Far-end line/MS PM enable	Controls the far-end performance monitoring on multiplex section level (SDH) or line level (SONET), respectively.	<i>enable, disable.</i>
Near-end path SES threshold	Specifies the near-end path SES threshold.	The range of possible values depends on the port rate and the plug-in unit used.

Parameter	Function	Possible values
Far-end path SES threshold	Specifies the far-end path SES threshold.	The range of possible values depends on the port rate and the plug-in unit used.
Incoming line SES threshold	Specifies the SES threshold (errors in a second) for incoming DS3 lines.	Integer in the range from 1 to 8000.
Incoming path SES threshold	Specifies the SES threshold (errors in a second) for incoming DS3 paths.	Integer in the range from 1 to 8000.
Far-end path SES threshold	Specifies the far-end SES threshold (errors in a second) for DS3 paths.	Integer in the range from 1 to 8000.
PM section/RS near-end SES threshold	Specifies the near-end SES threshold on regenerator section level (SDH) or section level (SONET), respectively.	Integer in the range from 1 to 64000.
PM section/RS near-end out SES threshold	Specifies the near-end outgoing SES threshold on STM-16 regenerator section level (SDH) or OC-48 section level (SONET), respectively, for transparent services.	The range of possible values depends on the port rate.
Near-end line/MS SES threshold	Specifies the near-end SES threshold on multiplex section level (SDH) or line level (SONET), respectively.	The range of possible values depends on the port rate.
PM line/MS far-end SES threshold	Specifies the far-end SES threshold (errors in a second) on multiplex section level (SDH) or line level (SONET), respectively.	The range of possible values depends on the port rate.
Far-end outgoing path SES PM threshold	Specifies the far-end SES threshold (errors in a second) for outgoing DS3 paths.	Integer in the range from 1 to 8000.
Outgoing path SES PM threshold	Specifies the SES threshold (errors in a second) for outgoing DS3 paths.	Integer in the range from 1 to 8000.

Parameter	Function	Possible values
TCA profile name	<p>Specifies the name of a pre-defined threshold crossing alert (TCA) profile to be used for the port in question. The TCA profiles are used to store the threshold values of the performance parameters related to a specific parameter group.</p> <p>TCA profiles exist for these groups of performance parameters:</p> <ul style="list-style-type: none"> Parameters related to the SDH Regenerator Section and Multiplex Section Parameters related to the SONET Section and Line Parameters related to SDH and SONET tributaries (including VCG tributaries) Parameters related to Ethernet and VCG ports Parameters related to transparent services (Optical Data Unit, ODU1) <p>A default profile (“DEFAULT”) is predefined for each of these TCA profile types.</p>	1 to 24 characters.
Physical TCA profile name	Specifies the name of the “Physical” TCA profile.	1 to 24 characters.
Reported payload type	Specifies the reported payload type for for transparent services on STM-16 (SDH) or OC-48 (SONET), respectively.	Two hexadecimal digits.

Control plane

In the **Control Plane** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Network interface	The port class of an ONNS capable port.	<i>None</i> – traditional; <i>CustomerClient</i> – Edge; <i>InternalNetwork</i> – internal network-to-network interface (iNNI); <i>UserNetworkInterface</i> – UNI; external network-to-network interface (eNNI)

Parameter	Function	Possible values
UNI network TNA type	The type of transport network assigned (TNA) address used for UNI ports.	<i>IPV4</i> – an IPv4, a 4-byte address represented by four dot-separated decimal values, each in the range from 0 to 255; <i>IPV6</i> – an IPv6 address, a 16-byte address represented by eight dash-separated hexadecimal values; <i>NSAP</i> – an NSAP address, a 20-byte address represented by a hexadecimal value.
UNI network TNA address	The value of the transport network assigned (TNA) address of the selected UNI port. The value depends on the type of TNA.	Depends on the UNI network TNA type.
UNI network logical port identifier	Unique identifier for a single UNI port within a TNA address	Integer in the range from 0 to 4294967295.
UNI client node identiy	The IP address of the client node of the UNI port.	Four dot-separated integer values, each in the range from 0 to 255.
ASTN propagation delay (msec)	Automatically switched transport network (ASTN) propagation delay value for iNNI ports.	Integer in the range from 0 to 255.
Cost	Administrative cost for iNNI ports.	Integer in the range from 0 to 65535.
Shared risk link group	Shared risk link groups ID list for iNNI ports. Shared risk link groups are groups of port connections that share the same risk. For instance: port connections that terminate on the same card, in the same network element or that share the same fiber duct.	A list of strings “N-N-N” or “N-N-N-N-N-N-N-N-N” where <i>N</i> is an integer in the range from 0 to 65535, step by 1.
Minimum NN crossconnect rate	For iNNI ports: the minimum cross-connect rate implemented by the switch fabric and the port/channels in the link bundle. This represents the minimum concatenated signal sub-rate at which the port can multiplex or demultiplex. The minimum NN cross-connect rate cannot be greater than the maximum NN cross-connect rate.	Depending on the port type, the following values are possible: <ul style="list-style-type: none"> VC3, VC4, VC44C, VC416C, VC-464C (SDH) STS1, STS3, STS12, STS48, STS192 (SONET).
Maximum NN crossconnect rate	For iNNI ports: the maximum cross-connect rate implemented by the switch fabric and the port/channels in the link bundle. This represents the minimum concatenated signal sub-rate at which the port can multiplex or demultiplex. The maximum NN cross-connect rate cannot be smaller than the minimum NN cross-connect rate.	Depending on the port type, the following values are possible: <ul style="list-style-type: none"> VC3, VC4, VC44C, VC416C, VC-464C (SDH) STS1, STS3, STS12, STS48, STS192 (SONET).



Parameters for Ethernet ports

Introduction

This section lists the parameters that can be modified for Ethernet ports. Note that not all parameters and possible values apply to all port types, plug-in units, and network element configurations.

For a number of parameters, the network elements can report the value *not applicable*. This value is for information purposes only, it cannot be entered.

Transmission

In the **Transmission** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Port mode	Indicates the monitoring state of the specified port.	Depending on the port rate and type the following values are possible: <ul style="list-style-type: none"> • <i>on</i> – the port is being monitored. • <i>auto</i> – the port is ready to transition into a monitored state, when a signal is detected. • <i>off</i> – the port is not being monitored.
Service condition	The status of the port concerning service involvement.	<ul style="list-style-type: none"> • <i>in service</i> – provisioning values for service will be accepted. • <i>out of service</i> – provisioning values for service will not be accepted.
Link pass thru mode	Controls the consequent action upon the receipt of a client signal fail (CSF) indication.	<i>Enable</i> – the receipt of CSF causes the laser to be switched off (this is the default setting); <i>Disable</i> – the laser will <i>not</i> be switched off upon the receipt of CSF.
Provisioned pause mode	The applicable pause mode.	<i>enable, disable.</i>
Provisioned flow control mode	Specify the configuration for the pause operation.	Depending on the type of plug-in unit used, possible values are: <i>auto, disable, asyntopartner, asyntolocal, sym.</i>
Auto negotiation mode	Controls the autonegotiation mode.	<i>enable, disable.</i>
Default user priority	The default priority for the port.	<i>high, low.</i>

Fault management

In the **Fault Management** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Alarm profile name	The name of a pre-defined alarm severity assignment profile (ASAP) to be used for the port in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.	1 to 24 characters.
Signal degrade threshold (10 Exp)	Sets the signal degrade threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before a Degraded Signal alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is "poisson".	Integer in the range from -5 to -9.
Signal fail threshold (10 Exp)	Sets the signal fail threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before an Excessive Bit Error Ratio alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is "poisson".	Integer in the range from -3 to -5.

Performance management

In the **Performance** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
TCA reset mode	Specifies the TCA mode.	<i>TRRTR</i> – implicit reset method, also known as transient condition method, for SDH and Ethernet ports only. <i>TR</i> – explicit reset method, also known as standing condition method.
Performance monitoring	Controls the performance monitoring.	<i>enable, disable.</i>
Near-end PM	Controls the near-end path performance monitoring.	<i>enable, disable.</i>
Far-end PM	Controls the far-end path performance monitoring.	<i>enable, disable.</i>

Parameter	Function	Possible values
TCA profile name	<p>Specifies the name of a pre-defined threshold crossing alert (TCA) profile to be used for the port in question. The TCA profiles are used to store the threshold values of the performance parameters related to a specific parameter group.</p> <p>TCA profiles exist for these groups of performance parameters:</p> <ul style="list-style-type: none"> Parameters related to the SDH Regenerator Section and Multiplex Section Parameters related to the SONET Section and Line Parameters related to SDH and SONET tributaries (including VCG tributaries) Parameters related to Ethernet and VCG ports Parameters related to transparent services (Optical Data Unit, ODU1) <p>A default profile (“DEFAULT”) is predefined for each of these TCA profile types.</p>	1 to 24 characters.

Spanning tree

In the **Spanning Tree** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
STP port priority	The priority of the port for the spanning tree protocol.	Integer in the range from 0 to 255.
Port path cost	The port path cost. For a port with the spanning tree protocol active, this parameter defines the contribution of this port to the path cost of paths towards the spanning tree root which included this port.	Integer in the range from 1 to 200000000.

Port path cost details

According to IEEE 802.1Q 1998, this parameter should be related to the bandwidth of the link in which the port participates. Link speed is mapped to port path costs as follows:

Link speed	Path cost
2 Mbps	10,000,000
4 Mbps	5,000,000
6 Mbps	3,400,000
8 Mbps	2,500,000
10 Mbps	2,000,000
50 Mbps	400,000
100 Mbps	200,000
1 Gbps	20,000
10 Gbps	2,000



Parameters for VCG ports

Introduction

This section lists the parameters that can be modified for VCG ports. Note that not all parameters and possible values apply to all port types, plug-in units, and network element configurations.

For a number of parameters, the network elements can report the value *not applicable*. This value is for information purposes only, it cannot be entered.

Transmission

In the **Transmission** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Port mode	Indicates the monitoring state of the specified port.	Depending on the port rate and type the following values are possible: <ul style="list-style-type: none"> • <i>on</i> – the port is being monitored. • <i>auto</i> – the port is ready to transition into a monitored state, when a signal is detected. • <i>off</i> – the port is not being monitored.
Input membership	Specifies whether the tributary shall take part in the transmission of its owning VCG in input direction.	<i>enable, disable.</i>
Output membership	Specifies whether the tributary shall take part in the transmission of its owning VCG in output direction.	<i>enable, disable.</i>
LCAS mode	The operation mode of the link capacity adjustment scheme (LCAS) for this VCG.	<i>on, off.</i>
LCAS hold-off time (ms)	The LCAS hold-off time. If a tributary is configured to be a member of the VCG, and a fault is detected for that tributary, then it is taken out of transmission by LCAS after the hold off time. By means of different hold-off times, it can be defined which protection should switch first. The hold-off time is configured on group level, that means all tributaries of a VCG have the same hold-off time.	Integer in the range from 0 to 10000 in steps of 100, and 99999.

Parameter	Function	Possible values
LCAS wait to restore time (min)	The LCAS wait-to-restore (WTR) time. If a tributary is configured to be a member of the VCG, and that tributary recovers from a faulty state then it is taken in again to transmission by LCAS after the wait-to-restore time. The wait-to-restore time is configured on group level, that means all tributaries of a VCG have the same wait-to-restore time.	Integer in the range from 0 to 60.
Consequent action mode	The consequent action to be taken in the egress direction (towards the synchronous port) in case a signal fail condition is detected on the ODU layer (STM-16 or OC-48).	<i>genericais</i> – generic AIS; <i>msais</i> – MS-AIS; <i>laseroff</i> – laser off.
Default user priority	The default priority for the port.	<i>high</i> , <i>low</i> .

Trace information

In the **Trace Information** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Transmitted trail trace format	Selects the format of the transmitted trail trace identifier (TTI).	Depending on the port and signal type, a subset of the following: <ul style="list-style-type: none"> <i>non-specific byte</i> – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). <i>specific byte (1-byte string)</i> – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). <i>16-byte string</i> – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). <i>64-byte string</i> – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).

Parameter	Function	Possible values
Transmitted trail trace value	<p>If the <i>transmitted trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i>, <i>16-byte string</i>, or <i>64-byte string</i>, the transmitted character string is set here. Since the possible values depend on the setting of the <i>transmitted trace display mode</i> parameter, it is recommended to set that parameter in advance.</p> <p>The field name is a hyperlink. Click it to open a window where you can enter the desired string.</p>	
Transmitted trace display mode	<p>If the <i>transmitted trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i>, <i>16-byte string</i>, or <i>64-byte string</i>, the format of the transmitted character string is set here.</p>	<i>ascii</i> , <i>hex</i> .
Expected trail trace format	<p>Selects the format of the expected trail trace identifier (TTI).</p>	<p>Depending on the port and signal type, a subset of the following:</p> <ul style="list-style-type: none"> • <i>non-specific byte</i> – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • <i>specific byte (1-byte string)</i> – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). • <i>16-byte string</i> – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • <i>64-byte string</i> – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).
Expected trail trace value	<p>If the <i>expected trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i>, <i>16-byte string</i>, or <i>64-byte string</i>, the transmitted character string is set here. Since the possible values depend on the setting of the <i>expected trace display mode</i> parameter, it is recommended to set that parameter in advance.</p> <p>The field name is a hyperlink. Click it to open a window where you can enter the desired string.</p>	

Parameter	Function	Possible values
Expected trace display mode	If the <i>expected trail trace format</i> parameter is set to <i>specific byte (1-byte string)</i> , <i>16-byte string</i> , or <i>64-byte string</i> , the format of the expected character string is set here.	<i>ascii, hex.</i>
Expected trail trace out format	Specifies the accepted trail trace format.	Depending on the port and signal type, a subset of the following: <ul style="list-style-type: none"> • <i>1</i>: non-specific byte – a single byte with a fixed hexadecimal value of 0x00 (ITU/ETSI mode 2). • <i>2</i>: specific byte (1-byte string) – a single byte (hexadecimal format using the printable T.50/ASCII character set) (SONET mode). • <i>16</i>: 16-byte string – a 16-bytes hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7 (ITU/ETSI mode 1). • <i>64</i>: 64-byte string – a 64-bytes hexadecimal format using the printable T.50/ASCII character set, with the last two bytes being a carriage return, line feed (SONET).
Trail trace mismatch detection mode	Controls the detection mode.	<i>enabled, disabled.</i>
Consequent action on trail trace mismatch	Enables / disables consequent action in case of a trace identifier mismatch detection. For SDH: Note that this function is only supported if the related trace read format is set to <i>16-byte string</i> .	<i>enabled, disabled.</i>

Fault management

In the **Fault Management** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Alarm profile name	The name of a pre-defined alarm severity assignment profile (ASAP) to be used for the port in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.	1 to 24 characters.

Parameter	Function	Possible values
Transparent alarm profile name	The alarm severity assignment profile (ASAP) of type “Fully Transparent Service” assigned to that VCG. This may be either the default ASAP or any other previously defined ASAP of that type.	1 to 24 characters.
Signal degrade/signal fail mode	Sets the preferred mode of bit error monitoring to monitor the bit error performance during transmission.	<ul style="list-style-type: none"> • <i>burst</i> – this mode of bit error monitoring means that a bursty distribution of bit errors is presumed (default setting for SDH ports). • <i>poisson</i> – this mode of bit error monitoring means that a random (“Poisson”) distribution of bit errors is presumed (default setting for SONET ports).
Bursty error threshold (%)	Defines the threshold value for bursty errors. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “burst”.	Integer in the range from 0 to 50 in steps of 5.
Bursty interval (sec)	Defines the measurement interval for bursty errors. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “burst”.	Integer in the range from 2 to 10.
Signal degrade threshold (10 Exp)	Sets the signal degrade threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before a Degraded Signal alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “poisson”.	Integer in the range from –5 to –9.
Signal fail threshold (10 Exp)	Sets the signal fail threshold, the value is an exponent of 10. It defines the bit error ratio (BER) that must be exceeded before an Excessive Bit Error Ratio alarm is reported. This parameter can only be set if the <i>signal degrade/signal fail mode</i> is “poisson”.	Integer in the range from –3 to –5.

Performance management

In the **Performance** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
TCA reset mode	Specifies the TCA mode.	<i>TRRTR</i> – implicit reset method, also known as transient condition method, for SDH and Ethernet ports only. <i>TR</i> – explicit reset method, also known as standing condition method.
Performance monitoring	Controls the performance monitoring.	<i>enable, disable.</i>
Near-end VCG PM	The near-end path performance monitoring activation status.	<i>enable, disable.</i>
Far-end VCG PM	The far-end path performance monitoring activation status.	<i>enable, disable.</i>
Near-end PM	Controls the near-end path performance monitoring.	<i>enable, disable.</i>
Far-end PM	Controls the far-end path performance monitoring.	<i>enable, disable.</i>
Near-end vcg SES threshold	The VCG near-end path SES declaration threshold indicating the number of errored blocks (SDH) or code violations (SONET) per second to declare a second severely errored.	Integer in the range from 1 to 163360.
Far-end vcg SES threshold	The VCG far-end path SES declaration threshold indicating the number of errored blocks (SDH) or code violations (SONET) per second to declare a second severely errored.	Integer in the range from 1 to 163360.
Near-end path SES threshold	Specifies the near-end path SES threshold.	The range of possible values depends on the port rate and the plug-in unit used.
Far-end path SES threshold	Specifies the far-end path SES threshold.	The range of possible values depends on the port rate and the plug-in unit used.

Parameter	Function	Possible values
TCA profile name	<p>Specifies the name of a pre-defined threshold crossing alert (TCA) profile to be used for the port in question. The TCA profiles are used to store the threshold values of the performance parameters related to a specific parameter group.</p> <p>TCA profiles exist for these groups of performance parameters:</p> <ul style="list-style-type: none"> Parameters related to the SDH Regenerator Section and Multiplex Section Parameters related to the SONET Section and Line Parameters related to SDH and SONET tributaries (including VCG tributaries) Parameters related to Ethernet and VCG ports Parameters related to transparent services (Optical Data Unit, ODU1) <p>A default profile (“DEFAULT”) is predefined for each of these TCA profile types.</p>	1 to 24 characters.

Control plane

In the **Control Plane** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
Network interface	The port class of an ONNS capable port.	<i>None</i> – traditional; <i>CustomerClient</i> – Edge; <i>InternalNetwork</i> – internal network-to-network interface (iNNI); <i>UserNetworkInterface</i> – UNI
UNI network TNA type	The type of transport network assigned (TNA) address used for UNI ports.	<i>IPV4</i> – an IPv4, a 4-byte address represented by four dot-separated decimal values, each in the range from 0 to 255]; <i>IPV6</i> – an IPv6 address, a 16-byte address represented by eight dash-separated hexadecimal values; <i>NSAP</i> – an NSAP address, a 20-byte address represented by a hexadecimal value.

Parameter	Function	Possible values
UNI network TNA address	The value of the transport network assigned (TNA) address of the selected UNI port. The value depends on the type of TNA.	Depends on the UNI network TNA type.
UNI network logical port identifier	Unique identifier for a single UNI port within a TNA address	Integer in the range from 0 to 4294967295.
UNI client node identiy	The IP address of the client node of the UNI port.	Four dot-separated integer values, each in the range from 0 to 255.

Spanning tree

In the **Spanning Tree** section of the **Port** page, the following parameters can be modified:

Parameter	Function	Possible values
STP port priority	The priority of the port for the spanning tree protocol.	Integer in the range from 0 to 255.
Port path cost	The port path cost. For a port with the spanning tree protocol active, this parameter defines the contribution of this port to the path cost of paths towards the spanning tree root which included this port.	Integer in the range from 1 to 200000000.

Port path cost details

According to IEEE 802.1Q 1998, this parameter should be related to the bandwidth of the link in which the port participates. Link speed is mapped to port path costs as follows:

Link speed	Path cost
2 Mbps	10,000,000
4 Mbps	5,000,000
6 Mbps	3,400,000
8 Mbps	2,500,000
10 Mbps	2,000,000
50 Mbps	400,000
100 Mbps	200,000
1 Gbps	20,000
10 Gbps	2,000



Provisioning of NE event controls

To inhibit the forwarding of autonomous messages

When to use

Use this task to inhibit the forwarding of autonomous messages on the user session or per system. Autonomous messages are messages which are provided by the system itself without a trigger via the management interface (for example alarms, switch reports)

Related information

For a more detailed explanation, please refer to the description of the INH-MSG command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Network Elements**.
 4. In the **Function** field, select **Inhibit Message**.
 5. Click **Go**.

Result: The **Inhibit Message** page is displayed.

- 3 In the **Affected sessions** field, select *Current* to inhibit messages for the current session.

-
- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To allow the forwarding of autonomous messages

When to use

Use this task to allow the forwarding of autonomous messages on the user session or per system. Autonomous messages are messages which are provided by the system itself without a trigger via the management interface (for example alarms, switch reports)

Related information

For a more detailed explanation, please refer to the description of the ALW-MSG-ALL command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Network Elements**.
 4. In the **Function** field, select **Allow All Messages**.
 5. Click **Go**.

Result: The **Allow All Messages** page is displayed.

- 3 In the **Affected sessions** field, select *Current* to allow messages for the current session.
-

- 4 *Optional, for expert users only:* The **NE Command panel** may be used to edit the native command language of the function.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



Provisioning of MDIs and MDOs

To retrieve the MDO configuration

When to use

Use this task to to retrieve the configuration associated with a miscellaneous output control (MDO).

Related information

For a more detailed explanation, please refer to the description of the RTRV-ATTR-CONT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **External Control and Monitoring Points**.
4. In the **Function** field, select **Retrieve Attribute Control**.
5. Click **Go**.

Result: The **Retrieve Attribute Control** page is displayed.

3 In the field **Port Identifier**, select either a single MDO (*misc_out1* to *misc_out8*) or *misc_outall* to retrieve information for all MDOs at once.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

- aid – access identifier
Indicates the MDO to which the information relates.
- contmsg – control message
This is the name associated to a MDO (environmental control).
- durmode – duration mode
Defines in which mode the device connected to the MDO is expected to be operated. It is a fixed value because this feature will be not supported by the system. This parameter is in for compatibility reason.
Range: CONTS (continuous duration)
- initcstat – initial control state
This value is always “RLS” (release). This parameter is in for compatibility reason.
- asgncond – assigned condition type
This parameter identifies the probable cause (type of alarm indication) which is assigned to an MDO. If one or more alarm(s) of this probable cause appears, then the MDO will be switched on.
The value “UNDEF” indicates that no probable cause is assigned.

END OF STEPS



To set the MDO configuration

When to use

Use this task to set the description associated with a miscellaneous output (MDO). This way you set the value that identifies the probable cause (type of alarm indication) which is assigned to an MDO.

Related information

For a more detailed explanation, please refer to the description of the SET-ATTR-CONT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Set Attribute Control**.
 5. Click **Go**.

Result: The **Set Attribute Control** page is displayed.

- 3** Change the entries or selections for any modifiable fields that you wish to update.
- **Port Identifier** – select a single MDO (*misc_out1* to *misc_out8*).
 - **Control message** – enter a string of up to 26 characters which must be surrounded by double quotes. The string will be used as name associated to the respective MDO. The string can consist of any lower-case or upper-case characters except double quotes and backslash.
 - **Assigned condition type** – Enter a valid condition type defined for the NE preceded by a comma. The value identifies the probable cause (type of alarm indication) which is assigned to an MDO. If one or more alarm(s) of this probable cause appears then the MDO will be switched on. Example “,LOS”. If the value is omitted, then the actual value will not be changed.
Range: All defined probable causes and “UNDEF:” if no probable cause is assigned.
-

- 4** Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To switch on an MDO

When to use

Use this task to to switch on (operate) a miscellaneous output control (MDO).

Related information

For a more detailed explanation, please refer to the description of the OPR-EXT-CONT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Operate External Control**.
 5. Click **Go**.

Result: The **Operate External Control** page is displayed.

- 3 In the field **Port Identifier**, select the MDO to switch on (*misc_out1* to *misc_out8*).
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To switch off an MDO

When to use

Use this task to switch off (release) a miscellaneous output control (MDO).

Related information

For a more detailed explanation, please refer to the description of the RLS-EXT-CONT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Release External Control**.
 5. Click **Go**.

Result: The **Release External Control** page is displayed.

- 3 In the field **Port Identifier**, select the MDO to switch off (*misc_out1* to *misc_out8*).
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To retrieve the MDO state

When to use

Use this task to retrieve of a single miscellaneous output control (MDO) or all MDOs.

Related information

For a more detailed explanation, please refer to the description of the RTRV-EXT-CONT command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Retrieve External Control**.
 5. Click **Go**.

Result: The **Retrieve External Control** page is displayed.

- 3 In the field **Port Identifier**, select the MDO for which the information should be retrieved (*misc_out1* to *misc_out8*). To retrieve information for all MDOs, leave the field empty or select the value *misc_outall*.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

- aid – access identifier
Indicates the MDO to which the information relates.
- dur – duration
Defines in which mode the device connected to the MDO is expected to be operated. It is a fixed value because this feature will be not supported by the system. This parameter is in for compatibility reason.
Range: *CONTS* (continuous duration).
- contstate – control state
The current state of the MDO.
Range:
 - *OPER* – operated, that means the MDO is switched on.
 - *RLS* – released, that means the MDO is switched off.

END OF STEPS



To retrieve the MDI configuration

When to use

Use this task to retrieve the alarm message, name, and assigned ASAP of a single miscellaneous discrete input (MDI) or all MDIs.

Related information

For a more detailed explanation, please refer to the description of the RTRV-ATTR-ENV command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Retrieve Attribute Environment**.
 5. Click **Go**.

Result: The **Retrieve Attribute Environment** page is displayed.

- 3 In the field **Port Identifier**, select the MDI for which the information should be retrieved (*misc_in1* to *misc_in8*). To retrieve information for all MDIs, leave the field empty or select the value *misc_inall*.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The output parameters for this function are:

- aid – access identifier
Indicates the MDI to which the information relates.
- envinv – environmental alarm inversion
Indicates for the MDI whether an alarm shall be generated if the port is on or if the port is off.
Range:
 - *YES* – the alarm will be inverted.
 - *NO* – the alarm will not be inverted.
- envmsg – environment message
The condition description which is associated with the MDI. This description will be sent with the alarm generated from the MDI port.
- envname – environmental point name
The name associated to an MDI. It is a description which can be retrieved by the management system. It is not to be mixed up with the envmsg parameter. The envname is just a name of the MDI port and not reported via the condition description of an alarm.
- pfname – profile name
The name of the alarm severity assignment profile (ASAP) that is assigned to the MDI.

END OF STEPS

□

To set the MDI configuration

When to use

Use this task to set the alarm message, the name, and the assigned alarm severity assignment profile (ASAP) of a miscellaneous discrete input (MDI).

Related information

For a more detailed explanation, please refer to the description of the SET-ATTR-ENV command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **External Control and Monitoring Points**.
 4. In the **Function** field, select **Set Attribute Environment**.
 5. Click **Go**.

Result: The **Set Attribute Environment** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **Port identifier** – select a single MDI (*misc_in1* to *misc_in8*).
 - **Alarm message** – enter a string of up to 32 characters which must be surrounded by double quotes. This is the condition description which is associated with the MDI. This description will be sent with the alarm generated from the MDI. The string can consist of any lower-case or upper-case characters except double quotes and backslash.

- **Point name** – enter a string of up to 26 characters which must be surrounded by double quotes. This is the name associated to an MDI. It is a description which can be retrieved by the management system. It is not to be mixed up with the alarm message parameter. The point name is just a name of the MDI port and not reported via the condition description of an alarm. The string can consist of any lower-case or upper-case characters except double quotes and backslash.
 - **Environmental alarm inversion** – indicates for the MDI whether an alarm shall be generated if the port is on or if the port is off.
Range:
 - *Invert alarm* – the alarm will be inverted.
 - *Do not invert alarm* – the alarm will not be inverted.
 - **Profile name** – the name of the alarm severity assignment profile (ASAP) that is assigned to the MDI. The ASAP must be of the type *ENV*. Range: up to 24 characters.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



Equipment protection

To retrieve equipment protection group information

When to use

Use this task to retrieve information related to a single equipment protection group or to all equipment protection groups.

Related information

For a more detailed explanation, please refer to the description of the RTRV-PROTN-GRP command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE. If you selected the target NE in the previous step, this field is already populated with your selection.
 2. In the **NE name** field, select the name of the target NE. If you selected the target NE in the previous step, this field is already populated with your selection.
 3. In the **Category** field, select **Protection Groups**.
 4. In the **Function** field, select **Retrieve Protection Group - 1+1 Equipment Protection Group**.
 5. Click **Go**.

Result: The **Retrieve Protection Group - 1+1 Equipment Protection Group** page is displayed.

- 3 In the field **Protection group identifier**, enter the ID of the protection group for which the information should be retrieved. In the field **Protection type**, select a type of equipment protection group.

The following table shows the possible combinations:

Type of equipment protection	Value for Protection group identifier	Value for Protection type
All	<i>1-1-eall</i>	ALL
High order switch fabric and timing	<i>1-1-estgrp</i>	Switch Fabric
System controller	<i>1-1-ectlgrp</i>	System Controller
Electrical 51 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP51 Circuit Pack
Electrical 155 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP155 Circuit Pack
Low order switch fabric	<i>1-1-eloxc1</i> The last character of this identifier is the digit one.	LOXC Circuit Pack

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

- 5 The output parameters for this function are:

- **aid** – access identifier
Specifies the 1+1 protection equipment group.
- **actunit** – active unit state
This value specifies which unit is currently selected within the protection group as active unit. The value *WKG* specifies that the worker unit is active. The value *PROTN* specifies that the protection unit is active.
- **protn** – protection unit
Specifies the protection circuit pack AID being a member of the 1+1 equipment protection group.

- *protnsiglvl* – protection fault status
Specifies the current fault status of the protection unit as used by the protection state machine. The value *EF* (equipment failed) is used if an equipment defect used as switch criteria is currently present for the protection unit. The value *NONE* is used if no such defect is currently present.
- *protype* – protection type
Specifies the type of the protection group.
Range:
 - *EQPTSWFBR* – high order switch fabric and timing protection
 - *EQPTCT*, – system controller protection
 - *EQPTEP155* – electrical 155 Mbps interfaces protection
 - *EQPTEP51* – electrical 51 Mbps interfaces protection
 - *EQPTLOXC* – low order switch fabric protection
- *swreq* – switch request state
Specifies the current switch request state of the protection state machine. The value *EQPTFAILED* (equipment failed) is used if an equipment failed condition is the current state. The value *FS* (forced switch) is used if a forced switch is the current state. The value *MS* (manual switch) is used if a manual switch is the current state. The value *NR* (no request) is used if no request is the current state.
- *wkg* – worker unit
Specifies the worker circuit pack AID being a member of the 1+1 equipment protection group.
- *wkgsiglvl* – worker fault status
Specifies the current fault status of the worker unit as used by the protection state machine. The value *EF* (equipment failed) is used if an equipment defect used as switch criteria is currently present for the worker unit. The value *NONE* is used if no such defect is currently present.

.....
 END OF STEPS



To add an equipment protection group

When to use

Use this task to add an equipment protection group.

You can add the following types of equipment protection groups:

- Electrical 51 Mbps interfaces protection
- Electrical 155 Mbps interfaces protection
- Lower-order switch fabric protection

The system automatically creates the following types of equipment protection groups:

- Higher-order switch fabric and timing protection
- System controller protection

Related information

For a more detailed explanation, please refer to the description of the ENT-PROTN-GRP command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Detailed configuration rules for equipment protection groups are also part of the LambdaUnite® *MSS User Operations Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.
 - 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Protection Groups**.
 4. In the **Function** field, select **Enter Protection Group - Equipment Protection Group**.
 5. Click **Go**.
-

Result: The **Enter Protection Group - Equipment Protection Group** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **Protection type** – select one of the following types (available values depend on the NE configuration):
 - *EQPTEP155* – electrical 155 Mbps interfaces protection
 - *EQPTEP51* – electrical 51 Mbps interfaces protection
 - *EQPTLOXC* – low order switch fabric protection
 - **Protection group Id** – the protection group ID as component of the protection group AID. For protection groups of electrical 155 Mbps interfaces or electrical 51 Mbps interfaces, enter a numerical value in the range *01* to *99*. For other protection types, enter *01*.
 - **Protection unit** – the protection circuit pack AID being a member of the 1+1 equipment protection group. You may copy the circuit pack ID from the **Slot/circuit pack view** page.
 - **Worker unit** – the worker circuit pack AID being a member of the 1+1 equipment protection group.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To operate an equipment protection group

When to use

Use this task to operate (to switch) an existing equipment protection group.

Related information

For a more detailed explanation, please refer to the description of the OPR-PROTNSW command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Protection Groups**.
4. In the **Function** field, select **Operate Protection Switch - 1+1 Equipment Group**.
5. Click **Go**.

Result: The **Operate Protection Switch - 1+1 Equipment Group** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

In the field **Protection group identifier**, enter the ID of the protection group for which the information should be retrieved. In the field **Protection type**, select a type of equipment protection group.

The following table shows the possible combinations:

Type of equipment protection	Value for Protection group identifier	Value for Protection type
Higher-order switch fabric and timing	<i>1-1-estgrp</i>	Switch Fabric
System controller	<i>1-1-ectlgrp</i>	System Controller
Electrical 51 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP51 Circuit Pack
Electrical 155 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP155 Circuit Pack
Lower-order switch fabric	<i>1-1-eloxcl</i> Note that the last character of this identifier is the digit one.	LOXC Circuit Pack

Destination specifies the destination of the switch command; that means which side shall be active in terms of the member role within the protection group after the switch has been executed. The following values are supported: *Worker*, *Protection*.

Switch command specifies the switch command to be executed by the protection state machine. Select one of the following values: *Forced switch* (for all equipment protection types), or *Manual switch* (for all equipment protection types but system controller protection).

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To release an equipment protection group

When to use

Use this task to release an existing equipment protection group, that means to clear protection switch requests.

Related information

For a more detailed explanation, please refer to the description of the RLS-PROTNSW command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Protection Groups**.
 4. In the **Function** field, select **Release Protection Switch - 1+1 Equipment Group**.
 5. Click **Go**.

Result: The **Release Protection Switch - 1+1 Equipment Group** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.

In the field **Protection group identifier**, enter the ID of the protection group for which the information should be retrieved. In the field **Protection type**, select a type of equipment protection group.

The following table shows the possible combinations:

Type of equipment protection	Value for Protection group identifier	Value for Protection type
Higher-order switch fabric and timing	<i>1-1-estgrp</i>	Switch Fabric
System controller	<i>1-1-ectlgrp</i>	System Controller
Electrical 51 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP51 Circuit Pack
Electrical 155 Mbps interfaces	<i>1-1-ee{01...99}</i>	EP155 Circuit Pack
Lower-order switch fabric	<i>1-1-eloxcl</i> Note that the last character of this identifier is the digit one.	LOXC Circuit Pack

Switch command specifies the switch command to be executed by the protection state machine. Select *Clear*.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To delete an equipment protection group

When to use

Use this task to delete an existing equipment protection group.

The following types of equipment protection groups can be deleted:

- Electrical 51 Mbps interfaces protection
- Electrical 155 Mbps interfaces protection
- Lower-order switch fabric protection

Related information

For a more detailed explanation, please refer to the description of the DLT-PROTN-GRP command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Protection Groups**.
 4. In the **Function** field, select **Delete Protection Group - Equipment Protection Group**.
 5. Click **Go**.

Result: The **Delete Protection Group - Equipment Protection Group** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.

In the field **Protection group identifier**, enter the ID of the protection group for which the information should be retrieved. In the field **Protection type**, select a type of equipment protection group.

The following table shows the possible combinations:

Type of equipment protection	Value for Protection group identifier	Value for Protection type
Electrical 51 Mbps interfaces	<i>1-1-ep{01...99}</i>	EP51 Circuit Pack
Electrical 155 Mbps interfaces	<i>1-1-ep{01...99}</i>	EP155 Circuit Pack
Lower-order switch fabric	<i>1-1-eloxc1</i> Note that the last character of this identifier is the digit one.	LOXC Circuit Pack

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



7 ONNS

Overview

Purpose

This chapter contains concepts and tasks that are used to operate the Optical Network Navigator System (ONNS) within the management system.

ONNS is not supported on the Lucent OMS PC Platform.

Contents

ONNS Concepts	7-3
ONNS Network Element Management	7-6
ONNS Port Parameters Provisioning	7-8
ONNS Multiplex Section Connection Provisioning Concepts	7-11
ONNS Service Connection Provisioning Concepts	7-13
ONNS MxN Service Group Connection Provisioning Concepts	7-19
Association of MxN Connections with Controlled Planes	7-23
ONNS Infrastructure Connection Provisioning Concepts	7-24
Modify Route Concepts for ONNS	7-26
Graphical Layout for ONNS	7-28
ONNS Database Synchronization	7-30
Filter ONNS NEs on the Network Map	7-32
Provision ASTN NE Port Parameters	7-33
Provision an ONNS Multiplex Section Connection	7-35
Modify ASTN NE Port Parameters for Multiplex Section Connections	7-41
View ONNS Connection Groups	7-43
View/Query ONNS ASTN Capacity Utilization	7-44

View ONNS Associated MxN Connection List	7-46
Associate a Tandem Connection to a Controlled Plane	7-47
Provision an ONNS Controlled Plane Service Connection	7-48
Provision an ONNS Mixed Plane Service Connection	7-56
Provision an OUC Connection for In Effect Steps	7-64
Add an ONNS MxN Service Group Network Connection	7-72
Add an ONNS MxN Working Connection to an Existing MxN Connection Group	7-79
Modify the Route of (Rearrange) an ONNS In Effect Connection	7-85
Delete Group for an ONNS MxN Connection Group	7-90
DB Delete Group for an ONNS MxN Connection Group	7-91
Cancel Group for an ONNS MxN Connection Group	7-92
Provision an ENNI ONNS Controlled Plane Service Connection	7-93
View ENNI Associated ASTN Connection List	7-100
Perform a Partial Database Synchronization for Network Connections	7-101



ONNS Concepts

Definition of ONNS

ONNS consists of software and hardware present on some NEs, which performs connection management functions for synchronous connections, across a network of Automatically Switched Transport Network (ASTN) NEs. The ONNS system consists of a number of ONNS modules. Each module resides on a different ASTN NE in the network.

The management system supports ONNS only for the *LambdaUnite*[®] MSS NE.

Definition of ENNI

The External Network-to-Network interface (E-NNI) is defined as a reference point between two control domains, which represents a service demarcation point supporting multi-domain connection management. An E-NNI connection can connect more than one control plane domains. The multi-domain E-NNI connection is set up between nodes using a single TL1 command issued from the management system.

The management system supports ENNI only for the *LambdaUnite*[®] MSS NE.

Definition of ASTN NE

An ASTN NE can to operate in an intelligent network domain. The ports of an ASTN NE can be controlled by ONNS. *LambdaUnite*[®] MSS is the only NE supported by the management system that can operate as an ASTN NE.

Functionality description

All ASTN NEs have a signalling element that facilitates automatic routing between them and other NEs in the network. This signalling element enables them to be managed by the ONNS. For NEs managed by ONNS, the management system interfaces with the ONNS for connection management (routing and implementation) purposes between ASTN NEs for data synchronization, alarms and notifications of port parameters, cross-connects, etc.

Administration of ONNS

ONNS capability is enabled on the management system by use of an installation parameter. When this parameter is set, the fields and pages related to ONNS will be displayed. For more information, see the *Lucent OMS Administration Guide*.

Pure ASTN Only Network Parameter

If the `ASTN_ONLY_NETWORK` system parameter has a value of `PURE`, the management system inventories the discovered ONNS connections, including MxN working connections, as Controlled Plane connections with a connection type of Regular.

ASTN Capacity Utilization

ASTN capacity utilization within ONNS is managed by the management system. Capability is provided to either view or query the ONNS topology data which includes available and total bandwidth between any pair of ONNS NEs.

Tandem Network Connections

Tandem network connections are used when a portion of a connection is set up in advance to the final end-to-end connection. Tandem connections are available for ONNS connections that have been created by means other than at the request of the management system. The Connection Type for these connections is Tandem. Tandem connections can be converted into Regular network connections via the **Associate to Controlled Plane** Go menu option on the Network Connection List.

A Tandem Network Connection (TNC) is one that is discovered when `ASTN_ONLY_NETWORK=PURE`.

For MxN Protection, a tandem network connection is one that is created by the management system that can be extended to become part of another network connection. TNCs can become end-to-end Controlled Plane connections.

MxN Connection Protection Group

An MxN Connection Protection Group is a group of ONNS connections consisting of a number of working connections and a number of protecting connections. An MxN Protected ONNS connection is one that belongs to the MxN protection group. Individual connections within an MxN Connection Protection Group are considered as tandem connections with an ASTN Protection Type of MxN Protected.

MxN Connection Protection Groups can be deleted when one of the members of the group is in the In Effect state. Groups can be cancelled when the group is in either the Planned, Local Design, Implementation Completed, or Implementation Failed state, or when the delete order for a connection group is in the Implementation Failed state. An MxN Connection Protection Group can be DB Deleted when the connection group is in either the Active or Local state.

An MxN working connection with a Protection Class of `MBYNWRK` can be added to an existing MxN Connection Group. Each new connection must be added separately to the existing Group. Each new connection is added as a Tandem connection with the

tagged setting set to No. MxN connections with a Protection Class of MBYNWRK can be deleted via the management system. MxN connections with a Protection Class of MBYNPRT cannot be deleted via the management system.

NOCON&SETUPFL State for ONNS Connections

When ONNS is unable to set up a user-requested connection, the ConnStatus field indicates a value of NOCON&SETUPFL, and no connection is set up on the NE.

If the ConnStatus field value is NOCON&SETUPFL, a non-MBYN connection is marked as an Implementation Failed state.

For an MBYN connection, if the working or protection connection ConnStatus field value is NOCON&SETUPFL, the connection is marked as an Implementation Failed state. When the NE deletes any working or protection connections been set up successfully, the management system marks those connections as Improperly Disconnected, unless the group is already in the In Effect state. In this case, when the NOCON&SETUPFL value is received, the group, which could have Improperly Disconnected connections, is changed to an Implementation Failed state.

If a new ONNS connection, with the same end points as the management system order that is in the Implementation Failed state, is created outside of the management system, the management system creates a new connection that fails at the Local Design step.

□

ONNS Network Element Management

Overview

The following information is conceptual information about ONNS Network Element management concepts. This information is meant to complement the tasks presented later in this section.

Identifying ONNS NEs

The management system interfaces with the ONNS subnetwork. During a database synchronization, all the NEs are automatically discovered by the management system. ASTN NEs contain a signalling element which identify them as ASTN NEs. The association between the ONNS and the ASTN NEs is done automatically, without intervention from the user.

OMS to NE communication for ONNS NEs

The management system establishes communication with the ASTN NEs automatically through the subnetwork auto discovery process. The management system uses the communication IP address to log in to the ASTN NE. This IP address is also the management IP (LAN) address.

The ASTN NE can also be added manually to the management system manually via OMS to NE communications. For more information, see OMS-to-NE Connections in the Lucent OMS Network Element Management Guide.

If the ASTN NE does not have a communication IP address, the user can set up communications to that NE via a GNE. By providing the GNE with the ASTN NE ID, the GNE maintains a mapping to the NSAP address of the ASTN NE. However, in the case where the ASTN NE is associated with ONNS, the ASTN NE must have the management system IP address.

For further information

For more conceptual information about OMS to NE connections for ONNS NEs, see the OMS-to-NE Connections section in the Lucent OMS Network Element Management Guide. The tasks in this chapter describe how to perform NE management functions for ONNS NEs.

ONNS domain

The ONNS domain is a collection of ASTN NEs that are capable of signalling among themselves and using the signal to maintain the neighboring topology data to provide connection management within that domain. Only a single ONNS domain is supported from the management. When communication is established the management system

pre-populates the ONNS domain name either based on user's input during installation or predefines ONNS domain name as ONNS Domain. All ONNS NEs are automatically placed in this domain.

ONNS NE icon

Once communication is established, the ASTN NEs associated with ONNS are represented on the network map by a unique icon. The icon indicates that the NE has an ONNS component.

The following depicts the *LambdaUnite*[®] MSS NE that is ONNS enabled:



ONNS NEs and their connections can be filtered for display on the Network Map.



ONNS Port Parameters Provisioning

The following information is conceptual information about port provisioning of ONNS ports. This information is meant to complement the tasks presented later in this section.

ONNS ports

The management system supports ONNS network connections only for the *LambdaUnite*[®] MSS NE.

Port provisioning

Bandwidth in the network is considered to be a “resource.” In order to allocate ports to ONNS, physical ports on NEs need to be assigned to ONNS. This process is known as “port provisioning.” Port allocation between the ASTN NE and traditional network resources is accomplished by assigning a specific domain type and network interface type to a port.

Domain type

The domain type indicates whether the ports are controlled by the management system or by ONNS.

- **Network-owned** - port resources that are network-facing and managed by the ONNS domain.

Network interface type can be set as follows:

- Internal network
- External Network

- **Management-owned** - port resources that are part of the managed plane and are not part of the ONNS domain.

Network interface type can be set as follows:

- None
- Customer/Client

Network interface type

The network interface type indicates the role that the port has been assigned in the network.

Network-owned ports can be assigned the following network interface type:

- **Internal network** — This type is assigned to a port that is “network” facing. A port of this type interfaces with other “internal network” ports within the ONNS domain (which is also known as the controlled plane). For these ports, the port class is set to **iNNI**.
- **External network** — This type is assigned to a port that is on the External Network facing side. For these ports, the port class is set to **ENNI**.

Management-owned ports can be assigned to any of the following network interface types:

- **Customer/Client** — This type is assigned to a port that is “client or customer” facing. A port of this type is owned by the management system, but interfaces with ports in the ONNS domain (which is also known as the controlled plane). For these ports, the port class is set to **EDGE**.
- **None** — This type is assigned to ports that do not interface with the ONNS domain. For these ports, the port class is set to **TRADITIONAL**.
- **External Network** — This type is assigned to ports that interface between two controlled plane domains (ONNS networks). For these ports, the port class is set to **ENNI**.

Port allocation for ONNS

The user assigns the port allocation for network owned ports. The management system sends port set up requests for ports at either ends (A and Z) of the connection. The connections terminating on ports assigned to the network are reserved for the ONNS subnetwork via the ONNS domain and are not available for other regular connections for the managed plane.

The user can assign the port allocation for network owned using the following two operational methods.

1. Method 1 is targeted towards designating network owned ports on the customer/client facing side. These ports can only be assigned for Management Owned: Network Interface Type as “Customer/Client”.
Ports that meet the following criteria are eligible to be allocated using this method:
 - a. Ports on a ASTN NE that are completely free, without an associated connection.
 - b. Ports on a ASTN NE that may be part of a line protection type, for example, 1+1 MSP/APS, 1x1 MSP/APS, 2F MSSPRING/BLSR, or 4F MSSPRING/BLSR.
If the line protection type is 1+1 MSP/APS or 1x1 MSP/APS, then the working port can be assigned as a client port
If the line protection type is 2F MSSPRING/BLSR, then the east and/or west port can be assigned as a client port.
If the line protection type is 4F MSSPRING/BLSR, then any of the ports associated with this group can be assigned as a client port.
2. Method 2 is targeted toward designating Network owned ports on the Internal Network facing side. These ports can only be assigned for Network Owned:Network Interface Type as “Internal Network”. The user can assign the SRLG, Cost and Propagation Delay as port parameters.

The ports that meet the following criteria are eligible to be allocated using this method:

- Ports on a ASTN NE that are termination ports for any unprotected link connection between two ASTN NEs.
- Ports on a ASTN that are NOT part of the following line protection schemes: 1+1 MSP/APS, 1x1 MSP/APS, 2F MSSPRING/BLSR, 4F MSSPRING/BLSR

Methods for configuring/modifying ONNS ports

Partitioned port resources can be configured or modified from the management system using several methods.

From the Ports page

ONNS port parameters can be configured and modified from the Ports page.

The Ports page contains the attributes for ONNS ports. Selecting the **View/modify port parameters** option from the Go list for a selected port displays all the port attributes of that port in the Port window. The **Control Plane** panel in this page lists the ONNS related port information such as Network Interface Type (Port Class), SRLG, Cost, Minimum Cross-connection rate, Maximum cross connection rate and ASTN Propagation Delay. The attributes cannot be modified if the client connection termination points of the port is involved in a cross-connection.

From the Modify Network Connections page

ONNS port parameters can be viewed and modified from the Modify Network Connections page.

The Modify Network Connections window contains attributes for ONNS ports. Selecting the **Modify parameters** option from the Go list for a selected physical network connection displays all the attributes of the connection. The Transmissions parameters panel contain the ONNS related port information such as Network Interface Type (Port Class), SRLG, Cost, Minimum Cross-connection rate, Maximum cross connection rate and ASTN Propagation Delay.

Additionally, ONNS attributes are displayed in the Network Connections page details panel. If there is a discrepancy in the user intended values versus the NE values at either the A-end or the Z-end, a discrepancy flag is displayed next to the relevant field in the Network Connections page details panel.

The user can view/modify the current values of the attributes by going to the Port page. The Network Connection page details, and the Modify network connections page always display the user intended value.



ONNS Multiplex Section Connection Provisioning Concepts

Overview

The following information is conceptual information about ONNS multiplex section connection provisioning concepts. This information is meant to complement the tasks presented later in this section.

Preconditions

Prior to provisioning any ONNS connections, communication between the management system and the ASTN NE must be completed successfully.

Additionally, in order for the user to request a connection through the ONNS domain, the actual physical connections (port connections) between the ASTN NEs must have been established as part of pre-provisioning operations and the connection status of each of these connections are declared usable by the NEs.

Supported multiplex section network connections

The following rates are supported for SDH/SONET ONNS multiplex section connections:

- STM-1/OC-3
- STM-4/OC-12
- STM-16/OC-48
- STM-64/OC-192
- STM-256/OC-768

ONNS connection parameters for multiplex section connections

When provisioning multiplex section network connections, additional ONNS parameters are provisionable from the Connections parameters panel, the Order parameters panel, and the Transmission parameters panel.

Connection parameters panel

The order of selection of fields in the Connection Parameters panel is as follows:

1. Select the connection rate.
2. Select the Domain type of the physical connection. Options are either **Network owned** or **Management owned**. The domain type may also be configured via the Port page, as long as the NE information is provided.
3. The Protection type is set to Unprotected by default, and cannot be changed by the user.

4. Select the NEs/Ports. The From and To NE Ports can be entered manually or automatically by using the hyperlink to the NE/Port Selection popup window.
Note: If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.
5. Connection name and Connection Name Format fields are optional.

Order parameters panel

The Order parameters panel contains additional parameters for multiplex section network connections. Completing these fields is optional.

Transmission parameters panel

The Transmission parameters panel contains additional parameters for physical network connections.

If the **Domain Type** is **Network Owned**, the following fields are displayed on the Transmission Parameters panel:

- **Network Interface Type** set to Internal Network or External Network
- **SRLG**
- **Cost**
- **ASTN Propagation Delay**. This field is not displayed when the Network Interface Type is External Network.
- **Minimum/Maximum cross connection rate**

Only ports with a value of **None**, **Internal Network** or **External Network** can be selected in the NE/Port Selection pop-up window.

If the **Domain Type** is **Management Owned**, the following fields are displayed on the Transmission Parameters panel:

- **Network Interface Type** with option to select **None**, or **Customer-Client**
- **SRLG** - No selection allowed
- **Cost** - No selection allowed
- **ASTN Propagation Delay** - No selection allowed
- **Minimum/Maximum cross connection rate** - No selection allowed



ONNS Service Connection Provisioning Concepts

Overview

The following information is conceptual information about ONNS service connection provisioning concepts. This information is meant to complement the tasks presented later in this section.

ONNS is not supported on the Lucent OMS PC Platform.

Preconditions

Prior to provisioning ONNS connections, communication between the management system and the ASTN NE must be completed successfully.

Additionally, in order for the user to request a connection through the ONNS domain, the actual physical connections (port connections) between the ASTN NEs must have been established as part of pre-provisioning operations and the connection status of each of these connections are declared usable by the NEs.

Category

During provisioning of ONNS service connections, a category must be specified. The following category types are available:

- **Controlled Plane** - the ONNS subnetwork connection starts and ends in the ONNS domain.
- **Managed Plane** - the connection starts and ends outside the ONNS domain without traversing the ONNS domain.

Parameter Panels

The following parameter panels apply for Controlled Plane categories:

- Connection Parameters
- Routing Parameters
- Order Parameters
- Assurance parameters

Protection types

The following ONNS ASTN protection types are supported for Controlled Plane categories:

- **Permanent 1+1 Protected**

Permanent 1+1 Protected - where the network connection is protected by a non-revertive connection when one of the paths of the 1+1 connection fails:

- **Non-revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path is permanent.
- **Revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path can revert back to the original path.
- **Network 1+1 Protected** - where the controlled plane is protected by the dedicated path capable of switching in case of failure

Network 1+1 Protected protection types can support the following **Reversion Modes**:

- **Non-revertive** - These are controlled plane connections where there is an autonomous restore (reroute) if the original path has a failure, but the connection does not revert to the original path if the failure on the original path clears. This is the default.
- **Revertive** - These are controlled plane connections where an autonomous restore (reroute) occurs if there is a failure on the original path and the connection reverts automatically when the failure on the original path clears.
- **Auto Re-route** - the following auto re-route modes are supported:
 - **Non-revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path is permanent.
 - **Revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path can revert back to the original path.
- **Unprotected** - no protection for the connection request through the ONNS domain.
- **Y Protected** - where two paths between one source node and two destination nodes are set up, and the signal is then bridged in the source node.
- **MxN Protected** - where a set of working connections shares a pool of pre-provisioned connections for rerouting and protecting the traffic. At the time of restoration, instead of determining a route to restore the traffic, the route from the pre-provisioned protecting connections pool is used to reroute.

ONNS connection parameters for ONNS service connections

The Connections parameters panel contains the following additional parameters.

- **Category** - only possible value is: **Controlled plane**.
- **Controlled Plane type** - Possible values are: **non-ENNI** or **ENNI**. Non-ENNI can be selected for regular ONNS connections spanning one control plane domain. ENNI can be selected for ONNS connections spanning multiple control plane domains
- **ASTN protection type** - possible values are: **Unprotected**, **Auto Re-route**, **Permanent 1+1 Protected**, **Network 1+1 protected**, or **MxN protected**.

- **ASTN protection mode** - possible values are: **Revertive** or **Non-revertive**. This field is displayed when the ASTN protection type is Auto re-route or Network 1+1 Protected.
- **ASTN restoration priority** - possible values are 0 through 7. This is only displayed when ASTN protection type is Auto. A value of “0” is high and “7” is low. Services with a low priority are primary candidates for pre-emption.
- **Controlled Plane Type** - possible values are: **non-ENNI** or **ENNI**.

Routing constraints

Routing constraints are parameters that makes a variety of routing decisions possible by ONNS.

Controlled plane routing constraints

When the **Category** field is set to **Control plane**, the following routing constraints are displayed during connection provisioning on the Routing parameters panel.

- **ASTN propagation delay** - the user can enter the maximum delay value associated between the A-NE and Z-NE. Possible values are 1 - 32767 milliseconds.
- **Exclude SRLG** - the user can exclude the Shared Risk Link Group IDs assigned to internal network ports from the end-to-end path. The user can select a list of SRLG IDs to exclude up to a maximum 25, selected from a pop-up window.
- **Explicit/Exclude ASTN nodes** - the user can include or exclude specified ASTN NEs from the end-to-end connection. The **Explicit ASTN nodes** field *is not* applicable to a Protection Type of **MxN Protected**.
- **Disjointness** - determines how disjointed the routes set up by ONNS can be. Either node can be a disjoint, or nodes and SRLGs can be disjoints depending on the ASTN protection type. This field is not applicable to a Protection Type of **MxN Protected**.

When the **Connection rate** is set to **VCG** with the **ASTN protection type** of server equals **Unprotected**, or the service path with the **service type** equal to **Concatenated** and the **ASTN protection type** of **Unprotected**, the **Group Setup Type** routing constraints are applicable

The Controlled Plane path information field is considered as Improperly Disconnected if the connection is not on the network, but does exist in the management system.

OUC Provisioning

OUC (ONNS-UPSR-Construct) refers to the grouping of the Customer/Client port of a pre-existing ONNS connection and an unused Customer/Client port on the same NE that will become part of a traditional UPSR. When adding an OUC connection to an existing ONNS connection, the Modify Route page is used. The construct assists in achieving the UPSR-mesh interworking.

Connection Shapes

Connection shapes for OUC provisioning must be set to add-drop A (bi), add-drop Z (bi), or double add-drop (bi) with a Category of Controlled Plane only. These connection shapes are not applicable for VCG servers and VCGs.

For add-drop connection shapes, any ASTN Protection Type can be selected *except* for Y Protected. For double add-drop connection shapes, any ASTN Protection Type can be selected. For an ASTN Y Protected protection type, the connection shape *must* be double add-drop, and the OUC is provisioned only on the From NE. Note that during OUC provisioning, the connection shape and the ASTN Protection type cannot be changed at the same time.

The following table details the Connection Shape and the applicable NE/Port ID GUI fields to be selected based on the existing ONNS ASTN Protection Type.

Connection Shape with OUC	Existing ASTN Protection Type	NE/Port ID GUI Fields
Add/Drop A (bi)	All values <i>except</i> Y Protected	From NE To NE From Port 1/Port 2 To Port 1
Add/Drop Z (bi)	All values <i>except</i> Y Protected	From NE To NE From Port 1 To Port 1/Port 2
Double Add/Drop (bi)	All values	From NE To NE From Port 1 To Port 1 From Port 2 To Port 2

Note: For MxN connections, in order to add an OUC connection that originally has a connection shape of Simple (bi), the MxN connection can be modified by changing the Connection shape of Simple (bi) to one of the following: Add/Drop A (bi), Add/Drop Z (bi), or Double Add/Drop (bi). This is accomplished on the Add Connections TDM form for MxN Service.

Add OUC to Existing ONNS Connection

Adding an OUC can occur under three circumstances, as detailed below:

- The OUC to be added could be existing as an uncorrelated OUC as a result of the Network OUC sync operation
- The OUC to be added could be one about which the management system has no information if it exists only on the CIT
- The OUC to be added to an existing ONNS connection does not exist in the CIT

Connection/Routing Parameter Allowable Changes

The following table details allowable connection/routing parameter changes from the Modify Route page.

Current ASTN Protection Type	Modified ASTN Protection Type	Other Connection/Routing Parameters That Can Be Changed
Unprotected	Auto Re-route with ASTN Protection Mode of Revertive	Restoration Priority Disjointness
Unprotected	Auto Re-route with ASTN Protection Mode of Non-Revertive	Restoration Priority Disjointness
Unprotected	Network 1+1 Protected	None
Auto Re-route with ASTN Protected Mode of Revertive	Unprotected	None
Auto Re-route with ASTN Protected Mode of Non-Revertive	Unprotected	None
Auto Re-route with ASTN Protected Mode of Revertive	Auto Re-route with ASTN Protected Mode of Non-Revertive	Restoration Priority
Auto Re-route with ASTN Protected Mode of Non-Revertive	Auto Re-route with ASTN Protected Mode of Revertive	Restoration Priority
Network 1+1 Protected	Unprotected	None
Auto Re-route	Auto Re-route	None
Unprotected	Unprotected	None
Network 1+1 Protected	Network 1+1 Protected	None

Deleting OUC with an Existing ONNS Connection

Deleting an OUC with an existing ONNS connection is done on the Modify Route page. If the OUCs that were deleted exist in the management system as correlated OUCs, they are then marked as uncorrelated after submitting the deletion from the ONNS connection through the Modify Route page. The connection associated with the OUC is marked with the Control Plane Path Information as Improperly Disconnected.

OUCs can also be deleted via the CIT. These OUCs then become uncorrelated. The user then must go to the Modify Route page and delete these uncorrelated OUCs from the management system.

Deletion of OUCs if ONNS Connection is Deleted

When an ONNS connection that has OUCs riding on it, either on one end or on both ends, is deleted from the management system, the OUCs are also deleted by ONNS. This then frees up the protection port that was used in the OUC, and the OUCs are marked as uncorrelated. The OUCs are deleted from the management system after the user performs the Modify Route action on this improperly disconnected connection.

□

ONNS MxN Service Group Connection Provisioning Concepts

Overview

The following information is conceptual information about ONNS MxN Service Group connection provisioning concepts. This information is meant to complement the tasks presented later in this section.

ONNS is not supported on the Lucent OMS PC Platform.

ONNS MxN Service network connections which have ASTN enabled can be accessed from the following path: **Connections > Connection Groups**.

Preconditions

Prior to provisioning ONNS connections, communication between the management system and the ASTN NE must be completed successfully.

Category

During provisioning of ONNS MxN service group connections, only the Controlled Plane category is available. The following describes this category type:

- **Controlled Plane** - the ONNS subnetwork connection starts and ends in the ONNS domain.

Protection types

The only available Protection type for ONNS MxN Service Group connections is the ASTN protection type of MxN Protected. ASTN Ratios can be selected.

MxN Protected is a set of working connections that shares a pool of pre-provisioned connections for rerouting and protecting the traffic. At the time of restoration, instead of determining a route to restore the traffic, the route from the pre-provisioned protecting connections pool is used to reroute.

The following list describes actions that can be performed for MxN Service Groups:

- Add to group
- Delete from group
- DB Delete from group
- Cancel from group
- Create the MxN Protected connections via the MxN Service Group page.
- Search for and display MxN Connection Groups via the Connection Group page.
- Delete the entire group via the Delete Go menu option.

- View members of a particular group from the Associated MxN Connection Group list Go menu option for a selected Connection Group.
- Associate MxN working tandem connections to a Controlled Plane.

MxN protected connection discovery and database maintenance

As a part of ONNS database synchronizations, the management system discovers all MxN protected connection groups and their contained service and protection connections. Note that only the connections in the group are reported and the MxN protected connection group must be derived using the connection group ID of the various connection. Likewise the management system updates and maintains this information based on the receipt of autonomous notifications via path change messages. The management system maintains the connection state and tracks route data that is not current with that of the NE for the connection, for example, when a service is using a protection connection. For the management systems that exclusively manage control plane domains, the management system automatically creates network connections from each connection segment of an MxN protected connection group.

ONNS connection parameters for ONNS MxN service group connections

MxN connections can be provisioned via the **New > TDM > MxN Service Group** path.

The Connections parameters panel contains the following additional parameters.

- **From NE/Port ID and To NE/Port ID fields** - Selections can be entered manually or by using the hyperlink to the NE/Port Selection popup window. Up to 64 CTPs can be selected for MxN provisioning.
- **MxN Connection Group Name**
- **Customer Name**
- **Connection Alias**
- **MxN Protection Ratio** - Can be 1:1, 1:2, or 1:3.

Connection Group List Page

The Connection Group page is accessed from the following path: **Connections > Connection Group**. The Connection Group page displays a search panel to locate MxN connection groups that meet specified search criteria. Once you have identified a specific connection group, you can either cancel it, delete it, or display its associated MxN connection list by selecting the appropriate Go menu option.

Connections can be provisioned and discovered on the Connection Group page.

Routing modes

For MxN service group connections, the routing mode is not applicable.

Routing constraints

Routing constraints are parameters that makes a variety of routing decisions possible. Based on whether the connection segment is control plane, different parameter will be displayed during connection provisioning.

Control plane routing constraints

The following routing constraints are displayed during MxN service group connection provisioning on the Routing parameters panel.

- **ASTN propagation delay** - the user can enter the maximum delay value associated between the A-NE and Z-NE unidirectionally. Possible values are 0 - 32767 milliseconds.
- **Exclude SRLG** - the user can exclude the Shared Risk Link Group IDs assigned to internal network ports. The user can select a list of SRLG IDs to exclude up to a maximum 25, selected from a pop-up window.
- **Explicit/Exclude ASTN nodes** - the user can include or exclude specified ASTN NEs from the connection. Explicit ASTN nodes *do not* apply for MxN connections.

Tandem Network Connections

ONNS connections created by means other than OMS that are inventoried in OMS are identified as network connections with an additional attribute qualifying them as Tandem Connections. Provisioned MxN connections and any discovered ONNS connections are inventoried as tandem connections. *Tandem connections* are specific types of network connections that can become part of another end-to-end network connection.

This end-to-end network connection can be a pure **Controlled Plane** connection, where the tandem connection is considered “tagged” to a network connection. In this case, no attributes are modified. Attributes are visible in the Controlled Plane part of the connection as read-only fields.

Tandem connections can become part of a network connection through the Associate to Controlled Plane Go Menu action item on the Network Connections Page. The Associate to Controlled Plane action converts the Tandem Network Connection to a Controlled Plane connection. Controlled Plane information cannot be changed by the user. Only MxN working connections can be associated.

Tandem connections are always inventoried with a Category equal to Controlled Plane before association from any ASTN protection type of connection.

For MxN connections, both the working and the protection connections are considered as Tandem connections. Only working connections can be associated with a network connection.

Adding connections to an existing MxN Connection Group

Individual working connections are added to an existing MxN Connection Group via the Add to Group Go menu item of the Associated MxN Connection List page, which opens the MxN Connection Group provisioning form. This path to the MxN Connection Group provisioning form allows the user to only enter one set of From/To Customer/Client ports. Other fields are read-only. Only *one* MxN working connection can be added and submitted at one time for a Connection Group.

When individual working connections are added to an existing MxN Connection Group, the management system inventories these connections as either Tandem or Regular based on system parameters.

Deleting connections to an existing MxN Connection Group

A Connection to the MxN Connection Group can be initiated from the Network Connections page, the Graphical Layout, or the Associated MxN Connection List page. Only connections with a protection class of MBYNWRK can be deleted through the management system; MBYNPRT protection class connections cannot be deleted through the management system.

If the MBYNWRK connection to be deleted has its Tagged parameter set to No, the management system deletes the MxN tandem working connection. If all of the connections in a specific Group are deleted at one time, the management system deletes that specific MxN Connection Group from the database.



Association of MxN Connections with Controlled Planes

General concepts

An MxN connection can be associated to a Controlled Plane.

The following are general concepts that apply to associating MxN connections to a Controlled Plane.

- You can associate MxN Working Connections to the Controlled Plane from the Network Connection List Go menu option of **Associate to Controlled Plane**.
- You can associate MxN Working Connections to the Controlled Plane from the Associated MxN Connection List Go menu option of **Associate to Controlled Plane**.
- If a Tandem Network Connection is to be associated to a Controlled Plane, the Tandem Network Connection is converted to a regular Controlled Plane connection when using the **Associate to Controlled Plane** option from either the Network Connection List or the Associated MxN Connection List.



ONNS Infrastructure Connection Provisioning Concepts

Overview

The following information is conceptual information about ONNS Infrastructure connection provisioning concepts. This information is meant to complement the tasks presented later in this section.

Important! ONNS Infrastructure connection provisioning addresses VCG servers in ONNS. VCG servers cannot be of MxN Protection type. VCG servers can be used to provision a VCG. ONNS Infrastructure connections only apply to the **Category** of Controlled Plane.

Preconditions

Prior to provisioning ONNS connections, communication between the management system and the ASTN NE must be completed successfully.

Category

During provisioning of ONNS infrastructure connections, a category must be specified. The following category types are available:

- **Controlled Plane** - the ONNS subnetwork connection starts and ends in the ONNS domain.

Protection types

The following ONNS ASTN protection types are supported for a Controlled Plane category.

- **Network 1+1 Protected** - where the controlled plane is protected by the dedicated path capable of switching in case of failure
Network 1+1 Protected protection types can support the following **Reversion Modes**:
 - **Non-revertive** - These are controlled plane connections where there is an autonomous restore (reroute) if the original path has a failure, but the connection does not revert to the original path if the failure on the original path clears. This is the default.
 - **Revertive** - These are controlled plane connections where an autonomous restore (reroute) occurs if there is a failure on the original path and the connection reverts automatically when the failure on the original path clears.
- **Permanent 1+1 Protected**- where the network connection is protected by a non-revertive connection when one of the paths of the 1+1 connection fails. Non-revertive - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path is permanent.

- **Auto Re-route** - the following auto re-route modes are supported:
 - **Non-revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path is permanent.
 - **Revertive** - ONNS automatically restores (re-routes) the path on a best-effort basis, however the re-routed path can revert back to the original path.
- **Unprotected** - no protection for the connection request through the ONNS domain.
- **Y Protected** - only for Controlled Plane categories. The **Y Protected** protection type *does not* apply for VCG servers.

ONNS connection parameters for ONNS Infrastructure connections

The Connections parameters panel contains the following additional parameters.

- **From NE/Port ID and To NE/Port ID fields** - Selections can be entered manually or by using the hyperlink to the NE/Port Selection popup window. The **From NE/Port ID** fields must be the VCG port. The **To NE/Port ID** fields can be a VCG port or a SONET/SDH port.
- **Provisioning of Server layer**
- **Connection name**
- **Customer name**

Routing constraints

Routing constraints are parameters that makes a variety of routing decisions possible. Based on whether the connection segment is control plane, different parameter will be displayed during connection provisioning.

Control plane routing constraints

The following routing constraints are displayed during MxN service group connection provisioning on the Routing parameters panel.

- **ASTN propagation delay** - the user can enter the maximum delay value associated between the From NE and the To NE. Possible values are 1 - 32767 milliseconds.
- **Exclude SRLG** - the user can exclude the Shared Risk Link Group IDs assigned to internal network ports. The user can select a list of SRLG IDs to exclude up to a maximum 25, selected from a pop-up window.
- **Explicit/Exclude ASTN nodes** - the user can include or exclude specified ASTN NEs from the connection.
- **Group SetUp Type** - the user can determine the Group SetUp Type if the ASTN protection type of the VCG server is **Unprotected**.



Modify Route Concepts for ONNS

The Modify Route feature, also referred to as a Rearrange feature, allows the user to modify specific attributes of an existing ONNS connection via a Rearrange order in the management system.

ONNS is not supported on the Lucent OMS PC Platform.

Important! If the ONNS connection for which you want to modify a route is in either the Planned or Local Design order step, you can follow the general procedures. If the ONNS connection for which you want to modify a route is in the In Effect order step, the procedures are specific to ONNS connections only.

You cannot add or delete an OUC if the ONNS connection is either in the Planned or Local Design order step. OUCs can only be added to, or deleted from, an ONNS connection that is in the In Effect order step. This is accomplished via the Modify Route page.

The Modify Route feature, also referred to as a Rearrange feature, allows the user to modify specific attributes of an existing ONNS connection via a Rearrange order in the management system. Modify Route for ONNS connections applies to:

- Controlled plane without Tandem network connections
- Controlled plane with Tandem network connections

The Modify Route feature with a changing ASTN protection type does not apply if the ASTN Protection type is MxN Protected or Y Protected. The Modify Route feature only applies to connections that are in one of the following steps: Planned Completed, Local Design Completed, or In Effect.

Modify Route is used to add an OUC to an existing ONNS Controlled Plane connection. Modify Route is also used to delete an OUC from an existing ONNS connection, or from an ONNS connection that has already been deleted. Note that an OUC can also be added or deleted from the CIT.

The Modify Route feature can be used to:

- Change Routing Constraints (Bridge and Roll) without changing the ASTN protection type
- Change the ASTN protection type and/or another ASTN value.
- Change connection shapes only, that is, either add or delete OUC. In this case, no other ASTN values can be modified.

After a Modify Route operation is performed, the end cross-connection shapes are changed based on the modified ASTN Protection type.

ONNS ASTN connections that are in the In Effect step can be modified using the Modify Route item in the Go menu of the Network Connections page and the Graphical Layout page.

The Modify Route feature allows changes to the following:

- ASTN Protection type or ASTN Protection mode
- Routing Constraints
- Restoration Priority

Note that the management system will not allow the user to change the ASTN Protection type and the Connection Shape at the same time.



Graphical Layout for ONNS

The following information is conceptual information about the graphical layout for ONNS. This information is meant to complement the tasks presented later in this section.

Management system functionality

The route management for ONNS subnetwork connection of the connections are shared between the management system and the edge ASTN NE in the path. The management system identifies and manages only the routes outside of the ONNS domain. During path setup, the management system sends connection requests to the edge ASTN NE for the ONNS subnetwork connections. The edge ASTN NE determines the route within the ONNS domain based on the protection type and constraint criteria specified by the user and executes path setup. The management system can place the ONNS subnetwork connection portion of the connection In-effect, even though the path details are unknown.

Control plane path state

The user has the capability to retrieve details of an ONNS route by opening the Graphical Layout of that specific connection. The **Control plane path information** field in the header portion of the Graphical Layout of the ONNS subnetwork connection informs the user about the status of the connection. This information is additionally found on the Connections page in the Details panel.

The following describes the possible control plane path states. These control plane path states also apply to Tandem connections.

- **Unknown** - the end-to-end route within the ONNS domain has not yet been discovered by the user via the management system.
- **Known** - the end-to-end route within the ONNS domain has been discovered after a successful discover route request from the user.
- **Stale** - the end-to-end route within the ONNS domain has changed and the details are unknown to the management system.

On the Graphical Layout, the Local, Partial, and Active designations indicate the state of the ONNS connection in the management system with respect to the Control Plane Path States.

If an ONNS connection is deleted from the CIT, the Graphical Layout displays the Control Plane Path Information as Path Improperly Disconnected.

Managing ONNS path states

After a new ONNS connection is placed in-effect, the user can perform a route discovery from the Job Updates page, by selecting the connection name. The route is discovered by the management system, and displayed on the graphical layout. The control plane path state changes from **Unknown** to **Known**.

If the route has changed within the ONNS domain, the control plane path state will be **Stale**. The route can be re-discovered by the management system, and brought back into sync by displaying the graphical layout from the Connections page. The control plane path state changes from **Stale** to **Known**.

Route Discovery

Details of an ONNS route are displayed for a specific route by highlighting the connection and opening the Graphical Layout from the Go menu of the Network Connection List page. The Graphical Layout page displays the end-to-end path to the user. This also applies to ONNS tandem connections that may or may not be associated with a network connection.

Tandem Connections

The management system displays tandem ONNS connections on the Graphical Layout page. The Graphical Layout header on the page indicates whether the connection displayed is a tandem connection, and whether the tandem connection is either **Unknown** or **Stale**.

Rearranged Connections

If a connection has been rearranged, only the new route is displayed on the Graphical Layout for the Controlled Plane part of the connection.



ONNS Database Synchronization

Overview

The following information is conceptual information about ONNS database synchronization concepts. This information is meant to complement the tasks presented later in this section.

Types of ONNS database synchronizations

Once communication is established between the management system and the ASTN NEs, the management system automatically performs a complete database synchronization, all information between the ONNS NEs and the management system is in sync.

ONNS connection synchronizations may also be manually performed to keep the management system's view of ONNS subnetwork connections (connections) in the network current with changes that have occurred in the network. There are three types of partial database synchronizations which, when run manually, contain this unique ONNS information.

- **Configuration - Cross Connection** - The management system receives cross-connection information for all cross connections, including the ONNS subnetwork.
- **Configuration - Port Parameters** - The management system receives the following port parameters from the ASTN NE:
 - Network Interface Type - indicates the attribute value. Possible values are: **None, Customer/Client, or Internal Network**
 - Minimum Cross-connection Rate - the smallest cross-connection rate supported by the physical termination port
 - Maximum Cross-connection Rate - the largest cross-connection rate supported by the physical termination port
 - Shared Risk Link Group (SRLG) - indicates the risk for the existing traffic.
 - Propagation Delay - Indicates the maximum delay value of the transmit portion of the port.
 - Cost - indicates the cost value associated with the port.

- **Configuration - Network Connections (ONNS)** - The management system synchronizes the following information about end-to-end connections initiated by the management system, set up by ONNS from the ASTN NEs:
 - Modified ONNS connections
 - Deleted ONNS connectionsIn order for the ONNS network connections synchronization to be completed successfully, port parameters and cross-connections synchronizations must have been performed and completed successfully.
- **Configuration - Network OUC Sync** - The management system synchronizes the OUC ports for an ONNS connection. This synchronization can be performed either network-wide or on a per NE basis. After a network-wide OUC synchronization, the OUCs are stored in the management system as uncorrelated OUCs.

Network Synchronization Discrepancies

There are two types of network discrepancies that can occur due to synchronization processes:

- **Creation of Tandem ONNS Connections** - Connections that exist in the network, but are not in the management system, are discovered and stored in the management system as Tandem Network Connections via a Network Synchronization. These Tandem Network Connections can be associated to a controlled plane connection.
- **Inconsistent Connections** - Connections are marked as inconsistent connections if the corresponding ONNS connection is deleted from the CIT. These connections can be associated to a controlled plane.

For further information

For more information about database synchronization concepts see Tools in the Lucent OMS Network Element Management Guide.



Filter ONNS NEs on the Network Map

When to use

Use this task to filter your view of the Network Map so that only NEs of the ONNS domain are displayed.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to filter your view of the Network Map so that only NEs of the ONNS domain are displayed.

- 1 Use the icons or object links to follow this path:

- **Network**

Result: The Network Map is displayed.

- 2 Click on the **Filter** tool in the toolbar.

Result: A submenu is displayed.

- 3 Select **ASTN**.

Result: The Network Map changes so only the ONNS domain NEs are displayed.

END OF STEPS



Provision ASTN NE Port Parameters

When to use

Use this task to provision the port parameters for an ASTN NE.

Related information

See the following topics:

- Provision ASTN NE Port Parameters task in the Lucent OMS Network Element Management Guide

Before you begin

Before you begin this task, ensure the following:

- The customer/client facing ports on the ASTN NEs are completely free with no connections associated them.
- Some port parameters have already been pre-provisioned.

Task

Complete the following steps to provision the port parameters for an ASTN NE.

- 1 View a list of ports, using the View a List of Physical Ports task in the Lucent OMS Network Element Management Guide.

Result: The list at the bottom of the Ports page is populated with a list of ports that meet your search criteria.

- 2 The **Native name** column of the table lists the names of the ports. Each name is a hyperlink.

Do one of the following:

- Click the name of the port you wish to provision.
- Click the radio button next to the port you wish to provision. From the Go menu, select **Display all contained ports** or **Display contained STS-n** and click the **Go** button.

Result: The Port page is displayed.

- 3 From the Port page, open the **Control Plane** panel.

Result: The ONNS control plane parameters are displayed.

.....

- 4 Enter the desired ASTN NE port parameters.
-

- 5 Click the **Submit** button.

Result: The parameters of the port are provisioned, and a confirmation is issued in the Messages panel. The Job Updates page is displayed, and reports the status of the modification of the port parameters.

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



Provision an ONNS Multiplex Section Connection

When to use

Use this task to provision both ENNI and non-ENNI ONNS multiplex section connection. Field displayed while provisioning an ONNS Multiplex Section Connection vary depending on the **Domain type** and the **Protection type** selected.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- Ensure the ASTN NEs are associated with ONNS.
- Port resources have been provisioned.
- Open your Job Updates window so that you can monitor the status of the added connection.

Task, Part 1 of 4: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ONNS multiplex section connection.

-
- 1 The Network Connections page is displayed.
-

- 2 Click the New tool.

A menu is displayed. Select **TDM connection**, and then select **Multiplex Section**.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed at the bottom of the Network Map.

- 3 *Optional.* On the Network Map, select two NEs to be the endpoints of the physical network connection.

Note: Only NEs in your domain are available for selection if you are a domain user.

- 4 In the **Connection rate** field, select a rate from the drop-down list.

If you selected the endpoint NEs, the **Connection rate** field offers only those rates supported by the selected NEs.

Result: The **Connection rate** field locks.

.....

5 Skip the **Service type** field, which is set by default to **Not applicable**.

.....

6 In the **Protection type** field select **Unprotected**.

.....

7 In the **Domain type** field, select **Network owned**.

.....

8 In the **NE** and **Port ID** fields, if you selected the endpoint NEs in Step 3, the NE fields are already populated with your selections. Go to next Step. To specify the endpoint NEs and ports for the connection, select one of the following methods:

- In the **From NE** and **To port ID** fields, enter the NE and port names.
- Use the following procedure to select the endpoint NEs and ports:
 1. Click on the **NE** or **Port ID** hyperlinks to display the NE/Ports Selection pop-up window. This window is used to specify the endpoint NEs and ports for the A-end and Z-end of the connection.
 2. Click on the **NEs/Ports** names in the tree panel to select the NEs and Ports for the A-end and Z-end of the network connection. As selections are made, the NEs and Port IDs appear on the Connection parameters panel.
 3. After the **NEs/Ports** are selected, close the NE/Ports Selection window.

Note # 1: Only NEs in your domain are available for selection if you are a domain user.

Note # 2: If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.

.....

9 Select the **Connection Name Format** from the drop-down list.

.....

10 In the **Connection name** field, enter a name for the connection. If you do not enter one, the management system generates one automatically.

-
- 11 The **Connection alias** field is present if a specific installation parameter was enabled during the installation of the management system. If this field is present, the management system automatically generates a connection alias. Accept it or enter a different alias for the connection.
-
- 12 Click the number 2 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Order parameters panel.

Result: The Order parameters panel is displayed.

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

Task, Part 2 of 4: Specify the Order parameters

Complete the following steps to provision the Order parameters of an ONNS Multiplex Section network connection.

-
- 1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
-
- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
-
- 3 In the **Order step** field, select the order step from the drop-down list.
-
- 4 In the **Order type** field, select either **Add** or **Modify**.
-
- 5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.
-
- 6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Customer priority** field, select a number 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The number 2 is the default.

.....

- 7 The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Quality of service** field, enter a 10-character string.

.....

- 8 In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-

- 9 In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.
-

- 10 In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
-

- 11 Click the number 3 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the transmission parameters panel.

Result: The Transmission parameters panel is displayed.

.....
 END OF STEPS

Task, Part 3 of 4: Specify the Transmission parameters

Complete the following steps to provision the Transmission parameters of an ONNS multiplex section connection.

.....

- 1 Select the **From Port Network Interface Type** from the drop-down list.

- 2 Select the **To Port Network Interface Type** from the drop-down list.
- 3 Use the **SLRG** link to select NE values.
- 4 Select the **Cost** from the drop-down list.
- 5 Select the **ASTN Propagation Delay** from the drop-down list.
- 6 Select the **minXcRate** from the drop-down list.
- 7 Select the **maxXcRate** from the drop-down list.
- 8 Click the number 3 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Transmission parameters panel.

Result: The Transmission parameters panel is displayed.

- 9 The **A Network Interface Type** field, and the **Z Network Interface Type** field are automatically set to **Internal Network** if the **Domain Type** is **Network Owned**.
- 10 The **Cost**, **SRLG** and the **ASTN Propagation Delay** fields are automatically set to **USE_NE_VALUES** if no values are selected.
- 11 In the **Minimum NN cross-connect rate** field and the **Maximum NN cross-connect rate** field, select the minimum and maximum cross-connection rates from the drop down list, or select **USE_NE_VALUES**.
- 12 Click the number 4 in the navigation aid to move to the Connection Creation Summary parameters panel, or click the Next button at the bottom of the Transmission Parameters panel.

Result: The Connection Creation Summary panel is displayed. The Summary panel presents all of the selections that have been made in the previous panels.

END OF STEPS

Task, Part 4 of 4: Review and submit the connection

Complete the following steps to review and submit an ONNS multiplex section connection.

1 Review the summary for this connection. Do one of the following:

- If you wish to return to a panel to change a selection, click the step number or the step text on the navigation aid, click the **Edit** button for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step.
- If the selections are all correct, click the **Submit** button to complete the addition of the Multiplex Section connection.

Result: The ONNS multiplex section connection is added.

2 Use the Job Updates page to show the addition of the ONNS multiplex section connection, and the progress of the order from planned to local design, and so on.

Result: The order stops at the order step that was specified on the Order parameters panel.

END OF STEPS



Modify ASTN NE Port Parameters for Multiplex Section Connections

When to use

Use this task to modify the ASTN NE port parameters of a multiplex section network connection.

Before you begin

Do the following:

- Ensure the ASTN NE is associated with ONNS and the session between the management system and the NE is up.
- Ensure there are no connections already provisioned between the ASTN NEs.
- Ensure that there is an in-effect order.
- Ensure that the management system is able to communicate with the NEs at the ends of the connection.
- Open your Job Updates window so you can monitor the status of the added connection.

Task

Complete the following steps to modify the parameters of a multiplex section network connection.

- 1 The Network Connections page is displayed. Click the radio button next to the multiplex section network connection for which the ASTN port parameters are to be modified.
-

- 2 From the Go menu, select **Modify parameters** and click the Go button.

Result: The Modify Connection page is displayed. This page includes a series of panels. The Connection parameters panel is displayed.

- 3 If desired, you may change any of the allowable ONNS entries in the Connections parameters or Transmission parameters panels.

Important! Depending on the connection selected, not all panels will be displayed.

- 4 Click the **Submit** button.

Result: The multiplex section network connection is modified.

The Job Updates page monitors the status of the modify parameters request. This page shows the modification of the physical network connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

When the order for the multiplex section network connection goes to the in-effect order step, the Network Map is updated with the multiplex section network connection.

END OF STEPS



View ONNS Connection Groups

When to use

Use this task to view ONNS Connection Groups.

Before you begin

Ensure that some MxN Connection Groups exist.

Task

Complete the following steps to view ONNS Connection Groups.

- 1 Use the icons or the object links to follow this path: **Connections > Connection Group**.

Result: The search panel of the Connection Group page is displayed.

- 2 Enter or select information in the following fields to filter the list of connection groups:
 - **Connection group name** - Enter the Connection group name to be displayed.
 - **Connection rate** - Select the Connection rate from the drop-down list.
 - **Sort** - Make selections in the Sort fields as needed.
-

- 3 Click the **Search** button.

Result: The list at the bottom of the Connection Group page is populated with a list of the Connection groups that meet your search criteria.

END OF STEPS



View/Query ONNS ASTN Capacity Utilization

When to use

Use this task to view and/or query ONNS ASTN capacity utilization information.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view and/or query ONNS ASTN capacity utilization information.

- 1 Use the icons or the object links to follow this path: **Network**.

Result: The Network Map is displayed.

- 2 On the Network Map, expand node icons until the link between two ONNS nodes for which you want to view or query a list of ASTN capacity utilization information is visible.
-

- 3 On the Network Map, right-click on the link between the two ONNS nodes.

Result: A menu is displayed.

- 4 Select **ASTN Topology Query**.

Result: The Capacity Utilization page is displayed. The ASTN Topology Query Search panel minimized, and the results data table is pre-populated with capacity utilization information specific to the ONNS link that you selected on the Network Map.

- 5 If you do not want to view any other ASTN capacity utilization information, you are done with this task.
-

- 6 If you want to view other ASTN capacity utilization information not displayed in the data results table, expand the ASTN Topology Query Search panel.

-
- 7** Enter the **From NE** or use the hyperlink to select the **From NE** from the Network Elements pop-up screen and click **OK**.

Result: The **From NE** field in the ASTN Topology Query Search panel reflects your entry or your selection.

- 8** Enter the **To NE** or use the hyperlink to select the **To NE** from the Network Elements pop-up screen and click **OK**.

Result: The **To NE** field in the ASTN Topology Query Search panel reflects your entry or your selection.

- 9** Click the **Search** button.

Result: The results data table is populated with information that meets your search criteria.

- 10** If you wish to initiate another ASTN capacity utilization query, return to Step 7. Otherwise, you are done with this task.

END OF STEPS



View ONNS Associated MxN Connection List

When to use

Use this task to view the ONNS Associated MxN Connection List.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view ONNS Associated MxN Connection List.

- 1 The Connection Group page is populated with a list of Connection Groups that meet your search criteria.

- 2 Click the radio button to the left of the Connection Group for which you want to view its associated MxN Connection list, or use the Connection Group name hyperlink in the data table populated with your search results.

- 3 Select **Associated MxN Connection list** from the **Go** menu, and click the Go button.

Result: The Associate MxN Connection List page is displayed for the Connection Group that meets your search criteria.

END OF STEPS



Associate a Tandem Connection to a Controlled Plane

When to use

Use this task to associate an ONNS Tandem Network Connection with a controlled plane. This task applies to all ASTN Protection types except Y Protected.

Before you begin

Ensure that Tandem network connections are inventoried in the management system.

Task

Complete the following steps to associate an ONNS Tandem Connection with a controlled plane.

- 1 The selected page is populated with a list of connections that meet your search criteria.

- 2 Click the radio button to the left of the Tandem Connection for which you want to associate a plane, and select **Associate to controlled plane** from the Go menu.

Result: The system associates the Tandem connection with a controlled plane and provides a message in the message text area. The Tandem network connection is converted to a Regular network connection

END OF STEPS



Provision an ONNS Controlled Plane Service Connection

When to use

Use this task to provision an ONNS service connection for a controlled plane.

A Group setup is applicable only to a connection with an ASTN Protection type of Unprotected.

For OUC provisioning, the connection shape and the ASTN Protection type must be selected. Note that the connection shape and the ASTN Protection type cannot be changed at the same time.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- For the controlled plane segment of the connection, ensure the ASTN NEs are associated with ONNS.
- Port resources have been provisioned.
- Open your Job Updates window so that you can monitor the status of the added connection.
- For OUC connections, ensure that the Order Step is Planned or Local Design.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ONNS controlled plane service connection.

1 The Network Connections page is displayed.

2 Click the New tool. A menu is displayed. Select **TDM connection**, and then select **Service** from the submenu.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed.

3 *Optional.* On the Network Map, select two NEs to be the endpoints of the ONNS control plane connection.

Note: Only NEs in your domain are available for selection if you are a domain user.

-
- 4 In the **Connection rate** field, select a rate from the drop-down list.

If you selected the endpoint NEs, the **Connection rate** field offers only those rates supported by the selected NEs.

Result: The **Connection rate** field locks.

- 5 In the **Service Type** field, select a service type for the connection from the drop-down list.
-

- 6 In the **Category** field, select **Controlled plane**.
-

- 7 Select the **Connection shape** from the drop-down list. For OUC connections, the only valid selections are **Add-drop (bi)** or **Double add-drop (bi)**.
-

- 8 The number and type of NE/Port ID fields selected is dependent on the Connection shape selected.

In the **NE** and **Port ID** fields, if you selected the endpoint NEs, the NE fields are already populated with your selections. Go to next Step if you do *not* change the **Connection shape**. If you do change the **Connection shape**, continue with this step. To specify the endpoint NEs and ports for the connection, select one of the following methods:

- In the **From NE** and **To port ID** fields, enter the NE and port names.
- Use the following procedure to select the endpoint NEs and ports:
 1. Click on the **NE** or **Port ID** hyperlinks to display the NE/Ports Selection pop-up window. This window is used to specify the endpoint NEs and ports for the A-end and Z-end of the connection.
 2. Click on the **NEs/Ports** names in the tree panel to select the NEs and Ports for the A-end and Z-end of the network connection. As selections are made, the NEs and Port IDs appear on the Connection parameters panel.

Important!: Depending on the **Connection shape** selected, you may need to select additional NE/Port fields. If you complete selecting NEs and Port IDs, and later return to change your selection, you may need to select additional NE/Port fields.
 3. After the **NEs/Ports** are selected, close the NE/Ports Selection window.

Note # 1: For Y connections, the endpoints are different. The **From NE/Port ID** is connected to two different **To NE/Port IDs**.

Note # 2: Only NEs in your domain are available for selection if you are a domain user.

Note # 3: If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.

.....

9 Select the **Connection Name Format** from the drop-down list.

.....

10 Enter the **Connection name** for the connection. If you do not enter one, the system generates one automatically.

.....

11 The **Connection alias** field is present if a specific installation parameter was enabled during the installation of the management system. If this field is present, the system automatically generates a connection alias. Accept it or enter a different alias for the connection.

.....

12 Select the **Customer name** from the drop-down list.

.....

13 In the **ASTN protection type** field, select one of the following protection types for the connection from the drop-down list.

- **Unprotected**
- **Network 1+1 protected**
- **Auto Re-Route**
- **Y Protected**
- **Permanent 1+1 Protected**

.....

14 In the **ASTN protection mode**, select **Revertive** or **Non-revertive**. If the **ASTN protection type** field selected was **Auto Re-Route**, go to Step 16.

.....

15 In the **ASTN restoration priority** field, select a value of **0** to **7**. This field is only valid if the ASTN Protection Type is Auto Re-route. A value of 0 is high and 7 is low. Services with a low priority are primary candidates for pre-emption. (This field is added to the panel when the **ASTN protection type** selected is **Network 1+1 protected**.) Go to next Step.

-
- 16** Click the number 2 in the navigation aid to move to the Routing parameters panel to entering the routing constraints for the ONNS domain. The fields in this panel are all optional, and your selections are based on the desired routing constraints for the connection.

Result: The Routing parameters panel is displayed.

END OF STEPS

Task, Part 2 of 5: Specify the Routing Parameters

Complete the following steps to provision the routing constraints parameters.

-
- 1** In the **ASTN propagation delay** field, enter the maximum delay value associated between the A and Z end NEs of the ONNS connection being provisioned.
-
- 2** In the **Choose** field, select either **Exclude ASTN nodes** or **Explicit ASTN nodes**.
- Result:** Based on your selection, either the **Exclude ASTN nodes** hyperlink will display, or the **Explicit ASTN nodes** hyperlink will display.
-
- 3** Click the hyperlink that is displayed.
- Result:** A pop-up window is displayed which allows you to select NEs to include in or exclude from the connection. Select the appropriate NEs, and click **OK**. The selected NEs appear in the **Explicit/Exclude ASTN Nodes** list.
-
- 4** Click the **Exclude SRLG List** hyperlink.
- Result:** The SRLG Selection pop-up window is displayed.
-
- 5** Click the SRLGs you wish to exclude from the connection, and click **OK**.
- Result:** The excluded SRLGs appear in the **Exclude SRLG List**.
-
- 6** *Optional.* Select the **Disjointness** from the drop-down list. Options are: **Fully SRLG, Complete,** or **Maximal**.

.....

7 *Optional.* Select the **Group Setup Type** from the drop-down list. This field only applies to VCGs for VCG servers with a Connection rate of VCG. Options are: **Mincost** (default) or **Minroutes**.

.....

8 Click the number 3 in the navigation aid to move to the Order parameters panel.

Result: The Order parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters.

.....

1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.

.....

2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.

.....

3 In the **Order step** field, select the order step from the drop-down list.

.....

4 In the **Order type** field, select **Add** .

.....

5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.

.....

6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Customer priority** field, select a number 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The number 2 is the default.

-
- 7** The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Quality of service** field, enter a 10-character string.

.....

- 8** In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-

- 9** In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.
-

- 10** In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
-

- 11** Click the number 4 in the navigation aid to move to the Assurance Parameters panel.

Result: The Assurance Parameters panel is displayed.

END OF STEPS

.....

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

.....

- 1** In the **15-minute collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 2** In the **15-minute monitoring** field, select either **End ports** or **None** from the drop-down menu.

.....

3 In the **15-minute intervals** field, select the appropriate timeframe from the drop-down menu.

.....

4 In the **24-hour collection type** field, select either **Collect, Monitor, or None**.

.....

5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.

.....

6 In the **24-hour intervals** field, select the appropriate timeframe from the drop-down menu.

.....

7 In the **Bi-dir 24-hour collection type** field, select either **Collect, Monitor, or None**.

.....

8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.

.....

9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.

.....

10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes**.

Result: If the request is successful, the NE assigns a TP to an Alarm Profile.

If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen

If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.

.....

11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes**.

.....

12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes**.

-
- 13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.

Result: The Connection Creation Summary panel is displayed.

END OF STEPS

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an ONNS controlled plane service connection.

-
- 1 Review the summary for this connection. Do one of the following:
- If you wish to change a selection, use the navigation aid to return to a panel, change a selection, and then return to this step.
 - If the selections are all correct, click the **Submit** button to complete the addition of the ONNS controlled plane service connection.

Result: The ONNS controlled plane service connection is added.

For OUC connections, the connection moves to the In Effect step state only if both the ONNS and the OUC network creations are successful. If either the ONNS network creation or the OUC network creation fail, the connection is moved to the Implementation Failed step state. In this case of failure, the ONNS connection exists in the management system as a regular network connection for all Protection types. The Command Deployment displays the reason for the failure.

The Job Updates page monitors the status of the add connection request. This page shows the addition of the connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

END OF STEPS



Provision an ONNS Mixed Plane Service Connection

When to use

Use this task to provision an ONNS service connection for a mixed plane.

A Group setup is applicable only to a connection with an ASTN Protection type of Unprotected.

For OUC provisioning, the connection shape and the ASTN Protection type must be selected. Note that the connection shape and the ASTN Protection type cannot be changed at the same time.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- For the controlled plane segment of the connection, ensure the ASTN NEs are associated with ONNS.
- Port resources have been provisioned.
- Open your Job Updates window so that you can monitor the status of the added connection.
- For OUC connections, ensure that the Order Step is Planned or Local Design.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ONNS controlled plane service connection.

1 The Network Connections page is displayed.

2 Click the New tool. A menu is displayed. Select **TDM connection**, and then select **Service** from the submenu.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed.

3 *Optional.* On the Network Map, select two NEs to be the endpoints of the ONNS control plane connection.

Note: Only NEs in your domain are available for selection if you are a domain user.

-
- 4 In the **Connection rate** field, select a rate from the drop-down list.
If you selected the endpoint NEs, the **Connection rate** field offers only those rates supported by the selected NEs.
Result: The **Connection rate** field locks.
-
- 5 In the **Service Type** field, select a service type for the connection from the drop-down list.
-
- 6 In the **Category** field, select **Controlled plane**.
-
- 7 Select the **Connection shape** from the drop-down list. For OUC connections, the only valid selections are **Add-drop A (bi)**, **Add-drop Z (bi)** or **Double add-drop (bi)**.
-
- 8 In the **Group Type** field, select connection aggregate.
-
- 9 Enter the **Connection Aggregate Name** for the connection.
-
- 10 Enter the **Connection name** for the connection. If you do not enter one, the system generates one automatically.
-
- 11 The **Connection alias** field is present if a specific installation parameter was enabled during the installation of the management system. If this field is present, the system automatically generates a connection alias. Accept it or enter a different alias for the connection.
-
- 12 Select the **Customer name** from the drop-down list.
-
- 13 In the **ASTN protection type** field, select one of the following protection types for the connection from the drop-down list.
- **Unprotected**
 - **Network 1+1 protected**
 - **Auto Re-Route**

- **Y Protected**
- **Permanent 1+1 Protected**

.....

14 In the **ASTN protection mode**, select **Revertive** or **Non-revertive**. If the **ASTN protection type** field selected was **Auto Re-Route**.

.....

15 In the **ASTN restoration priority** field, select a value of **0** to **7**. This field is only valid if the ASTN Protection Type is Auto Re-route. A value of 0 is high and 7 is low. Services with a low priority are primary candidates for pre-emption. (This field is added to the panel when the **ASTN protection type** selected is **Network 1+1 protected**)

.....

16 Click the number 2 in the navigation aid to move to the Routing parameters panel to entering the routing constraints for the ONNS domain. The fields in this panel are all optional, and your selections are based on the desired routing constraints for the connection.

Result: The Routing parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 2 of 5: Specify the Routing Parameters

Complete the following steps to provision the routing constraints parameters.

.....

1 In the **ASTN propagation delay** field, enter the maximum delay value associated between the A and Z end NEs of the ONNS connection being provisioned.

.....

2 In the **Choose** field, select either **Exclude ASTN nodes** or **Explicit ASTN nodes**.

Result: Based on your selection, either the **Exclude ASTN nodes** hyperlink will display, or the **Explicit ASTN nodes** hyperlink will display.

.....

3 Click the hyperlink that is displayed.

Result: A pop-up window is displayed which allows you to select NEs to include in or exclude from the connection. Select the appropriate NEs, and click **OK**. The selected NEs appear in the **Explicit/Exclude ASTN Nodes** list.

.....

4 Click the **Exclude SRLG List** hyperlink.

.....

Result: The SRLG Selection pop-up window is displayed.

- 5 Click the SRLGs you wish to exclude from the connection, and click **OK**.

Result: The excluded SRLGs appear in the **Exclude SRLG List**.

- 6 *Optional.* Select the **Disjointness** from the drop-down list. Options are: **Fully SRLG, Complete,** or **Maximal**.

- 7 *Optional.* Select the **Group Setup Type** from the drop-down list. This field only applies to VCGs for VCG servers with a Connection rate of VCG. Options are: **Mincost** (default) or **Minroutes**.

- 8 Click the number 3 in the navigation aid to move to the Order parameters panel.

Result: The Order parameters panel is displayed.

END OF STEPS

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters.

- 1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
- 3 In the **Order step** field, select the order step from the drop-down list.
- 4 In the **Order type** field, select **Add** .

5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.

6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Customer priority** field, select a number 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The number 2 is the default.

7 The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Quality of service** field, enter a 10-character string.

8 In the **Ignore alarm** field, turn this parameter on or off.

- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-

9 In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.

10 In the **Comments** field, enter any notes that you want to store as part of the record for this connection.

11 Click the number 4 in the navigation aid to move to the Assurance Parameters panel.

Result: The Assurance Parameters panel is displayed.

END OF STEPS

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

- 1 In the **15-minute collection type** field, select either **Collect, Monitor, or None**.
- 2 In the **15-minute monitoring** field, select either **End ports** or **None** from the drop-down menu.
- 3 In the **15-minute intervals** field, select the appropriate timeframe from the drop-down menu.
- 4 In the **24-hour collection type** field, select either **Collect, Monitor, or None**.
- 5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
- 6 In the **24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
- 7 In the **Bi-dir 24-hour collection type** field, select either **Collect, Monitor, or None**.
- 8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
- 9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
- 10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes**.

Result: If the request is successful, the NE assigns a TP to an Alarm Profile.

If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen

If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.

11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes**.

12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes**.

13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.

Result: The Connection Creation Summary panel is displayed.

END OF STEPS

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an ONNS mixed plane service connection.

-
- 1** Review the summary for this connection. Do one of the following:
- If you wish to change a selection, use the navigation aid to return to a panel, change a selection, and then return to this step.
 - If the selections are all correct, click the **Submit** button to complete the addition of the ONNS mixed plane service connection.

Result: The ONNS mixed plane service connection is added.

For OUC connections, the connection moves to the In Effect step state only if both the ONNS and the OUC network creations are successful. If either the ONNS network creation or the OUC network creation fail, the connection is moved to the Implementation Failed step state. In this case of failure, the ONNS connection exists in the management system as a regular network connection for all Protection types. The Command Deployment displays the reason for the failure.

The Job Updates page monitors the status of the add connection request. This page shows the addition of the connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

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



Provision an OUC Connection for In Effect Steps

When to use

Use this task to provision an ONNS OUC connection for a controlled plane. This task applies to connections in the In Effect Order step only.

For OUC provisioning, the connection shape and the ASTN Protection type must be selected. Note that the connection shape and the ASTN Protection type cannot be changed at the same time.

OUC provisioning cannot be done on a connection with a Connection rate of VCG.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- For the controlled plane segment of the connection, ensure the ASTN NEs are associated with ONNS.
- Port resources have been provisioned.
- Open your Job Updates window so that you can monitor the status of the added connection.
- Ensure that the ONNS connection is in the In Effect order step.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ONNS OUC In Effect connection.

1 The Network Connections page is displayed.

2 Click the New tool. A menu is displayed. Select **TDM connection**, and then select **Service** from the submenu.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed.

3 *Optional.* On the Network Map, select two NEs to be the endpoints of the ONNS control plane connection with an Interface Type of Customer/Client.

Note: Only NEs in your domain are available for selection if you are a domain user.

-
- 4 In the **Connection rate** field, select a rate from the drop-down list.
- If you selected the endpoint NEs, the **Connection rate** field offers only those rates supported by the selected NEs.
- Result:** The **Connection rate** field locks.
-
- 5 In the **Service Type** field, select a service type for the connection from the drop-down list.
-
- 6 In the **Category** field, select **Controlled plane**.
-
- 7 Select the **Connection shape** from the drop-down list. For OUC connections, the only valid selections are **Add-drop A (bi)**, or **Add-drop Z (bi)**, **Double add-drop (bi)**. Select **Add-drop (bi)** if there is to be a UPSR only on one end of the ONNS domain.
- These **Connection shape** selections are not applicable for VCG servers with a **Connection rate** of **VCG**.
-
- 8 In the **NE** and **Port ID** fields, if you selected the endpoint NEs, the NE fields are already populated with your selections. Go to next Step. To specify the endpoint NEs and ports for control plane connection with an Interface Type of Customer/Client, select one of the following methods:
- In the **From NE** and **To port ID** fields, enter the NE and port names.
 - Use the following procedure to select the endpoint NEs and ports. For the first time that you are selecting Ports in this process, you are selecting the From Port 1 and the To Port 1.
 1. Click on the **NE** or **Port ID** hyperlinks to display the NE/Ports Selection pop-up window. This window is used to specify the endpoint NEs and ports for the A-end and Z-end of the connection.
 2. Click on the **NEs/Ports** names in the tree panel to select the NEs and Ports for the A-end and Z-end of the network connection. As selections are made, the NEs and Port IDs appear on the Connection parameters panel.
 3. After the **NEs/Ports** are selected, close the NE/Ports Selection window.
- Note # 1:** Only NEs in your domain are available for selection if you are a domain user.
- Note # 2:** If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.

If you are adding only one OUC Customer/Client to the ONNS Controlled Plane, repeat Steps 1 through 3 above to add a free Customer/Client port for the OUC port to the A End of the ONNS Controlled Plane. You are adding the From Port 2 field. This creates a three-ended connection. In order to perform this selection, the Connection shape selected must be **Add/Drop A (bi)** or **Add/Drop Z (bi)**.

If you are adding two OUC Customer/Clients ports to the ONNS Controlled Plane, repeat this step again to add free Customer/Client ports for the OUC ports to both the A End of the ONNS Controlled Plane and to the Z End of the ONNS Controlled Plane. You are adding the From Port 2 and the To Port 2 fields. This creates a four-ended connection. In order to perform this selection, the Connection shape selected must be **Double add-drop (bi)**.

.....

9 Select the **Connection Name Format** from the drop-down list.

.....

10 Enter the **Connection name** for the connection. If you do not enter one, the system generates one automatically.

.....

11 The **Connection alias** field is present if a specific installation parameter was enabled during the installation of the management system. If this field is present, the system automatically generates a connection alias. Accept it or enter a different alias for the connection.

.....

12 Select the **Customer name** from the drop-down list.

.....

13 In the **ASTN protection type** field, select the protection type for the connection from the drop-down list based on the following criteria.

- If the **Connection shape** selected is **Add/Drop A (bi)** or **Add/Drop Z (bi)**, select any **ASTN protection type** *except* **Y Protected**.
- If the **Connection shape** selected, is **Double Add/Drop (bi)**, any **ASTN protection type** can be selected. If the OUC is only to be provisioned on the **From NE**, you *must* select **Y Protected**.

If you selected either **Unprotected** or **Y Protected** as the **ASTN protection type**.

If you selected **Network 1+1** as the **ASTN protection type**.

If you selected **Auto Re-Route** as the **ASTN protection type**.

-
- 14** In the **ASTN protection mode**, select **Revertive** or **Non-revertive**. If the **ASTN protection type** field selected is **Auto Re-Route**.
-
- 15** *Optional.* In the **ASTN restoration priority** field, select a value of **0** to **7**. A value of 0 is high and 7 is low. Services with a low priority are primary candidates for pre-emption. (This field is added to the panel when the **ASTN protection type** selected is **Network 1+1 protected**).
-
- 16** Click the number 2 in the navigation aid to move to the Routing parameters panel to entering the routing constraints for the ONNS domain. The fields in this panel are all optional, and your selections are based on the desired routing constraints for the connection.

Result: The Routing parameters panel is displayed.

.....
 END OF STEPS

Task, Part 2 of 5: Specify the Routing Parameters

Complete the following steps to provision the routing constraints parameters of an ONNS OUC connection.

-
- 1** In the **ASTN propagation delay** field, enter the maximum delay value associated between Port-A and Port-Z.
-
- 2** In the **Choose** field, select either **Exclude ASTN nodes** or **Explicit ASTN nodes**.
- Result:** Based on your selection, either the **Exclude ASTN nodes** hyperlink will display, or the **Explicit ASTN nodes** hyperlink will display.
-
- 3** Click the hyperlink that is displayed.
- Result:** A pop-up window is displayed which allows you to select NEs to include in or exclude from the connection. Select the appropriate NEs, and click **OK**. The selected NEs appear in the **Explicit/Exclude ASTN Nodes** list.
-
- 4** Click the **Exclude SRLG List** hyperlink.

Result: The SRLG Selection pop-up window is displayed.

.....

- 5 Click the SRLGs you wish to exclude from the connection, and click **OK**.

Result: The excluded SRLGs appear in the **Exclude SRLG List**.

.....

- 6 *Optional.* Select the **Disjointness** from the drop-down list. Options are: **Fully SRLG, Complete,** or **Maximal**.
-

- 7 *Optional.* Select the **Group Setup Type** from the drop-down list. This field only applies to VCGs for VCG servers with a Connection rate of VCG. Options are: **Mincost** (default) or **Minroutes**.
-

- 8 Click the number 3 in the navigation aid to move to the Order parameters panel.

Result: The Order parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters of an ONNS OUC connection.

.....

- 1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
-

- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
-

- 3 In the **Order step** field, select the order step from the drop-down list.
-

- 4 In the **Order type** field, select **Add**.
-

-
- 5** In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.
-
- 6** In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-
- 7** In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
-
- 8** Click the number 4 in the navigation aid to move to the Assurance Parameters panel.
- Result:** The Assurance Parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

.....

- 1** In the **15-minute collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 2** In the **15-minute monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 3** In the **15-minute intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 4** In the **24-hour collection type** field, select either **Collect**, **Monitor**, or **None**.

.....
5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
.....

6 In the **24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
.....

7 In the **Bi-dir 24-hour collection type** field, select either **Collect, Monitor,** or **None.**
.....

8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
.....

9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
.....

10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes.**

Result: If the request is successful, the NE assigns a TP to an Alarm Profile.

If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen

If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.
.....

11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes.**
.....

12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes.**
.....

13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.

Result: The Connection Creation Summary panel is displayed.

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

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an ONNS OUC connection.

- 1 Review the summary for this connection. Do one of the following:
 - If you wish to change a selection, use the navigation aid to return to a panel, change a selection, and then return to this step.
 - If the selections are all correct, click the **Submit** button to complete the addition of the ONNS controlled plane connection.

Result: The ONNS/OUC controlled plane connection is added and is in the In Effect Order step.

If either the ONNS network creation or the OUC network creation fail, the connection is moved to the Implementation Failed step state. In this case of failure, the ONNS connection exists in the management system as a regular network connection for all Protection types. The Command Deployment displays the reason for the failure.

The Job Updates page monitors the status of the add connection request. This page shows the addition of the connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

END OF STEPS



Add an ONNS MxN Service Group Network Connection

When to use

Use this task to add an ONNS MxN Service Group network connection.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- If either of the endpoint NEs is to be a non-managed NE, it must be added using the Add an OMS-to-NE Connection task in the Lucent OMS Network Element Management Guide.
- If either of the endpoint NEs is to be a non-managed NE, it is recommended that the endpoint port be manually added using the Add a Port to a Non-managed NE task in the Lucent OMS Network Element Management Guide.
- Open/view your Job Updates window so that you can monitor the status of the added connection.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ONNS MxN Group Service network connection.

- 1 Open the Network Map page.

Result: If you chose the View a List of Network Connections, the Network Connections page is populated with a list of network connections that meet your search criteria. If you chose the Network Map path, the Network Map is displayed.

- 2 Click the New tool.

Various submenus are displayed. Select **TDM connection**, and then select **MxN Service Group** from the **TDM connection** submenu.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed.

- 3 In the **Connection rate** field, select a rate from the drop-down list.

Result: The **Connection rate** field locks.

4 Select the **Service Type** from the drop-down list.

5 Leave the **Connection shape** field set to **Simple (bi)**.

6 Leave the **Category** field set to **Controlled plane**.

7 In the **From/To NE/Port ID** fields, the number of NE/port ID pairs of fields displayed depends on the shape specified in the **Connection shape** field.

In the **NE** and **Port ID** fields, do one of the following to specify the endpoint NEs and ports for the connection.

- In the **NE** and **Port ID** fields, enter the NE and port names.
- Use the following procedure to select the endpoint NEs and ports. Up to 64 endpoints can be provisioned.
 1. Click the **NE** or **Port ID** hyperlinks to display the NE/Ports Selection pop-up window. This window is used to specify the endpoint NEs and ports for the From and To ends of the physical network connection and the contained logical connection.
 2. Click the **NEs/Ports** names in the tree panel to select the NEs and Ports for the From and To ends of the network connection. As selections are made, the NEs and Port IDs appear on the Connection parameters panel.
 3. After the **NEs/Ports** are selected, close the NE/Ports Selection window.

Note # 1: Only NEs in your domain are available for selection if you are a domain user.

Note # 2: If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.

8 The **ASTN Protection type** field set by default to **MxN Protected**.

9 Select the **ASTN Protection ratio** from the drop-down list.

10 Enter the **MxN Connection Group name**.

.....

11 Select the customer for the connection from the **Customer name** drop-down list.

.....

12 Click the number 2 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Routing parameters panel.

Result: The Routing Parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 2 of 5: Specify the Routing Parameters

Complete the following steps to provision the Routing parameters of an ONNS MxN Service Group network connection.

.....

1 In the **ASTN propagation delay** field, enter the maximum delay value associated between Port-A and Port-Z unidirectionally.

.....

2 In the **Choose** field, click the Exclude ASTN Nodes checkbox to exclude ASTN Nodes.

.....

3 Click the **Exclude SRLG List** hyperlink.

Result: The SRLG Selection pop-up window is displayed.

.....

4 Click the SRLGs you wish to exclude from the connection, and click **OK**.

Result: The excluded SRLGs appear in the **Exclude SRLG List**.

.....

5 Click the SRLGs you wish to exclude from the connection, and click **OK**.

Result: The excluded SRLGs appear in the **Exclude SRLG List**.

.....

6 Click the number 3 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Order parameters panel.

.....

END OF STEPS

.....

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters of an ONNS MxN Service Group network connection.

- 1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
- 3 In the **Order step** field, select the order step from the drop-down list.
- 4 In the **Order type** field, select **Add**.
- 5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.
- 6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Customer priority** field, select a number 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The number 2 is the default.
- 7 The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Quality of service** field, enter a 10-character string.

-
- 8** In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-
- 9** In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.
-
- 10** In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
-
- 11** Click the number 4 in the navigation aid to move to the Assurance Parameters panel.

Result: The Assurance Parameters panel is displayed.

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

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

.....

- 1** In the **15-minute collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 2** In the **15-minute monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 3** In the **15-minute intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 4** In the **24-hour collection type** field, select either **Collect**, **Monitor**, or **None**.

-
- 5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 6 In the **24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 7 In the **Bi-dir 24-hour collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes**.
- Result:** If the request is successful, the NE assigns a TP to an Alarm Profile.
- If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen
- If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.
-
- 11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes**.
-
- 12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes**.
-
- 13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.
- Result:** The Connection Creation Summary panel is displayed.

.....

END OF STEPS

.....

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an ONNS MxN Service Group network connection.

1 Review the summary for this connection. Do one of the following:

- If you wish to return to a panel to change a selection, click the step number or the step text on the navigation aid, click the **Edit** button for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step.
- If the selections are all correct, click the **Submit** button.

Result: The ONNS MxN Service Group network connection is added. The appropriate link connections are created. An order for the network connection is created in the management system. For managed NEs, the terminating ports are put in service.

2 Use the Job Updates page to monitor the status of the add connection request.

Result: This page shows the addition of the network connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

When the order for the network connection goes to the In Effect order step, the Network Map is updated with the service or infrastructure network connection.

END OF STEPS



Add an ONNS MxN Working Connection to an Existing MxN Connection Group

When to use

Use this task to add an ONNS MxN working connection to an existing MxN Service Group network connection.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- If either of the endpoint NEs is to be a non-managed NE, it must be added using the Add an OMS-to-NE Connection task in the Lucent OMS Network Element Management Guide.
- If either of the endpoint NEs is to be a non-managed NE, it is recommended that the endpoint port be manually added using the Add a Port to a Non-managed NE task in the Lucent OMS Network Element Management Guide.
- Open/view your Job Updates window so that you can monitor the status of the added connection.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the Connection parameters of a connection to add to an ONNS MxN Group Service network connection.

- 1 Click the radio button to the left of the connection that you want to add to a connection group. Valid selections are connections with a **Protection Type** of **MBYNWRK** only.

- 2 Select **Add to Group** from the Go menu.

Result: The MxN Connection Group connection provisioning page is displayed.

- 3 The following fields are pre-populated and are read-only. They are populated based on your connection selection.
 - **Category** - pre-populated with Controlled Plane
 - **Connection Group Name**- pre-populated with the name of the Connection Group
 - **Connection rate** - pre-populated with the connection rate of the Connection Group

- **ASTN Protection type** - pre-populated with MxN Protected
- **ASTN From/To NEs** - pre-populated with the ASTNs of the Connection Group
- **ASTN Protection ratio** - pre-populated with the Protection ratio of the Connection Group

-
- 4 Only one set of **From/To NE/Port ID** fields that are Customer/Client ports can be entered/selected.

In the **From/To NE/Port ID** fields, do one of the following:

- In the **NE** and **Port ID** fields, enter the NE and port names.
- Use the following procedure to select the endpoint NEs and ports. Up to 64 endpoints can be provisioned.
 1. Click the **NE** or **Port ID** hyperlinks to display the NE/Ports Selection pop-up window. This window is used to specify the endpoint NEs and ports for the From and To ends of the physical network connection and the contained logical connection.
 2. Click the **NEs/Ports** names in the tree panel to select the NEs and Ports for the From and To ends of the network connection. As selections are made, the NEs and Port IDs appear on the Connection parameters panel.
 3. After the **NEs/Ports** are selected, close the NE/Ports Selection window.

Note # 1: Only NEs in your domain are available for selection if you are a domain user.

Note # 2: If the Port User Label system parameter is activated, and a Port User Label has been assigned to any of the ports applicable in this step, the Port User Label field is populated with the Port User Label name associated to the native port name.

-
- 5 Click the number 2 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Routing parameters panel.

Result: The Routing Parameters panel is displayed.

END OF STEPS

Task, Part 2 of 5: Specify the Routing parameters

All Routing constraints are read-only based on the Connection Group selected.

-
- 1 Click the number 3 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Summary parameters panel.

END OF STEPS

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters of an ONNS MxN Service Group network connection.

- 1 In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
- 3 In the **Order step** field, select the order step from the drop-down list.
- 4 In the **Order type** field, select **Add**.
- 5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the scheduled data and time from a calendar. This field is displayed only if scheduling has been turned on. This field is not displayed if scheduling is not supported, if the Order Step is other than Planned or Local Design, or for Ethernet Orders, Merged Orders, or Rearrange Orders.
- 6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Customer priority** field, select a number 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The number 2 is the default.
- 7 The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.

In the **Quality of service** field, enter a 10-character string.

-
- 8** In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
-
- 9** In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.
-
- 10** In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
-
- 11** Click the number 4 in the navigation aid to move to the Assurance Parameters panel.

Result: The Assurance Parameters panel is displayed.

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

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

.....

- 1** In the **15-minute collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 2** In the **15-minute monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 3** In the **15-minute intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 4** In the **24-hour collection type** field, select either **Collect**, **Monitor**, or **None**.

-
- 5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 6 In the **24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 7 In the **Bi-dir 24-hour collection type** field, select either **Collect**, **Monitor**, or **None**.
-
- 8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.
-
- 9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.
-
- 10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes**.
- Result:** If the request is successful, the NE assigns a TP to an Alarm Profile.
- If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen
- If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.
-
- 11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes**.
-
- 12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes**.
-
- 13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.
- Result:** The Connection Creation Summary panel is displayed.

.....

END OF STEPS

.....

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an add to group connection to an ONNS MxN Service Group network connection.

1 Review the summary for this connection. Do one of the following:

- If you wish to return to a panel to change a selection, click the step number or the step text on the navigation aid, click the **Edit** button for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step.
- If the selections are all correct, click the **Submit** button.

Result: The newly-created connection can now be associated with a Controlled Plane.

The newly-created connection can be viewed on the Network Connection page and the Associated MxN Connection List page.

2 Use the Job Updates page to monitor the status of the add MBYNWRK connection request. MBYNPRT connections are not monitored by the Job Updates page.

Result: This page shows the addition of the network connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

When the order for the network connection goes to the In Effect order step, the Network Map is updated with the service or infrastructure network connection.

END OF STEPS



Modify the Route of (Rearrange) an ONNS In Effect Connection

When to use

Use this task to modify the route (rearrange) of an ONNS In Effect connection. Also use this task to add or delete an OUC to an existing ONNS Controlled Plane connection.

The Modify Route feature with a changing ASTN protection type does not apply to In Effect Controlled Plane connections where the ASTN Protection Type is MxN Protected or Y Protected. The Modify Route function cannot be performed on an improperly disconnected connection or on VCG servers. The Connection Alias field can only be modified on the Modify Connection Parameters page.

The Modify Route feature can be used to:

- Change Routing Constraints (Bridge and Roll) without changing the ASTN protection type
- Change the ASTN protection type and/or another ASTN value
- Change connection shapes only, that is, either add or delete OUC. In this case, no other ASTN values can be modified.

If you are using this page to add or to delete an OUC connection from an ONNS connection by changing the Connection shape, you cannot change the ASTN Protection type, any Routing Parameters, or any Assurance Parameters.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- Open/view your Job Updates window so that you can monitor the status of the added connection.
- Ensure that the Route is in the In Effect Order Step.
- Ensure that the Category is Controlled Plane.

Task, Part 1 of 4: Modify the Connection Parameters

Complete the following steps to modify the Connection parameters (rearrange) of an ONNS connection and/or to add an OUC to an existing ONNS connection.

- 1 Use one of the following paths to access the Modify Route page for a Controlled Plane In Effect connection:
 - **Connections > Network Connections.** Then search for connections meeting your criteria, click the radio button in the resulting search data table, and select the **Modify route** option from the Go menu.
 - **Connections > Network Connections.** Then search for connections meeting your criteria, click the radio button in the resulting search data table, and select the **Graphical layout** option from the Go menu. From the Graphical Layout page, select the **Modify route** option from the Go menu.

Result: The Modify Route page displays.

- 2 In the Connection Parameters panel of the Modify Route page, any fields can be changed. However, if you change the **ASTN Protection type** and/or the **Routing Parameters**, the **Connection shape** cannot be changed at the same time, and an error is displayed. And conversely, if you change the **Connection shape**, the **ASTN Protection type** and/or the **Routing Parameters** *cannot* be changed.
-

- 3 Click the number 2 in the navigation aid to move to the Routing Parameters panel.

Result: The Routing Parameters panel is displayed.

END OF STEPS

Task, Part 2 of 4: Modify the Routing Parameters

Complete the following steps to modify the routing parameters (rearrange) of an ONNS connection and/or to add an OUC to an existing ONNS connection.

If you have changed the **Connection shape**, you cannot change any Routing Parameters. You can change Routing parameters as long as you have *not* changed the **Connection shape**.

- 1 Modify any allowable parameters. Allowable parameters are based on the ASTN Protection type.

-
- 2 Click the number 3 in the navigation aid to move to the Order parameters panel.

Result: The Order Parameters panel is displayed.

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

Task, Part 3 of 4: Specify the Order parameters

Complete the following steps to provision the Order parameters of an ONNS controlled plane rearrange connection or to add OUC to an existing ONNS connection. Modify any fields as appropriate.

-
- 1 *Optional.* In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter one, the management system generates one automatically.
.....
 - 2 *Optional.* In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
.....
 - 3 *Optional.* In the **Order step** field, select the order step from the drop-down list.
.....
 - 4 *Optional.* In the **Order type** field, select **Modify**.
.....
 - 5 *Optional.* In the **Ignore alarm** field, turn this parameter on or off.
 - If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.
.....
 - 6 *Optional.* In the **Comments** field, enter any notes that you want to store as part of the record for this connection.
.....
 - 7 Click the number 4 in the navigation aid to move to the Modify Route Summary parameters panel.

Result: The Modify Route Summary panel is displayed. The Summary panel presents all of the selections that have been made in the previous panels.

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

Task, Part 4 of 4: Review and submit the connection

Complete the following steps to review and submit an ONNS Rearrange connection or to add an OUC to an existing ONNS connection.

.....

1 Review the summary for this connection. Do one of the following:

- If you wish to return to a panel to change a selection, click the step number or the step text on the navigation aid, click the **Edit** button for that panel, or click the hyperlink for that panel. Change the appropriate information, and then return to this step.
- If the selections are all correct, click the **Submit** button to complete the addition of the rearranged connection.

Result: If the OUCs are already in the network:

- A “soft” rearrange order is triggered by the management system and is In Effect. The OUC ports are marked as In Effect.
- The ONNS connection is correlated with the OUC ports.
- If uncorrelated OUCs exist with the specific ports selected, they are now correlated to the ONNS connection.
- The connection is marked as Stale if it was previously marked as Known.

If the OUCs are not in the network:

- A “soft” rearrange order is triggered by the management system and is In Effect. The OUC ports are marked as In Effect.
- The ONNS connection is correlated with the OUC ports.
- If no uncorrelated OUCs exist with the specific ports selected, the management system will create OUCs to the From and/or To NE as determined by the connection shape.
- The connection is marked as Stale if it was previously marked as Known.

A “soft” rearrange order for the ONNS connection is triggered by the management system. If uncorrelated OUCs exist with the specific ports selected, they are now correlated to the ONNS connection. If a rearrange is attempted on an improperly disconnected connection, an error message is displayed.

-
- 2 Use the Job Updates page to show the addition of the ONNS rearranged connection.

END OF STEPS



Delete Group for an ONNS MxN Connection Group

When to use

Use this task to delete a group for an ONNS MxN Connection Group.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to delete an ONNS MxN Connection Group.

- 1 The Connection Group page is populated with a list of Connection Groups that meet your search criteria.

- 2 Click the radio button to the left of the Connection Group for which you want to delete the MxN Connection Group, or use the Connection Group name hyperlink in the data table populated with your search results.

- 3 Select **Delete group** from the **Go** menu, and click the Go button.

Result: The MxN Connection Group selected is deleted as follows:

- If at least one of the group members is in the In Effect state, the Group is deleted.
- If some of the group connections are not in the In Effect state, these connections are removed from the management system database.

If any members of the Group selected to be deleted are in a Tagged state of Yes, with a Connection Type of Tandem, the group will not be deleted.

END OF STEPS



DB Delete Group for an ONNS MxN Connection Group

When to use

Use this task to DB Delete a group for an ONNS MxN Connection Group.

Before you begin

Ensure that the MxN Connection Group to be DB Deleted is in either the Active or Local state.

Task

Complete the following steps to DB Delete an ONNS MxN Connection Group.

- 1 The Connection Group page is populated with a list of Connection Groups that meet your search criteria.

- 2 Click the radio button to the left of the Connection Group for which you want to DB Delete the MxN Connection Group, or use the Connection Group name hyperlink in the data table populated with your search results.

- 3 Select **DB Delete group** from the **Go** menu, and click the Go button.

Result: The MxN Connection Group selected is DB Deleted.

END OF STEPS



Cancel Group for an ONNS MxN Connection Group

When to use

Use this task to cancel a group for an ONNS MxN Connection Group.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to cancel an ONNS MxN Connection Group.

- 1 The Connection Group page is populated with a list of Connection Groups that meet your search criteria.

- 2 Click the radio button to the left of the Connection Group for which you want to cancel the MxN Connection Group, or use the Connection Group name hyperlink in the data table populated with your search results.

- 3 Select **Cancel group** from the **Go** menu, and click the Go button.

Result: The MxN Connection Group selected is cancelled as follows:

- If the Connection Group is built via the management system, a command is sent to clean up the Connection Group if the Order step is Implementation.
- If the Connection Group is built via the CIT, no command is sent to the NEs, and the user must manually clean up the MxN connections from the CIT.
- If the Connection Group is in either the Planned or Local Design state, the Connection Group is DB Deleted.
- If the Connection Group is in the Implementation Completed state, the Connection Group is deleted.
- If the Connection Group is in the Implementation failed state, the Connection Group is deleted.

END OF STEPS



Provision an ENNI ONNS Controlled Plane Service Connection

When to use

Use this task to provision an ENNI ONNS service connection for a controlled plane.

This task has multiple parts.

Before you begin

Do the following:

- Ensure that the management system is able to communicate with all NEs in the connection.
- For the controlled plane segment of the connection, ensure the ASTN NEs are associated with ONNS.
- Port resources have been provisioned.
- Open your Job Updates window so that you can monitor the status of the added connection.

Task, Part 1 of 5: Specify the Connection parameters

Complete the following steps to provision the connection parameters of an ENNI ONNS controlled plane service connection.

1 The Network Connections page is displayed.

2 Click the New tool. A menu is displayed. Select **TDM connection**, and then select **Service** from the submenu.

Result: The Add Connection page is displayed. This page includes a Network Map and a series of provisioning panels. The Connection parameters panel is displayed.

3 *Optional.* On the Network Map, select two NEs to be the endpoints of the ENNI ONNS control plane connection.

Note: Only NEs in your domain are available for selection if you are a domain user.

4 In the **Category** field, select **Controlled plane**.

In the **Controlled Plane Type** field, select **ENNI**. The default value is **non-ENNI**.

-
- 5 The **Connection Alias** field is present if a specific installation parameter was enabled during the installation of the management system. If this field is present, the system automatically generates a connection alias. Accept it or enter a different alias for the connection.
-
- 6 In the **Connection Name** field, enter the connection name.
-
- 7 For ENNI connections, the **Service Type** is undetermined. This is read only field.
-
- 8 Select the **Connection shape** from the drop-down list. For ENNI connections, the only valid selection is simple (bi).
-
- 9 Select the **Group Type** from the drop-down list. Options are : **None** and **Connection Aggregate**. The default value is none.
-
- 10 The **Connection Aggregate Name** displays the connection aggregate name for the ENNI connection. This field is displayed if the Group type selected is Connection aggregate.
-
- 11 The From and To NEs fields display the ONNS enabled TDM NEs, if you have selected Controlled Plane Type as ENNI. The NE fields are already populated with your selections. When OMS supports multi-vendor control plane domains for ENNI, Lucent OMS will display the black boxes.
-
- 12 The Port ID field displays the Customer/Client ports, TNA Type, TNA Address, and Logical Port ID, if you have selected Controlled Plane Type as ENNI.
- **TNA Type** values are: **IPV4TNAADDR TNA**, **IPV6TNAADDR TNA**, or **NSAPTNAADDR TNA**. The default value is **IPV4TNAADDR TNA**.
 - **TNA Address** - TNA Address depends on the TNA Type selection. IPV4 TNA Address is an ID of a TNA address in IPv4 format. Example:
IPV4TNAADDR=135.13.3.119.
 - **Logical port ID** - Logical port ID is a numeric value indicating specific physical ports within a TNA Address. It is a number with range $lpidn = 0..42946967295$. The number of logical ports in a TNAaddress is ≤ 512 .

-
- 13** The **Source/Destination labels** displays the Source/Destination labels for the ENNI connection. The label will be assigned as follows based on the selected CTP: label is of the form S-U-K-L-M. The values of K,L,M are always 0. The value of S represents STS3/VC4. The value of U represents STS1/VC3.
-
- 14** In the **Service Level** field, select protection types for the connection from the drop-down list.
-
- 15** Select the **Link Protection Type** from the drop-down list. Possible values are: **0x1** and **1+1**. The default value is 0x1.

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

Task, Part 2 of 5: Specify the Routing Parameters

Complete the following steps to provision the routing constraints parameters.

.....

- 1** *Optional:*Select the **Exclude Link Resource Class** to exclude certain ENNI links from the end-to-end connection. Links that have a particular bit set in the class will be excluded.
-
- 2** *Optional*Select the **Include Link Resource Class** to include certain ENNI links from the end-to-end connection. Links that have a particular bit set in the class will be included from the routing.
-
- 3** Click the number 3 in the navigation aid to move to the Order parameters panel.

Result: The Order parameters panel is displayed.

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

Task, Part 3 of 5: Specify the Order parameters

Complete the following steps to provision the Order parameters.

.....

- 1** In the **Order number** field, enter a unique number that identifies the network connection order. If you do not enter the unique number, the management system generates the unique number automatically.

-
- 2 In the **Due date** field, enter the due date. You can click the calendar icon to select the due date from a calendar.
-
- 3 In the **Order step** field, select the order step from the drop-down list.
-
- 4 In the **Order type** field, select **Add** .
-
- 5 In the **Scheduled date/time** field, enter the scheduled date and time. You can click the calendar icon to select the date and time from a calendar. This field is displayed only if the scheduling has been turned on. This field is not displayed if the scheduling is not supported and when the Order Step is other than Planned or Local Design, Ethernet Orders, Merged Orders, and Rearrange Orders.
-
- 6 The **Customer priority** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.
- In the **Customer priority** field, select a number between 0-9. This field indicates the order in which each customer has priority on the network. 0 is the highest priority; 9 is the lowest priority. The default value is 2.
-
- 7 The **Quality of service** field is present if a specific installation parameter was enabled during the installation of the management system. This field is not displayed for Ethernet Orders.
- In the **Quality of service** field, enter a character string with maximum length of 10 characters.
-
- 8 In the **Ignore alarm** field, turn this parameter on or off.
- If the parameter is checked, the parameter is turned on and the ability of the connection to go In Effect *will not* be impacted by the alarm status of its server connection and end ports.
 - If the parameter is not checked, the parameter is turned off and the ability of the connection to go In Effect *will* be impacted by the alarm status of its server connection and end ports.

.....

9 In the **Protection Order number** field, enter the protection order number. This field is only displayed for provisioning a digital link that is part of a 1x1 MSP/APS Protection Group.

.....

10 In the **Comments** field, enter any notes that you want to store as part of the record for this connection.

.....

11 Click the number 4 in the navigation aid to move to the Assurance Parameters panel.

Result: The Assurance Parameters panel is displayed.

.....

END OF STEPS

.....

Task, Part 4 of 5: Specify the Assurance parameters

Complete the following steps to provision the Assurance parameters.

.....

1 In the **15-minute collection type** field, select either **Collect, Monitor, or None**.

.....

2 In the **15-minute monitoring** field, select either **End ports** or **None** from the drop-down menu.

.....

3 In the **15-minute intervals** field, select the appropriate time frame from the drop-down menu.

.....

4 In the **24-hour collection type** field, select either **Collect, Monitor, or None**.

.....

5 In the **24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.

.....

6 In the **24-hour intervals** field, select the appropriate time frame from the drop-down menu.

.....

7 In the **Bi-dir 24-hour collection type** field, select either **Collect, Monitor, or None**.

.....

.....

8 In the **Bi-dir 24-hour monitoring** field, select either **End cross-connects** or **None** from the drop-down menu.

.....

9 In the **Bi-dir 24-hour intervals** field, select the appropriate timeframe from the drop-down menu.

.....

10 In the **Assign Alarm Profile** field, select either the **Yes** or **No** choice to assign/not assign an alarm profile. The default is **Yes**.

Result: If the request is successful, the NE assigns a TP to an Alarm Profile.

If the NE does not assign a TP to an Alarm Profile, an error message is displayed on the Job Updates screen.

If the Assign Alarm Profile is set to **No**, no changes to the TP ASAP assignment are made by the management system.

.....

11 The **Profile Name** is a read-only field. This field is only displayed if the Assign Alarm Profile is set to **Yes**.

.....

12 In the **Alarm Reporting** field, select either the **Yes** or **No** choice to request/reject alarm reporting. The default is **Yes**.

.....

13 Click the number 5 or the step text link in the navigation aid, or use the Next button at the bottom right of the panel, to move to the Connection Creation Summary panel.

Result: The Connection Creation Summary panel is displayed.

.....

END OF STEPS

.....

Task, Part 5 of 5: Review and submit the connection

Complete the following steps to review and submit an ENNI ONNS controlled plane service connection.

.....

1 Review the summary for this connection. Do one of the following:

- If you wish to change a selection, use the navigation aid to return to a panel, change a selection, and then return to this step.
 - If the selections are all correct, click the **Submit** button to complete the addition of the ENNI ONNS controlled plane service connection.
-

Result: The ENNI ONNS controlled plane service connection is added.

The Job Updates page monitors the status of the add connection request. This page shows the addition of the connection, and the progress of the order from planned to local design, and so on. The order stops at the order step that was specified on the Order parameters panel.

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



View ENNI Associated ASTN Connection List

When to use

Use this task to view the ENNI Associated ASTN Connection List.

Before you begin

This task does not have any preconditions.

Task

Complete the following steps to view the ENNI Associated ASTN Connection List.

- 1 From the Network Connection page or from the Graphical Layout, select **Associated ASTN Connection List** from the **Go** menu, and click the Go button.

Result: The ENNI Associated ASTN Connection List page is displayed for the ENNI Connection list that meets your search criteria.

END OF STEPS



Perform a Partial Database Synchronization for Network Connections

When to use

Use this task to perform a partial database synchronization for network connections.

Related information

See the following topic:

- Perform a Partial Database Synchronization for Network Connections task in the Lucent OMS Network Element Management Guide

Before you begin

Ensure that the management system is communicating with the NE. (If it is not, this feature cannot work.)

Task

Complete the following steps to perform a partial database synchronization for ONNS network connections.

- 1 In the top navigation bar select **My network > Job updates**.

Result: The Job Updates page is displayed. This page allows you to monitor the status of the task.

- 2 Do one of the following:

- Use the icons or the object links to follow this path: **Network**. The Network Map is displayed. Right-click an NE icon. From the Node menu, select **Session > Database synchronization**.
- Use the icons or the object links to follow this path: **Network Elements**. The Network Elements page is displayed. Click the radio button to the left of the NE for which you wish to perform a database synchronization. From the Go menu, select **Initiate database synchronization**, and click the **Go** button.
- Use the icons or the object links to follow this path: **Tools > Database Synchronizations**.

Result: The Database Synchronizations page is displayed.

- 3 Click on the **New** tool in the search panel or in the toolbar.

Result: The Initiate Database Synchronization page is displayed.

- 4 In the **Database synchronization type** field, select **Configuration - Network Connections** .
-

- 5 In the **Database synchronization scope** field, make a selection to indicate with which NE or group of NEs the management system should synchronize as follows:
- In the **All NEs in network** field, select the radio button.
 - In the **All NEs in following network adapter server** field, select a network adapter server from the **NA name** drop-down list.
 - In the **All NEs in following network communications group** field, either enter the NCG name, or click on the **NCG name** hyperlink to display the Network Communications Group Selection pop-up window. This window is used to select an NCG from a list.
 - In the **The following NE:** field, either enter the NE name, or click on the **NE name** hyperlink to display the Network Elements pop-up window. This window is used to select an NE from a list.
-

- 6 Click the **Submit** button.

Result: The partial network connections database synchronization is performed, and a confirmation is issued in the Messages panel. The Job Updates page reports the status of the network connections partial database synchronization.

END OF STEPS



8 Timing provisioning concepts

Overview

Purpose

This chapter presents concept information related to timing provisioning on *LambdaUnite*® MSS network elements using Lucent OMS.

Contents

NE timing – general functional overview	8-2
Timing interfaces	8-6
Timing references	8-9
Timing link switches	8-12
The internal timing generator	8-18
Timing quality	8-20
Timing protection	8-21
Synchronization characteristics – external timing inputs	8-23
Synchronization characteristics – external timing outputs	8-25
Synchronization characteristics – assigned timing references	8-30
Synchronization characteristics – system timing	8-35

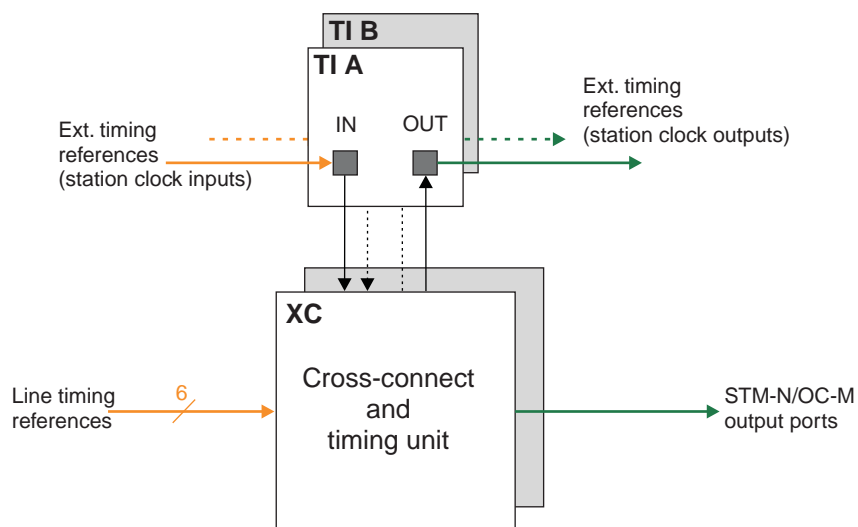


NE timing – general functional overview

Introduction

Each *LambdaUnite*[®] MSS network element provides two external timing inputs (station clock inputs) and two external timing outputs (station clock outputs), located on the timing interfaces (TI A and TI B) which are accessible from the rear side of the shelf.

A station clock input is an external interface where an external timing reference signal can be supplied. A station clock output is an external interface where an external timing reference signal can be made available which can be used to synchronize other equipment in the same office. Besides the external timing references, up to six line timing references (clock information derived from STM-*n* or OC-*m* input ports) can be used for synchronization purposes.



The timing reference information is processed by the system timing function located on the cross-connection and timing units (XC160, XC320, XC640).

NE synchronization mode

The synchronization characteristics of a *LambdaUnite*[®] MSS system depend on the configurable NE synchronization mode. The NE synchronization mode basically impacts the NE-internal functional details, the expected external timing reference signals, the synchronization status message (SSM) handling, and the output timing mode of operation.

LambdaUnite[®] MSS network elements support these NE synchronization modes:

SDH synchronization mode	The system timing complies with SDH synchronization requirements. The SDH synchronization mode should be chosen when a <i>LambdaUnite</i> [®] MSS network element is to be integrated into an SDH network environment.
SONET synchronization mode	The system timing complies with SONET synchronization requirements. The SONET synchronization mode should be chosen when a <i>LambdaUnite</i> [®] MSS network element is to be integrated into a SONET network environment.

The NE-internal functional details that depend on the NE synchronization mode will subsequently be explained in more detail.

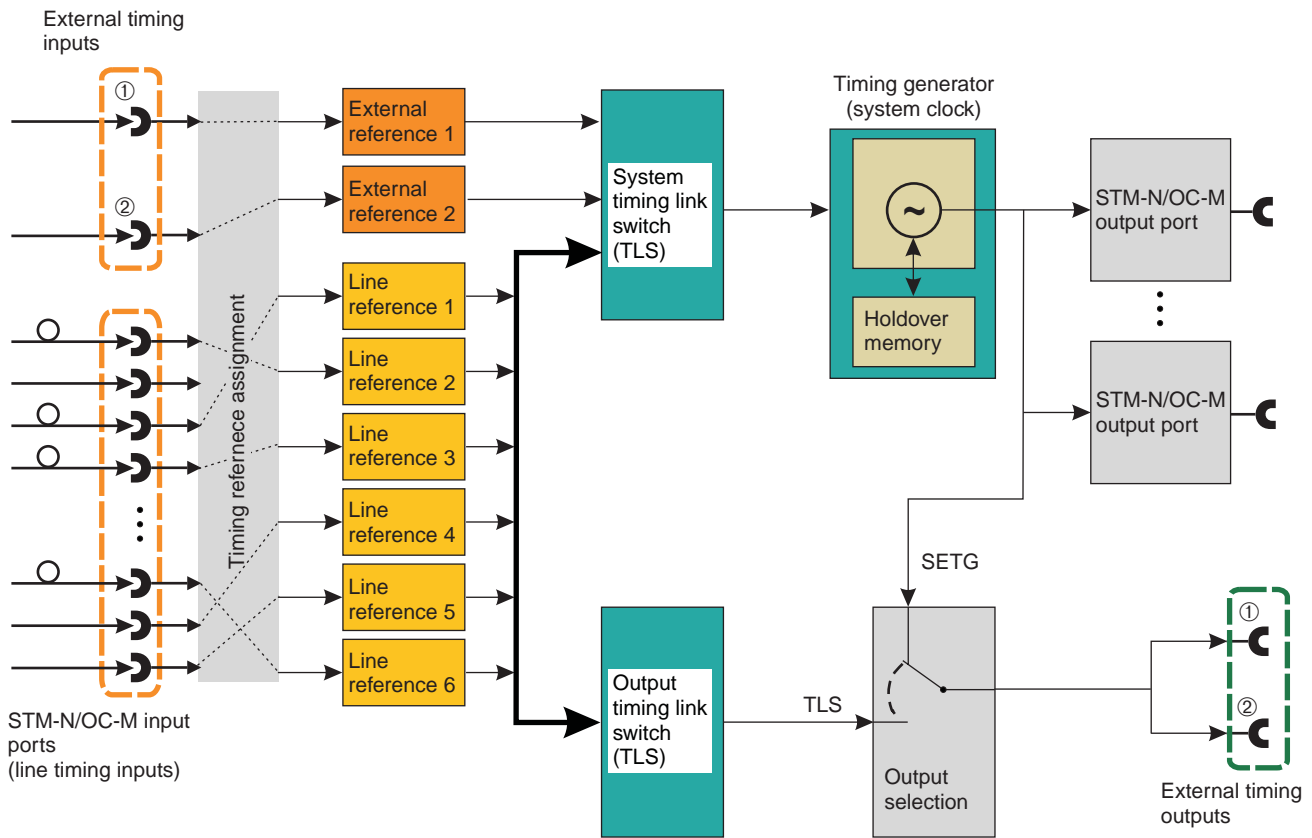
SDH- and SONET-specific functional implementation

The implementations of the timing functionality for SDH and SONET are very similar. However, they differ in some details. The SDH implementation has a separate output timing link switch for example, while the SONET implementation has two hardwired output lines.

The following two functional block diagrams serve to illustrate both the commonalities as well as the differences. However, not all aspects can be covered in these diagrams (for example the supported types of external timing input signals). These aspects will be dealt with in the subsequent sections.

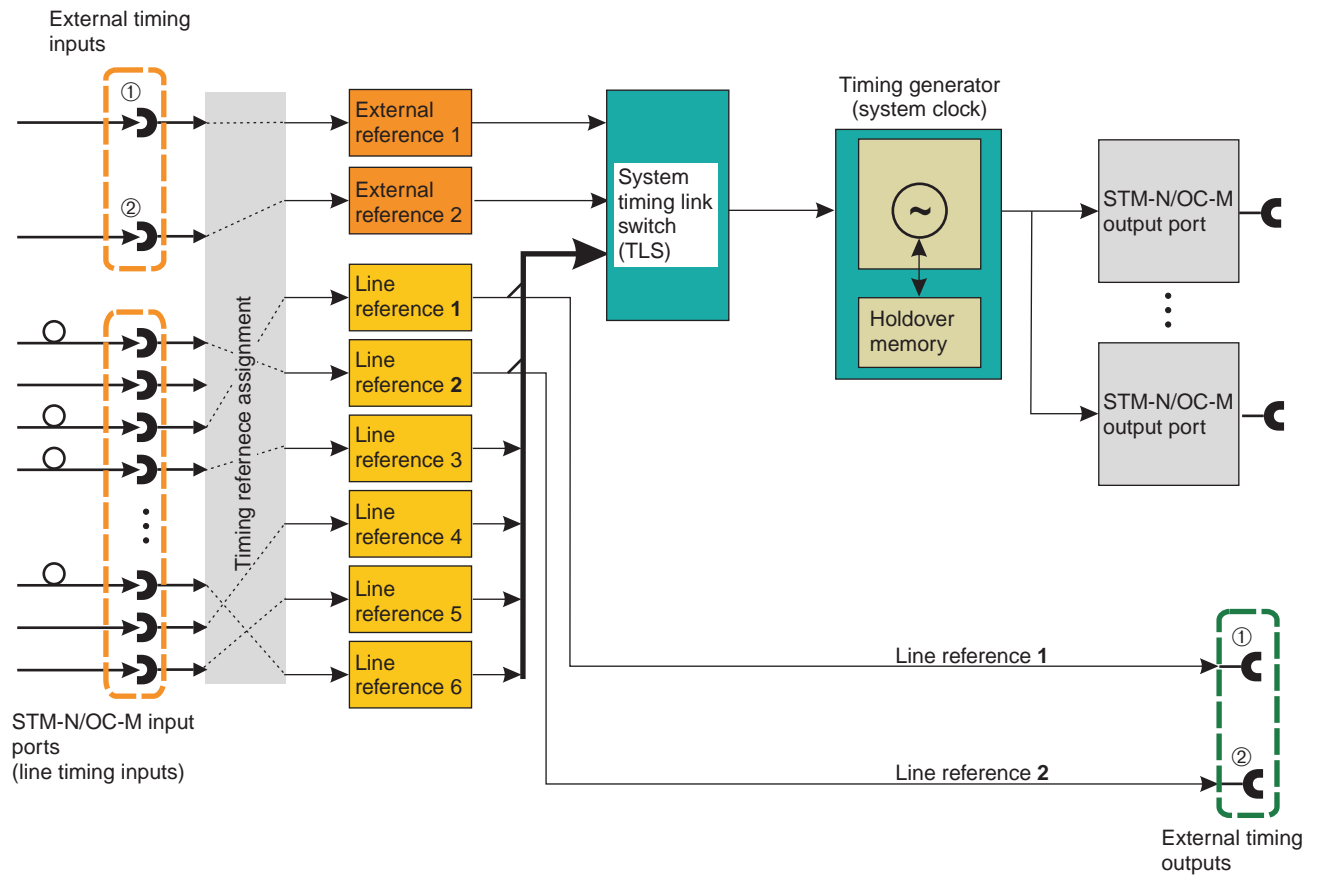
SDH-specific timing functionality

The following functional block diagram gives an overview of the SDH-specific timing functionality of a *LambdaUnite*[®] MSS network element:



SONET-specific timing functionality

The following functional block diagram gives an overview of the SONET-specific timing functionality of a *LambdaUnite*® MSS network element:



□

Timing interfaces

Overview

Each *LambdaUnite*[®] MSS network element can be equipped (from the rear side of the shelf) with up to two timing interfaces (TI A, TI B).

Each timing interface provides an external timing input and an external timing output.

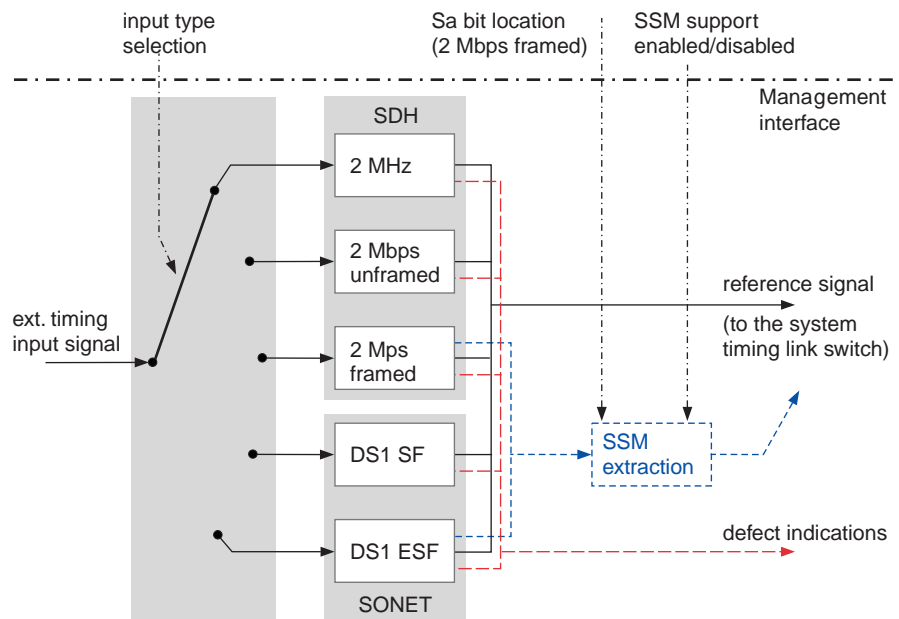
External timing inputs

An external timing input (station clock input) is an interface port which is specifically used to extract a synchronization reference to be used in the network element. A station clock input can be used for timing purposes only, it cannot be used for data transport.

The format of the station clock input signal is provisionable. These signal formats are supported, depending on the NE synchronization mode:

- SDH synchronization mode:
 - 2048 kHz (2 MHz) acc. to ITU-T Rec. G.703. This is the default setting in the SDH synchronization mode.
 - Unframed 2 Mbps acc. to ITU-T Rec. G.703.
 - Framed 2 Mbps acc. to ITU-T Rec. G.703 with a frame/multiframe structure acc. to G.704.
- SONET synchronization mode:
 - DS1 Superframe Format (DS1 SF) with B8ZS line code acc. to the Telcordia Technologies GR-499-CORE standard.
 - DS1 Extended Superframe Format (DS1 ESF) with B8ZS line code acc. to the Telcordia Technologies GR-499-CORE standard. This is the default setting in the SONET synchronization mode.

The following diagram gives a functional overview (including the provisioning options):



At the external timing inputs, the incoming signal is terminated, and the timing reference information is derived. Furthermore, the external timing input signal is monitored for defects, and the Synchronization Status Message (SSM) is extracted, where applicable (2 Mbps framed and DS1 ESF input signals with SSM support enabled). The SSM is used by the system timing link switch to select the best available reference signal.

Lockout of an external timing input

It is possible to temporarily lockout an external timing input. A locked out timing input is not available for timing reference selection.

External timing outputs

The external timing outputs (station clock outputs) can be used to synchronize other equipment in the same office.

The format of the station clock output signals is provisionable. These signal formats are supported, depending on the NE synchronization mode:

- SDH synchronization mode:
 - 2048 kHz (2 MHz) acc. to ITU-T Rec. G.703. This is the default setting in the SDH synchronization mode.
 - Unframed 2 Mbps acc. to ITU-T Rec. G.703.
 - Framed 2 Mbps acc. to ITU-T Rec. G.703 with a frame/multiframe structure acc. to G.704.
- SONET synchronization mode:
 - DS1 Superframe Format (DS1 SF) with B8ZS line code acc. to the Telcordia Technologies GR-499-CORE standard.
 - DS1 Extended Superframe Format (DS1 ESF) with B8ZS line code acc. to the Telcordia Technologies GR-499-CORE standard. This is the default setting in the SONET synchronization mode.

The clock reference for the station clock outputs also depends on the NE synchronization mode:

- SDH synchronization mode:

The timing reference signal for the external timing outputs can be derived either from the NE-internal timing generator (SETG, “Synchronous Equipment Timing Generator”), or, via the output timing link switch (TLS), from the line timing references 1 to 6.

The same timing reference signal is available at both station clock outputs.
- SONET synchronization mode:

The timing reference signals for the external timing outputs are derived *directly* from the line timing references 1 and 2:

 - The timing reference signal for the external timing output 1 is derived directly from line timing reference 1.
 - The timing reference signal for the external timing output 2 is derived directly from line timing reference 2.

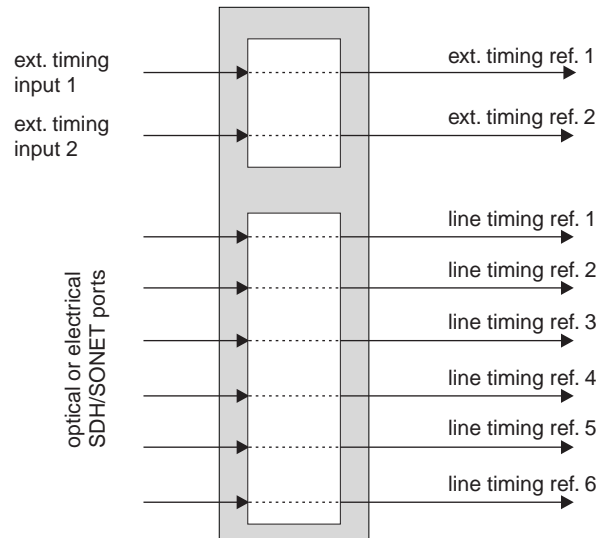
It is possible to provision different signal formats for the two station clock output signals.

□

Timing references

Up to eight timing references

The total number of timing references is limited to eight, two external timing references and six line timing references:



External timing references

There is a direct and fix relation between the two external timing inputs (station clock inputs) and the two external timing references:

- Ext. timing input 1 → ext. timing reference 1
- Ext. timing input 2 → ext. timing reference 2

However, the two external timing inputs are *not automatically assigned* as external timing references. This assignment needs to be done manually (and individually for both external timing references), and the internal timing generator needs to be operated in locked mode for the external timing reference assignment to take effect.

Important! When the system clock is locked to an external timing reference, then removing or replacing the standby cross-connection and timing unit (XC160, XC320, XC640) causes the external timing reference to be declared failed temporarily, and a timing reference switch will occur.

You have the following options:

- Before removing or replacing the standby cross-connection and timing unit, make sure that the system clock is *not* locked to an external timing reference by manually switching to a different timing reference, or entering the forced holdover mode.
- Accept the intermediate timing reference switch (traffic is *not* affected).

Line timing references

Up to six out of the available incoming SDH/SONET transport signals can be assigned as line timing references. An 8-kHz timing reference signal is then derived from the inherent clock information.

The assignment needs to be done manually by specifying an SDH/SONET port as a line timing reference.

Important! Please observe these guidelines concerning the line timing reference assignment:

a	Only one SDH/SONET port <i>per port unit</i> can be assigned as a line timing reference.
b	The line timing reference assignment will have no effect on the system timing unless the Clock Mode of the System Timing is set to Locked .
c	Due to their role in the internal data communication between port units and the cross-connection and timing unit, it is <i>not possible</i> to select one of the following input ports as a line timing reference: <ul style="list-style-type: none"> • 2.5-Gbps port units (OP2G5): port 4 • 622-Mbps port units (OP622): ports 6, 7, 13, and 14 This applies to all OP2G5 or OP622 port units, and independent of the slot position where they are installed.
d	The OPT2G5 input signals <i>cannot</i> be used as line timing references because the Multiplex Section (MS) layer is neither terminated nor monitored on the OPT2G5 port unit. On the multiplex section (MS) layer, the synchronization status message (SSM) functionality is located in the client signal.
e	EP51/EL36 port units: EC-1 or DS3 input signals <i>cannot</i> be used as line timing references. In the outgoing direction, however, the synchronization status message (SSM) is supported.
f	When you assign a line timing reference while the timing generator operates in autonomous holdover mode, then a Loss of Synchronisation alarm will be reported for 10 seconds which, however, can be ignored. The timing functionality is not impaired.
g	GE1 and GE10PL1 port units: Gigabit Ethernet input signals at GE1, 1GEPL, or 10GEPL ports <i>cannot</i> be used as line timing references.

- h The input signals of port 4 and port 8 of an OP2G5D/PAR8 port unit *cannot* be used as line timing references.

Timing reference selection

The *LambdaUnite*[®] MSS timing function is designed such that always the most suitable clock source is selected for synchronization.

The selection is based on the quality of the available timing reference signals in combination with their provisionable priority:

- If the **System SSM Mode** is set to **QL Enable** (that means the SSM information is evaluated), then initially the signal with the highest quality level is used as the 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 SSM 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 autonomously enters the holdover mode.

□

Timing link switches

Two types of timing link switches

LambdaUnite[®] MSS supports two types of timing link switches:

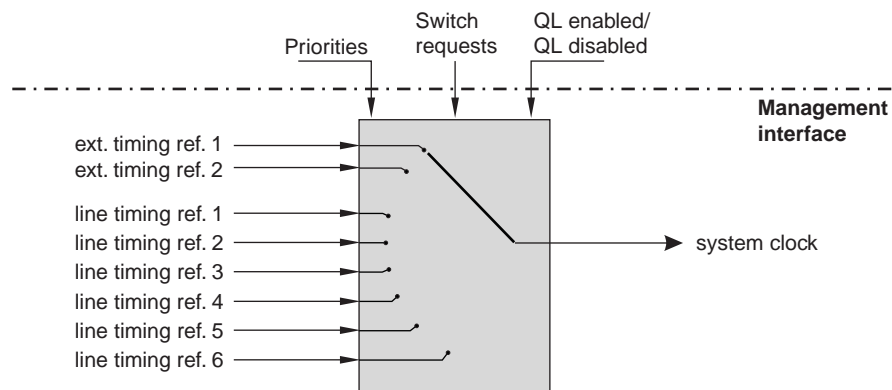
- System timing link switch
- Output timing link switch (only in the SDH synchronization mode)

Automatic timing reference selection

A timing link switch (TLS) allows reference switching between all possible timing references. By means of a provisional input port priority scheme and, optionally, quality levels (QLs, determined by evaluating the synchronization status message (SSM)), one of the inputs is selected as the reference to be forwarded to either the internal timing generator (in the case of the system timing link switch), or to the external timing output selection (in the case of the output timing link switch).

System timing link switch

The system timing link switch has access to all available timing references (external as well as line timing references). It is used to supply the internal timing generator with the best available clock source. The internal timing generator then provides the clock information for the SDH/SONET output ports.



Re-synchronization after frequency offsets

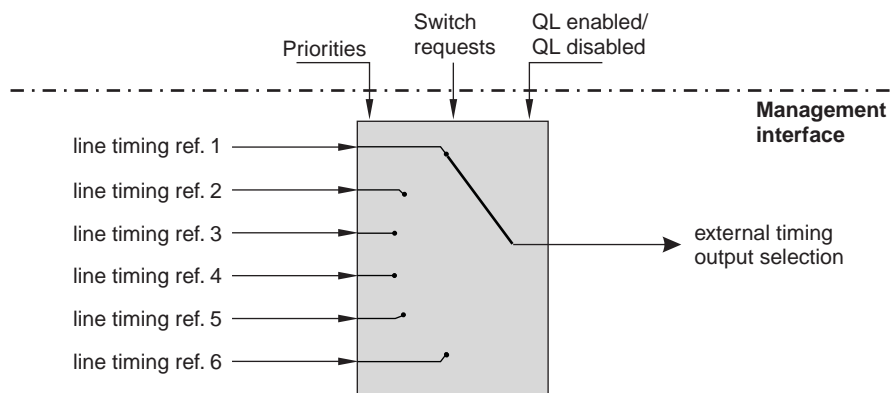
In case of a frequency offset at a timing input port which is currently used as the active system timing reference, a re-synchronization process starts which may last up to 180 seconds, depending on the size of the frequency step (a frequency offset of 5 ppm requires a re-synchronization period of approximately 24 seconds, for example).

Usually, frequency offsets up to 12 ppm do not cause a timing reference protection switch, and are not externally visible. However, should it happen that you perform an XC protection switch immediately after such a frequency offset, then an output timing reference switch and even TXI failures might occur which will afterwards be cleared autonomously.

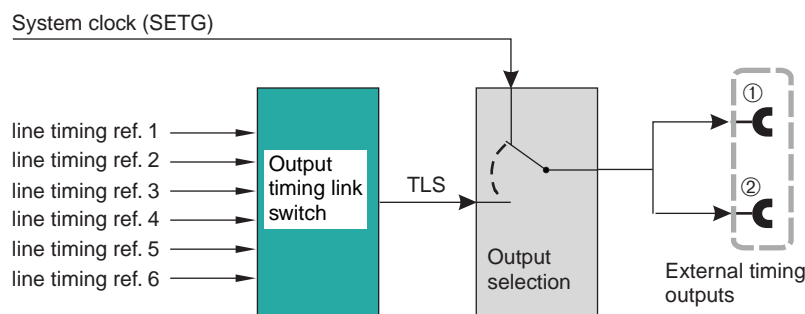
Output timing link switch

The output timing link switch is only supported in the SDH synchronization mode.

The output timing link switch has access to all available line timing references. It has no access to the external timing references because this could lead to undesirable synchronization loops in the office.



The output timing link switch is used to provide the external timing output selection with the best available line timing reference. Alternatively, the clock source for the external timing outputs can also be derived from the internal timing generator (synchronous equipment timing generator, SETG).



Reference priorities

An input of a timing link switch can be assigned a priority between “1” (highest priority) and “8” (lowest priority). Furthermore, it is also possible to assign a priority of “0”, which means to disable the corresponding input. It is possible to assign the same priority to multiple inputs.

Priority	Meaning	
0		Disabled
1	Highest priority	Enabled
↓	↓	
8	Lowest priority	

The selection between revertive and non-revertive mode is achieved via the priority setting of a timing reference. All references with the same priority are non-revertive timing references. If two timing references are the same in terms of quality level (QL) provisioning, revertive switching is provisioned by giving one timing reference a higher priority than the other. The timing reference with the highest priority always will be the active timing reference (if both are available).

In the default setting, all inputs are disabled (priority = 0).

Besides the possibility to permanently disable an input of a timing link switch, it is also possible to temporarily exclude an input.

Timing reference switching

LambdaUnite[®] MSS systems provide revertive timing reference switching between the enabled inputs of a timing link switch.

The selection criteria for the automatic timing reference selection are based on quality and priority, and can be provisioned to one of the following modes:

Quality level (QL) enabled mode (default setting)	The automatic timing reference selection is based on the incoming quality level (= Synchronization Status Message (SSM)) in combination with the reference priority.
Quality level (QL) disabled mode	The automatic timing reference selection is based on the reference priority only.

Manual timing reference switching is also possible by means of specific switch requests.

Timing reference switching in QL-enabled mode

In the QL-enabled mode, the timing reference selection is according to the following criteria, provided that no external forced or manual switch request is active:

1. The active timing reference is selected from all the enabled inputs (enabled and not locked out) which have a quality level better than “Do not use for synchronization” (DNU/DUS).
2. Out of these timing references, the reference with the highest quality level is selected.

The following order of quality levels applies (in decreasing order of quality from left to right):

- SDH: PRC → SSU_T → SSU_L → SEC → DNU
- SONET: PRS → STU → ST2 → ST3 → DUS

If there is more than one reference with the same highest quality level, then the reference with the highest priority is selected, if the priority is unique. If a group of references has the same highest priority (and the same highest quality level), then the existing reference selection remains unchanged if the selected reference is among this group. Otherwise, an arbitrary reference from this group is selected.

3. If a timing reference can be selected, then the output of the timing link switch forwards the corresponding quality level.
If no timing reference can be selected, then the output forwards the signal status “Unacceptable” and the quality level “Do not use for synchronization” (DNU/DUS).

The automatic timing reference selection is triggered by the following events:

- The QL-enabled mode is activated, and no external forced or manual switch request is active.
- A change of the quality level is detected on an enabled input (enabled and not locked out), and no external forced switch request overrides the autonomous selection.
- A change of reference priority is detected on an enabled input (enabled and not locked out), and no external forced or manual switch request overrides the autonomous selection.
- An active external forced or manual switch request is cleared.
- Timing references are enabled or cleared from lockout, while no external forced or manual switch is active.
- The currently active timing reference is disabled or locked out.

Timing reference switching in QL-disabled mode

In the QL-disabled mode, the timing reference selection is according to the following criteria, provided that no external forced or manual switch request is active:

1. The active timing reference is selected from all the enabled inputs (enabled and not locked out) which have a “Normal” signal status.
2. Out of these timing references, the reference with the highest priority is selected. If a group of references has the same highest priority, then the existing reference selection remains unchanged if the selected reference is among this group. Otherwise, an arbitrary reference from this group is selected.
3. If a timing reference can be selected, then the output of the timing link switch forwards the signal status “Normal”.
If no timing reference can be selected, then the output forwards the signal status “No Signal”.

In case the **System SSM Mode** is set to **QL Disable**, then the signal forwarded by the output timing link switch depends on the timing generator operational mode as follows:

Timing generator operational mode	Signal forwarded by the output timing link switch
Normal	“Do not use for synchronization” (DNU/DUS) in both synchronization modes
Locked	
Forced Holdover	
Free Running	“Do not use for synchronization” (DNU) in the SDH synchronization mode, “Synchronized - Traceability Unknown” (STU) in the SONET synchronization mode
Autonomous Holdover	

The automatic timing reference selection is triggered by the following events:

- The QL-disabled mode is activated, and no external forced or manual switch request is active.
- A change of the signal status is detected on an enabled input (enabled and not locked out), and no external forced switch request overrides the autonomous selection.
- A change of reference priority is detected on an enabled input (enabled and not locked out), and no external forced or manual switch request overrides the autonomous selection.
- An active external forced or manual switch request is cleared.
- Timing references are enabled or cleared from lockout, while no external forced or manual switch is active.
- The currently active timing reference is disabled or locked out.

External switch requests

These external switch requests exist:

Switch request	Meaning
Lockout	can be used to temporarily disable (lock out) an input of a timing link switch. The “ABN” LED on the user panel is lit while this request is active, and a corresponding abnormal condition event will be shown.
Clear lockout	clears (reverts) a lockout request.
Forced switch to reference	can be used to force the selection of a desired (not locked out) timing reference for timing reference selection. The “ABN” LED on the user panel is lit while this request is active, and a corresponding abnormal condition event will be shown.
Manual switch to reference	can be used to switch to another (not locked-out) timing reference, provided that the quality of the desired timing reference equals the quality of the previously active timing reference.
Clear reference switch	clears (reverts) a manual or forced switch request.
Clear wait-to-restore (not applicable to the SDH output timing link switch)	can be used to terminate the wait-to-restore period, i.e. to reset the wait-to-restore timer immediately.



The internal 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 internal timing generator on the cross-connection and timing unit which generates one common internal clock. When two cross-connection and timing units are present in the NE, a 1+1 non-revertive protection of the timing function is provided.

System timing operational modes

The *LambdaUnite*[®] MSS internal timing generator can be operated in one of the following modes:

- *Locked mode*
The system clock is locked to one of the two external timing references or one of the six line timing references.
- *Free-running mode*
The internal timing generator is supplying timing to the system, uncorrected by any external or line timing references, and independent from historical reference data. This is the default value of the system timing operational mode (especially needed for the initial startup of an NE when no valid timing references are assigned). The “ABN” LED on the user panel is lit as long as the timing generator operates in the free-running mode, and a corresponding abnormal condition event will be shown.
It is strongly recommended to switch from the free-running mode to the locked mode as soon as valid timing references are available and assigned.
- *Holdover mode*
The timing generator autonomously enters the holdover mode if all timing reference signals fail (autonomous holdover mode). The internal oscillator on the timing generator supplies a clock signal with a frequency that matches the last known good reference frequency as close as possible within the limits of the internal oscillator’s frequency accuracy (holdover accuracy). The timing generator will revert to normal operation (locked mode) as soon as the incoming timing reference signal becomes acceptable again.
Additionally it is also possible to force the internal oscillator on the timing generator into the holdover mode (forced holdover mode).
Switching to the holdover mode is only possible from the locked mode.
The “ABN” LED on the user panel is lit as long as the timing generator operates in the *forced holdover* mode, and a corresponding abnormal condition event will be shown. *No* abnormal condition will be indicated when the timing generator operates in the *autonomous holdover* mode.

Important! When you assign a line timing reference while the timing generator operates in autonomous holdover mode, then a Loss of Synchronisation alarm will be reported for 10 seconds which can be ignored. The timing functionality is not impaired.



Timing quality

Synchronization status message

A *synchronization status message (SSM)* is defined for SDH/SONET transport signals, and for framed 2-Mbps and DS1 ESF external timing input signals.

The purpose of the SSM is to signal the reference clock quality level from NE to NE to:

- enable the timing generator to extract the timing reference signal with the best quality,
- make it possible to autonomously enter the holdover mode in case there is no suitable timing reference signal, and to
- prevent timing loops.

These timing quality levels are defined (top down in decreasing order of timing quality):

SDH	SONET	Timing quality
PRC	PRS	<i>best</i> timing quality
SSU-T	STU	↓
SSU-L	ST2	↓
SEC	ST3	↓
DNU	DUS	↓



Timing protection

Timing reference protection switching

If the **system SSM 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 SSM 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 Mbps acc. to G.703)
- 6 reference signals derived from the incoming STM- n /OC- m line signals ($n = 1, 4, 16, 64, m = 3, 12, 48, 192$).

Timing equipment protection switching

A network element can contain two cross-connection and timing units (XC160, XC320, XC640) on which the timing function is located. If there are two timing functions, then 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 cross-connection and timing unit as the active one which was active before the system reset operation.

If only one cross-connection and timing unit is present (worker) and the protection cross-connection and timing unit is inserted, *LambdaUnite*[®] MSS is in a warm-up state for about 6 minutes. During this time the system timing quality is set to “Do not use for synchronization” (DNU/DUS). During this state it is not allowed to perform a manual switch command to the standby cross-connection and timing unit.

Wait-to-restore time

If a timing signal is restored, then – after a defined period of time (wait-to-restore time, WTR) – a decision is made based on the timing quality and on priority selection criteria, which signal to select. If the same signal has the best quality and/or highest priority, then the same signal will be selected, else another signal.



Synchronization characteristics – external timing inputs

Overview

LambdaUnite[®] MSS provides two external timing inputs:

- **External Input 1**
- **External Input 2**

The configuration parameters of these external timing inputs are described in the following.

External input signal format

The **External input signal format** is the format of the external timing input signal.

These external timing input signal formats are supported:

SDH synchronization mode	2MHZ : 2-MHz signal (default setting) 2MBIT-FRAMED : framed 2-Mbps signal 2MBIT-UNFRAMED : unframed 2-Mbps signal
SONET synchronization mode	SF (DS1 Super Frame) ESF (DS1 Extended Super Frame)

ISSM support

The *synchronization status message (SSM)* support can be enabled for framed 2-Mbps (SDH synchronization mode) and ESF (SONET synchronization mode) external timing input signals.

Possible settings of the **ISSM Support** parameter are:

SUPPORTED	The SSM support is <i>enabled</i> . This is the default setting in the SONET synchronization mode.
NOT-SUPPORTED	The SSM support is <i>disabled</i> . This is the default setting in the SDH synchronization mode.

Sa bit location

This parameter is only applicable in the SDH synchronization mode, and only in case the selected signal format is **2MBIT-FRAMED**, and **SSM Support** is enabled.

If the **SSM Support** is disabled, then the value of the **SA bit Location** parameter is of no relevance.

If the **SSM Support** parameter is enabled, then the SSM is extracted from the Sa bits starting at the location defined by the **SA bit Location** parameter.

Possible values are:

- **SA4** (default setting)
- **SA5**
- **SA6**
- **SA7**
- **SA8**



Synchronization characteristics – external timing outputs

Overview

The system provides two external timing output ports. Depending on the system timing mode, the output ports have different meanings:

- **SDH synchronization 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.
- **SONET synchronization 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 **Prov. Source Selection** parameter:

SETG (Synchronous Equipment Timing Generator)	The output signal is derived from the system clock.
TLS (Timing Link Switch)	The output signal is derived from the Timing Link Switch.

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 cross-connection and timing units (worker in slot 9, protection in slot 10). If at least one of the two cross-connection and timing 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 cross-connection and timing unit (XC). The **External Output 1** is connected to the XC in slot 9 (worker) while the **External Output 2** is connected to the XC in slot 10 (protection). If only one cross-connection and timing unit is present, then an output signal is available only at the corresponding external timing output port (provided that the output is enabled).

Derived output timing

Parameter	Possible values	Meaning
External output enable	ENABLE , DISABLE (default)	This parameter indicates whether a timing signal is forwarded to the output port.
External timing output selection	SDH mode: <ul style="list-style-type: none"> • SETG (default setting) • TLS SONET mode: <ul style="list-style-type: none"> • LINE1 • LINE2 	<p>This parameter indicates from which source the external timing signal is derived.</p> <p>SDH mode:</p> <ul style="list-style-type: none"> • SETG (Synchronous Equipment Timing Generator) The external timing output signal is derived from the system clock. • TLS (Timing Link Switch) The external timing output signal is derived from one of the six timing references. <p>In principle, the same selection criteria apply as for system timing. The following preconditions must be fulfilled for a timing reference to be selectable as an external timing output signal:</p> <ul style="list-style-type: none"> – The Output Ref. Priority must be enabled (i.e. must have a value between 1 and 6, but must <i>not</i> be disabled). – The Lockout Status must be set to No Lockout. – If the System SSM Mode is set to QL Enable, then signals with a valid quality level other than “Do not use for synchronization” (DNU/DUS) can be selected. <p>SONET mode:</p> <ul style="list-style-type: none"> • The external timing output port 1 is fix connected to the line timing reference 1. • The external timing output port 2 is fix connected to the line timing reference 2.

Signal settings

Parameter	Possible values	Meaning
External Timing Output Format	SDH synchronization mode: <ul style="list-style-type: none"> • 2MHZ (default setting) • 2MBIT-FRAMED • 2MBIT-UNFRAMED SONET synchronization mode: <ul style="list-style-type: none"> • SF • ESF (default setting) 	This parameter shows the signal format of the outgoing timing signal: <ul style="list-style-type: none"> • SDH synchronization mode: <ul style="list-style-type: none"> – 2MHZ: 2-MHz signal – 2MBIT-FRAMED: framed 2-Mbps signal For framed 2-Mbps timing signals, the generation and evaluation of synchronization status message (SSM) information on the timing quality is supported as per ITU-T Rec. G.704. – 2MBIT-UNFRAMED: unframed 2-Mbps signal • SONET synchronization mode: <ul style="list-style-type: none"> – SF: DS1 Super Frame – ESF: DS1 Extended Super Frame For DS1 ESF timing signals, the generation and evaluation of synchronization status message (SSM) information on the timing quality is supported as per the Telcordia Technologies GR-253-CORE standard.
Cable Equalization	<ul style="list-style-type: none"> • 20% (default setting) • 40% • 60% • 80% • 100% 	The Cable Equalization parameter is available in the SONET synchronization mode only. It determines the timing output cable equalization to adjust the specified timing reference output signal power (in order to compensate a given cable attenuation). All percentage values relate to the given max. cable attenuation of 3 dB: <ul style="list-style-type: none"> • 0.6 dB cable attenuation → 20% cable equalization • 1.2 dB cable attenuation → 40% cable equalization • 1.8 dB cable attenuation → 60% cable equalization • 2.4 dB cable attenuation → 80% cable equalization • 3 dB cable attenuation → 100% cable equalization

Regenerator

Parameter	Possible values	Meaning
Timing Regenerator Loop Delay	0 ... 60 s The default value is 10 s .	Delay during which DNU/DUS (do not use) is maintained after the Regenerator Loop conditions are no longer present.

Parameter	Possible values	Meaning
Timing Regenerator Loop	<p><i>SDH synchronization mode:</i></p> <p>This parameter serves to avoid timing loops in the office between the timing outputs and one or both of the timing inputs through a stand-alone synchronization equipment (SASE) office clock.</p> <p>The meaning of the possible settings is as follows:</p> <ul style="list-style-type: none"> • DISABLE (default setting) The regenerator loop functionality is disabled. Timing loops are not considered. • EXTREF1: External reference 1 If the quality level of the incoming framed 2-Mbps timing signal at the external timing input 1 is equal to the quality level of the timing signal that is transmitted to the external timing output ports, “Do not use for synchronization” (DNU) is inserted for the outgoing timing signal as a timing loop might be present. • EXTREF2: External reference 2 If the quality level of the incoming framed 2-Mbps timing signal at the external timing input 2 is equal to the quality level of the timing signal that is transmitted to the external timing output ports, “Do not use for synchronization” (DNU) is inserted for the outgoing timing signal as a timing loop might be present. • BOTH The regenerator loop functionality is applied to both external timing inputs. <p>Timing loops might occur, if the NE forwards timing to an SASE via one or both of the external timing output ports, and at the same time receives a timing signal from the same SASE via one or both of the external timing input ports. If Regenerator Loop is set, and the system clock is operated in the locked mode, and derived from an external timing input signal, then “Do not use for synchronization” (DNU) is forwarded to the timing outputs to avoid such timing loops.</p> <hr/> <p><i>SONET synchronization mode:</i></p> <p>This parameter serves to avoid timing loops in the office between the timing outputs and one or both of the timing inputs through a building integrated timing supply (BITS) office clock.</p> <p>The meaning of the possible settings is as follows:</p> <ul style="list-style-type: none"> • ENABLE (default setting) The regenerator loop functionality is applied to both external timing inputs. • DISABLE The regenerator loop functionality is disabled. Timing loops are not considered. <p>Timing loops might occur, if the NE forwards timing to a BITS via one or both of the external timing output ports, and at the same time receives a timing signal from the same BITS via one or both of the external timing input ports. If Regenerator Loop is set, and the system clock is operated in the locked mode, and derived from an external timing input signal, then “Do not use for synchronization” (DUS) is forwarded to the timing outputs to avoid such timing loops.</p>	

SSM parameters

Parameter	Possible values	Meaning
External output SA bit Location	SA4 (default setting) SA5, SA6, SA7, SA8	This parameter is only applicable in the SDH synchronization mode, and only in case the selected signal format is 2MBIT-FRAMED , and SSM Support is enabled. If the SSM Support is disabled, then the value of the SA bit Location parameter is of no relevance. If the SSM Support parameter is enabled, then the SSM is extracted from the Sa bits starting at the location defined by the SA bit Location parameter.
External timing output AIS Mode	AIS MODE, QL MODE (default)	This parameter is only supported in case the selected signal format is framed 2-Mbps (SDH synchronization mode), or DS1 ESF (SONET synchronization mode), respectively. It specifies which type of signal (AIS or DNU/DUS) will be inserted into the outgoing timing signal if the signal quality is below the quality acceptance level (Acc. QL for AIS), or if “Do not use for synchronization” (DNU/DUS) is forced to be consistently inserted into the outgoing timing signal (Sync Message Force DNU / Sync Message Force DUS).
Accept. qual level-out thrs. AIS	SDH synchronization mode: PRC, SSUT, SSUL, SEC (default setting) SONET synchronization mode: PRS, STU, ST2., ST3 (default setting)	This parameter defines the quality acceptance level for external timing output signals. When the incoming signal is below this level, then AIS or “Do not use for synchronization” (DNU/DUS) will be inserted into the external timing output signal, depending on the AIS Mode setting.

Alarming

Parameter	Possible values	Meaning
ASAP	Any specific ASAP of type “System Timing”, or the default ASAP of type “System Timing” (“DEFAULT”).	The assigned alarm severity assignment profile (ASAP) of type “System Timing”.



Synchronization characteristics – assigned timing references

Overview

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
One or two external net clock input signals (2048 kHz, 2048 kbps acc. to ITU-T recommendations, or DS1 SF or ESF acc. to Telcordia Technologies standards)
- Line timing references
Up to six reference signals derived from the available incoming SDH/SONET transport signals.

Active system timing reference

Parameter	Possible values	Meaning
Timing Reference Identifier	NONE (default setting) EXTREF1 EXTREF2 LINE1 ... LINE6	The currently active system timing reference which is used to derive the system clock in the locked mode of system timing. The value NONE is displayed if no timing reference is assigned, or if all timing references have failed.

Timing references

The timing references include the line timing references and the external timing references. The parameters of the line timing references and the external timing references are explained in the following tables.

Line timing references

The following table shows the possible settings of the line timing references:

Parameter	Possible values	Meaning
Timing Ref. assigned	Not connected	The respective timing reference source is not used.
	Port AID of an SDH/SONET port	The clock information is derived from the respective SDH/SONET transport signal.
Sys. Tim. Ref. Prio.	Priority 0 (Disabled) ... Priority 8. (default setting)	The configured priority of the respective timing reference signal.

Parameter	Possible values	Meaning
Quality Provisioned	SDH synchronization mode: PRC SSUT SSUL SEC AUTO (default setting)	The quality level of the respective timing reference assigned by provisioning. If the provisioned quality level is AUTO , then the incoming SSM Value is used as the quality level. Otherwise, if the provisioned quality level has any value other than AUTO , then the incoming SSM Value is <i>not</i> used, but this provisioned value is used as the quality level.
	SONET synchronization mode: PRS STU ST2 ST3 AUTO (default setting)	
	SONET synchronization mode: PRS STU ST2 ST3 DUS NONE (default setting)	
Timing Output Ref. Priority	Disabled, 1 (highest priority), 2, 3, ..., 6 (lowest priority)	This parameter is applicable in the <i>SDH synchronization mode</i> only! It shows the priority assigned to the timing reference signal for the usage as an output timing reference.
ASAP name	Any specific ASAP of type “System Timing”, or the default ASAP of type “System Timing” (“DEFAULT”).	The alarm severity assignment profile (ASAP) of type “System Timing” assigned to the respective timing reference.
Timing Port Mode Monitoring	Monitored, Not Monitored	This parameter indicates whether the respective timing port will be monitored for timing reference failures (Monitored) or not (Not Monitored). If a timing port is set to Not Monitored , then no timing reference failure alarms will be reported for that port.

External timing references

The table below shows the possible settings of the external timing references:

Parameter	Possible values	Meaning
Port AID	Not connected	The respective timing reference source is not used.
	Port AID of an external timing input port (exttmg0, exttmg1)	The clock information is derived from the respective external timing input port.

Parameter	Possible values	Meaning
Sys. Tim. Ref. Prio.	Disable (default setting) 1 (highest priority), 2, 3, ... 8 (lowest priority)	The configured priority of the respective timing reference signal.
Signal Status	Normal	The timing reference signal is fault-free.
	Failed	The timing reference signal failed.
	Wait-To-Restore	The timing reference signal has failed and is now being restored. A waiting period is implemented for a defined time (wait-to-restore time) to see whether the signal is stable, before the system switches back to it.
	Not-Connected	The timing reference is not used.
Lockout Status	Lockout	The Lockout Status determines if the respective timing reference can be used as a system timing reference (No Lockout) or not (Lockout).
	No Lockout	
QL Value	SDH synchronization mode: PRC SSUT SSUL SEC DNU (default setting)	The quality level of the timing reference port. If the provisioned quality level (cf. QL Provisioned) has any value other than AUTO , then the quality level is the same as the QL Provisioned . If the provisioned quality level is AUTO , then the quality level has the same value as the incoming SSM Value .
	SONET synchronization mode: PRS STU ST2 ST3 DUS (default setting)	
Input QL Status	Valid, Invalid, Not Supported, Not Applicable	Indicates the validity of the incoming quality level: <ul style="list-style-type: none"> • Valid The quality level is a valid Synchronization Status Message (SSM) and stable. • Invalid The quality level is <i>not</i> a valid SSM, or instable. • Not Supported Evaluating the SSM is not supported on the respective interface due to the chosen format of the input signal (e.g. in case of a 2-MHz timing input signal). • Not Applicable No port is assigned to the current timing reference, or the assigned timing reference experiences a reference fail.

Parameter	Possible values	Meaning
QL Provisioned	SDH synchronization mode: PRC SSUT (default setting) SSUL SEC AUTO	The quality level of the respective timing reference assigned by provisioning. If the provisioned quality level is AUTO , then the incoming SSM Value is used as the quality level. Otherwise, if the provisioned quality level has any value other than AUTO , then the incoming SSM Value is <i>not</i> used, but this provisioned value is used as the quality level.
	SONET synchronization mode: PRS STU ST2 ST3 AUTO (default setting)	
SSM Value	SDH synchronization mode: PRC SSUT SSUL SEC DNU UNSTABLE NONE (default setting)	The quality level as received from the external signal when the signal has a valid Input QL Status (see above).
	SONET synchronization mode: PRS STU ST2 ST3 DUS NONE (default setting)	
Output Ref. Priority	Not applicable	This parameter is <i>not applicable to external timing references!</i> In the SDH synchronization mode, the value "Not applicable" is displayed on the graphical user interface. In the SONET synchronization mode, the Output Ref. Priority is <i>not</i> displayed on the graphical user interface.
Output Lockout State	Not applicable	This parameter is <i>not applicable to external timing references!</i> In the SDH synchronization mode, the value "Not applicable" is displayed on the graphical user interface. In the SONET synchronization mode, the Output Lockout State is <i>not</i> displayed on the graphical user interface.

Parameter	Possible values	Meaning
ASAP	Any specific ASAP of type “System Timing”, or the default ASAP of type “System Timing” (“DEFAULT”).	The Alarm Severity Assignment Profile (ASAP) of type “System Timing” assigned to the respective timing reference.
Detail		By means of the Detail button, more detailed information on the available ASAPs of type “System Timing” can be retrieved.
Timing Port Mode	Monitored, Not Monitored	This parameter indicates whether the respective timing port will be monitored for timing reference failures (Monitored) or not (Not Monitored). If a timing port is set to Not Monitored , then no timing reference failure alarms will be reported for that port.



Synchronization characteristics – system timing

General system timing parameters

Parameter	Possible value	Meaning
System SSM Mode	QL Enable, QL Disable	<p>This parameter indicates whether the synchronization status message (SSM) is evaluated for the selection of the timing reference from which the system timing is derived (QL Enable) or not (QL Disable).</p> <p>In case the System SSM Mode is set to QL Disable, then the System Quality Level Status is DNU in the SDH synchronization mode, and STU in the SONET synchronization mode.</p>
Wait to Restore	<p>SDH synchronization mode: 1 ... 60 minutes in steps of 1 minute (default setting: 5 minutes)</p> <p>SONET synchronization mode:</p> <ul style="list-style-type: none"> • 0 • 20 seconds (default setting) • 1 ... 60 minutes in steps of 1 minute • Infinite 	<p>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.</p> <p>An “infinite” wait-to-restore time can be used in situations when enough timing references are available, and you do not want to use a timing reference again that has failed before. The respective timing reference can be made available again only by means of a Clear Wait to Restore command.</p>

Clock

Parameter	Possible value	Meaning
Clock Mode	Free Running (default setting) Locked	<p>The operational mode of the internal timing generator:</p> <ul style="list-style-type: none"> • Free Running The free-running mode is selected. The internal timing generator 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.

Alarming

Parameter	Possible values	Meaning
ASAP	Any specific ASAP of type “System Timing”, or the default ASAP of type “System Timing” (“DEFAULT”).	The assigned alarm severity assignment profile (ASAP) of type “System Timing”.



9 Timing provisioning tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to timing provisioning.

Contents

To retrieve synchronization information	9-2
To set the synchronization - assigned timing reference	9-7
To set the synchronization - external timing input	9-9
To set the synchronization - external timing output	9-11
To set the synchronization - system timing	9-14
To release the synchronization switch (REF)	9-16
To release the synchronization switch (MOD)	9-18
To operate the synchronization switch (MOD)	9-20
To release the synchronization switch (OUTREF)	9-22
To operate the synchronization switch (REF)	9-24
To operate the synchronization switch (OUTREF)	9-26



To retrieve synchronization information

When to use

Use this task to display the provisioning and operational information of the synchronization attributes as set by the SET-SYCN command and after initial system start-up. It also displays the status of the external timing reference input and output ports.

Related information

For a more detailed explanation, please refer to the description of the RTRV-SYCN command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Retrieve Synchronization**.
 5. Click **Go**.

Result: The **Retrieve Synchronization** page is displayed.

- 3 This parameter displays the active timing reference, which the system clock is currently using for locked mode of system timing.

Use the field **Identifier** to specify the requested information as the following table shows:

To retrieve information related to...	select...
system timing,	<i>system</i> .
assigned timing references,	<i>exttmg0</i> , <i>exttmg1</i> , or <i>exttmgall</i> .
external timing references,	<i>extref1</i> , <i>extref2</i> , or <i>extrefall</i> .
external timing outputs,	<i>exttmg0_out</i> , <i>exttmg1_out</i> , or <i>exttmg_outall</i> .
line timing,	<i>line1</i> to <i>line6</i> , or <i>lineall</i> .
all timing parameters	<i>all</i> .

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

5 The general output *cammand parameter* is:

- **aid** – access identifier
Shows the category to which the information in the respective output line is related to.

The output parameters for *system timing* are:

- **active_ref** – active timing reference status
Displays the active timing reference, which the system clock is currently using for locked mode of system timing.
- **clkmod** – clock mode
Specifies the provisioned operational mode of the system timing.
- **clkmod_stat** – system clock mode status
Specifies the state of the system clock.
- **refsw_stat** – reference switch status
Is a state of the system timing.
- **stratum_level** – stratum level status
This parameter provides information about the level of the system clock.
- **syncmsg** – system synchronization status messaging mode
This parameter is used to enable or disable the SSM protocol.

- **sysql_stat** – system quality level status
Indicates the overall system timing quality level status.
- **timing** – ASAP name
Specifies the name of the ASAP (alarm severity assignment profile) that is assigned to timing.
- **wtr** – wait to restore
Specifies the provisioned wait to restore timer used for all timing ports for revertive switching. This is the amount of time it takes to switch from lower priority to higher priority references.
- **wu_stat** – warm up status
This parameter is an attribute of the timing pack hardware design. At initial start up of the system and at replacing of the active or standby timing function the system is in warm-up state.

The output parameters for *output timing* (instance only valid for SDH) are:

- **active_oref_stat** – active output timing reference status
Displays the current selected timing reference of the timing link switch for the external output.
- **orefswr_stat** – output timing reference switch request status
Indicates the output timing reference switch request state.

The output parameters for *assigned timing reference* are:

- **extout_pri** – timing output reference priority
Specifies the priority assignment of the timing link switch of the external output timing. This parameter is only for SDH and for line timing references.
- **inql** – assigned timing reference quality value
Displays the input synchronization message for each port of the timing link switch provisioning of the system timing and of the output timing.
- **inql_stat** – input quality status
Indicates the synchronization messaging quality level status for the specified timing reference.
- **ql_prov** – quality provisioned
Defines the quality for the specified timing reference to a fixed SSM value. It is the provisioned quality level sync message value that will be received on timing references.
- **ref_lock** – timing reference lockout status
Displays the timing reference lockout state to the specified timing reference. It is the input status for each port of the timing link switch provisioning of the system timing.
- **ref_stat** – assigned timing reference signal status
Is a status of each timing reference.

- **sclkref_lockstat** – station clock output timing reference lockout state
Indicates the assigned station clock output timing reference lockout state. This parameter is only for SDH and for line timing references.
- **syncref_pri** – system timing reference priority
Defines the priority for assigned timing references. When multiple input references have been given the same priority value, it implies non-revertive switching between the associated references. Otherwise, it implies revertive switching to the reference with the highest assigned priority.
- **tpmode** – timing port mode monitoring
Specifies the monitoring status of the timing port.
- **tpql_in** – incoming SSM value of the timing port
Indicates the QL value for the timing port.
- **tref_aid** – timing reference assigned port AID
Specifies the port AID of the assigned timing reference AID.

The output parameters for *external timing input* are:

- **ext_if** – external input signal format
Specifies the format of the external timing input.
- **ext_isa** – external input sa bit location
Defines the external input Sa bit location.
- **ext_issm** – external input ssm support
Specifies if the SSM mode is supported or not on the external timing input port.

The output parameters for *external timing output* are:

- **ext_equ** – cable equalization
Specifies the timing output cable equalization to adjust the specified timing reference output signal power. This parameter is valid only for DS1 (SONET).
- **ext_of** – external output signal format
Specifies the external output signal format.
- **ext_osa** – external output sa bit location
Defines the external output Sa bit location.
- **ext_out_sig_stat** – external output signal status
Indicates the external output signal status.
- **extout_en** – external timing output enabling/disabling
Specifies whether the external timing output is enabled or disabled.
- **extout_prov** – external timing output selection
Specifies the operation mode of the external output timing.
- **extout_ssm** – external timing output AIS mode
Specifies which value will be send when the signal level is below the quality acceptance level or when *frcdus* is enabled.

- **frcdus** – forced DNU/DUS
Specifies the synchronization messaging forced DNU/DUS enable or disable for the timing output port. DUS applies to SONET and DNU applies to SDH.
- **loopdelay** – timing regenerator loop delay
Indicates the delay in the SASE/BITS loop operation. The values are represented by seconds in steps of 1 seconds per loop.
- **ql_out** – quality of the external timing output port
Indicates the quality value on the signal for the timing output port.
- **qlout_tais** – acceptance quality level for output threshold AIS
Indicates the provisioned quality acceptance level for external timing output.
- **regen_loop** – timing regenerator loop
Specifies the avoiding of loops over the SASE/BITS clocks.

END OF STEPS



To set the synchronization - assigned timing reference

When to use

Use this task to set the assign timing references, to modify, or remove them.

Related information

For a more detailed explanation, please refer to the description of the SET-SYCN command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Set Synchronization - Assigned Timing Reference**.
 5. Click **Go**.

Result: The **Set Synchronization - Assigned Timing Reference** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **Timing reference identifier** – select either a single access identifier *extref1*, *extref2* or (*Line 1* to *Line 6*) to separate the parameters related to assigned timing references.
 - **Timing output ref. priority** – select either a single parameter *Priority 0 (Disabled)* or (*Priority 1* to *Priority 6*) to specify the priority assignment of the timing link switch of the external output timing.

- **Quality provisioned** – select a single parameter to define the quality for the specified timing reference to a fixed SSM value.
 - SONET: *AUTO*, *PRS*, *STU*, *ST2*, or *ST3*.
 - SDH: *AUTO*, *PRC*, *SSUL*, *SSUT*, or *SEC*.The “AUTO” value implies sync message support and is rejected if SSM is not supported for the assigned timing reference.
- **System timing ref. priority** – select either a single parameter *Priority 0 (Disabled)* or (*Priority 1 to Priority 8*) to define the priority for assigned timing references.
- **ASAP name** – enter an alphanumeric string with 1 to 24 characters to specifies the name of the “ASAP” (alarm severity assignment profile) that is assigned to timing. A hyphen is additionally allowed in the name.
- **Timing port mode monitoring** – select either a single parameter *Monitored* or *Not-Monitored* to specify the monitoring status of the timing port.
- **Timing ref. assigned port AID** – enter the timing reference assigned port AID to specify the port AID of the assigned timing reference AID.
Note: The parameter is rejected, if the timing reference is already assigned to timing port.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To set the synchronization - external timing input

When to use

Use this task to set the external timing input port attributes, to modify, or to remove them.

Related information

For a more detailed explanation, please refer to the description of the SET-SYNCN command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Set Synchronization - External Timing Input**.
 5. Click **Go**.

Result: The **Set Synchronization - External Timing Input** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **External timing identifier** – select a single access identifier *exttmg0* or *exttmg1* to separate the parameters related to assigned timing references.
 - **External input signal format** – select the format of the external timing input:
 - SONET: *Super Frame* or *Extended Super Frame*.
 - SDH: *2 MHz*, *2 Mbit-unframed*, or *2 Mbit-framed*.

- **External input sa bit location** – select *SA4*, *SA5*, *SA6*, *SA7*, or *SA8* to define the external input Sa bit location.
 - **External input ssm support** – select *Supported* or *Not-Supported* to specify whether the SSM mode on the external timing input port is supported or not.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To set the synchronization - external timing output

When to use

Use this task to set the external timing output port attributes, to modify or to remove them.

Related information

For a more detailed explanation, please refer to the description of the SET-SYNCN command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Set Synchronization - External Timing Output**.
 5. Click **Go**.

Result: The **Set Synchronization - External Timing Output** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **External timing identifier** – select a single access identifier *exttmg*, *exttmg0_out*, or *exttmg1_out* to separate the parameters related to assigned timing references.
 - **Cable equalization** – select *20*, *40*, *60*, *80*, or *100* to specify the timing output cable equalization to adjust the specified timing reference output signal power for DS1 (SONET) only. The values are represented by percentage (100% = 3.0 dB, 80% = 2.4 dB; 60% = 1.8 dB; 40% = 1.2 dB and 20% = 0.6 dB).

- **External output signal format** – select the format of the external output signal format:
 - SONET: *Super Frame* or *Extended Super Frame*.
 - SDH: *2 MHz, 2 Mbit-unframed*, or *2 Mbit-framed*.
- **External output sa bit location** – select *SA4, SA5, SA6, SA7*, or *SA8* to define the external output Sa bit location.
- **External output enabling/disabling** – select *Enable* or *Disable* to specify whether the external timing output is active or not.
- **External timing output selection** – select a single parameter to define the operation mode of the external output timing:
 - SONET: *Line 1* or *Line 2*.
 - SDH: *SETG* or *TLS*.

The value “SETG” means the system clock, the value “TLS” means the output.
- **External timing output AIS mode** – select *AIMODE* or *QLMODE* to specify which value will be send when the signal level is below the quality acceptance level or when *frcdus* is enabled.
- **Forced DNU/DUS** – select *Enable* or *Disable* to enable or disable the synchronization messaging forced DNU (SDH)/DUS (SONET) for the timing output port.
- **Timing regenerator loop delay** – enter a numeric value in the range from 0 to 60 in 1 second steps to indicate the delay in the SASE/BITS loop operation.
- **Accept qual lvl - out thrs AIS** – select the provisioned quality acceptance level for the external timing output:
 - SONET: *PRS, STU, ST2*, or *ST3*
 - SDH: *PRC, SSUL, SSUT*, or *SEC*
- **Timing regenerator loop** – select the avoiding of loops over the SASE/BITS clocks:
 - SONET: *Enable* or *Disable*.
 - SDH: *Disable, extref1, extref2*. or *both*.
- **ASAP name** – enter an alphanumeric string with 1 to 24 characters to specify the name of the ASAP (alarm severity assignment profile) that is assigned to timing. A hyphen is additionally allowed in he name.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To set the synchronization - system timing

When to use

Use this task to set the system timing clock mode, or to modify or to remove the related attributes..

Related information

For a more detailed explanation, please refer to the description of the SET-SYNCN command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Set Synchronization - System Timing**.
 5. Click **Go**.

Result: The **Set Synchronization - System Timing** page is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **System identifier** – select the access identifier *system* to separate the parameters related to assigned timing references.
 - **Clock mode** – select *Free Running* or *Locked* to specify the provisioned operational mode of the system timing.
 - **Sync status messaging mode** – select *Enable* or *Disable* to enable or disable the SSM protocol.

- **ASAP name** – enter an alphanumeric string with 1 to 24 characters to specifies the name of the ASAP (alarm severity assignment profile) that is assigned to timing. A hyphen is additionally allowed in the name.
- **Wait to restore** – specify the provisioned wait to restore timer used for all timing ports for revertive switching. This is the amount of time it takes to switch from lower priority to higher priority references.
 - SONET: either an alphanumeric value set *0SEC*, *20SEC*, *99* (infinite), or *0MIN* to *60MIN* in 1 minute steps.
 - SDH: either an alphanumeric value set *0SEC* or *0MIN* to *60MIN* in 1 minute steps.The values “0SEC” and “0MIN” can be used for SONET and SDH to provision a zero wait to restore time.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To release the synchronization switch (REF)

When to use

Use this task to release (clear) timing reference switching.

Related information

For a more detailed explanation, please refer to the description of the RLS-SYNCNSW-REF command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Release Synchronization Switch REF**.
 5. Click **Go**.

Result: The **Release Synchronization Switch REF** page is displayed.

- 3 In the field **Destination**, select the timing reference to which the command relates (*extref1*, *extref2* or *line1* to *line6*).
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To release the synchronization switch (MOD)

When to use

Use this task to release (clear) the forced request on the timing mode so that it will return to the provisioned locked mode from the holdover mode.

Related information

For a more detailed explanation, please refer to the description of the RLS-SYNCNSW-MOD command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Release Synchronization Switch MOD**.
 5. Click **Go**.

Result: The **Release Synchronization Switch MOD** page is displayed.

- 3 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To operate the synchronization switch (MOD)

When to use

Use this task to request a change from the provisioned synchronization mode to forced holdover state.

Related information

For a more detailed explanation, please refer to the description of the OPR-SYNCNSW-MOD command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Operate Synchronization Switch MOD**.
 5. Click **Go**.

Result: The **Operate Synchronization Switch MOD** page is displayed.

- 3 In the field **Switch command**, select *Forced Switch* to force system timing from the locked mode to the holdover mode (clock backup request).
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To release the synchronization switch (OUTREF)

When to use

Use this task to release (clear) external output timing switch (for SDH only).

Related information

For a more detailed explanation, please refer to the description of the RLS-SYNCNSW-OUTREF command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Release Synchronization Switch OUTREF**.
 5. Click **Go**.

Result: The **Release Synchronization Switch OUTREF** page is displayed.

- 3 In the field **Destination**, select the timing reference to which the command relates (*line1* to *line6*).
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

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



To operate the synchronization switch (REF)

When to use

Use this task to request the NE to operate manual or forced synchronization reference protection switch or to lockout synchronization reference.

Related information

For a more detailed explanation, please refer to the description of the OPR-SYNCNSW-REF command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Timing References**.
4. In the **Function** field, select **Operate Synchronization Switch REF**.
5. Click **Go**.

Result: The **Operate Synchronization Switch REF** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Switch command** – specify the desired switching function:
 - *Lock out timing reference* – the reference which is addressed by the “Destination” parameter, will be locked out by the user and cannot be used as a timing reference signal until the lockout is cleared.
 - *Forced switch* – to force selection of the external timing output determined by the “Destination” parameter.

- *Manual switch* – a manual selection of the external timing output determined by the “Destination” parameter.
 - *Clear wait-to-restore period* – the reference which is addressed by the “Destination” parameter will be terminated. The signal status will return to normal.
 - **Destination** – select the timing reference to which the command relates *extref1*, *extref2*, or (*line1* to *line6*).
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To operate the synchronization switch (OUTREF)

When to use

Use this task to request the NE to operate manual or forced synchronization reference protection switch or external timing output protection switch (for SDH only), to lockout synchronization reference, or external output timing (for SDH only) switching.

Related information

For a more detailed explanation, please refer to the description of the OPR-SYCNNSW-OUTREF command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Procedure

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Timing References**.
 4. In the **Function** field, select **Operate Synchronization Switch OUTREF**.
 5. Click **Go**.

Result: The **Operate Synchronization Switch OUTREF** page is displayed.

- 3** Change the entries or selections for any modifiable fields that you wish to update.
- **Switch command** – specify the desired switching function:
 - *Lock out timing reference* – the reference which is addressed by the “Destination” parameter, will be locked out by the user and cannot be used for external timing output until the lockout is cleared.
 - *Forced switch* – to force selection of the external timing output determined by the “Destination” parameter.
 - *Manual switch* – a manual selection of the external timing output determined by the “Destination” parameter.
 - **Destination** – select the timing reference to which the command relates (*line1* to *line6*).
-

- 4** Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



10 Traffic provisioning concepts

Overview

Purpose

This chapter presents concept information related to traffic provisioning on *LambdaUnite*[®] MSS network elements using Lucent OMS.

Contents

SDH/SONET traffic provisioning concepts	10-2
Cross-connections	10-2
Lower-order cross-connections (LOXC)	10-8
Path protection (SNCP/UPSR)	10-13
Line protection (MSP/APS)	10-15
Ring protection (MS-SPRing/BLSR)	10-17
Dual node interworking / Dual ring interworking (DNI/RNI)	10-22
Ethernet traffic provisioning concepts	10-23
<i>TransLAN</i> [®] Ethernet over SDH implementation	10-23
Virtual concatenation	10-25
Virtual LAN	10-27
Tagging schemes	10-29
Spanning tree protocol	10-30
Link path through	10-32



SDH/SONET traffic provisioning concepts

Cross-connections

Cross-connection shapes

The supported cross-connection shapes (as shown in the graphical display of a cross-connection) are listed in the following table:

Cross-connection shape	Diagram	Management system symbol
<i>Simple (uni)</i> , a unidirectional point-to-point connection		
<i>Simple (bi)</i> , a bidirectional point-to-point connection		
<i>Add-drop A (uni)</i> , part of a unidirectional path protection scheme		
<i>Add-drop Z (uni)</i> , part of a unidirectional path protection scheme		
<i>Add-drop (bi)</i> , part of a bidirectional path protection scheme		

Cross-connection shape	Diagram	Management system symbol
<p><i>Double add-drop (bi), part of a bidirectional path protection scheme</i></p>		
<p><i>Interconnect-W (bi)</i></p>		
<p><i>Interconnect-P (bi)</i></p>		

Interfaces and ports

The *LambdaUnite*[®] MSS add/drop multiplexer in its basic configuration is a single shelf that interfaces electrical STM-1 and optical STM-1/OC-3, STM-4/OC-12, STM-16/OC-48 and STM-64/OC-192 lines to an SDH/SONET-standard MS-SPRing/BLSR protected ring. It has 32 universal slots that support flexible electrical and 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 (for example 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 and STM-16 1+1 MS-SPRing
- 4-fiber MS-SPRing port protection group used for STM-64 and STM-16 1+1 MS-SPRing transoceanic protocol
- 2-fiber MS-SPRing port protection group used for STM-64, and STM-16 1+1 MS-SPRing
- 1+1 MSP port protection group used for STM-64, STM-16, STM-4, and STM-1 1+1 MSP
- 1:1 MSP port protection group used for STM-64, STM-16, STM-4 and STM-1 1:1 MSP
- 2-fiber BLSR port protection group used for OC-192, and OC-48 1+1 BLSR
- 4-fiber BLSR port protection group used for OC-192 and OC-48 1+1 BLSR
- 1+1 APS port protection group used for OC-192, OC-48, OC-12, and OC-3 1+1 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 configurable 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.

Transmission interfaces

LambdaUnite[®] MSS includes the following electrical and optical port units:

Interface type	Transmission rate	Wavelength
Optical	STM-64/OC-192	1.5 μm (long reach)
		1.5 μm (intermediate reach)
		1.3 μm (intra office)
		<i>LambdaXtreme</i> [®] Transport compatible (128 colors)
		OLS 1.6T compatible (80 colors)
		passive WDM compatible (16 colors)
		IEEE802.3ae 1000GBASE-EW WAN PHY interworking
	STM-16/OC-48	1.5 μm (long reach)
		1.3 μm (long reach)
		1.3 μm (short reach / intra office)
		passive WDM compatible (32 colors)
	STM-4/OC-12	1.3 μm (intermediate reach)
	STM-1/OC-3	1.3 μm (intermediate reach)
GE1/SX4, 1 GbEthernet	1000BASE-SX	
GE10PL1, 1 Gb Ethernet, 10 Gb Ethernet	1000BASE-SX	
Electrical	STM-1	intra office electrical interface Each unit contains eight independent unidirectional ports.

Switch capacity

The total full non-blocking switch capacity is 320 Gbps (6144 STS-1/2048 VC-4s).

The total full non-blocking lower order switch capacity is 40 Gbps (for example, 16.128 bidirectional or 32.256 unidirectional cross-connected VT1.5 signals).

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

The following cross-connection levels are supported in the LOXC application of the *LambdaUnite*[®] MSS:

- LOVT1 (SONET)
- LOVC3 (SDH)
- LOVC12 (SDH).

Cross-connection types supported by the LOXC application

The LOXC application supports the following cross-connection types

- 1WAY:
Unprotected unidirectional cross-connection
- 2WAY:
Unprotected bidirectional cross-connection
- 1WAYPROT:
Protected unidirectional cross-connection

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.



Lower-order cross-connections (LOXC)

Overview

This section gives an overview about the features related to lower-order cross-connections (LOXC).

Signal rates

The main purpose of the LOXC function is to cross-connect lower-order tributaries on the following levels:

- VT1.5 (SONET),
- VC-12 (SDH),
- (LO) VC-3 (SDH).

For this purpose, substructured higher-order signals need to be terminated before the embedded lower-order signals can be cross-connected.

Supported signals with lower-order substructure are:

- STS-1 (SONET) carrying VT1.5 signals,
- VC-4 (SDH) carrying LO VC-3 or VC-12 signals (or a mix of it).

Any type of concatenated signal is not supported (despite VC-4 could be interpreted as STS-3C).

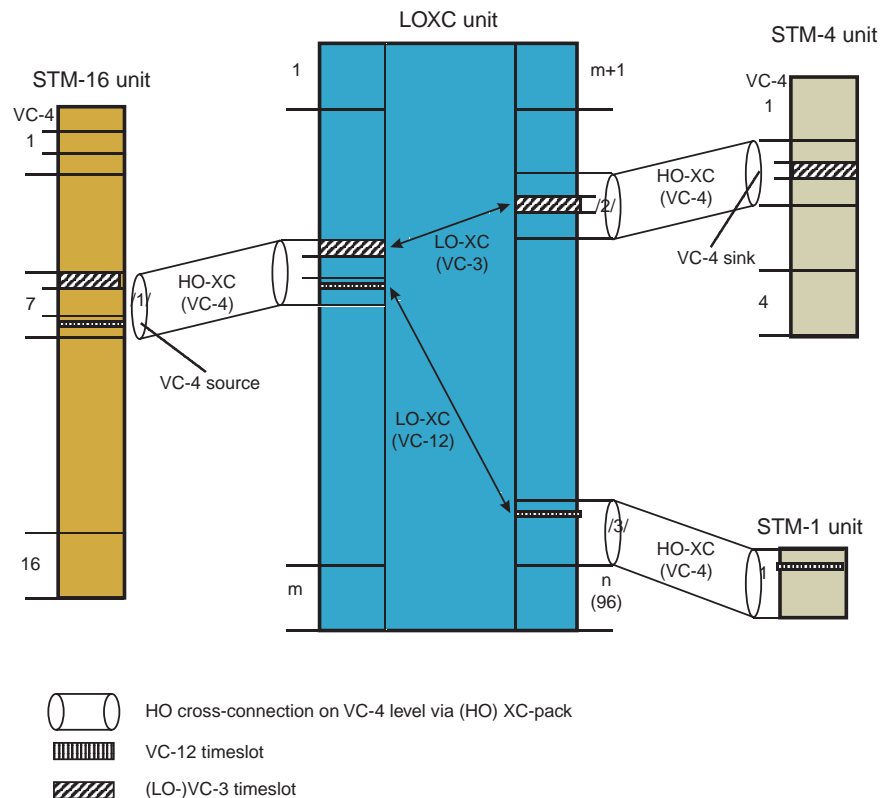
Connectivity types

The LOXC function supports following types of cross-connections:

- uni-/bidirectional unprotected cross-connections
- 1:2 broadcasting
- AU3/AU4 conversion.

Configuration specifications

The following figure shows an example for the switching of lower-order cross-connections between an STM-16 unit and an STM-4 unit (switching on lower-order VC-3 level) and an STM-1 unit (switching on VC-12 level).



Restrictions

For configuring a lower-order cross-connection the following rules have to be considered:

- For LOXC/1 a switch capacity of max. 96 VC-4 equivalents is available which corresponds to 15G.
- For LOXC40G2S/1 a switch capacity of max. 768×768 VC-3 (lower-order), 16128×16128 VC-12, or 21504×21504 VT1.5 equivalents is available which corresponds to 40 G.
- To activate the lower-order cross-connection unit (LOXC), depending on the type of LOXC used, the switching capacity of the respective circuit pack has to be set to
 - 15 Gbps, in the case of an LOXC/1,
 - 40 Gbps, in the case of an LOXC40G2S/1.
- The *System Interface Standard Default* of all ports to be used for a lower-order cross-connection must be set to same value, either SDH or SONET.

Lower-order VC access for MS-SPRing

The system supports the provisioning of cross-connections on LO-VC level from, to, and between MS-SPRing ports. It is also supported to enter source and destination node information for that HO-VC the cross-connected LO-VC is part of.

Important! This feature does not ask for HO-VC unsquelching (node type 2) or LO-VC squelching (node type 3) as this is not standardized for SDH.

Important! The same provisioning (LO-CCs from, to, and between MS SPRING ports) has to be rejected for SONET BLSR ports

Important! This feature does not include input legs of LO path protected cross-connections from MS-SPRING ports.

Mapping schemes

For *LambdaUnite*[®] MSS the following mappings are supported:

- SDH:
 - VC-12 and VC-3 – this means according to the SDH multiplex scheme:
 - VC-12 → TU-12 (3×) → TUG-2 (7×) → TUG-3 (3×) → VC-4 → AU-4
 - VC-3 → TU-3 → TUG-3 (3×) → VC-4 → AU-4
- SONET:
 - VT1.5 – this means according to the SONET multiplex scheme:
 - VT1.5 (4×) → VT group → STS-1
 - SDH: 33 // 6312 // 4212-13 // 2112-13-2112 // 13-4212 // 23-2112 // / 2112-23
 - SONET: 2811²²

AU-3/AU-4 conversion cross-connections

AU-3/AU-4 conversion cross-connections allow the conversion of a higher order STS-1 (SONET) to a lower order VC-3 (SDH), and the mapping into a higher order VC-4. From a cross-connection provisioning point of view, an AU-3/AU-4 conversion cross-connection is a cross-connection between a higher order STS-1 and a lower order VC-3 tributary.

Supported conversions

The following types of conversion cross-connections are supported:

- SONET (STS-1) to SDH (AU-4) conversion
- DS3 signal to TU-3/VC-4 conversion

The following cross-connection types are supported on the ITM-CIT:

- 1-Way Conversion Cross Connection
Unprotected conversion cross-connection
- 2-Way Conversion Cross-Connection
Protected conversion cross-connection

Important! Conversion cross-connections are only possible if a lower order cross-connection unit of type *LOXC40G2S/1* or *LOXC40G3S/1* is used and the LOXC interface standard is set to SDH.

The source or destination of a conversion cross-connection may *not* reside on one of the following types of port units:

- OPT2G5
- GE1
- GE10PL1

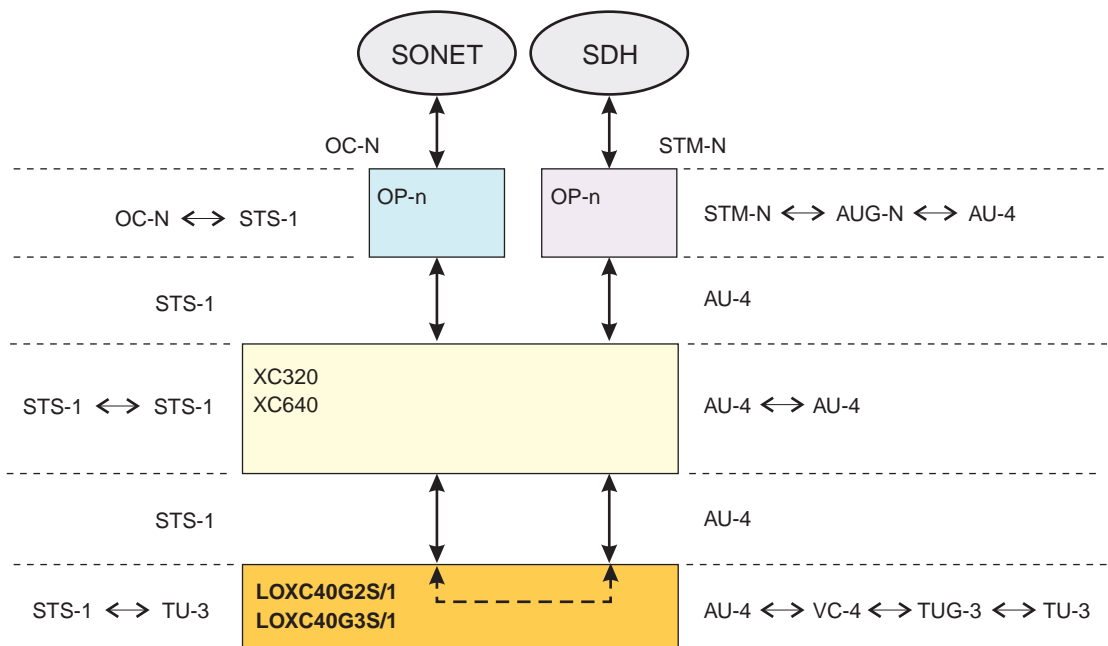
Supported cross-connection rates

The following values are supported on the ITM-CIT:

- **AU3TU3** for higher order STS-1 input to lower order VC-3 output
- **TU3AU3** for lower order VC-3 input to higher order STS-1 output

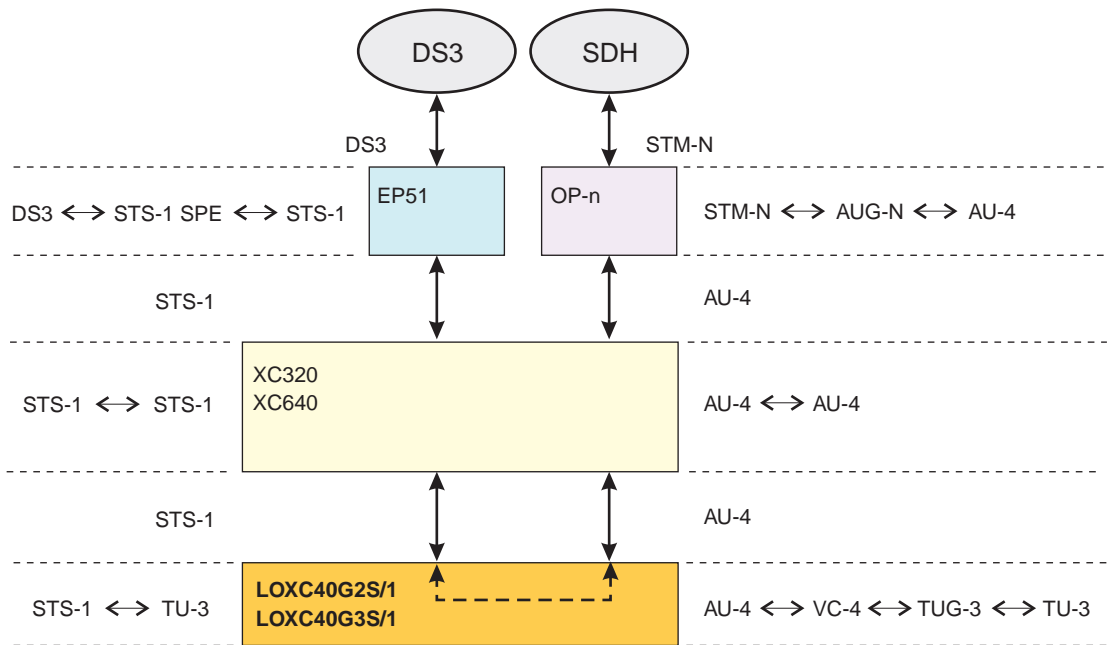
Example: SONET (STS-1) to SDH (AU-4) conversion

The AU-3/AU-4 conversion functionality can be used to convert SONET signals (STS-1) into TU-3/TUG-3 substructured VC-4 signals.



Example: DS3 signal to TU-3/VC-4 conversion

The AU-3/AU-4 conversion functionality can be used to map DS3 signals into TU-3/TUG-3 substructured VC-4 signals:



□

Path protection (SNCP/UPSR)

Principles

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.

The object associated to a path-protected cross-connection topology that is provisioned to provide path-level protection switching for all the constituent signals carried by the cross-connection is called path protection group. A path protection group consists of one or more constituent path selectors. LO path protection groups always consist of only one constituent path selector.

LambdaUnite[®] MSS supports both, SONET and SDH path protection features:

- SDH: *subnetwork connection protection (SNCP)*
- SONET: *unidirectional path-switched ring (UPSR)*

SNCP

SNCP is 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, general, 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.

The LOXC application supports SNC/I for the following cross connection types:

- VC-12
- (LO) VC-3
- 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.

The LOXC application supports SNC/N for the following cross connection types:

- VC-12 (SDH)
- (LO) VC-3

UPSR

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 operates 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, for example on path layer indications including path layer defects and maintenance signals.

LambdaUnite[®] MSS supports UPSR protection, also within logical ring applications.

UPSR on lower order tributaries are supported for VT1.5 connections.

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.

□

Line protection (MSP/APS)

Principles

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.

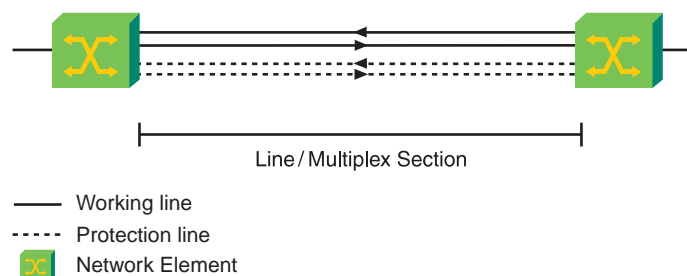
LambdaUnite[®] MSS supports both, SONET and SDH line protection features.

- SDH: 1+1 multiplex section protection (MSP) on STM-64, STM-16, STM-4 and STM-1 interfaces
- SONET: 1+1 linear automatic protection switch (APS) on OC-192, OC-48, OC-12 and OC-3 interfaces

1+1 MSP/APS functional description

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:



Mode of operation

In the *LambdaUnite*[®] MSS systems the 1+1 MSP/APS operate unidirectional or bidirectional in non-revertive or revertive mode.

1:1 MSP protection functional description

For STM-64, STM-16, STM-4, and STM-1 optical ports, a 1:1 MSP protection is possible. In a 1:1 MSP configuration low-priority traffic can be transmitted via the protection port as long as no protection switch occurs. If the traffic of the working section has to be switched to the protection section, the low-priority traffic is lost (1:1 MSP with preemptible protection access). The K1 and K2 bytes of the SOH within the protection section define the automatic protection switch (APS) protocol as defined in ITU-T G.841.

The MSP 1:1 protection is very similar to the MSP 1+1 protection. The difference is that MSP 1:1 supports extra traffic on the protection port. The protection group will retrieve the tributary data from the tributaries of the working port and forward it to the protection port.

Mode of operation

In the *LambdaUnite*[®] MSS system, the 1:1 MSP is working in revertive mode. It can be established as bidirectional protection.



Ring protection (MS-SPRing/BLSR)

Principles

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)*

Transoceanic protocol (TOP)

LambdaUnite[®] MSS supports 4-fiber MS-SPRing transoceanic protocol protection schemes on the 10-Gbps interfaces. The protection scheme complies with ITU-T Rec. G.841.

This section defines the support of undersea cable applications in an SDH network using a 4-fiber MS-SPRing configuration. These applications frequently encounter distances between nodes that are greater than the overall circumference designed for the MS-SPRing (that is > 1200 km). This application is the transoceanic protocol without extra traffic (TOP-WO) and the transoceanic protocol with restoration of extra traffic (TOP+EX). Extra traffic is allowed during normal conditions and is preempted when a protection switch is requested. The TOP+EX preempts the extra traffic initially, but re-establishes extra traffic assigned to protection bandwidth that is not required for restoration of the failed services. The extra traffic is re-established as part of the protection switching processing.

MS-SPRing protection schemes

The following MS-SPRing protection schemes can be configured:

- 2-fiber MS-SPRing on STM-64, and STM-16 interfaces
- 4-fiber MS-SPRing on STM-64 and on STM-16 interfaces
- 4-fiber MS-SPRing with transoceanic protocol on STM-64 and on STM-16 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.

Configuration rules

A 4-fiber MS-SPRing 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 group (east protection port or west protection port).

In a 2-fiber or 4-fiber MS-SPRing the total number of nodes may not exceed 16, not more than one node is allowed per each NE in the same ring.

BLSR protection schemes

The following BLSR protection schemes can be configured:

- 2-fiber BLSR on OC-192 and on OC-48 interfaces
- 4-fiber BLSR on OC-192 and on OC-48 interfaces

The protection scheme complies with the ANSI T1.105.01 Standard and provides in a future release also preemptible protection access (PPA). 4-fiber BLSR for the OC-48 interfaces will be supported in future.

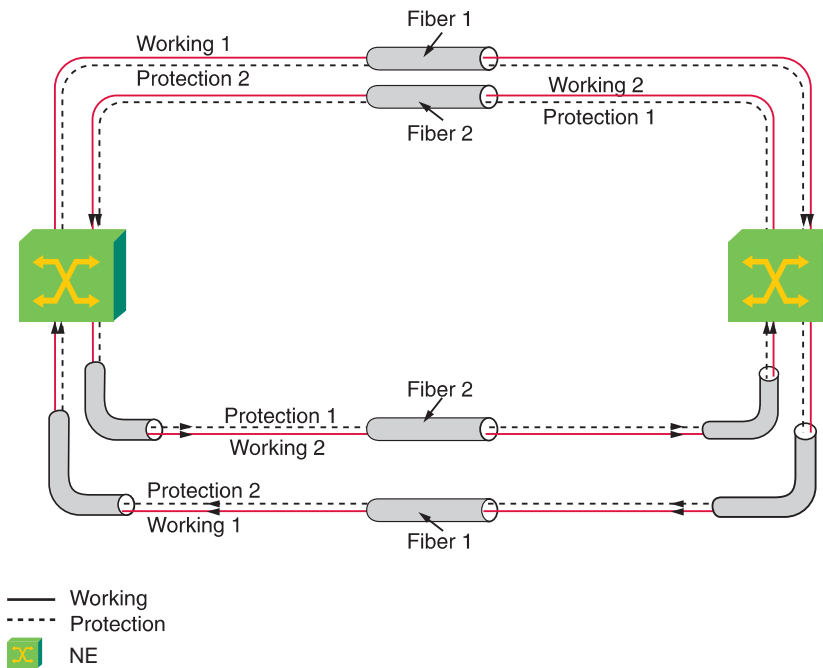
Configuration rules

A 4-fiber BLSR group can only be provisioned successfully, if there is no line timing reference assigned to the protection port of the spans of the BLSR group (east protection port or west protection port).

In a 2-fiber or 4-fiber BLSR the total number of nodes may not exceed 16, not more than one node is allowed per each NE in the same ring.

Traffic disposition

The following figure shows working and protection traffic disposition in a *LambdaUnite*[®] MSS 2-fiber MS-SPRing/BLSR.



Self-healing rings

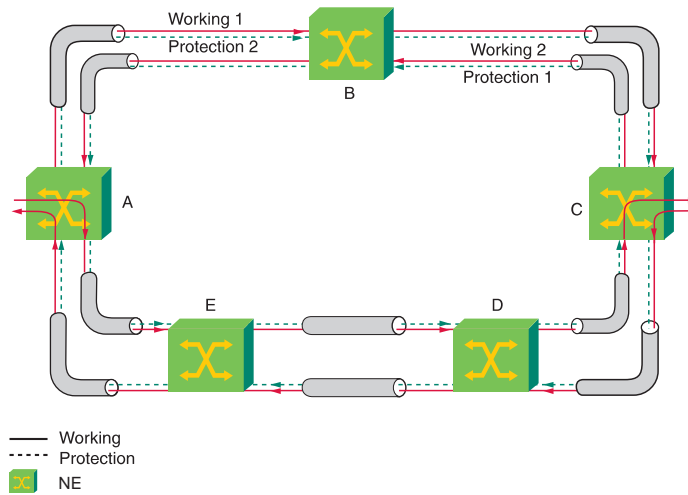
LambdaUnite[®] MSS MS-SPRings/BLSRs are self healing, that means transport is automatically restored after node or fiber failures.

In case of a 2-fiber 10Gbps MS-SPRing/BLSR, each line carries 32 VC-4/STS-3c equivalent time slots of working capacity plus 32 VC-4/STS-3c equivalent time slots of protection capacity. For 2-fiber 2.5 Gbps MS-SPRing/BLSR, the working and protection capacity is eight VC-4/STS-3c equivalents time slots.

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.

Traffic flow example

The following figure shows normal (non-protection-switched) traffic flow in a *LambdaUnite*[®] MSS 2-fiber MS-SPRing/BLSR.

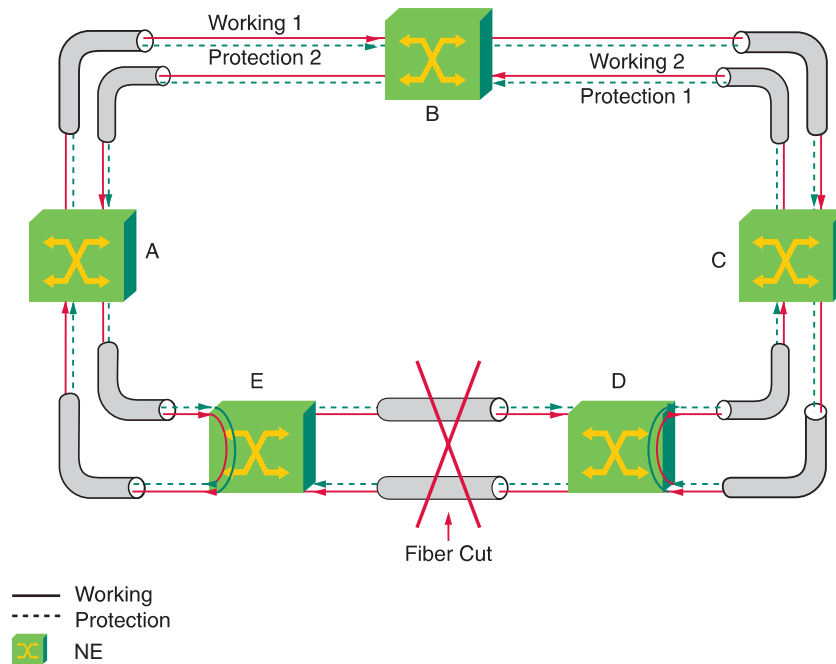


Protection switching

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. Service is reestablished on the protection capacity in less than 50 ms 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 the previous example, 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.

□

Dual node interworking / Dual ring interworking (DNI/RNI)

Overview

Dual node interworking (DNI) and *dual ring interworking (DRI)* 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.

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.

DNI/DRI is a network topology whereby two rings are interconnected at two nodes on each ring. It provides a high degree of survivability of the traffic crossing from one ring to the other.

Drop and continue

Drop and continue is a method used in one ring for interconnecting with another ring. One of the interconnecting nodes dual feeds the traffic both toward the other ring and toward the other interconnecting node within the same ring, so that the same traffic is transmitted to the other ring at two different nodes. The implementation of the drop and continue method depends on the type of the ring. It is different in a BLSR/MS-SPRing and in a UPSR/SNCP ring.

The DRI functionality is compliant with ANSI T1.105.01 and Telcordia GR-1230-CORE and GR-1400-CORE standards. The DNI functionality is also compliant with ITU-T G.842 standard.

DNI/DRI SNCP or UPSR

LambdaUnite[®] MSS supports DNI/DRI between two SNCP or UPSR protected rings.



Ethernet traffic provisioning concepts

TransLAN[®] Ethernet over SDH implementation

Overview

This section describes in brief some related features of *LambdaUnite*[®] MSS:

- Virtual concatenation
- Link Capacity Adjustment Scheme (LCAS)
- Virtual LAN
- Repeater mode
- VLAN tagging
- Multipoint mode
- VLAN trunking
- Spanning Tree Protocol (STP)
- Rapid spanning tree protocol (rSTP)
- Generic VLAN Registration Protocol
- Link path through (LPT)

In addition, it is highly recommended to consult the *TransLAN*[®] *Ethernet SDH Transport Solution Applications and Planning Guide*, 365-377-002 (109608364) when planning to use *LambdaUnite*[®] MSS for Ethernet applications.

TransLAN[®] principles

TransLAN[®] is the collective term for the Ethernet SDH Transport Solution which includes the transport of Ethernet (up to 10 Mbps), Fast Ethernet (100 Mbps), and Gigabit Ethernet (1 Gbps) payload data over an SDH network.

The *TransLAN*[®] Ethernet cards allow direct interconnection of data equipment over an SDH transport network. The external data equipment could be an Ethernet switch, an IP router, or a host system such as a user PC or a web server.

The *TransLAN*[®] implementations all use standardized protocols to transport Ethernet frames over the SDH network. First, the generic framing procedure (GFP) or the proprietary Ethernet over SDH (EoS) method, a pre-standard GFP on several first generation *TransLAN*[®] card types, is used to encapsulate the Ethernet frames into the SDH transmission payload. Secondly, virtual concatenation and LCAS are used to allocate a flexible amount of WAN bandwidth for the transport of Ethernet frames.

TransLAN[®] supports IEEE 802.3 Ethernet frames as well as “Ethernet II” frames (“DIX frames”).

Although optimized for IP, *TransLAN*® is an Ethernet transport technology. It is transparent to all layer 3 protocols (IP, IPX, DECnet, etc.).

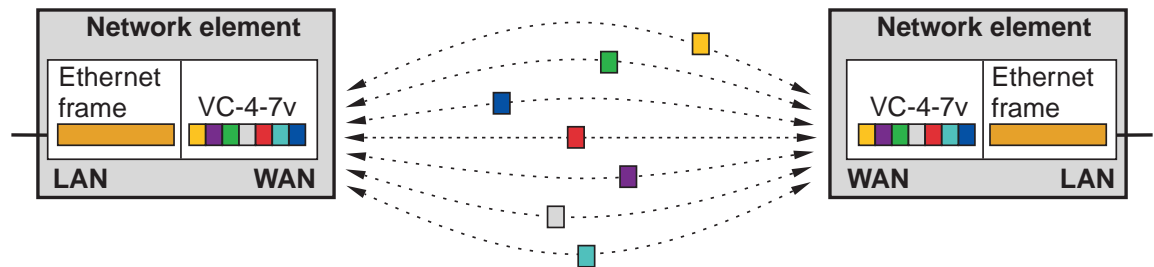


Virtual concatenation

Principles

The GE1 interface supported by *LambdaUnite*[®] MSS allows you to transport Gigabit Ethernet (GbE) signals over SONET/SDH networks by encapsulating Ethernet packets in virtually concatenated Synchronous Payload Envelopes (SPEs, SONET) or Virtual Containers (VCs, SDH).

The following figure shows the principle of virtual concatenation in a point-to-point Gigabit Ethernet (GbE) application example. Protection of the STS-1-Kv/VC-4-Kv traffic is possible via UPSR/SNCP, via 1+1 line APS / 1+1 MSP 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 virtual containers a differential delay will occur between the individual virtual containers. This differential delay has to be compensated and the individual virtual containers 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 loosing 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 LCAS provides automatic decrease of bandwidth in case of link failure and reestablishment after link recovery.

The following unidirectional and bidirectional virtual concatenations are supported:

- STS-1- K v, where $K = 1$ up to 21 in steps of 1
- VC-4- K v, where $K = 1$ up to 7 in steps of 1.

The GE1 circuit pack allows to transport Gigabit Ethernet signals efficiently over SONET or SDH networks by encapsulating Ethernet packets in virtually concatenated VC-4 or STS-1s, using the LCAS. This protection-by-load-sharing feature allows for efficient use of protection bandwidth, that can be added/removed hitlessly for Ethernet applications.



Virtual LAN

Principles

Virtual Local Area Networks (VLANs) can be used to establish broadcast domains within the network as routers do, but they cannot forward traffic from one VLAN to another. Routing is still required for inter-VLAN traffic. Optimal VLAN deployment is predicated on keeping as much traffic from traversing the router as possible.

VLAN supports the following advantages:

- Easy provisioning of VLANs
- Consistency of the VLAN membership information across the network
- Optimization of VLAN broadcast domains in order to save bandwidth
- Isolated service for different customers.

The operator configures VLANs on LAN ports, and GVRP takes care of configuring VLANs on Wide Area Network (WAN) ports in the most optimized way.

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.

Multipoint mode

LambdaUnite[®] MSS supports Ethernet multipoint applications for specific network topologies, for example if an end user has more than 2 sites that need to be connected. It is also possible to support multiple end users on the same Ethernet network, sharing the available bandwidth on the WAN ports over the SONET/SDH network.

The virtual switch implemented on the GE1 interface is a logical grouping of Ethernet ports and Virtual Concatenation Group (VCG) ports that share interconnect and a common set of properties. The virtual switch is automatically instantiated as soon as the VLAN tagging mode is set to IEEE802.1Q multipoint mode. All 4 LAN ports and all 4 WAN ports of the GE1 circuit pack are part of the single virtual switch.

Regarding multipoint Ethernet service a more general terminology is needed to cover the functions of LAN and WAN ports. The new application focused terms are:

- customer LAN ports (the default for LAN ports)
- network WAN ports (the default for WAN ports)
- network LAN ports
- customer WAN ports.

By default, network ports participate in STP and GVRP, and customer ports have a PVID and a Valid VLAN list assigned. LAN ports default to customer port role and WAN ports to network role. All default values can be overridden.

VLAN trunking

Trunking applications are those applications where traffic of multiple end users is handed-off via a single physical Ethernet interface to a router or switch for further processing. This scenario is also called “back-hauling”, since all traffic is transported to a central location, for example a point-of-presence (PoP) of a service provider. Trunking applications can be classified into two topology types, trunking in the hub-node and distributed aggregation in the access network.



Tagging schemes

Principles

LambdaUnite[®] MSS systems support these tagging schemes:

- IEEE 802.1Q VLAN tagging
- Transparent tagging

IEEE 802.1Q VLAN tagging

All frames on the network links have a single VLAN tag. This tag is either the tag that was created by the end user equipment; or it is inserted on the ingress “customer” port (the default VLAN id) by the *TransLAN*[®] switch. On egress customer ports the earlier inserted VLAN tag is removed if a default VLAN id is provided on that port; it should be the same VLAN id as on the associated ingress ports. To ensure customer isolation, you must allocate VLANs to customers and to the customer ports, and ensure that VLANs don’t overlap. The IEEE 802.1Q VLAN tagging scheme supports VLAN trunking, i.e. traffic from multiple different end users is multiplexed over one physical interface towards an IP router in an ISP POP. End user identification and isolation is done via the VLAN tag.

Transparent tagging

The “transparent tagging” scheme, also known as “double tagging” or “VPN tagging”, is a Alcatel-Lucent proprietary tagging scheme.

All frames that enter the network are prefixed with a customer identification (CID) tag. Each customer port on the network is assigned a CID. As all frames are prefixed, there is no difference between end user frames that were originally VLAN tagged or untagged, only the CID is used in Ethernet switching decisions. There is no need for an operator to coordinate the end user VLAN schemes, but CIDs must be assigned consistently per customer over the whole Ethernet network. VLAN trunking is not supported, due to the proprietary tagging scheme.

□

Spanning tree protocol

Principles

The *spanning tree protocol (STP)* is a standard Ethernet method for eliminating loops and providing alternate routes for service protection. Standard STP depends on information sharing among Ethernet switches/bridges to reconfigure the spanning tree in the event of a failure. The STP algorithm calculates the best loop-free path throughout the network. STP defines a tree that spans all switches in the network; it e.g. uses the capacity available bandwidth on a link (path cost) to find the optimum tree. It forces redundant links into a standby (blocked) state. If a link fails or if a STP path cost changes the STP algorithm reconfigures the Spanning Tree topology and may reestablish previously blocked links. The STP also determines one switch that will be the root switch; all leaves in the Spanning Tree extend from the root switch.

Rapid spanning tree protocol

Rapid spanning tree protocol (rSTP) reduces the time that the STP protocol needs to reconfigure after network failures. Instead of several tens of seconds, rSTP can reconfigure in less than a second. The actual reconfiguration time depends on several parameters, the two most prominent are the network size and complexity. IEEE802.1w describes the standard implementation for rSTP.

Generic VLAN registration protocol

Generic VLAN registration protocol (GVRP) is an additional protocol that simplifies VLAN assignment on network ports and ensures consistency among switches in a network. Further it prevents unnecessary broadcasting of Ethernet frames by forwarding VLAN frames only to those parts of the network that have customer ports with that VLAN ID.

The operator configures VLANs on customer ports, and GVRP will take care of configuring VLANs on network ports – in the most optimized way. Note that GVRP and Spanning Tree Protocol interact with each other. After a stable Spanning Tree is determined (at initialization or after a reconfiguration due to a failure) the GVRP protocol will recompute the best VLAN assignments on all network ports, given the new spanning tree topology.

The provisioned VLANs on customer ports are called static VLAN entries; the VLANs assigned by GVRP are called dynamic VLAN entries. The dynamic VLAN entries need not be stored in NE's database.

GVRP can be enabled (default) or disabled per virtual switch:

- In the enabled case up to 247 VLANs can be supported through GVRP; an alarm will be raised if more than 247 VLANs are provisioned on an Ethernet network. This limitation depends on the processor performance.
- If GVRP is disabled, up to 4093 VLANs per Gigabit Ethernet circuit pack port are supported.



Link path through

Principles

The Gigabit Ethernet interfaces on the *LambdaUnite*[®] MSS network elements support the so-called *link pass through (LPT)* mode.

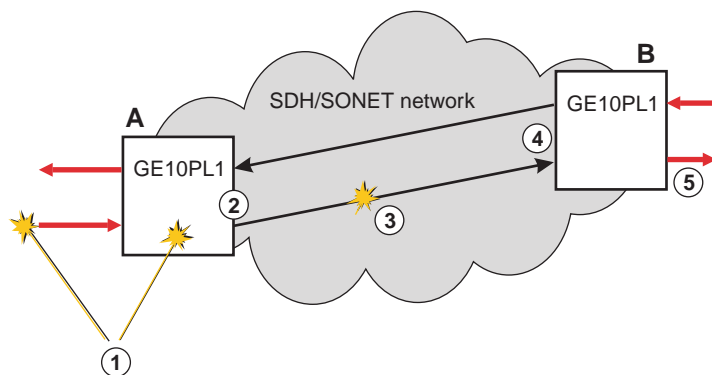
The LPT mode can be used to enable or improve network protection schemes on the equipment external to the *TransLAN*[®] systems.

The LPT mode can be enabled or disabled per GbE port.

Important! The LPT mode is only supported on GbE ports (LAN ports) that operate in a *strict one-to-one association* with a WAN port using *GFP encapsulation*.

Important! Link path through (LPT) is not supported by the Gigabit Ethernet transmission unit GE1.

Please refer to the following figure for clarification and further reference.



If an upstream GbE fiber failure (e.g. a fiber cut) or equipment failure (1) is detected at node A, then a Client Signal Fail (CSF) indication is inserted into the GFP-encapsulated signal (2). If such a CSF indication or a Server Signal Fail (SSF) condition (due to a failure on the transmission line (3) for example) is detected at node B (4), then this can be used to trigger the inhibition of the transmitter at the LAN egress port (5) as a consequent action.

Important! Please note that once the LPT mode is activated on a LAN port, any requests to have more than two ports on the associated virtual switch will be rejected. In order to increase the number of ports on the virtual switch, the LPT mode first has to be disabled.

□

11 Traffic provisioning tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to traffic provisioning.

Contents

Provisioning of cross-connections	11-4
To view all cross-connections	11-4
To view lower-order cross-connections	11-8
To view higher-order cross-connections	11-12
To add an uncorrelated lower-order cross-connection	11-16
To create a 1-Way conversion cross-connection	11-19
To create a 2-Way conversion cross-connection	11-23
To add an uncorrelated higher-order cross-connection	11-27
To modify a lower-order cross-connection's topology	11-30
To modify a higher-order cross-connection's topology	11-34
To modify a cross-connection's parameters	11-38
To change a higher-order cross-connection from ONNS to traditional mode	11-41
To roll the input of a lower-order cross-connection from one tributary port to another	11-43
To roll the input of a higher-order cross-connection from one tributary port to another	11-46
To delete a cross-connection	11-49

To retrieve ONNS to UPSR/SNCP constructs	11-52
To add an ONNS to UPSR/SNCP construct	11-54
To delete an ONNS to UPSR/SNCP construct	11-56
Provisioning of path protection groups (SNCP, UPSR)	11-58
To view a list of path protection groups (SNCP, UPSR)	11-58
To modify a path protection group (SNCP, UPSR)	11-60
To operate a path protection group switch (SNCP, UPSR)	11-62
To operate an SNCP VC-4 protection group switch on constituent members	11-64
Provisioning of MSP protection groups	11-66
To view a list of 1+1 or 1x1 MSP protection groups	11-66
To add a 1+1 MSP protection group	11-67
To add a 1x1 MSP protection group	11-69
To modify a 1+1 or 1x1 MSP protection group	11-71
To delete a 1+1 or 1x1 MSP protection group	11-73
To operate an MSP protection switch	11-75
Provisioning of APS protection groups	11-77
To view a list of 1+1 or 1x1 APS protection groups	11-77
To add a 1+1 APS protection group	11-78
To add a 1x1 APS protection group	11-80
To modify a 1+1 or 1x1 APS protection group	11-82
To delete a 1+1 or 1x1 APS protection group	11-84
To operate an APS protection switch	11-86
Provisioning of MS-SPRing protection groups	11-88
To view a list of 2-fiber MS-SPRing protection groups	11-88
To add a 2-fiber MS-SPRing protection group	11-89
To modify a 2-fiber MS-SPRing protection group	11-91
To delete a 2-fiber MS-SPRing protection group	11-93
To operate a 2-fiber MS-SPRing protection switch	11-95
To view a list of 4-fiber MS-SPRing protection groups	11-97
To add a 4-fiber MS-SPRing protection group	11-98
To modify a 4-fiber MS-SPRing protection group	11-100
To delete a 4-fiber MS-SPRing protection group	11-102

To operate a 4-fiber MS-SPRing protection switch	11-104
Provisioning of BLSR protection groups	11-106
To view a list of 2-fiber BLSR protection groups	11-106
To add a 2-fiber BLSR protection group	11-107
To modify a 2-fiber BLSR protection group	11-109
To delete a 2-fiber BLSR protection group	11-111
To operate a 2-fiber BLSR protection switch	11-113
To view a list of 4-fiber BLSR protection groups	11-115
To add a 4-fiber BLSR protection group	11-116
To modify a 4-fiber BLSR protection group	11-118
To delete a 4-fiber BLSR protection group	11-120
To operate a 4-fiber BLSR protection switch	11-122



Provisioning of cross-connections

To view all cross-connections

When to use

Use this task to view information on existing cross-connection in the NE.

Related information

For a more detailed explanation, please refer to the description of the RTRV-CRS-ALL command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Retrieve Cross-connections ALL**.
 5. Click **Go**.

Result: The **Retrieve Cross-connections ALL** page is displayed.

-
- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **Input Access Identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection. Note: To view all cross-connections enter *1-1-#-#-all-all-all*.
 - **Protection Group Name** – enter an alphanumeric user-defined string of up to 24 characters to identify a path protection group or let this field empty. Upper and lower case, spaces and periods are allowed. Value must be included in quotes.

-
- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

-
- 5 The output parameters for this function are:

- `in_aid` – input access identifier
Specifies the tributary which is the source of the cross-connection.
- `out_aid` – output identifier
Specifies the tributary which is the sink of the cross-connection.
- `in_aid2` – input access identifier 2
This parameter is applicable to and is present for path-protected cross-connections only and specifies either the source of the protection leg or the source of the working leg.
- `rate` – equivalent to the input parameter “modifier”
Indicates the cross-connection rate.
- `loca` – location-a
Specifies the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and DROP connections only. The “loca” parameter value is an empty string for ADD and non-BLSR connections. A 2-way cross-connection is considered to be a DROP if the “out_aid” is a non BLSR tributary.
- `locastate` – squelch map data status for “location-a”
Indicates the validity and the source of the “loca” value.

- `locz` – location-z
specifies the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and ADD connections. The “locz” parameter value is an empty string for DROP and non-BLSR connections. A 2-way cross-connection is considered to be a ADD if the “in_aid” is a non BLSR tributary.
- `loczstate` – squelch map data status for “location-z”
Indicates the validity and the source of the “locz” value.
- `lpbkstat` – loopback-status
Specifies whether a cross-connection loopback exists on the input tributary or the output tributary of the cross-connection.
- `omode` – output mode
Specifies the output mode of the cross-connection.
- `repleg` – reported leg pair
Provides compact information about the leg(s) of cross-connections.
- `rtnomode` – return output mode
Specifies the output mode for the return direction of the cross-connection.
- `rtntaccstat` – return test access status
Indicates whether the input tributary of the return direction (destination-to-source) of a 2-way cross-connection is cross-connected or bridged to a test access tributary of a test session. In the case of a 1-way cross-connection the parameter shall be omitted.
- `rtnxcappl` – return cross-connection application
This parameter is a numeric value which indicates the application for which the return cross-connection is used in the context of compound cross-connection topologies.
- `rtnxnum` – return cross-connection number
This parameter is a multiple-digit number identifying the cross-connection number for the return direction (destination to source i.e. “out_aid” to “in_aid”) of a 2-way cross-connection.
- `taccstat` – test access status
Indicates whether the input tributary of a 1-way cross-connection or the input tributary of the source-to-destination direction of a 2-way cross-connection is crossconnected or bridged to a test access tributary of a test session.
- `xcappl` – cross-connection application
This parameter is a numeric value which indicates the application for which the cross-connection is used in the context of compound cross-connection topologies. The parameter is not further processed in the NE, but only stored (when establishing or modifying the cross-connection) and returned when retrieving the cross-connection.

- `xnum` – cross-connection number
This parameter is a multiple digit number, identifying each leg in a specific compound cross-connection.
- `xconcls` – cross-connection class
Identifies, whether the cross-connection has been setup in the TRADITIONAL way by an operator via the “ENT-CRS” command or via the NN application as part of an ENT-PATH command. This parameter therefore also indicates who is the owner of the cross-connection and can modify or delete it.

END OF STEPS



To view lower-order cross-connections

When to use

Use this task to view information on existing lower-order cross-connections in the NE.

Related information

For a more detailed explanation, please refer to the description of the RTRV-CRS-*{modifier}* command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For *{modifier}* select:

- **LOVT1.5, LOVC3, or LOVC12.**

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Retrieve Cross-connection Low Order {layer}**, where *{layer}*:
 - **VT1.5, VC-3, or VC-12**
5. Click **Go**.

Result: The **Retrieve Cross-connection Low Order {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

-
- 3** In the field **Input Access Identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.

Note: To view all cross-connections enter *1-1-#-#-all-all-all-all*.

-
- 4** Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

-
- 5** The output parameters for this function are:

- `in_aid` – input access identifier
Specifies the tributary which is the source of the cross-connection.
- `out_aid` – output identifier
Specifies the tributary which is the sink of the cross-connection.
- `in_aid2` – input access identifier 2
This parameter is applicable to and is present for path-protected cross-connections only and specifies either the source of the protection leg or the source of the working leg.
- `rate` – equivalent to the input parameter “modifier”
Indicates the cross-connection rate.
- `loca` – location-a
Specifies the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and DROP connections only. The “loca” parameter value is an empty string for ADD and non-BLSR connections. A 2-way cross-connection is considered to be a DROP if the “out_aid” is a non BLSR tributary.
- `locastate` – squelch map data status for “location-a”
Indicates the validity and the source of the “loca” value.
- `locz` – location-z
specifies the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and ADD connections. The “locz” parameter value is an empty string for DROP and non-BLSR connections. A 2-way cross-connection is considered to be a ADD if the “in_aid” is a non BLSR tributary.

- `loczstate` – squelch map data status for “location-z”
Indicates the validity and the source of the “locz” value.
- `lpbkstat` – loopback-status
Specifies whether a cross-connection loopback exists on the input tributary or the output tributary of the cross-connection.
- `omode` – output mode
Specifies the output mode of the cross-connection.
- `repleg` – reported leg pair
Provides compact information about the leg(s) of cross-connections.
- `rtnomode` – return output mode
Specifies the output mode for the return direction of the cross-connection.
- `rntaccstat` – return test access status
Indicates whether the input tributary of the return direction (destination-to-source) of a 2-way cross-connection is cross-connected or bridged to a test access tributary of a test session. In the case of a 1-way cross-connection the parameter shall be omitted.
- `rtnxcapp1` – return cross-connection application
This parameter is a numeric value which indicates the application for which the return cross-connection is used in the context of compound cross-connection topologies.
- `rtnxcnum` – return cross-connection number
This parameter is a multiple-digit number identifying the cross-connection number for the return direction (destination to source i.e. “out_aid” to “in_aid”) of a 2-way cross-connection.
- `taccstat` – test access status
Indicates whether the input tributary of a 1-way cross-connection or the input tributary of the source-to-destination direction of a 2-way cross-connection is crossconnected or bridged to a test access tributary of a test session.
- `xcapp1` – cross-connection application
This parameter is a numeric value which indicates the application for which the cross-connection is used in the context of compound cross-connection topologies. The parameter is not further processed in the NE, but only stored (when establishing or modifying the cross-connection) and returned when retrieving the cross-connection.
- `xnum` – cross-connection number
This parameter is a multiple digit number, identifying each leg in a specific compound cross-connection.
- `xconcls` – cross-connection class
Identifies, whether the cross-connection has been setup in the TRADITIONAL way by an operator via the “ENT-CRS” command or via the NN application as part of an ENT-PATH command. This parameter therefore also indicates who is the owner of the cross-connection and can modify or delete it.

END OF STEPS



To view higher-order cross-connections

When to use

Use this task to view information on existing higher-order cross-connections in the NE.

Related information

For a more detailed explanation, please refer to the description of the `RTRV-CRS-{modifier}` command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For `{modifier}` select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Retrieve Cross-connection {layer}**, where `{layer}`:
 - **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
 - **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**
 5. Click **Go**.

Result: The **Retrieve Cross-connection {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

-
- 3** Change the entries or selections for any modifiable fields that you wish to update.
- **Input Access Identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection. Note: To view all cross-connections enter *1-1-#-#-all-all-all*.
 - **Protection Group Name** – enter an alphanumeric user-defined string of up to 24 characters to identify a path protection group or let this field empty. Upper and lower case, spaces and periods are allowed. Value must be included in quotes.

-
- 4** Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

-
- 5** The output parameters for this function are:
- **in_aid** – input access identifier
Specifies the tributary which is the source of the cross-connection.
 - **out_aid** – output identifier
Specifies the tributary which is the sink of the cross-connection.
 - **in_aid2** – input access identifier 2
This parameter is applicable to and is present for path-protected cross-connections only and specifies either the source of the protection leg or the source of the working leg.
 - **rate** – equivalent to the input parameter “modifier”
Indicates the cross-connection rate.
 - **loca** – location-a
Specifies the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and DROP connections only. The “loca” parameter value is an empty string for ADD and non-BLSR connections. A 2-way cross-connection is considered to be a DROP if the “out_aid” is a non BLSR tributary.
 - **locastate** – squelch map data status for “location-a”
Indicates the validity and the source of the “loca” value.

- `locz` – location-z
specifies the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR THROUGH, INTER-BLSR and ADD connections. The “locz” parameter value is an empty string for DROP and non-BLSR connections. A 2-way cross-connection is considered to be a ADD if the “in_aid” is a non BLSR tributary.
- `loczstate` – squelch map data status for “location-z”
Indicates the validity and the source of the “locz” value.
- `lpbkstat` – loopback-status
Specifies whether a cross-connection loopback exists on the input tributary or the output tributary of the cross-connection.
- `omode` – output mode
Specifies the output mode of the cross-connection.
- `repleg` – reported leg pair
Provides compact information about the leg(s) of cross-connections.
- `rtnomode` – return output mode
Specifies the output mode for the return direction of the cross-connection.
- `rtntaccstat` – return test access status
Indicates indicates whether the input tributary of the return direction (destination-to-source) of a 2-way cross-connection is cross-connected or bridged to a test access tributary of a test session. In the case of a 1-way cross-connection the parameter shall be omitted.
- `rtnxcapp1` – return cross-connection application
This parameter is a numeric value which indicates the application for which the return cross-connection is used in the context of compound cross-connection topologies.
- `rtnxnum` – return cross-connection number
This parameter is a multiple-digit number identifying the cross-connection number for the return direction (destination to source i.e. “out_aid” to “in_aid”) of a 2-way cross-connection.
- `taccstat` – test access status
Indicates whether the input tributary of a 1-way cross-connection or the input tributary of the source-to-destination direction of a 2-way cross-connection is crossconnected or bridged to a test access tributary of a test session.
- `xcapp1` – cross-connection application
This parameter is a numeric value which indicates the application for which the cross-connection is used in the context of compound cross-connection topologies. The parameter is not further processed in the NE, but only stored (when establishing or modifying the cross-connection) and returned when retrieving the cross-connection.

- `xnum` – cross-connection number
This parameter is a multiple digit number, identifying each leg in a specific compound cross-connection.
- `xconcls` – cross-connection class
Identifies, whether the cross-connection has been setup in the TRADITIONAL way by an operator via the “ENT-CRS” command or via the NN application as part of an ENT-PATH command. This parameter therefore also indicates who is the owner of the cross-connection and can modify or delete it.

END OF STEPS



To add an uncorrelated lower-order cross-connection

When to use

Use this task to establish an uncorrelated lower-order cross-connection between tributaries in the NE.

Important! In the standard way of operation it is not necessary and not recommended to add cross-connections separately in the network elements. Lucent OMS creates the necessary cross-connections automatically with the implementation of network connections.

The “{modifier}” indicates the cross-connection “rate” of the tributary for which the command is applied to. There is no difference if the “rate” is specified as a SONET-rate or as SDH-rate for the establishment of the cross-connection.

Related information

For a more detailed explanation, please refer to the description of the ENT-CRS-`{modifier}` command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For `{modifier}` select:

- **LOVT1, LOVC3, or LOVC12.**

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Enter Cross-connection Low Order {layer}**,

where {layer}:

- **VT1.5, VC-3, or VC-12**

5. Click **Go**.

Result: The **Enter Cross-connection Low Order {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

3 Change the entries or selections for any of the fields that are modifiable:

- **Input port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
Note:
 - In case of a 1-way cross-connection, the source of a cross-connection is unambiguous. In this case the cross-connection will be retrieved by the RTRV-CRS, which has the identical “in_aid”.
 - In case of a 2-way cross-connection, the source is not defined (the source could be the “in_aid” or “out-aid” of the cross-connection). In this case both aids (“in_aid” or “out-aid”) of the cross-connection can be used as the “in_aid” parameter of the RTRV-CRS command.
- **Output port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the tributary which is the sink of the cross-connection.
- **Crossconnection topology** – select *1 way*, *2 way*, or *1 way path protected* to specify the topology of the cross-connection to be established.
- **Protection leg input port ID** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the protection leg. This parameter is applicable to path-protected cross-connections only.
- **Hold off timer (msec)** – enter either a value from 0 to 99 ms in 1 step increments or a value from 100 to 10000 ms in 100 step increments to specify the value of the hold-off timer for automatic protection switching. This parameter is applicable to path-protected cross-connections only and shall be omitted for non path-protected cross-connections.
- **Output mode** – select *Normal output*, *Unequipped signal*, or *AIS signal* to specify the output mode of the cross-connection.
- **Path protection group name** – enter an alphanumeric user-defined string of up to 24 characters to identify a path protection group. Upper and lower case, spaces and periods are allowed. Value must be included in quotes.
- **Revertive mode enable** – select either a single parameter *Enable*, or *Disable* to specify whether the path protection operates in revertive mode or non-revertive-mode. This parameter is applicable to path-protected cross-connections only and shall be omitted for non path-protected cross-connections.

- **Return output mode** – select *Normal output*, *Unequipped signal*, or *AIS signal*. This parameter is only applicable for 2-way cross-connections and is omitted for 1-way and path-protected cross-connections.
- **SNCP Type** – select *SNCI*, *SNCN*, or *Not applicable* to specify the SNCP mode, that means the switch criteria used for automatic protection switching. This parameter is mandatory for path-protected cross-connections and only applicable to them. The parameter shall be omitted for non path-protected cross-connections.
- **Wait to restore time (min)** – enter a value from 0 min. to 60 min. to specify the value of the wait-to-restore time for automatic protection switching. This parameter is applicable to path-protected cross-connections only and is omitted for non path-protected cross-connections.
- **Crossconnection application** – enter a numeric value from 0 to 255 to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
- **Crossconnection number** – enter a 12-digit numeric value to identify each leg in a specific compound cross-connection. Compound cross-connections are a composition of several atomic cross-connections in order to form complex scenarios.
- **Source node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). This parameter is required for BLSR. In addition the special character underscore (“_”) and the password characters are allowed.
- **Destination node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR. In addition the special character underscore (“_”) and the password characters are allowed.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To create a 1-Way conversion cross-connection

When to use

Use this procedure to provision a AU-3/AU-4 conversion cross-connection.

AU-3/AU-4 conversion cross-connections allow the conversion of a higher order STS-1 (SONET) to a lower order VC-3 (SDH), and the mapping into a higher order VC-4. From a cross-connection provisioning point of view, an AU-3/AU-4 conversion cross-connection is a cross-connection between a higher order STS-1 and a lower order VC-3 tributary. A conversion cross-connection has a higher order or AU3 side and a lower order or TU3 side.

Related information

For related information, see:

Traffic provisioning concepts

Traffic provisioning tasks

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.

Prerequisites

For configuring a 2 way or 1-WAY conversion cross-connections the following rules have to be considered:

- None of the related HO tributaries has been already cross-connected, (this includes. loopbacks, test access)
- None of the related LO tributaries as embedded in the used HO VC-4 Tributary has been already cross-connected with a cross connection other than a TU-3/AU-3 conversion cross-connection,
- No different manual sub-structuring has been established for the related HO VC-4 tributary
- The conversion cross-connection is type 2
- For LOXC 1

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:

- CIT software

Configuration rules

Important! Conversion cross-connections are only possible if a lower order cross-connection unit of type *LOXC40G2S/1* or *LOXC40G3S/1* is used and the LOXC interface standard is set to SDH.

The source or destination of a conversion cross-connection may *not* reside on one of the following types of port units:

- OPT2G5
- GE1
- GE10PL1

Instructions



CAUTION

Service-disruption hazard

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 From the CIT **System View** main menu select **Configuration** → **Cross-Connection** → **Create**.

Result: The **Create New Cross Connection** window appears.

- 2 Define the cross-connection rate in the drop-down list box **Rate:**. The following values (depending on the **System Interface Standard Default**) are possible:
 - **AU3TU3** for higher order STS-1 input to lower order VC-3 output
 - **TU3AU3** for lower order VC-3 input to higher order STS-1 output
-

- 3 Define the type of cross-connection by clicking on the respective radio button in the group box **XC Application**, select **1-Way Conversion Cross Connection**
-

- 4 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 display can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted. Ports are not selectable for lower order cross-connection rates, they can only be expanded.

- 5 Expand one port in the list and select one displayed tributary.

Additional info If a tributary is substructured, **Trib # (PTF)** is displayed.

Result: In the list box **Tributary** on the right, the AIDs of all lower order tributaries belonging to the respective port are displayed.

- 6 Select the lower order tributary which shall be used as the source and click on the **Select...** button.
-

- 7 Click on **Select...** to select the destination tributary.

Result: The **Ptn Grp** selection tab appears. In the list box of the **Ptn Grp** selection tab the system is displayed. The display can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted. Ports are not selectable for lower order cross-connection rates, they can only be expanded.

- 8 Expand one port in the list and select one displayed VC-4 tributary.

Result: In the list box **Tributary** on the right, the AIDs of all lower order tributaries belonging to the respective port are displayed.

- 9 Select the tributary which shall be used as the destination and click on the **Select...** button.

Result: 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.

- 10 The fields **XC Application**, **Source NE Name** and **Destination NE Name** display the previous decisions.
-

- 11 Select the **Output Mode**. 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.
-

- 12 Type a number for the cross-connection in the field **XC Number** or use the automatically generated one.
-

- 13 Click on the **OK** button to apply your settings.

Result: A confirmation window appears. If you are sure, .confirm

END OF STEPS



To create a 2-Way conversion cross-connection

When to use

Use this procedure to provision a 2-Way AU-3/AU-4 conversion cross-connection. AU-3/AU-4 conversion cross-connections allow the conversion of a higher order STS1 (SONET) signal or VC3 (SDH) signal to a lower order SDH VC3, and the mapping into a higher order VC4. From cross-connection provisioning point of view, an AU-3/AU-4 conversion cross-connection is a cross-connection between a higher order STS1 or VC3 tributary and a higher order VC3 tributary. A conversion cross-connection has a higher order or AU3 side and a lower order or TU3 side.

Related information

For related information, see:

- Traffic provisioning concepts
- Traffic provisioning tasks

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.

Prerequisites

For configuring a 2 way or 1-WAY HO-LO conversion cross-connections the following rules have to be considered:

- None of the related HO tributaries has been already cross-connected,(Incl. loop backs , test access)
- None of the related LO tributaries as embedded in the used HO VC4 Tributary has been already cross-connected with a cross connection other than a TU3 AU3 conversion cross-connection,
- No different manual sub-structuring has been established for the related HO VC4 Tributary
- The conversion cross-connection is type 2
- For LOXC 1

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:

- CIT

Configuration rules

Important! Conversion cross-connections are only possible if a lower order cross-connection unit of type *LOXC40G2S/1* or *LOXC40G3S/1* is used.

The source or destination of a conversion cross-connection may *not* reside on one of the following types of port units:

- OPT2G5
- GE1
- GE10PL1

Instructions**CAUTION****Service-disruption hazard**

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 From the CIT **System View** main menu select **Configuration** → **Cross-Connection** → **Create**.

Result: The **Create New Cross Connection** window appears.

- 2 Define the cross-connection rate in the drop-down list box **Rate:**. The following values (depending on the **System Interface Standard Default**) are possible:
 - **AU3TU3** for Higher order VC3/STS input to Lower Order VC3 output
 - **TU3AU3** for Lower order VC3 input to Higher Order VC3/STS1 output

-
- 3 Define the type of cross-connection by clicking on the respective radio button in the group box **XC Application**, select **2-Way Conversion Cross-Connection**.
-
- 4 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 display can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted. Ports are not selectable for LO XC rates, they can only be expanded.
-
- 5 Expand one port in the list and select one displayed tributary.
- Additional info** If a tributary is sub-structured, **Trib # (PTF)** is displayed.
- Result:** In the list box **Tributary** on the right, the AIDs of all tributaries belonging to the respective port are displayed.
-
- 6 Select the tributary which shall be used as the source and click on the **Select...** button.
-
- 7 Click on **Select...** to select the destination tributary.
- Result:** The **Ptn Grp** selection tab appears. In the list box of the **Ptn Grp** selection tab the system is displayed. The display can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted. Ports are not selectable for LO XC rates, they can only be expanded.
-
- 8 Select the tributary which shall be used as the destination and click on the **Select...** button.
- Result:** 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.
-
- 9 The fields **XC Application**, **Source NE Name** and **Destination NE Name** display the previous decisions.

.....
10 Select the **Output Mode**. 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.

.....
11 Type a number for the cross-connection in the field **XC Number** or use the automatically generated one.

.....
12 Click on the **OK** button to apply your settings.

Result: A confirmation window appears. If you are sure, confirm.

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



To add an uncorrelated higher-order cross-connection

When to use

Use this task to establish an uncorrelated higher-order cross-connection between tributaries in the NE.

Important! In the standard way of operation it is not necessary and not recommended to add cross-connections separately in the network elements. Lucent OMS creates the necessary cross-connections automatically with the implementation of network connections.

The “{modifier}” indicates the cross-connection “rate” of the tributary for which the command is applied to. There is no difference if the “rate” is specified as a SONET-rate or as SDH-rate for the establishment of the cross-connection.

Related information

For a more detailed explanation, please refer to the description of the ENT-CRS-{modifier} command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For {modifier} select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.
 - 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Enter Cross-connection {layer}**,
-

where {layer}:

- **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
- **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**

5. Click **Go**.

Result: The **Enter Cross-connection {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.

Note:

- In case of a 1-way cross-connection the source of a cross-connection is unambiguous. In this case the cross-connection will be retrieved by the RTRV-CRS, which has the identical “in_aid”.
- In case of a 2-way cross-connection the source is not defined (the source could be the “in_aid” or “out-aid” of the cross-connection). In this case both aids (“in_aid” or “out-aid”) of the cross-connection can be used as the “in_aid” parameter of the RTRV-CRS command.
- **Output port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the tributary which is the sink of the cross-connection.
- **Crossconnection topology** – select *1 way*, *2 way*, or *1 way path protected* to specify the topology of the cross-connection to be established.
- **Protection leg input port ID** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the protection leg. This parameter is applicable to path-protected cross-connections only.
- **Hold off timer (msec)** – enter either a value from *0* to *99* ms in 1 step increments or a value from *100* to *10000* ms in 100 step increments to specify the value of the hold-off timer for automatic protection switching. This parameter is applicable to path-protected cross-connections only and shall be omitted for non path-protected cross-connections.
- **Source node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). This parameter is required for BLSR. In addition the special character underscore (“_”) and the password characters are allowed.
- **Protection source node NE name** – enter a string of up to 20 characters to specify the TID associated with “in_aid2” of the protection leg of a path-protected cross-connection. In addition the special character underscore (“_”) and the password characters are allowed.

- **Destination node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR. In addition the special character underscore (“_”) and the password characters are allowed.
- **Output mode** – select *Normal output*, *Unequipped signal*, or *AIS signal* to specify the output mode of the cross-connection.
- **Path protection group name** – enter an alphanumeric user-defined string of up to 24 characters to identify a path protection group. Upper and lower case, spaces and periods are allowed. Value must be included in quotes.
- **Revertive mode enable** – select either a single parameter *Enable*, or *Disable* to specify whether the path protection operates in revertive mode or non-revertive-mode. This parameter is applicable to path-protected cross-connections only and shall be omitted for non path-protected cross-connections.
- **Return output mode** – select *Normal output*, *Unequipped signal*, or *AIS signal*. This parameter is only applicable for 2-way cross-connections and is omitted for 1-way and path-protected cross-connections.
- **SNCP Type** – select *SNCI*, *SNCN*, or *Not applicable* to specify the SNCP mode, that means the switch criteria used for automatic protection switching. This parameter is mandatory for path-protected cross-connections and only applicable to them. The parameter shall be omitted for non path-protected cross-connections.
- **Wait to restore time (min)** – enter a value from 0 min. to 60 min. to specify the value of the wait-to-restore time for automatic protection switching. This parameter is applicable to path-protected cross-connections only and is omitted for non path-protected cross-connections.
- **Crossconnection application** – enter a numeric value from 0 to 255 to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
- **Crossconnection number** – enter a 12-digit numeric value to identify each leg in a specific compound cross-connection. Compound cross-connections are a composition of several atomic cross-connections in order to form complex scenarios.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To modify a lower-order cross-connection's topology

When to use

Use this task to modify a lower-order cross-connection's topology between a 1-way point-to-point cross-connection and a path-protected cross-connection.

Important! In the standard way of operation it is not necessary and not recommended to modify cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the modification of network connections.

The "{modifier}" indicates the cross-connection "rate" of the tributary for which the command is applied to.

For a 1-way point-to-point to a path-protected conversion, the existing point-to-point cross-connection leg is converted into a single atomic path-protected cross-connection between the logical input AID of the existing point-to-point cross-connection, the specified protection logical input AID and logical output AID of the existing point-to-point cross-connection. The leg comprised of the AIDs of the existing point-to-point cross-connection shall be designated as the path protection group working leg at the time the cross-connection is converted.

If the command is applied to a 2-way cross-connection it will be split up automatically in two 1-way cross-connections. The command will be executed on the specified `in_aid` to `out_aid` direction, the reverse direction will remain unprotected. Refer also to chapter Detailed behaviour for more.

For a path-protected to a 1-way point-to-point conversion, it can be selected, which logical input AID of the existing legs (working leg or the protection leg) of the path-protected cross-connection shall stay as logical input AID of the created point-to-point cross-connection. This can be done by specifying the surviving leg of the existing path protection group as working leg at the time the cross-connection is converted.

Related information

For a more detailed explanation, please refer to the description of the `CNVT-CCT-{modifier}` command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For {modifier} select:

- **LOVT1, LOVC3, or LOVC12.**

**CAUTION****Service-disruption hazard**

Modification of a cross-connection may be traffic affecting.

Before starting to modify a cross-connection, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before modifying any of the cross-connections included in that path.

Task

-
- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.
-
- 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Convert Cross-connection Topology Low Order {layer}**,
where {layer}:
 - **VT1.5, VC-3, or VC-12**
 5. Click **Go**.

Result: The **Convert Cross-connection Topology Low Order {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter a low order *logical port identifier* or may copy the *logical port identifier* from the ports page to specify
 - 1-way Point-to-Point to a path-protected conversion, the source of the unprotected cross-connection.
 - respectively path-protected to a 1-way point-to-point conversion, the AID of the input leg which shall stay as source of the created unprotected cross-connection.
- **Output port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the sink of the cross-connection.
- **Protection leg input port ID** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the input leg for a path-protected to a 1-way Point-to-Point conversion which shall be dropped.
- **New cross connect topology** – select either a single parameter *1 way*, or *1 way path protected* to specify the new cross-connection topology.
- **Hold off timer (msec)** – enter a value from 0 to 99 ms in 1 step increments or a value from 100 to 10000 ms in 100 step increments to specify the “hold-off time” for automatic protection switching used by the protection state machine.
- **New input port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source aid of the new leg when converting from a point-to-point to a path-protected cross-connect.
- **New source node NE name** – enter a string of up to 20 characters to specify the new source TID if the “newinaid” is in a BLSR protection group. It specify that add node which is related to the protection leg input. “newloca” will be stored as the “loca2” parameter. In addition the special character underscore (‘_’) and the password characters are allowed.
- **Original cross connect topology** – select either a single parameter *1 way*, or *1 way path protected* to specify the original cross-connection topology.
- **Revertive mode enable** – select either a single parameter *Enable*, or *Disable* to specify whether revertive or non-revertive mode is used as operation mode of the protection group. The value “ENABLE” is used if the protection group operates in revertive mode. The value “DISABLE” is used if the protection group operates in non-revertive mode.

- **SNCP Type** – select either a single parameter *SNCI*, *SNCN*, or *Not applicable* to specify the type of the path protection w.r.t. switch criteria used by the protection state machine. The value *SNCI* (Inherent) is used if server signal fail is used as switch criteria. The value *SNCN* (Non-Intrusive) is used if server signal fail and defects supervised by a non-intrusive path monitor are used as switch criteria. The value “Not applicable” is used if one of the tributary inputs is related to a port operating in SONET mode.
 - **Wait to restore time (min)** – enter a value from (0 to 60) min to specify the wait to restore time used by the protection state machine operating in revertive mode.
 - **Crossconnection application** – enter a numeric value from (0 to 255) to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
 - **Crossconnection number** – enter a 12-digit numeric value to identify each leg in a specific compound cross-connection. Compound cross-connections are a composition of several atomic cross-connections in order to form complex scenarios.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To modify a higher-order cross-connection's topology

When to use

Use this task to modify a higher-order cross-connection's topology between a 1-way point-to-point cross-connection and a path-protected cross-connection.

Important! In the standard way of operation it is not necessary and not recommended to modify cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the modification of network connections.

The "{modifier}" indicates the cross-connection "rate" of the tributary for which the command is applied to.

For a 1-way point-to-point to a path-protected conversion, the existing point-to-point cross-connection leg is converted into a single atomic path-protected cross-connection between the logical input AID of the existing point-to-point cross-connection, the specified protection logical input AID and logical output AID of the existing point-to-point cross-connection. The leg comprised of the AIDs of the existing point-to-point cross-connection shall be designated as the path protection group working leg at the time the cross-connection is converted.

If the command is applied to a 2-way cross-connection it will be split up automatically in two 1-way cross-connections. The command will be executed on the specified `in_aid` to `out_aid` direction, the reverse direction will remain unprotected. Refer also to chapter Detailed behaviour for more.

For a path-protected to a 1-way point-to-point conversion, it can be selected, which logical input AID of the existing legs (working leg or the protection leg) of the path-protected cross-connection shall stay as logical input AID of the created point-to-point cross-connection. This can be done by specifying the surviving leg of the existing path protection group as working leg at the time the cross-connection is converted.

Related information

For a more detailed explanation, please refer to the description of the `CNVT-CCT-{modifier}` command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For {modifier} select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**

**CAUTION****Service-disruption hazard**

Modification of a cross-connection may be traffic affecting.

Before starting to modify a cross-connection, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before modifying any of the cross-connections included in that path.

Task

-
- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

 - 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Convert Cross-connection Topology {layer}**, where {layer}:
 - **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
 - **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**
 5. Click **Go**.

Result: The **Convert Cross-connection Topology {layer}** page is displayed. The respective {layer} page depends on the selection of the corresponding {layer} refer to item 4 of this step.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify
 - 1-way Point-to-Point to a path-protected conversion, the source of the unprotected cross-connection.
 - respectively path-protected to a 1-way point-to-point conversion, the AID of the input leg which shall stay as source of the created unprotected cross-connection.
- **Output port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the sink of the cross-connection.
- **Protection leg input port ID** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the input leg for a path-protected to a 1-way Point-to-Point conversion which shall be dropped.
- **New cross connect topology** – select either a single parameter *1 way*, or *1 way path protected* to specify the new cross-connection topology.
- **Hold off timer (msec)** – enter a value from 0 to 99 ms in 1 step increments or a value from 100 to 10000 ms in 100 step increments to specify the “hold-off time” for automatic protection switching used by the protection state machine.
- **New input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source aid of the new leg when converting from a point-to-point to a path-protected cross-connect.
- **New source node NE name** – enter a string of up to 20 characters to specify the new source TID if the “newinaid” is in a BLSR protection group. It specifies that add node which is related to the protection leg input. “newloca” will be stored as the “loca2” parameter. In addition the special character underscore (‘_’) and the password characters are allowed.
- **Original cross connect topology** – select either a single parameter *1 way*, or *1 way path protected* to specify the original cross-connection topology.
- **Path protection group name** – enter an alphanumeric user-defined string of up to 24 characters to identify a path protection group. Upper and lower case, spaces and periods are allowed. Value must be included in quotes.
- **Revertive mode enable** – select either a single parameter *Enable*, or *Disable* to specify whether revertive or non-revertive mode is used as operation mode of the protection group. The value “ENABLE” is used if the protection group operates in revertive mode. The value “DISABLE” is used if the protection group operates in non-revertive mode.

- **SNCP Type** – select either a single parameter *SNCI*, *SNCN*, or *Not applicable* to specify the type of the path protection w.r.t. switch criteria used by the protection state machine. The value *SNCI* (Inherent) is used if server signal fail is used as switch criteria. The value *SNCN* (Non-Intrusive) is used if server signal fail and defects supervised by a non-intrusive path monitor are used as switch criteria. The value “Not applicable” is used if one of the tributary inputs is related to a port operating in SONET mode.
 - **Wait to restore time (min)** – enter a value from (0 to 60) min to specify the wait to restore time used by the protection state machine operating in revertive mode.
 - **Crossconnection application** – enter a numeric value from (0 to 255) to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
 - **Crossconnection number** – enter a 12-digit numeric value to identify each leg in a specific compound cross-connection. Compound cross-connections are a composition of several atomic cross-connections in order to form complex scenarios.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To modify a cross-connection's parameters

When to use

Use this task to modify cross-connection parameters.

Important! In the standard way of operation it is not necessary and not recommended to modify cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the modification of network connections.

Related information

For a more detailed explanation, please refer to the description of the ED-CRS-`{modifier}` command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For lower-order cross-connections `{modifier}` select:

- **LOVT1, LOVC3, or LOVC12.**

For higher-order cross-connections`{modifier}` select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**



CAUTION

Service-disruption hazard

Modification of a cross-connection may be traffic affecting.

Before starting to modify a cross-connections parameters, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before modifying any of the cross-connections included in that path.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

-
- 2 Do the following:
1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select:
 - Edit Cross-connection Low Order {layer}**, where {layer}
 - **VT1.5, VC-3, or VC-12.**
 - Edit Cross-connection {layer}**, where {layer}
 - **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
 - **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**
 5. Click **Go**.

Result: The **Edit Cross-connection Low Order {layer}** page respective the **Edit Cross-connection {layer}** page depending on the selection of the corresponding {layer} of item 4 of this step is displayed.

-
- 3 Change the entries or selections for any modifiable fields that you wish to update.
- **Input port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
 - **Output port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the tributary which is the sink of the cross-connection.
 - **Source node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is added to the BLSR (bidirectional line-switched ring). In addition the special character underscore ('_') and the password characters are allowed.
 - **Destination node NE name** – enter a string of up to 20 characters to specify the TID of the node at which service is dropped from the BLSR (bidirectional line-switched ring). This parameter is required for BLSR. In addition the special character underscore ('_') and the password characters are allowed.
 - **Output mode** – select a single parameter *Normal output*, *Unequipped signal*, or *AIS signal* to specify the output mode of the cross-connection.

- **Crossconnection application** – enter a numeric value from (0 to 255) to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
 - **Crossconnection number** – enter a 12-digit numeric value to identify each leg in a specific compound cross-connection. Compound cross-connections are a composition of several atomic cross-connections in order to form complex scenarios.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To change a higher-order cross-connection from ONNS to traditional mode

When to use

Use this task to change a higher-order cross-connection from ONNS to traditional mode by setting the cross-connection *class* parameter to “TRADITIONAL”.

Important! In the standard way of operation it is not necessary and not recommended to change cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the change of network connections.

Related information

For a more detailed explanation, please refer to the description of the ED-NNCRS-*{modifier}* command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For *{modifier}* select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**



CAUTION

Service-disruption hazard

Modification of a cross-connection may be traffic affecting.

Before starting to change a cross-connections parameters, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before changing any of the cross-connections included in that path.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Edit NN Cross-connection {layer}**, where {layer}:
 - **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
 - **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**
5. Click **Go**.

Result: The **Edit NN Cross-connection {layer}** page depending on the selection of the corresponding {layer} of item 4 of this step is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
 - **Output port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the tributary which is the sink of the cross-connection.
 - **Cross connection class** – select *Traditional* to identify whether the cross-connection has been switched explicitly on the traditional way via an ENT-CRS command or implicitly via setting up an ONNS path.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To roll the input of a lower-order cross-connection from one tributary port to another

When to use

Use this task to roll the input of a cross-connection from a given tributary to another tributary while leaving the output unchanged.

Important! In the standard way of operation it is not necessary and not recommended to roll cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the roll modification of network connections.

The “{modifier}” indicates the cross-connection “rate” of the tributary for which the command is applied to. There is no difference if the “rate” is specified as a SONET-rate or as SDH-rate for the deleting of the old and establishing of the new cross-connection.

Related information

For a more detailed explanation, please refer to the description of the ENT-ROLL-*{modifier}* command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For {modifier} select:

- **LOVT1**,
- **LOVC3**, or
- **LOVC12**.
- **TU3AU3**
for Lower order VC3 input to Higher Order VC3/STS1 output
Only applicable in the moment for SONET - SDH conversion.



CAUTION

Service-disruption hazard

Rolling of a cross-connection may be traffic affecting.

Before starting to roll a cross-connection, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before rolling any of the cross-connections included in that path.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Enter Roll Low Order {layer}**, where {layer}:

- **VT1.5, VC-3, or VC-12**
- **TU3AU3**

for Lower order VC3 input to Higher Order VC3/STS1 output
Only applicable in the moment for SONET - SDH conversion.

5. Click **Go**.

Result: The **Enter Roll Low Order {layer}** page depending on the selection of the corresponding {layer} of item 4 of this step is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
- **Output port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the sink of the cross-connection.
- **New input port identifier** – enter a low order *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the new cross-connection to be established
- **New source node NE name** – enter a string of up to 20 characters to specify the new source TID if the “newinaid” is in a BLSR protection group. In addition the special character underscore (‘_’) and the password characters are allowed.

- **Crossconnection application** – enter a numeric value from (0 to 255) to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
 - **Crossconnection number** – enter a 12-digit numeric value to identify each cross-connection leg in a specific compound cross-connection. topology. This parameter is optional – if not entered, the default is used.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To roll the input of a higher-order cross-connection from one tributary port to another

When to use

Use this task to roll the input of a cross-connection from a given tributary to another tributary while leaving the output unchanged.

Important! In the standard way of operation it is not necessary and not recommended to roll cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the roll modification of network connections.

The “{modifier}” indicates the cross-connection “rate” of the tributary for which the command is applied to. There is no difference if the “rate” is specified as a SONET-rate or as SDH-rate for the deleting of the old and establishing of the new cross-connection.

Related information

For a more detailed explanation, please refer to the description of the ENT-ROLL-{modifier} command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For {modifier} select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**
- **AU3TU3**
for Higher order VC3/STS input to Lower Order VC3 output Only applicable in the moment for SONET - SDH conversio



CAUTION

Service-disruption hazard

Rolling of a cross-connection may be traffic affecting.

Before starting to roll a cross-connection, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before rolling any of the cross-connections included in that path.

Task

-
- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

 - 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
 4. In the **Function** field, select **Enter Roll {layer}**, where {layer}:
 - **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
 - **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**
 - **AU3TU3**
for Higher order VC3/STS input to Lower Order VC3 output Only applicable in the moment for SONET - SDH conversio
 5. Click **Go**.

Result: The **Enter Roll {layer}** page depending on the selection of the correponding {layer} of item 4 of this step is displayed.

 - 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **Input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
 - **Output port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the sink of the cross-connection.
 - **New input port identifier** – enter a *logical port identifier* or copy the *logical port identifier* from the **Ports** page to specify the source of the new cross-connection to be established
 - **New source Node NE name** – enter a string of up to 20 characters to specify the new source TID if the “newinaid” is in a BLSR protection group. In addition the special character underscore (‘_’) and the password characters are allowed.
-

- **New path protection group name** – enter an alphanumeric user-defined string of up to 24 characters to specify the name of the new path protection group. This parameter is applicable if a leg of a path-protected cross-connection is rolled – the parameter in this case is optional and if not entered the default is used. For non path-protected cross-connection this parameter does not apply and is omitted.
 - **Crossconnection application** – enter a numeric value from (0 to 255) to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.
 - **Crossconnection number** – enter a 12-digit numeric value to identify each cross-connection leg in a specific compound cross-connection. topology. This parameter is optional – if not entered, the default is used.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To delete a cross-connection

When to use

Use this task to delete a cross-connection in the NE.

Important! In the standard way of operation it is not necessary and not recommended to delete cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the deletion of network connections.

The “{modifier}” indicates the cross-connection “rate” of the tributary for which the command is applied to. There is no difference if the “rate” is specified as a SONET rate or as an SDH-rate for the deletion of the cross-connection

Related information

For a more detailed explanation, please refer to the description of the DEL-CRS-{modifier} command in the LambdaUnite® *MSS Operations System Engineering Guide*.

For lower-order cross-connections {modifier} select:

- **LOVT1, LOVC3, or LOVC12.**

For higher-order cross-connections {modifier} select:

- **STS1, STS12, STS192, STS3, or STS48,**
- **VC3, VC4, VC416C, VC44C, or VC464C.**



CAUTION

Service-disruption hazard

Deletion of a cross-connection may be traffic affecting.

Before starting to delete a cross-connections parameters, ensure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before deleting any of the cross-connections included in that path.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select:

Delete Cross-connection Low Order {layer}, where {layer}

- **VT1.5, VC-3, or VC-12.**

Delete Cross-connection {layer}, where {layer}

- **STS-1, STS-12c, STS-192c, STS-3c, or STS-48c,**
- **VC-3, VC-4, VC-4-16c, VC-4-4c, or VC-4-64c.**

5. Click **Go**.

Result: The **Delete Cross-connection Low Order {layer}** page respective the **Delete Cross-connection {layer}** page depending on the selection of the corresponding {layer} of item 4 of this step is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Input port identifier** – enter either a low order *logical port identifier* or only a *logical port identifier* or copy the respective *logical port identifier* from the **Ports** page to specify the source of the cross-connection.
- **Output port identifier** – enter either a low order *logical port identifier* or only a *logical port identifier* or copy the respective *logical port identifier* from the **Ports** page to specify the tributary which is the sink of the cross-connection.

- **Crossconnection topology** – select either a single parameter *1 way*, *2 way*, or *1 way path protected* to specify the topology of the cross-connection to be established.
 - **Protection leg input port ID** – enter either a low order *logical port identifier* or only a *logical port identifier* or copy the respective *logical port identifier* from the **Ports** page to specify the source of the protection leg. This parameter is applicable to path protected cross-connections only.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



To retrieve ONNS to UPSR/SNCP constructs

When to use

Use this task to retrieve ONNS to UPSR/SNCP constructs.

Related information

For a more detailed explanation, please refer to the description of the RTRV-0UC command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Retrieve ONNS to UPSR/SNCP Constructs**,
5. Click **Go**.

Result: The **Retrieve ONNS to UPSR/SNCP Constructs** is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Working port identifier** – enter a *port identifier* or copy the *port identifier* from the **Ports** page to specify the working tributary of the OUC.
 - **OUC directionality** – enter either a single parameter *Bidirectional*, *Unidirectional add*, or *Unidirectional drop* to specify the directionality of the OUC.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

- 5 The output parameters for this function are:
- wrk_aid – working tributary access identifier
Specifies the working tributary of the OUC.
 - prt_aid – protection tributary access identifier
Specifies the protection tributary of the OUC.
 - ouc_dir – OUC directionality
Specifies the directionality of the OUC.

END OF STEPS



To add an ONNS to UPSR/SNCP construct

When to use

Use this task to add an ONNS to UPSR/SNCP construct.

Important! In the standard way of operation it is not necessary and not recommended to add cross-connections separately in the network elements. Lucent OMS creates the necessary cross-connections automatically with the implementation of network connections.

Related information

For a more detailed explanation, please refer to the description of the ENT-0UC command in the LambdaUnite® *MSS Operations System Engineering Guide*.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.

2 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of the target NE (if not already present).
3. In the **Category** field, select **Cross-connections**.
4. In the **Function** field, select **Enter ONNS to UPSR/SNCP Constructs**,
5. Click **Go**.

Result: The **Enter ONNS to UPSR/SNCP Constructs** page is displayed.

3 Change the entries or selections for any modifiable fields that you wish to update.

- **Working port identifier** – enter a *port identifier* or copy the *port identifier* from the **Ports** page to specify the working tributary of the OUC.
- **Protection port identifier** – enter a *port identifier* or copy the *port identifier* from the **Ports** page to specify the protection tributary of the OUC.

- **OUC directionality** – select *Bidirectional*, *Unidirectional add*, or *Unidirectional drop* to specify the directionality of the OUC.
- **Hold off timer (msec)** – enter either a numeric value from 0 ms to 99 ms in 1 ms step increments or a value from 100 to 10000 ms in 100 ms step increments to specify the value of the hold-off timer to specify the hold-off time for automatic protection switching used by the protection state machine of the path protection groups created via OUC creation.
- **Revertive mode enable** – select *Enable* or *Disable* to specify whether revertive or non-revertive mode is used as operation mode of the protection groups created via OUC creation. “Enable” is used if the protection operates in revertive mode, “Disable” is used if the protection operates in non-revertive mode.
- **SNCP Type** – select *SNCI*, *SNCN*, or *Not applicable* to specify the type of the path protection related to switch criteria used by the protection state machine of the path protection groups created via OUC creation.
- **Wait to restore time (min)** – enter a numeric value from 0 min. to 60 min. to specify wait-to-restore time used by the protection state machine operating in revertive mode of the path protection groups created via OUC creation.
- **Crossconnection application** – enter a numeric value from 0 to 255 to indicate the application for which the cross-connection is used in the context of compound cross-connection topologies.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element’s response to the submitted function.

END OF STEPS



To delete an ONNS to UPSR/SNCP construct

When to use

Use this task to delete an ONNS to UPSR/SCCP construct.

Important! In the standard way of operation it is not necessary and not recommended to delete cross-connections separately in the network elements. Lucent OMS deletes the cross-connections automatically with the deletion of network connections.

Related information

For a more detailed explanation, please refer to the description of the DEL-0UC command in the LambdaUnite® *MSS Operations System Engineering Guide*.



CAUTION

Service-disruption hazard

Deletion of a cross-connection may be traffic affecting.

Before starting to delete a cross-connection, make sure that it is not in use. The traffic provided on the respective path must have previously been removed (for example rerouted to another path) before deleting any of the cross-connections included in that path.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **NE Management Functions**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Session** → **NE Management Functions**.

Result: The **NE Management Functions** page is displayed.
 - 2 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of the target NE (if not already present).
 3. In the **Category** field, select **Cross-connections**.
-

4. In the **Function** field, select **Delete ONNS to UPSR/SNCP Constructs**,
5. Click **Go**.

Result: The **Delete ONNS to UPSR/SNCP Constructs** is displayed.

- 3 Change the entries or selections for any modifiable fields that you wish to update.
 - **Working port identifier** – enter a *port identifier* or copy the *port identifier* from the **Ports** page to specify the working tributary of the OUC.
 - **OUC directionality** – enter a single parameter *Bidirectional*, *Unidirectional add*, or *Unidirectional dropp* to specify the directionality of the OUC to be deleted.
-

- 4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **NE Management Functions** page. The bottom panel of the **NE Management Functions** page now shows the network element's response to the submitted function.

END OF STEPS



Provisioning of path protection groups (SNCP, UPSR)

To view a list of path protection groups (SNCP, UPSR)

When to use

Use this task to view a list of path protection groups.

LambdaUnite[®] MSS supports both, SONET and SDH path protection features:

- SDH: *subnetwork connection protection (SNCP)*
- SONET: *unidirectional path-switched ring (UPSR)*

Lucent OMS displays the settings and options for one network type at a time. To switch between the SDH flavor and the SONET flavor of the user interface, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **SNCP** or **UPSR**, respectively.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of path protection groups in the NE that meet your search criteria.

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



To modify a path protection group (SNCP, UPSR)

When to use

Use this task to modify a path protection group.

LambdaUnite[®] MSS supports both, SONET and SDH path protection features:

- SDH: *subnetwork connection protection (SNCP)*
- SONET: *unidirectional path-switched ring (UPSR)*

Lucent OMS displays the settings and options for one network type at a time. To switch between the SDH flavor and the SONET flavor of the user interface, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **SNCP** or **UPSR**, respectively.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the path protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Protection group general information** page is displayed.

- 4 Change the entries or selections for any modifiable fields that you wish to update.
- **Path protection group name** – enter a text string with 1 to 24 characters to specify the path protection group name. This parameter is only used with VC-4 applications.
 - **Wait to restore time (Minute)** – enter a value from 0 min. to 60 min. in 1 min. increments to specify the wait-to-restore time used in the revertive mode. If the revertive mode is set to “Disabled”, this field is not available.
 - **Revertive mode** – select **Enabled** or **Disabled**.
 - **Holdoff timer (Milli.Sec)** – enter a value to specify the hold-off time for automatic protection switching used by the protection state machine.
 - VC-12, LO-VC-3, VT1.5: from 0 to 100 ms in 25 ms increments, or from 100 to 10000 ms in 100 ms increments
 - HO-VC-3, VC-4, STS- : from 0 to 100 ms in 1 ms increments, or from 100 to 10000 ms in 100 ms increments
 - **SNCP protection type** – select **SNCP**, **SNCP**, or **Not Applicable** to specify the type of the path protection.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the SNCP protection group is modified.

END OF STEPS



To operate a path protection group switch (SNCP, UPSR)

When to use

Use this task to operate a path protection group switch.

LambdaUnite[®] MSS supports both, SONET and SDH path protection features:

- SDH: *subnetwork connection protection (SNCP)*
- SONET: *unidirectional path-switched ring (UPSR)*

Lucent OMS displays the settings and options for one network type at a time. To switch between the SDH flavor and the SONET flavor of the user interface, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **SNCP** or **UPSR**, respectively.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of path protection groups in the NE that meet your search criteria.

3 Click the radio button next to the path protection group you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Operate Protection Switch** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

From the **Switch Operation** menu, select the switch command you wish to execute: *Manual switch...*, *Forced switch...*, *Lockout*, or *Clear*.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the protection switch is executed.

END OF STEPS



To operate an SNCP VC-4 protection group switch on constituent members

When to use

Use this task to view and/or operate an subnetwork connection protection (SNCP) VC-4 protection group switch on constituent members (manual to working).

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **SNCP**.
 5. In the **Rate** field, select **VC-4**, **VC-4-4c**, **VC-4-16c**, or **VC-4-64c**.
 6. Click **Search**.
Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

- 3 Click the radio button next to the SNCP VC-4 protection group you wish to view and/or execute a protection switch. From the **Go** menu, select **View/Operate Protection Switch On Constituent Members** and click **Go**.

Result: The **Constituent Member Protection Groups** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

Click the radio button next to the constituent member protection group you wish execute a protection switch. From the **Go** menu, select the desired switch command *Manual switch...*, *Forced switch...*, *Lockout*, or *Clear* and click **Go**.

Result: A confirmation window is displayed asking you to confirm the protection switch.

5 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Constituent Member Protection Groups** page, and the constituent member protection group switch is executed.

END OF STEPS



Provisioning of MSP protection groups

To view a list of 1+1 or 1x1 MSP protection groups

When to use

Use this task to view a list of 1+1 or 1x1 multiplex section protection (MSP) protection groups.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 MSP** or **1x1 MSP**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 1+1 MSP protection group

When to use

Use this task to add a 1+1 multiplex section protection (MSP) protection group in an NE. To prepare a fully functional protected multiplex section, a matching MSP protection group has to be established in the NE on the opposite end of the multiplex section as well. After the MSP protection groups have been set up on both sides, the protected multiplex section can be added as a network connection.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **1+1 MSP**.
4. In the **Rate** field, select **STM-1**, **STM-4**, **STM-16**, or **STM-64**. When the rate has been selected, the panel **Protection group parameters** opens.
5. In the **Protection group name** field, enter a number between *001* and *999*.
6. In the **Working** field, select a working port AID. If not selectable, this parameter is unavailable. If the APS protocol (item 8) is set to “Optimized”, the field name changes to **Primary**.

7. In the **Protection** field, select a protection port AID. If not selectable, this parameter is unavailable. If the APS protocol (item 8) is set to “Optimized”, the field name changes to **Secondary**.
 8. In the **APS protocol** field, select **Bidirectional**, **Unidirectional**, or **Optimized**.
 9. In the **Revertive mode** field, select **Enabled** or **Disabled**. If the APS protocol (item 8) is set to “Optimized”, this field is unavailable.
 10. In the **Wait to restore time** field, select a value from 0 to 60 min. in 1 step increments to specify the wait-to-restore time used in the revertive mode. If the Wait to restore time (item 9) is “Disabled”, this field is unavailable.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the MSP protection group is added.

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



To add a 1x1 MSP protection group

When to use

Use this task to add a 1x1 multiplex section protection (MSP) protection group in an NE. To prepare a fully functional protected multiplex section, a matching MSP protection group has to be established in the NE on the opposite end of the multiplex section as well. After the MSP protection groups have been set up on both sides, the protected multiplex section can be added as a network connection.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **1x1 MSP**.
4. In the **Rate** field, select **STM-1**, **STM-4**, **STM-16**, or **STM-64**. When the rate has been selected, the panel **Protection group parameters** opens.
5. In the **Protection group name** field, enter a number between *001* and *999*.
6. In the **Working** field, select a working port AID. If not selectable, this parameter is unavailable.

7. In the **Protection** field, select a protection port AID. If not selectable, this parameter is unavailable.
 8. In the **APS protocol** field, leave the default selection (**Bidirectional**) unchanged.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the MSP protection group is added.

END OF STEPS

.....



To modify a 1+1 or 1x1 MSP protection group

When to use

Use this task to modify a 1+1 or 1x1 multiplex section protection (MSP) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 MSP** or **1x1 MSP**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the MSP protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

- 4 Change the entries or selections for any modifiable fields that you wish to update.
- **Wait to restore time (Minute)** – select a value from 0 to 60 min. in 1 step increments to specify the wait-to-restore time used in the revertive mode. If the Revertive mode field selection is “Disabled”, this field is unavailable.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a pre-defined alarm severity assignment profile (ASAP) to be used for the protection group in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **DCC line/MS protection mode** – select **Enabled** or **Disabled** to specify whether the line/MS DCC channel is switched as part of the line/MS protection group.
 - **DCC section/RS protection mode** – select **Enabled** or **Disabled** to specify whether the section/RS DCC channel is switched as part of the line/MS protection group.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the MSP protection group is modified.

END OF STEPS



To delete a 1+1 or 1x1 MSP protection group

When to use

Use this task to delete a 1+1 or 1x1 multiplex section protection (MSP) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 MSP** or **1x1 MSP**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the MSP protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

.....

4 Click Yes.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the protection group is deleted.

END OF STEPS

.....



To operate an MSP protection switch

When to use

Use this task to execute a multiplex section protection (MSP) protection switch.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **1+1 MSP** or **1x1 MSP**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.
Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

- 3 Click the radio button next to the MSP protection group for which you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

From the **Switch Operation** menu, select the switch command you wish to execute (*Manual switch...*, *Forced switch...*, *Lockout*, or *Clear*).

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the MSP protection switch is executed.

END OF STEPS



Provisioning of APS protection groups

To view a list of 1+1 or 1x1 APS protection groups

When to use

Use this task to view a list of 1+1 or 1x1 automatic protection switch (APS) protection groups.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 APS** or **1x1 APS**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 1+1 APS protection group

When to use

Use this task to add a 1+1 automatic protection switch (APS) protection group in an NE. To prepare a fully functional protected multiplex section, a matching APS protection group has to be established in the NE on the opposite end of the multiplex section as well. After the APS protection groups have been set up on both sides, the protected multiplex section can be added as a network connection.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path: **Network Elements** → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

 - 2 Click on the **New** tool in the toolbar.
Result: The **Add Protection Group** page is displayed.

 - 3 Do the following:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group type** field, select **1+1 APS**.
 4. In the **Rate** field, select **OC-3**, **OC-12**, **OC-48**, or **OC-192**. When the rate has been selected, the panel **Protection group parameters** opens.
 5. In the **Protection group name** field, enter a number between *001* and *999*.
 6. In the **Working** field, select a working port AID. If not selectable, this parameter is unavailable. If the APS protocol (item 8) is set to “Optimized”, the field name changes to **Primary**.
-

7. In the **Protection** field, select a protection port AID. If not selectable, this parameter is unavailable. If the APS protocol (item 8) is set to “Optimized”, the field name changes to **Secondary**.
8. In the **APS protocol** field, select **Bidirectional**, **Unidirectional**, or **Optimized**.
9. In the **Revertive mode** field, select **Enabled** or **Disabled**. If the APS protocol (item 8) is set to “Optimized”, this field is unavailable.
10. In the **Wait to restore time** field, select a value from 0 to 60 min. in 1 step increments to specify the wait-to-restore time used in the revertive mode. If the Wait to restore time (item 9) is “Disabled”, this field is unavailable.

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the APS protection group is added.

END OF STEPS



To add a 1x1 APS protection group

When to use

Use this task to add a 1x1 automatic protection switch (APS) protection group in an NE. To prepare a fully functional protected multiplex section, a matching APS protection group has to be established in the NE on the opposite end of the multiplex section as well. After the APS protection groups have been set up on both sides, the protected multiplex section can be added as a network connection.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **1x1 APS**.
4. In the **Rate** field, select **OC-3**, **OC-12**, **OC-48**, or **OC-192**. When the rate has been selected, the panel **Protection group parameters** opens.
5. In the **Protection group name** field, enter a number between *001* and *999*.
6. In the **Working** field, select the working port AID. If not selectable, this parameter is unavailable.

7. In the **Protection** field, select a protection port AID. If not selectable, this parameter is unavailable.
 8. In the **APS protocol** field, leave the default selection (**Bidirectional**) unchanged.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the APS protection group is added.

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



To modify a 1+1 or 1x1 APS protection group

When to use

Use this task to modify a 1+1 or 1x1 automatic protection switch (APS) protection group.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 APS** or **1x1 APS**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the APS protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

- 4 Change the entries or selections for any modifiable fields that you wish to update.
 - **Wait to restore time (Minute)** – select a value from 0 to 60 min. in 1 step increments to specify the wait-to-restore time used in the revertive mode. If the Revertive mode field selection is “Disabled”, this field is unavailable.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a pre-defined alarm severity assignment profile (ASAP) to be used for the “protection group” in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **DCC line/MS protection mode** – select **Enabled** or **Disabled** to specify whether the line/MS DCC channel is switched as part of the line/MS protection group.
 - **DCC section/RS protection mode** – select **Enabled** or **Disabled** to specify whether the section/RS DCC channel is switched as part of the line/MS protection group.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the APS protection group is modified.

END OF STEPS



To delete a 1+1 or 1x1 APS protection group

When to use

Use this task to delete a 1+1 or 1x1 automatic protection switch (APS) protection group.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **1+1 APS** or **1x1 APS**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the APS protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

4 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the protection group is deleted.

END OF STEPS



To operate an APS protection switch

When to use

Use this task to execute an automatic protection switch (APS) protection group switch.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **1+1 APS** or **1x1 APS**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the APS protection group for which you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

From the **Switch Operation** menu, select the switch command you wish to execute (*Manual switch...*, *Forced switch...*, *Lockout*, or *Clear*).

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the APS protection switch is executed.

END OF STEPS



Provisioning of MS-SPRing protection groups

To view a list of 2-fiber MS-SPRing protection groups

When to use

Use this task to view a list of 2-fiber multiplex section-shared protection ring (MS-SPRing) protection groups.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 2-fiber MS-SPRing protection group

When to use

Use this task to add a 2-fiber multiplex section-shared protection ring (MS-SPRing) protection group in an NE.

A requirement for this kind of protection is an enabled MS DCC on both line sides in each NE. To prepare a fully functional 2-fiber multiplex section-shared protection ring, a matching MS-SPRing protection group has to be established in all NEs of the ring configuration. After the MS-SPRing protection groups have been set up on all NEs, the management system automatically add the ring without any user intervention when certain conditions are met. When the ring is automatically added, the ring is added to the database, and the Network Map is updated with the new ring.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **2F MSSPRING**.
4. In the **Rate** field, select **STM-16** or **STM-64**. When the rate has been selected, the **Protection group parameters** panel opens.

5. In the **Protection group name** field, enter a number between *001* and *999*.
 6. In the **Ring ID** field, enter up to 15 alphanumeric and/or special characters (for example “~{Ring25}”).
 7. In the **East** field, select the east port AID. If not selectable, this parameter is unavailable.
 8. In the **West** field, select the west port AID. If not selectable, this parameter is unavailable.
 9. In the **Auto ring discovery** field, select **Enabled** or **Disabled**.
 10. In the **Automatic squelch map calculation** field, select **Enabled** or **Disabled**.
 11. In the **Ring circuit alarm mode** field, select **Enabled** or **Disabled**.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the 2-fiber MS-SPRing protection group is added.

END OF STEPS

.....



To modify a 2-fiber MS-SPRing protection group

When to use

Use this task to modify a 2-fiber multiplex section-shared protection ring (MS-SPRing) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the MS-SPRing protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

- 4 Change the entries or selections for any of the fields that are modifiable:
- **Ring ID** – enter a text string with 1 to 15 characters to specify the ring ID.
 - **Wait to restore time (Minute)** – select a value from 0 to 12 min. in 1 step increments or 99 (infinite) to specify the wait-to-restore time for ring switches in revertive mode.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a pre-defined alarm severity assignment profile (ASAP) to be used for the protection group in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **Auto ring discovery** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic ring discovery algorithm will assign nodeID values to each node in the ring and construct the necessary ring map information. All nodes in the ring must be Alcatel-Lucent network elements. If disabled, the user will assign the Node ID value manually.
 - **Automatic squelch map calculation** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic squelch map calculation is switched on. If disabled, the function is switched off.
 - **Ring circuit alarm mode** – select **Enabled** or **Disabled** to enable or disable ring circuit alarms for the local 2-fiber MS-SPRing protection group.
-

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the 2-fiber MS-SPRing protection group is modified.

END OF STEPS



To delete a 2-fiber MS-SPRing protection group

When to use

Use this task to delete a 2-fiber multiplex section-shared protection ring (MS-SPRing) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the MS-SPRing protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

4 Click Yes.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the MS-SPRing protection group is deleted.

END OF STEPS



To operate a 2-fiber MS-SPRing protection switch

When to use

Use this task to execute a 2-fiber multiplex section-shared protection ring (MS-SPRing) protection switch (manual to working).

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

-
- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

 - 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **2F MSSPRING**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.
Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

 - 3 Click the radio button next to the MS-SPRing protection group for which you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4

**CAUTION****Service-disruption hazard**

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.

Change the entries or selections for any modifiable fields that you wish to update.

- **Switch type** – select *Span* or *Ring* to specify what type of protection switching is used for the MS-SPRing protection group.
- **Destination side** – select **East** or **West** to specify the destination ring side to which the switch command is to be applied.
- **Switch operation** – select the switch command you wish to execute. Depending on the selection of the **Switch type** the following values are possible:
 - for switch type “Span”: *Lockout* or *Clear*.
 - for switch type “Ring”: *Forced*, *Manual*, or *Clear*.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the 2-fiber MS-SPRing protection switch is executed.

END OF STEPS



To view a list of 4-fiber MS-SPRing protection groups

When to use

Use this task to view a list of 4-fiber multiplex section-shared protection ring (MS-SPRing) protection groups.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **4F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 4-fiber MS-SPRing protection group

When to use

Use this task to add a 4-fiber multiplex section-shared protection ring (MS-SPRing) protection group in an NE.

A requirement for this kind of protection is an enabled MS DCC on both line sides in each NE. To prepare a fully functional 2-fiber multiplex section-shared protection ring, a matching MS-SPRing protection group has to be established in all NEs of the ring configuration. After the MS-SPRing protection groups have been set up on all NEs, the management system automatically add the ring without any user intervention when certain conditions are met. When the ring is automatically added, the ring is added to the database, and the Network Map is updated with the new ring.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **4F MSSPRING**.
4. In the **Rate** field, select **STM-16**, or **STM-64**. When the rate has been selected, the **Protection group parameters** panel opens.

5. In the **Protection group name** field, enter a number between *001* to *999*.
 6. In the **Ring ID** field, enter up to 15 alphanumeric and special characters (for example “~{Ring25}”).
 7. In the **East working** field, select the east port AID. If not selectable, this parameter is unavailable.
 8. In the **East protection** field, select the east port AID for protection group. If not selectable, this parameter is unavailable.
 9. In the **West** field, select the west port AID. If not selectable, this parameter is unavailable.
 10. In the **West protection** field, select the west port AID for protection group. If not selectable, this parameter is unavailable.
 11. In the **Ring protection protocol** field the following selections depending on the Rate selection (item 4) are possible:
 - for rate type “STM-16”: **Standard**, or **Transoceanic**
 - for rate type “STM-64”: **Standard**, **Transoceanic-shortened**, or **Transoceanic-TOPEX**
 12. In the **Auto ring discovery** field, select **Enabled** or **Disabled**.
 13. In the **Automatic squelch map calculation** field, select **Enabled** or **Disabled**.
 14. In the **Ring circuit alarm mode** field, select **Enabled** or **Disabled**.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the 4-fiber MS-SPRing protection group is added.

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



To modify a 4-fiber MS-SPRing protection group

When to use

Use this task to modify a 4-fiber multiplex section-shared protection ring (MS-SPRing) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **4F MSSPRING**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.
Result: The **Protection groups** page is populated with a list of protection groups in the NE that meet your search criteria.

- 3 Click the radio button next to the MS-SPRing protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

- 4 Change the entries or selections for any modifiable fields that you wish to update.
 - In the **Ring protection protocol** field the following selections depending on the Rate selection are possible:
 - for rate type “STM-16”: **Standard**, or **Transoceanic**
 - for rate type “STM-64”: **Standard**, **Transoceanic-shortened**, or **Transoceanic-TOPEX**
 - **New Ring ID** – enter a text string with 1 to 15 characters to specify the new ring identification name.
 - **Wait to restore time (Minute)** – select a value from 0 to 12 min. in 1 step increments or 99 (infinite) to specify the wait-to-restore time for ring switches in revertive mode.
 - **Auto ring discovery** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic ring discovery algorithm will assign nodeID values to each node in the ring and construct the necessary ring map information. All nodes in the ring must be Alcatel-Lucent network elements. If disabled, the user will assign the Node ID value manually.
 - **Automatic squelch map calculation** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic squelch map calculation is switched on. If disabled, the function is switched off.
 - **Ring circuit alarm mode** – select **Enabled** or **Disabled** to enable or disable ring circuit alarms for the local 4-fiber MS-SPRing protection group.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a pre-defined alarm severity assignment profile (ASAP) to be used for the “protection group” in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **Span wait to restore** – select a value 0 to 12 min. in 1 step increments or 99 (infinite) to specify the wait to restore time for span switches used by the protection state machine operating in revertive mode.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the 4-fiber MS-SPRing protection group is modified.

END OF STEPS



To delete a 4-fiber MS-SPRing protection group

When to use

Use this task to delete a 4-fiber multiplex section-shared protection ring (MS-SPRing) protection group.

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **4F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the MS-SPRing protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

4 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the MS-SPRing protection group is deleted.

END OF STEPS



To operate a 4-fiber MS-SPRing protection switch

When to use

Use this task to execute a 4-fiber multiplex section-shared protection ring (MS-SPRing) protection switch (manual to working).

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **4F MSSPRING**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the MS-SPRing protection group you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

Change the entries or selections for any modifiable fields that you wish to update.

- **Switch type** – select *Span* or *Ring* to specify what type of protection switching is used for the MS-SPRing protection group.
- **Destination side** – click the radio button **East** or **West** to specify the destination ring side to which the switch command is to be applied.
- **Switch operation** – select the switch command you wish to execute. Depending on the selection of the **Switch type** the following values are possible:
 - for switch type “Span”: *Forced, Manual, Lockout, or Clear.*
 - for switch type “Ring”: *Forced, Manual, or Clear.*

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the MS-SPRing protection switch is executed.

END OF STEPS



Provisioning of BLSR protection groups

To view a list of 2-fiber BLSR protection groups

When to use

Use this task to view a list of 2-fiber bidirectional line switched ring (BLSR) protection groups.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 2-fiber BLSR protection group

When to use

Use this task to add a 2-fiber bidirectional line switched ring (BLSR) protection group in an NE.

A requirement for this kind of protection is an enabled MS DCC on both line sides in each NE. To prepare a fully functional 2-fiber bidirectional line switched ring, a matching BLSR protection group has to be established in all NEs of the ring configuration. After the BLSR protection groups have been set up on all NEs, the management system automatically add the ring without any user intervention when certain conditions are met. When the ring is automatically added, the ring is added to the database, and the Network Map is updated with the new ring.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **2F BLSR**.
4. In the **Rate** field, select **OC-48** or **OC-192**. When the rate has been selected, the **Protection group parameters** panel opens.

5. In the **Protection group name** field, enter a number between *001* and *999*.
 6. In the **Ring ID** field, enter up to 15 alphanumeric and/or special characters (for example “~{Ring25}”).
 7. In the **East** field, select the east port AID. If not selectable, this parameter is unavailable.
 8. In the **West** field, select the west port AID. If not selectable, this parameter is unavailable.
 9. In the **Auto ring discovery** field, select **Enabled** or **Disabled**.
 10. In the **Automatic squelch map calculation** field, select **Enabled** or **Disabled**.
 11. In the **Ring circuit alarm mode** field, select **Enabled** or **Disabled**.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the BLSR protection group is added.

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



To modify a 2-fiber BLSR protection group

When to use

Use this task to modify a 2-fiber bidirectional line switched ring (BLSR) protection group.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the BLSR protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

- 4 Change the entries or selections for any modifiable fields that you wish to update.
- **Ring ID** – enter a text string with 1 to 15 characters to specify the ring ID.
 - **Wait to restore time (Minute)** – select a value from 0 min. to 12 min. in 1 min. step increments or 99 (infinite) to specify the wait-to-restore time for ring switches in revertive mode.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a predefined alarm severity assignment profile (ASAP) to be used for the protection group in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **Auto ring discovery** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic ring discovery algorithm will assign node ID values to each node in the ring and construct the necessary ring map information. All nodes in the ring must be Alcatel-Lucent network elements. If disabled, the user will assign the node ID value manually.
 - **Automatic squelch map calculation** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic squelch map calculation is switched on. If disabled, the function is switched off.
 - **Ring circuit alarm mode** – select **Enabled** or **Disabled** to enable or disable ring circuit alarms for the local 2-fiber MS-SPRing protection group.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the 2-fiber BLSR protection group is modified.

END OF STEPS



To delete a 2-fiber BLSR protection group

When to use

Use this task to delete a 2-fiber bidirectional line switched ring (BLSR) protection group.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the BLSR protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

.....

4 Click Yes.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the BLSR protection group is deleted.

END OF STEPS

.....



To operate a 2-fiber BLSR protection switch

When to use

Use this task to execute a 2-fiber bidirectional line switched ring (BLSR) protection switch (manual to working).

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **2F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the BLSR protection group you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4

**CAUTION****Service-disruption hazard**

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.

Change the entries or selections for any modifiable fields that you wish to update.

- **Switch type** – select *Span* or *Ring* to specify the type of protection switching used for the BLSR protection group.
- **Destination side** – click the radio button **East** or **West** to specify the destination ring side to which the switch command shall be applied.
- **Switch operation** – select the switch command you wish to execute. Depending on the selection of the **Switch type** the following values are possible:
 - for switch type “Span”: *Lockout* or *Clear*.
 - for switch type “Ring”: *Forced*, *Manual*, or *Clear*.

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the BLSR protection switch is executed.

END OF STEPS



To view a list of 4-fiber BLSR protection groups

When to use

Use this task to view a list of 4-fiber bidirectional line switched ring (BLSR) protection groups.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **4F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

END OF STEPS



To add a 4-fiber BLSR protection group

When to use

Use this task to add a 4-fiber bidirectional line switched ring (BLSR) protection group in an NE.

A requirement for this kind of protection is an enabled MS DCC on both line sides in each NE. To prepare a fully functional 4-fiber bidirectional line switched ring, a matching BLSR protection group has to be established in all NEs of the ring configuration. After the BLSR protection groups have been set up on all NEs, the management system automatically add the ring without any user intervention when certain conditions are met. When the ring is automatically added, the ring is added to the database, and the Network Map is updated with the new ring.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path: **Network Elements** → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Click on the **New** tool in the toolbar.

Result: The **Add Protection Group** page is displayed.

3 Do the following:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group type** field, select **4F BLSR**.
4. In the **Rate** field, select **OC-48**, or **OC-192**. When the rate has been selected, the **Protection group parameters** panel opens.

5. In the **Protection group name** field, enter a number between *001* to *999*.
 6. In the **Ring ID** field, enter up to 15 alphanumeric and special characters (for example “~{Ring25}”).
 7. In the **East working** field, select the east port AID. If not selectable, this parameter is unavailable.
 8. In the **East protection** field, select the east port AID for protection group. If not selectable, this parameter is unavailable.
 9. In the **West working** field, select the west port AID. If not selectable, this parameter is unavailable.
 10. In the **West protection** field, select the west port AID for protection group. If not selectable, this parameter is unavailable.
 11. In the **Ring protection protocol** field the following selections depending on the Rate selection (item 4) are possible:
 - for rate type “OC-48”: **Standard**, or **Transoceanic**
 - for rate type “OC-192”: **Standard**, **Transoceanic-shortened**, or **Transoceanic-TOPEX**
 12. In the **Auto ring discovery** field, select **Enabled** or **Disabled**.
 13. In the **Automatic squelch map calculation** field, select **Enabled** or **Disabled**.
 14. In the **Ring circuit alarm mode** field, select **Enabled** or **Disabled**.
-

4 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add Protection Group** page, and the BLSR protection group is added.

END OF STEPS



To modify a 4-fiber BLSR protection group

When to use

Use this task to modify a 4-fiber bidirectional line switched ring (BLSR) protection group.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.
Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **4F BLSR**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.
Result: The **Protection groups** page is populated with a list of protection groups in the NE that meet your search criteria.

- 3 Click the radio button next to the BLSR protection group you wish to modify. From the **Go** menu, select **Modify protection group** and click **Go**.

Result: The **Modify Protection Group** page is displayed.

-
- 4 Change the entries or selections for any modifiable fields that you wish to update.
- In the **Ring protection protocol** field the following selections depending on the Rate selection are possible:
 - for rate type “OC-48”: **Standard**, or **Transoceanic**.
 - for rate type “OC-192”: **Standard**, **Transoceanic-shortened**, or **Transoceanic-TOPEX**.
 - **New Ring ID** – enter a text string with 1 to 15 characters to specify the new ring identification name.
 - **Wait to restore time (Minute)** – select a value from 0 to 12 min. in 1 step increments or 99 (infinite) to specify the wait-to-restore time for ring switches in revertive mode.
 - **Auto ring discovery** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic ring discovery algorithm will assign nodeID values to each node in the ring and construct the necessary ring map information. All nodes in the ring must be Alcatel-Lucent network elements. If disabled, the user will assign the Node ID value manually.
 - **Automatic squelch map calculation** – select **Enabled** or **Disabled**. If this parameter is enabled, the automatic squelch map calculation is switched on. If disabled, the function is switched off.
 - **Ring circuit alarm mode** – select **Enabled** or **Disabled** to enable or disable ring circuit alarms for the local 2-fiber MS-SPRing protection group.
 - **Alarm severity assignment profile** – enter a string with 1 to 24 characters to specify a pre-defined alarm severity assignment profile (ASAP) to be used for the protection group in question. An ASAP is a list of alarms which can occur in a network element and which each have an alarm severity assigned.
 - **Span wait to restore** – select a value from 0 to 12 min. in 1 step increments or 99 (infinite) to specify the wait-to-restore time for span switches in revertive mode.

-
- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Modify Protection Group** page, and the 4-fiber BLSR protection group is modified.

END OF STEPS



To delete a 4-fiber BLSR protection group

When to use

Use this task to delete a 4-fiber bidirectional line switched ring (BLSR) protection group.

Before you begin

Make sure that the SONET flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

- 1 Do one of the following:
 - Use the object links to follow this path:
Network Elements → **Protection Groups**.
 - On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

- 2 Complete the following steps to specify the criteria for your search:
 1. In the **NE type** field, select a type of NE (if not already present).
 2. In the **NE name** field, select the name of a target NE (if not already present).
 3. In the **Protection group name** field, type the protection group name (optional).
 4. In the **Protection group type** field, select **4F BLSR**.
 5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
 6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3



CAUTION

Service-disruption hazard

Deletion of a protection could cause a traffic interruption.

Click the radio button next to the BLSR protection group you wish to delete. From the **Go** menu, select **Delete protection group** and click **Go**.

Result: A confirmation window is displayed asking you to confirm the deletion.

4 Click **Yes**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Groups** page, and the BLSR protection group is deleted.

END OF STEPS



To operate a 4-fiber BLSR protection switch

When to use

Use this task to execute a 4-fiber bidirectional line switched ring (BLSR) protection switch (manual to working).

Before you begin

Make sure that the SDH flavor of the management system user interface is active. To change the setting, use the respective options in **My Preferences** → **Preferences** → **Application Preferences** → **Terminology**.

Task

1 Do one of the following:

- Use the object links to follow this path:
Network Elements → **Protection Groups**.
- On the Network Map, right-click the NE upon which you wish to execute a management function. From the **Node** menu, select **Network Element** → **Protection Groups**.

Result: The **Protection Groups** page is displayed.

2 Complete the following steps to specify the criteria for your search:

1. In the **NE type** field, select a type of NE (if not already present).
2. In the **NE name** field, select the name of a target NE (if not already present).
3. In the **Protection group name** field, type the protection group name (optional).
4. In the **Protection group type** field, select **4F BLSR**.
5. In the **Rate** field, select the port rate (optional). The default selection is **All**.
6. Click **Search**.

Result: The **Protection Groups** page is populated with a list of protection groups in the NE that meet your search criteria.

3 Click the radio button next to the BLSR protection group you wish to execute a protection switch. From the **Go** menu, select **Operate protection switch** and click **Go**.

Result: The **Protection Switch** page is displayed.

4  **CAUTION**
Service-disruption hazard

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.

Change the entries or selections for any modifiable fields that you wish to update.

- **Switch type** – select *Span* or *Ring* to specify what type of protection switching is used for the BLSR protection group.
- **Destination side** – click the radio button **East** or **West** to specify the destination ring side to which the switch command shall be applied.
- **Switch operation** – select the switch command you wish to execute. Depending on the selection of the **Switch type** the following values are possible:
 - for switch type “Span”: *Forced, Manual, Lockout, or Clear.*
 - for switch type “Ring”: *Forced, Manual, or Clear.*

5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Protection Switch** page, and the BLSR protection switch is executed.

END OF STEPS



12 Software and NE database management concepts

Overview

Purpose

This chapter presents concept information related to software update on *LambdaUnite*[®] MSS network elements using Lucent OMS.

Contents

Functionality description	12-2
Software upgrade	12-5



Functionality description

Types of NE software

The management system is able to manage the software of NEs in the network.

There are two types of NE software:

- Applications, such as NE generics
- Data files, such as NE database versions. These contain the configuration data of the NE. It is commonly known as *management information base (MIB)* or as a *backup*.

To manage NE software

The management system allows you to manage software in the following ways:

- Manage NE generics on the management system
- Manage NE generics on the NE
- Manage NE database on the management system
- Manage NE database on the NE

In addition, the management system is able to perform tasks associated with software management on a scheduled basis. The tasks can be scheduled to run as a one-time activity to be started on a specific day and time or as a periodic activity to be started on a recurring day and time.

Manage NE generics on the management system

Software management for NE generics on the management system includes the ability to add an NE generic to the management system from a local removable media, delete an NE generic from the management system, transfer an NE generic from the management system to an NE, support file management capabilities for the NE generics files from the management system, view in-progress NE generic transfers, and abort in-progress NE generic transfers.

Maximum number of NE generics stored on the management system

The maximum number of NE generics able to be stored on the management system is six.

Manage NE software generics on NEs

The management system displays the software generics and the attributes that are present on the NEs. Additionally, the user can transfer a software generic from the management system to an NE, transfer a software generic from NE to NE, activate a software generic on an NE, abort an in-progress software transfer, commit an NE generic and revert to the inactive NE generic.

An upgrade of an NE generic occurs in the following steps:

1. “To add an NE generic to the management system” (p. 13-4)
2. “To transfer an NE generic from the management system to an NE” (p. 13-6)
3. “To activate an NE generic on an NE” (p. 13-17)
4. “To commit an NE generic on an NE” (p. 13-20)
5. “To revert an NE generic on an NE” (p. 13-22)

An NE generic can be added to the management system file system from CD-ROM. For file transfer from CD-ROM, the user simply physically loads the CD-ROM because the management system can automatically mount the CD-ROM file system. It is also possible to use other commonly available tools and applications to get software files into the management system file system (for example, use file transfer software, such as FTP, to transfer software to the management system over a network).

The management system can store a maximum of six NE generic releases per NE type. When the maximum is reached, one release must be deleted before another can be added. The management system does not automatically overwrite the oldest one.

Activate NE generics

This feature allows the user to retrieve the release number of the NE generic that is active on the NE, retrieve the release number of the NE generic on the NE that is the standby (that is, the NE generic that resides in the inactive partition of the NE), and activate the standby NE generic.

Available functions are:

- **Activate: Standard** – the generic is activated immediately.
- **Activate: Trial** – the generic is activated for a trial phase. It is possible to revert back to the previous generic together with the restoration of the last matching database.
When the trial phase is finished successfully, the generic can be committed. Otherwise it is possible to revert it.

Manage NE database on the management system

An NE database file is a binary image of the complete memory of the NE. Copies of the NE database file can be backed up onto the management system and used to perform NE restoration.

NE database backup can be performed on-demand or per a schedule. The **Scheduled Tasks** page is used to schedule backups. A default of up to three backup files can be saved on the management system per NE. When this limit is reached, the oldest file is overwritten. For smaller networks, it is possible to have more than three backup files. See your Lucent representative for more information.

The management system displays the view of NE database stored on the management system. The user can view the software memory files and their attributes. The user can also perform other software management tasks such as create an NE database backup on the management system, and restore NE database from a management system backup.

Manage NE database on the NE

The management system displays the view of NE database stored on an NE. It allows the user to view the NE software memory files and their attributes. It also allows the user to perform other software management tasks, such as create an NE database backup on the management system, abort in progress NE database transfer, activate NE database and restore NE database from a management system backup.

Scheduling software management tasks

The management system allows searching for and scheduling the following software management tasks:

- NE database backup
- Transfer NE generic from management system to NE
- Transfer NE generic from NE to NE
- Activate NE generic
- Activate NE database
- Activate: NE generic and memory



Software upgrade

Introduction

The NE software is stored on the controller unit of the NE. To upgrade this software the new software must be downloaded on the NE. This can be done from the management system.

System controller software

The main unit 1 contains the software to control and support the NE. The *manufacturers executable code (MEC)* file contains the complete software package for one NE. The software in the main unit 1 is also used to provide a basic configuration to the units connected to the main unit 1. These other assigned units obtain the appropriate part of the software package from the main unit 1 during the system start-up or when a unit is inserted.

The main unit 2 (if present) is synchronized (image database only) to main unit 1. If a provisioning database is present on the main unit 1 card this database will be dropped immediately after insertion/recovery.

Two memory stores

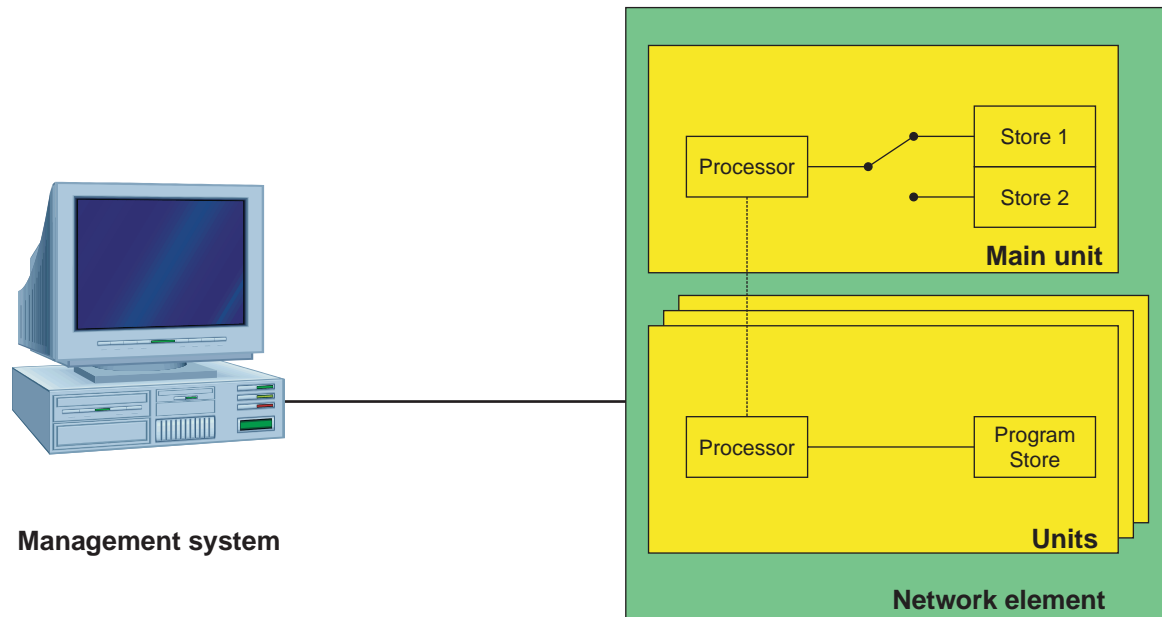
On the main unit 1 there are two memory stores that can contain each a different MEC. The store with the software that is executed is called the active store and the other store is called the backup store. In case of a software upgrade, the management system downloads a complete software package to the backup store of the main unit 1.

Switch stores

With a switch command from the management system, the software in the backup store can be made active. The switch command switches between the two stores, thus the active store becomes the backup store and vice versa.

Diagram

The use of software stores is shown in the following figure:



Commit the software

After confirmation of a switch command between the active and backup store, the management system loses its association with the NE for approximately 10 minutes. If the management system can renew the association with the NE the active store is committed. If the active store is not committed within two hours after the switch, the NE will switch back to the old software load.

□

13 Software and NE database management tasks

Overview

Purpose

This chapter informs about how to perform the most common tasks related to software management.

Contents

Tasks related to NE generics	13-3
To view a list of NE generics stored on the management system	13-3
To add an NE generic to the management system	13-4
To delete an NE generic from the management system	13-5
To transfer an NE generic from the management system to an NE	13-6
To schedule the transfer of an NE generic from the management system to an NE	13-8
To view a list of in-progress transfers of NE generics	13-11
To abort an in-progress NE generic transfer	13-12
To view a list of NE generics stored on an NE	13-15
To activate an NE generic on an NE	13-17
To commit an NE generic on an NE	13-20
To revert an NE generic on an NE	13-22
To schedule NE generic activation	13-24
Tasks related to NE databases	13-28
To view a list of NE database versions stored on the management system	13-28
To view a list of NE database versions stored on an NE	13-31
To back up NE database versions onto the management system	13-32

To schedule the backup of an NE database version onto the management system	13-37
To restore an NE database version from the management system to an NE	13-39



Tasks related to NE generics

To view a list of NE generics stored on the management system

When to use

Use this task to view a list of NE generics stored on the management system.

Task

1 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

2 In the **Software type** field, select **NE generic**.

3 In the **Software stored on** field, select **Management system**.

4 In the **NE type** field, select a type of NE or select **All**.

5 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

END OF STEPS



To add an NE generic to the management system

When to use

Use this task to add an NE generic to the management system.

Task

-
- 1 Insert the CD-ROM that contains the NE generic into the CD-ROM drive of the server.
-

2

Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 3 In the **Software operation** field, select *Add NE generic to management system* and click **Go**.

Result: The **Add NE Generic to Management System** page is displayed.

- 4 In the **NE type** field, select a type of NE.
-

- 5 Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Add NE Generic to Management System** page, and the NE generic is added to the management system. The management system logs this activity in the **User Activity Log**. The CD-ROM is unmounted automatically, and the user can push the “Eject” button to retrieve the CD-ROM from the drive.

END OF STEPS



To delete an NE generic from the management system

When to use

Use this task to delete an NE generic from the management system.

Task

- 1 Use the object links to follow this path:
 - **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 2 In the **Software type** field, select **NE generic**.
- 3 In the **Software stored on** field, select **Management system**.
- 4 In the **NE type** field, select a type of NE or select **All**.
- 5 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

- 6 Click the radio button next to the NE generic that you wish to delete. From the **Go** menu, select **Delete NE generic from management system** and click **Go**.

Result: A confirmation window is displayed.

- 7 Confirm that you want to proceed with the deletion.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Software** page, and the software is deleted from the management system. The management system logs this activity in the **User Activity Log**.

END OF STEPS



To transfer an NE generic from the management system to an NE

When to use

Use this task to transfer an NE generic from the management system to an NE.

Important! The transfer of an NE generic from the management system to an NE is a lengthy process that may take up to a few hours to complete.

Before you begin

Because each type of NE has individual requirements (hardware and software) and the order in which certain steps must be performed is particular to the NE, the documentation for the NEs should be consulted for software installation and upgrade procedures.

Task

- 1 In the top navigation bar select **My network** → **Job updates**.
Result: The **Job Updates** page is displayed. The **Background Task Status** section of this page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:
 - **Network Elements** → **Software****Result:** The **Search** section of the **Software** page is displayed.

- 3 In the **Software type** field, select **NE generic**.

- 4 In the **Software stored on** field, select **Management system**.

- 5 In the **NE type** field, select a type of NE or select **All**.

- 6 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

- 7 Click the radio button next to the NE generic that you wish to transfer. From the **Go** menu, select **Download from management system to NE** and click **Go**.

Result: The **Download from management system to NE** page is displayed.

- 8 Select the NE to which the NE generic will be transferred.
-

- 9 When downloading the NE Generic to the inactive partition the following questions will be displayed:

- **Reload if file being transferred is the same as the current inactive release?**
Select **No** if you do *not* want to transfer the NE Generic to any NE where the inactive release of the NE is the same as the NE generic being downloaded, else **Yes**.
 - **Reload if file being transferred is the same as the current active release?**
Select **No** if you do *not* want to transfer the NE generic to any NE where the active release of the NE is the same as the NE generic being downloaded, else **Yes**.
 - **Reload if file being transferred is older than the current active release?**
Select **No** if you do *not* want to transfer the NE generic to any NE where the active release of the NE is older than the NE generic being downloaded, else **Yes**.
-

- 10 Click **Submit**.

Result: A confirmation window is displayed asking you to confirm the transfer of the NE generic.

- 11 Click **Yes**.

Result: The system initiates the software transfer from the management system to the NE. The management system notes the progress of the operation in the **Background Task Status** section of the **Job Updates** page, and logs this activity in the **User Activity Log**.

END OF STEPS



To schedule the transfer of an NE generic from the management system to an NE

When to use

Use this task to schedule the transfer of an NE generic from the management system to an NE.

Task

-
- 1 Use the object links to follow this path:
 - **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

 - 2 In the **Software type** field, select **NE generic**.
 - 3 In the **Software stored on** field, select **Management system**.
 - 4 In the **NE type** field, select a type of NE or select **All**.
 - 5 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

 - 6 Click the radio button next to the NE generic to which you want to schedule the software transfer. From the **Go** menu, select **Schedule download from management system to NE** and click **Go**.

Result: The **Schedule download from management system to NE** page is displayed. It is prepopulated with read-only information about the selected NE generic and, depending on the NE type. Additional fields may be displayed to provide further selections.

 - 7 From the preselected **NE list**, select the **Available** NE to which the NE generic will be transferred.

When downloading the NE Generic to the inactive partition, the following questions will be displayed:

- **Reload if file being transferred is the same as the current inactive release?**
Select **No** if you do *not* want to transfer the NE generic to any NE where the inactive release of the NE is the same as the NE generic being downloaded, else **Yes**.
- **Reload if file being transferred is the same as the current active release?**
Select **No** if you do *not* want to transfer the NE generic to any NE where the active release of the NE is the same as the NE generic being downloaded, else **Yes**.
- **Reload if file being transferred is the older than the current active release?**
Select **No** if you do *not* want to transfer the NE generic to any NE where the active release of the NE is older than the NE generic being downloaded, else **Yes**.
- Click **Schedule**.

Result: The **Schedule download from management system to NE** page is displayed. It is prepopulated with read-only information in the **Task type** and the task-specific window. Additional fields in the **Schedule options** window may be displayed to provide further selections.

-
- 8 To schedule the frequency, click the calendar icon after the **Scheduled Date** field.

Result: A **Date/Time Chooser** window is displayed. Select the scheduled start date.

-
- 9 In the **Schedule options** panel change the entries or selections for any modifiable fields that you wish to update:

- In the **Scheduled time** field, enter the time in the format “hh:mm:ss”. The time entered applies for both the start and end date
- In the **Scheduled task name** field, enter a user defined name for the scheduled task or allow the system to generate a default value. Note: The scheduled task name cannot be modified once the task is created.
- In the **Number of retries** field, select the number of times (1 to 4) the scheduled task will be retried in case of error or *no retries*.
- In the **Execution Interval** field, select the number of hours this task should be performed from the drop down list. Possible values are from 1 hour to 12 hours and *Continuous*.
- In the **Retry interval** field, select the interval of time that will pass between retries. Possible values are 1 min. to 60 min.

-
- 10 Click **Submit**.

Result: The scheduled task is added.

END OF STEPS

Reference

For detailed information about how to view a list of scheduled tasks, how to modify scheduled tasks, and how to delete scheduled tasks, refer to *Lucent OMS Network Element Management Guide – Tools – Scheduled Tasks*.



To view a list of in-progress transfers of NE generics

When to use

Use this task to view a list of in-progress transfers of NE generics.

Task

1 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

2 In the **Software type** field, select **NE generic**.

3 In the **Software stored on** field, select **Management system**.

4 In the **NE type** field, select a type of NE or select **All**.

5 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

6 Click the radio button next to any entry in the list. From the **Go** menu, select **View in progress NE generic transfers** and click **Go**.

Result: The **Software** page is displayed, and includes a list of NE generic transfers that are in-progress and met the search criteria in the previous step.

END OF STEPS



To abort an in-progress NE generic transfer

When to use

Use this task to abort an in progress NE generic transfer. Both management system to NE and NE to NE transfers can be aborted.

There are three methods for this task.

Task, method 1: from the In-Progress NE Generic Transfers page

- 1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 3 In the **Software type** field, select **NE generic**.
-

- 4 In the **Software stored on** field, select **Management system**.
-

- 5 In the **NE type** field, select a type of NE or select **All**.
-

- 6 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the management system that meet your search criteria.

- 7 Click the radio button next to any entry in the list. From the **Go** menu, select **View in progress NE generic transfers** and click **Go**.

Result: The **Software** page is displayed, and includes a list of NE generic transfers that are in-progress and met the search criteria in the previous step.

- 8 Click the radio button next to the transfer you wish to halt. From the **Go** menu, select **Abort NE generic transfer** and click **Go**.
-

Result: The **Abort NE generic transfer** window opens.

9 Click **Submit**.

Result: A confirmation window is displayed asking you to confirm the halt of the NE generic transfer.

10 Click **OK**.

Result: The selected NE generic transfer is halted.

The management system notes the progress of two tasks in the **Job Updates** page. The original transfer task is marked as *failed*, and the abort task is marked as *success*. The management system logs these activities in the **User Activity Log**.

END OF STEPS

Task, method 2: from the list of NE generics stored on an NE

1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

3 In the **Software type** field, select **NE generic**.

4 In the **Software stored on** field, select **NE**.

5 In the **NE type** field, select a type of NE.

6 Do one of the following:

- In the **NE Name** field, select the name of NE in question.
- In the **NE Name** field, select **All** and populate the field **NE Generic** with the respective version number.

Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

-
- 7 Click the radio button next to the transfer you wish to halt. From the **Go** menu, select **Abort NE generic transfer** and click **Go**.

Result: The **Abort NE generic transfer** window opens.

-
- 8 Click **Submit**.

Result: A confirmation window is displayed asking you to confirm the halt of the NE generic transfer.

-
- 9 Click **OK**.

Result: The selected NE generic transfer is halted.

The management system notes the progress of two tasks in the **Job Updates** page. The original transfer task is marked as *failed*, and the abort task is marked as *success*. The management system logs these activities in the **User Activity Log**.

END OF STEPS



To view a list of NE generics stored on an NE

When to use

Use this task to view a list of NE generics stored on an NE.

Task

-
- 1 Use the object links to follow this path:
 - **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

 - 2 In the **Software type** field, select **NE generic**.

 - 3 In the **Software stored on** field, select **NE**.

 - 4 In the **NE type** field, select a type of NE.

 - 5 Do one of the following:
 - In the **NE Name** field, select the name of NE in question.
 - - In the **NE Name** field, select **All**.
 - In the field **NE generic partition**, select either **Active** or **Inactive**.
 - In the field **NE generic type**, select **Release number**, if you want to specify the release number (for example “5.0.1”) or **Item code**, if you want to specify the item code (for example “SCA358”) of the NE generic in question.
 - Populate the field **NE Generic** with the respective version number. The **NE generic** label is a hyperlink to the **NE Generic Selection** page from which to select the NE generic to include in the search criteria. As an alternative, type in an NE generic name in the text box.

Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

END OF STEPS



To activate an NE generic on an NE

When to use

Use this task to activate an NE generic on an NE.

Task

- 1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 3 In the **Software type** field, select **NE generic**.
-

- 4 In the **Software stored on** field, select **NE**.
-

- 5 In the **NE type** field, select a type of NE.
-

- 6 Do one of the following:

- In the **NE Name** field, select the name of NE in question.
- In the **NE Name** and the **NE generic partition** fields, select **All**.

If you want to specify, select:

- In the field **NE generic partition** either **Active** or **Inactive**.
- In the field **NE generic type** the **Release number** (for example “5.0.1”) or the **Item code** (for example “SCA358”) of the NE generic in question.

Populate the field **NE Generic** with the respective version number. The **NE Generic** label is a hyperlink to the **NE Generic Selection** page from which to select the NE generic to include in the search criteria. As an alternative, type in an NE generic name in the text box.

Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

-
- 7 Click the radio button next to the NE for which you wish to activate the inactive NE generic.

From the **Go** menu, select **Activate** and click **Go**.

Result: The **Activate NE generic** page is displayed. In that page, most of the fields are pre-populated according to your previous selections.

-
- 8 Change the entries or selections for any modifiable fields that you wish to update.

- **Activation type** – select *Standard* if you want to perform a normal activation, or *Trial* if the *LambdaUnite*[®] MSS is to be used. Using the option *Trial*, it is possible to revert back to the previous generic together with the restoration of the last matching database.
- **Activation order** – select **System default** to use the default rules for establishing the order of NEs within the grouping, or select **User defined** to place the NE in the queue using the order defined in the **Selected NE** list.
- **Activate NEs** – select one of the following radio buttons to determine if the NEs in a grouping can exit the management system queue as long as resources are available or if an activation of an NE in the grouping can only be initiated if the activation of the previous NE in the grouping is complete:
 - **In parallel** – when executing the activation request, the management system allows all NEs in the grouping to exit the queue as long as resources are available.
 - **In series** – when executing the activation request, the management system only allows one NE in the grouping to have an NE generic activation in progress at a time. All other NE generic activations for NEs in the grouping must remain in the queue.

- **Stop on failure** – select **No** to instruct the management system to proceed with activation requests for all NEs in the grouping regardless of the result of the activations of other NEs in the grouping. Select **Yes** to instruct the management system to fail all other NE activation requests in the queue for the grouping when any NE activation in the grouping fails. Activation requests in progress at an NE for other NEs in the grouping are unaffected.
- **Continue if the inactive NE generic is the same as the current active NE generic** – specify whether or not the activation process should continue if the inactive NE generic is the same as the current active NE generic. If you select *no*, when the management system is executing the download request, it does not attempt to activate software for any NE where the inactive release of the NE is the same as the active release of the NE.
- **Continue if the inactive NE generic is the older than the current active NE generic** – specify whether or not the activation process should continue if the inactive NE generic is the older than the current active NE generic. If you select *no*, when the management system is executing the download request, it does not attempt to activate software for any NE where the inactive release of the NE is older than the active release of the NE.

Click **Submit**.

Result: The NE generic in the inactive partition is installed in the active partition and the NE reboots to update the current running version of the software.

The management system notes the progress of the operation in the **Job Updates** page, and logs this activity in the **User Activity Log**.

END OF STEPS



To commit an NE generic on an NE

When to use

Use this task to commit an NE generic that is in *trial* mode phase on an NE. That way you terminate the trial phase of a newly installed software.

Task

- 1 In the top navigation bar, select **My network** → **Job updates**.
Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:
 - **Network Elements** → **Software****Result:** The **Search** section of the **Software** page is displayed.

- 3 In the **Software type** field, select **NE generic**.

- 4 In the **Software stored on** field, select **NE**.

- 5 In the **NE type** field, select a type of NE.

- 6 Do one of the following:
 - In the **NE Name** field, select the name of NE in question.
 - In the **NE Name** field, select **All** and populate the field **NE Generic** with the respective version number.Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

-
- 7 Click the radio button next to the NE for which you wish to commit the NE generic.

From the **Go** menu, select **Commit NE Generic** and click **Go**.

Result: A confirmation message appears.

-
- 8 Click **OK**.

Result: The NE generic in the active partition is committed to the inactive partitions. The trial phase of the new software version is terminated.

The management system notes the progress of the operation in the **Job Updates** panel, and logs this activity in the **User Activity Log**.

END OF STEPS



To revert an NE generic on an NE

When to use

Use this task to revert to the inactive software load on the NE. This task replaces the active software load (in a trial phase) with the previous running NE generic. Software loads that have been previously committed cannot be reverted.

Task

- 1 In the top navigation bar, select **My network** → **Job updates**.
Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:
 - **Network Elements** → **Software****Result:** The **Search** section of the **Software** page is displayed.

- 3 In the **Software type** field, select **NE generic**.

- 4 In the **Software stored on** field, select **NE**.

- 5 In the **NE type** field, select a type of NE.

- 6 Do one of the following:
 - In the **NE Name** field, select the name of NE in question.
 - In the **NE Name** field, select **All** and populate the field **NE Generic** with the respective version number.Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

-
- 7 Click the radio button next to the NE for which you wish to revert to the inactive NE generic.

From the **Go** menu, select **Revert NE generic** or **Revert NE generic: Install now** and click **Go**.

Result: A confirmation message appears.

-
- 8 Click **OK**.

Result: The previously installed NE generic is installed in the active partition.

The management system notes the progress of the operation in the **Job Updates** panel, and logs this activity in the **User Activity Log**.

END OF STEPS



To schedule NE generic activation

When to use

Use this task to schedule an NE generic activation.

Task

1 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

2 In the **Software type** field, select **NE generic**.

3 In the **Software stored on** field, select **NE**.

4 In the **NE type** field, select a type of NE.

5 Do one of the following:

- In the **NE Name** field, select the name of NE in question.
- In the **NE Name** field, select **All** and populate the field **NE Generic** with the respective version number.

Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE generics stored on the NE.

The following applies to the search results:

- If the search criteria is for a specific NE, the search results table includes matches in both the active and inactive NE partitions.
- If the search criteria is for a specific NE generic, the list of entries in the search results table include all NEs that contain an active release matching the search criteria.

Additionally, the list includes all software generics on any NE that has a matching software generic in the active release. For example, if the software generic in the active version of the NE matches the search criteria but the generic in the inactive partition does not, both still appear in the search results table. This means that some rows of the table may have a different release than the selected search criteria.

-
- 6 Click the radio button next to the NE for which you wish to schedule activation of the inactive NE generic.

From the **Go** menu, select **Schedule activate** and click **Go**.

Result: The **Activate NE generic** page is displayed. In that page, most of the fields are prepopulated according to your previous selections.

- 7 Change the entries or selections for any modifiable fields that you wish to update.
- **Activation type** – select *Standard* if you want to perform a normal activation, or *Trial* if the *LambdaUnite*[®] MSS is to be used. Using the option *Trial*, it is possible to revert back to the previous generic together with the restoration of the last matching database.
 - **Activation order** – select **System default** to use the default rules for establishing the order of NEs within the grouping, or select **User defined** to place the NE in the queue using the order defined in the **Selected NE** list.
 - **Activate NEs** – select one of the following options to determine if the NEs in a grouping can exit the management system queue as long as resources are available or if an activation of an NE in the grouping can only be initiated if the activation of the previous NE in the grouping is complete:
 - **In parallel** – when executing the activation request, the management system allows all NEs in the grouping to exit the queue as long as resources are available.
 - **In series** – when executing the activation request, the management system only allows one NE in the grouping to have an NE generic activation in progress at a time. All other NE generic activations for NEs in the grouping must remain in the queue.
 - **Stop on failure** – select **No** to instruct the management system to proceed with activation requests for all NEs in the grouping regardless of the result of the activations of other NEs in the grouping. Select **Yes** to instruct the management system to fail all other NE activation requests in the queue for the grouping when any NE activation in the grouping fails. Activation requests in progress at an NE for other NEs in the grouping are unaffected.

- **Continue if the inactive NE generic is the same as the current active NE generic** – specify whether or not the activation process should continue if the inactive NE generic is the same as the current active NE generic. If you select *no*, when the management system is executing the download request, it does not attempt to activate software for any NE where the inactive release of the NE is the same as the active release of the NE.
- **Continue if the inactive NE generic is the older than the current active NE generic** – specify whether or not the activation process should continue if the inactive NE generic is the older than the current active NE generic. If you select *no*, when the management system is executing the download request, it does not attempt to activate software for any NE where the inactive release of the NE is older than the active release of the NE.

Click **Schedule**.

Result: The **Schedule activate NE generic** page is displayed.

- 8 Change the entries or selections for any modifiable fields that you wish to update.
- **Scheduled Date** – select the date from which the scheduled task should begin from the pop-up calendar.
 - **Scheduled time** – enter the scheduled time for the task to begin. Enter a value using the format *hh:mm:ss* ([0 to 23]:[0 to 59]:[0 to 59]).
 - **Scheduled task name** enter an optional name for the scheduled task or allow the system to generate a default value. Once created, the scheduled task name cannot be modified.
 - **Number of retries** – select the number of times (1 to 4) the scheduled task will be retried in case of error or *no retries*.
 - **Execution interval** – specify the interval at which the scheduled task should begin. Possible values are 1 hour to 12 hours in 1 hour increments and the value “Continuous”.
 - **Retry interval** – select the interval of time that will pass between retries. Possible values are 1 min. to 60 min.

Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Schedule activate NE generic** page, and the scheduled task is added.

END OF STEPS

Reference

For detailed information about how to view a list of scheduled tasks, how to modify scheduled tasks, and how to delete scheduled tasks, refer to *Lucent OMS Network Element Management Guide – Tools – Scheduled Tasks*.



Tasks related to NE databases

To view a list of NE database versions stored on the management system

When to use

Use this task to view a list of NE database versions (that means backups of the MIBs) stored on the management system.

Task

- 1 Use the object links to follow this path:
 - **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 2 In the **Software operation** field, select **Search**.
- 3 In the **Software type** field, select **NE database**.
- 4 In the **Software stored on** field, select **Management system**.
- 5 In the **NE type** field, select a type of NE.
- 6 In the **NE name** field, select the name of an NE or select **All**.
- 7 In the **NE generic partition** field, select the type of partition (optional):
 - **Active** – the software currently running on the NE.
 - **Inactive** – the software is stored in the inactive or backup partition of the NE.
 - **All**

- 8 In the **NE generic type** field, select either the *Release number* or *Item code* format for the NE generic (optional).

-
- 9 In the **NE generic** field, the NE generic label is a hyperlink to the **NE Generic Selection** page from which to select the NE generic to include in the search criteria, or type in an NE generic name in the text box. (optional).
-
- 10 Populate the **NE group search** field, select the radio button to perform a search by one of the following options below (optional).
- When searching for an NE generic on NE, the available radio buttons are: **Ring** and **Aggregate**.
- When searching for an NE database on the management system, the available radio buttons are: **Ring**, **Aggregate**, and **NCG**.
- Meaning of the options:
- **Aggregate** – the aggregate label is a hyperlink to the **Aggregate Selection** page from which to select aggregates to include in the search criteria, or type in an aggregate name in the text box.
 - **Ring** – the ring label is a hyperlink to the **Ring Selection** page from which to select rings to include in the search criteria, or type in a ring name in the text box.
 - **NCG** – the NCG label is a hyperlink to the **NCG Selection** page from which to select NCGs to include in the search criteria, or type in an NCG name in the text box.
-
- 11 In the **Backup Status** field, select the backup status. Valid for the backup NE database on the management system operation only (optional).
- If the selected **NE type** or **NE name** is **All**, the possible values in the drop down list are: **Last backups**, **Last successful backups**, **Failed backups**, **In progress backups**, or **No successful backups**.
 - If the selected **NE name** is any value except **All**, the possible values in the drop down list are: **All backups**, **Last backup**, or **All successful backups**.
-
- 12 In the **Date and time: from** field, enter the date and time. Click on the calendar icon to display the **Date/Time Chooser** from which to select the date and time (optional).
-
- 13 In the **Date and time: to** field, enter the date and time. Click on the calendar icon to display the **Date/Time Chooser** from which to select the date and time (optional).
-
- 14 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on the management system that meet your search criteria.

END OF STEPS



To view a list of NE database versions stored on an NE

When to use

Use this task to view a list of NE database versions stored on an NE.

Task

1 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

2 In the **Software operation** field, select **Search**.

3 In the **Software type** field, select **NE database**.

4 In the **Software stored on** field, select **NE**.

5 In the **NE type** field, select a type of NE.

6 In the **NE name** field, select the name of an NE.

7 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on an NE that meet your search criteria.

END OF STEPS



To back up NE database versions onto the management system

When to use

Use this task to back up NE database versions, that means to back up the MIB onto the management system.

There are two methods for this task.

Task, method 1: from the list of NE database versions on the management system

- 1 In the top navigation bar select **My network** → **Job updates**.
Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:
 - **Network Elements** → **Software****Result:** The **Search** section of the **Software** page is displayed.

- 3 In the **Software operation** field, select **Search**.

- 4 In the **Software type** field, select **NE database**.

- 5 In the **Software stored on** field, select **Management system**.

- 6 In the **NE type** field, select a type of NE.

- 7 In the **NE name** field, select the name of an NE or select **All**.

- 8 In the **NE generic partition** field, select the type of partition (optional):
 - **Active** – the software currently running on the NE.
 - **Inactive** – the software is stored in the inactive or backup partition of the NE.
 - **All**

-
- 9 In the **NE generic type** field, select either the Release number or Item code format for the NE generic (optional).
-
- 10 In the **NE generic** field, the NE generic label is a hyperlink to the **NE Generic Selection** page from which to select the NE generic to include in the search criteria, or type in an NE generic name in the text box. (optional).
-
- 11 Populate the **NE group search** field, select the radio button to perform a search by one of the following options below (optional).
- When searching for an NE generic on NE, the available radio buttons are: **Ring** and **Aggregate**.
- When searching for an NE database on the management system, the available radio buttons are: **Ring**, **Aggregate**, and **NCG**.
- Meaning of the options:
- **Aggregate** – the aggregate label is a hyperlink to the **Aggregate Selection** page from which to select aggregates to include in the search criteria, or type in an aggregate name in the text box.
 - **Ring** – the ring label is a hyperlink to the **Ring Selection** page from which to select rings to include in the search criteria, or type in a ring name in the text box.
 - **NCG** – the NCG label is a hyperlink to the **NCG Selection** page from which to select NCGs to include in the search criteria, or type in an NCG name in the text box.
-
- 12 In the **Ring** field, the ring label is a hyperlink to the Search for Rings page from which to select the Ring rate and Ring type to include in the search criteria, or type in an Ring name in the text box. (optional).
-
- 13 In the **Backup Status** field, select the backup status. Valid for the backup NE database on the management system operation only (optional).
- If the selected **NE type** or **NE name** is **All**, the possible values in the drop down list are: **Last backups**, **Last successful backups**, **Failed backups**, **In progress backups**, or **No successful backups**.
 - If the selected **NE name** is any value except **All**, the possible values in the drop down list are: **All backups**, **Last backup**, or **All successful backups**.

14 In the **Date and time: from** field, enter the date and time. Click on the calendar icon to display the **Date/Time Chooser** from which to select the date and time (optional).

15 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on the management system that meet your search criteria.

16 Click the **New** tool in the toolbar.

Result: A confirmation window is displayed asking you to confirm the backup.

17 Click **Backup to management system**.

Result: The **Backup to management system** window opens.

18 To specify the NEs from which you want to start a backup, choose one of the following in the **Selected NEs** section:

- **All NEs in the network**
 - **All NEs of type** – select a type of NE from the list.
 - **All NEs in Aggregate** – type the name of the aggregate in the text field, or click on the hyperlink to display the **Aggregate Selection** window. Select the radio button next to the ring you would like to include in your search criteria, and click **OK**.
 - **All NEs in NCG** – type the name of the network communications group (NCG) in the text field, or click on the hyperlink to display the **NCG Selection** window. Select the radio button next to the NCG you would like to include in your search criteria, and click **OK**.
 - **NE list for NE type** – select a type of NE from the list, then use the arrow keys to move NEs between the **Available NEs** list and the **Selected NEs** list.
-

19 Use the **Backup if status for NE has not changed since the last backup?** to specify whether or not the backup process should continue if the status for NE has not changed since the last backup.

If you specify *no*, the management system determines whether an NE configuration has potentially changed since the last memory backup was made to the system. The NE configuration is considered to have potentially changed if either the system has

received an autonomous message from the NE reporting a database change or if the system has lost communication with the NE at any time since the last memory backup of that type. If the NE has not changed since the last backup, the NE is excluded from the backup request.

20 Click **Submit**.

Result: A confirmation window is displayed.

21 Click **Yes**.

Result: The selected NE database versions are transferred to the management system. As the files are transferring, the management system notes the percentage of the transfer that has completed in the **Job Updates** page, and logs this activity in the **User Activity Log**.

END OF STEPS

Task, method 2: from the list of NE database versions on the NE

1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

3 In the **Software operation** field, select **Search**.

4 In the **Software type** field, select **NE database**.

5 In the **Software stored on** field, select **NE**.

6 In the **NE type** field, select a type of NE.

.....

7 In the **NE name** field, select the name of an NE.

.....

8 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on an NE that meet your search criteria.

.....

9 Click the radio button next to the NE that you wish to backup to the management system. From the **Go** menu, select **Backup to management system** and click **Go**.

Result: The **Backup to management system** page opens populated with appropriate values.

.....

10 Verify the settings, then click **Submit**.

Result: The selected NE database versions are transferred to the management system. As the files are transferring, the management system notes the percentage of the transfer that has completed in the **Job Updates** page, and logs this activity in the **User Activity Log**.

.....

END OF STEPS

.....



To schedule the backup of an NE database version onto the management system

When to use

Use this task to schedule the backup of an NE database version onto the management system.

Task

1 Do one of the following:

- View a list of NE database versions stored on the management system, using the task [“To view a list of NE database versions stored on the management system”](#) (p. 13-28). The list at the bottom of the **Software** page is populated with a list of NE database versions that meet your search criteria. From the **Go** menu, select **Schedule Backup to Management System** and click **Go**.
- View a list of NE database versions stored on an NE, using the task [“To view a list of NE database versions stored on an NE”](#) (p. 13-31). The list at the bottom of the **Software** page is populated with a list of NE database versions that meet your search criteria. Click the radio button next to any NE database version. The NE will always back up the active version. From the **Go** menu, select **Schedule backup to management system** and click **Go**.

Result: The first section of the **Schedule backup to management system** page is displayed. This page contains pre-populated information about the backup.

2 Verify the information presented, then click **Schedule**.

Result: The second section of the **Schedule Backup to Management System** page is displayed. It allows you to precisely schedule the backup.

3 To schedule the backup frequency, select one of the following:

- **Daily starting on** – complete this section if the task is to be scheduled daily. Select the date and time for which the scheduled task should begin and end from the pop-up calendars.
- **Weekly starting on** – complete this section if the task is to be scheduled weekly. Select the date and time for which the scheduled task should begin and end from the pop-up calendars.

- **Once every month starting on** – complete this section if the task is to be scheduled once a month. Select the date and time for which the scheduled task should begin and end from the pop-up calendars.
 - **Every N days starting on** – complete this section if the task is to be scheduled every *N* days where *N* is a variable number. Select the date and time for which the scheduled task should begin and end from the pop-up calendars. Specify *N*, which may be a period of every two to six days, in the field **Every**.
-

4 Provide additional details for the backup to be scheduled:

- **Scheduled time** – enter the scheduled time for the task to begin. Enter a value using the format *hh:mm:ss* ([0 to 23]:[0 to 59]:[0 to 59]).
- **Scheduled task name** enter an optional name for the scheduled task or allow the system to generate a default value. Once created, the scheduled task name cannot be modified.
- **Number of retries** – select the number of times (1 to 4) the scheduled task will be retried in case of error or *no retries*.
- **Execution interval** – specify the interval at which the scheduled task should begin. Possible values are 1 to 12 hours in 1 hour increments and the value “Continuous”.
- **Retry interval** – select the interval of time that will pass between retries. Possible values are 1 to 60 minutes.

Click **Submit**.

Result: A progress indication followed by a confirmation is issued in the **Message** section of the **Schedule Backup to Management System** page, and the scheduled task is added.

END OF STEPS

Reference

For detailed information about how to view a list of scheduled tasks, how to modify scheduled tasks, and how to delete scheduled tasks, refer to *Lucent OMS Network Element Management Guide – Tools – Scheduled Tasks*.



To restore an NE database version from the management system to an NE

When to use

Use this task to restore an NE database (MIB) version on the management system (also known as a backup file) to an NE.



CAUTION

Service-disruption hazard

Restoring an NE database (MIB) from the management system to the network element will cause a disruption in communication and may be traffic affecting.

Ensure that the NE database restoration is really necessary. It is a good idea to create a backup of the current NE database before initiating the restoration.

Task, method 1: from the list of NE database versions on the management system

- 1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

- 2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

- 3 In the **Software operation** field, select **Search**.
-

- 4 In the **Software type** field, select **NE database**.
-

- 5 In the **Software stored on** field, select **Management system**.
-

- 6 In the **NE type** field, select a type of NE.
-

- 7 In the **NE name** field, select the name of an NE, or select **All**.
-

-
- 8 In the **NE generic partition** field, select the type of partition (optional):
- **Active** – the software currently running on the NE.
 - **Inactive** – the software is stored in the inactive or backup partition of the NE.
 - **All**
-

- 9 In the **NE generic type** field, select either the release number or item code format for the NE generic (optional).
-

- 10 In the **NE generic** field, the NE generic label is a hyperlink to the **NE Generic Selection** page from which to select the NE generic to include in the search criteria. Alternatively, type in an NE generic name in the text field. (optional).
-

- 11 In the **NE group search** field, select the option to perform a search by one of the following options below (optional).

When searching for an NE generic on NE the available options are: **Ring** and **Aggregate**.

When searching for an NE database on the management system, the available options are: **Ring**, **Aggregate**, and **NCG**.

Meaning of the options:

- **Aggregate** – the aggregate label is a hyperlink to the **Aggregate Selection** page from which to select aggregates to include in the search criteria. Alternatively, type in an aggregate name in the text field.
 - **Ring** – the ring label is a hyperlink to the **Ring Selection** page from which to select rings to include in the search criteria. Alternatively, type in a ring name in the text field.
 - **NCG** – the NCG label is a hyperlink to the **NCG Selection** page from which to select NCGs to include in the search criteria. Alternatively, type in an NCG name in the text field.
-

- 12 In the **Backup Status** field, select the backup status. Valid for the backup NE database on the management system operation only (optional).
- If the selected **NE type** or **NE name** is **All**, possible values are: **Last backups**, **Last successful backups**, **Failed backups**, **In progress backups**, or **No successful backups**.
 - If the selected **NE name** is any value except **All**, possible values are: **All backups**, **Last backup**, or **All successful backups**.
-

.....

13 In the **Date and time: from** field, enter the date and time. Click on the calendar icon to display the **Date/Time Chooser** from which to select the date and time (optional).

.....

14 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on the management system that meet your search criteria.

.....

15 Click the radio button next to the NE database version that you wish to restore to an NE. From the **Go** menu, select **Restore to NE** and click **Go**.

Result: A confirmation window is displayed.

.....

16 Click **Yes**.

Result: The restoration is initiated. The management system notes the progress of the operation in the **Job Updates** page, and logs this activity in the **User Activity Log**. A reboot and a service interruption will occur on the NE.

.....

END OF STEPS

.....

Task, method 2: from the list of NE database versions on the NE

.....

1 In the top navigation bar select **My network** → **Job updates**.

Result: The **Job Updates** page is displayed. This page allows you to monitor the status of the task.

.....

2 Use the object links to follow this path:

- **Network Elements** → **Software**

Result: The **Search** section of the **Software** page is displayed.

.....

3 In the **Software operation** field, select **Search**.

.....

4 In the **Software type** field, select **NE database**.

.....

.....
5 In the **Software stored on** field, select **NE**.
.....

6 In the **NE type** field, select a type of NE.
.....

7 In the **NE name** field, select the name of an NE.
.....

8 Click **Search**.

Result: The list at the bottom of the **Software** page is populated with a list of the NE database versions stored on an NE that meet your search criteria.
.....

9 Click the radio button next to the NE to be restored. From the **Go** menu, select **Restore from management system** and click **Go**.

Result: The **Restore NE database from management system** page is displayed. This page shows a list of all memory versions (backup files) stored on the management system for the selected NE.
.....

10 Select the memory version (backup file) to be restored and click **Submit**.

Result: The restoration is initiated. The management system notes the progress of the operation in the **Job Updates** page, and logs this activity in the **User Activity Log**. A reboot and a service interruption will occur on the NE.
.....

END OF STEPS
.....



Glossary

A **access point identifier (API)**

To check whether a path is correctly provisioned a path trace can be set. A label (for example a word) is sent along the path from one termination point to the other. This label is called *trail trace identifier (TTI)*. If the TTI is a specific string, this string is called *access point identifier (API)*. If the expected API equals the accepted API, the transmission path is well provisioned.

acknowledged information transfer service (AITS)

A LAPD mode.

In the *acknowledged information transfer service (AITS)*, PDUs are numbered and transmitted sequentially, and acknowledgment PDUs are sent back from the receiver to the sender. If a PDU is lost, that is, if the sender gets no acknowledgment, the PDU is retransmitted.

AFI

See [“authority and format identifier” \(p. GL-2\)](#).

AIS

See [“alarm indication signal” \(p. GL-1\)](#).

AITS

See [“acknowledged information transfer service” \(p. GL-1\)](#).

alarm indication signal (AIS)

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.

API

See [“access point identifier” \(p. GL-1\)](#).

APS

See [“automatic protection switching” \(p. GL-2\)](#).

Area

See “[area identifier](#)” (p. GL-2).

area identifier (Area)

Part of the NSAP address indicating the routing area to which a node belongs.

authority and format identifier (AFI)

Part of the NSAP address specifying the NSAP address format.

automatic protection switching (APS)

SONET protection mechanisms for linear and ring applications.

B **bidirectional line switched ring (BLSR)**

A SONET ring protection mechanism.

BLSR

See “[bidirectional line switched ring](#)” (p. GL-2).

D **data communication channel (DCC)**

The *data communication channels (DCC)* are part of the data communication network (DCN). The channels are used to exchange management data between the management system and the network elements. The channels are also used for communication between the different network elements (for example remote logins).

data communication network (DCN)

A *data communication network (DCN)* is used for the exchange of management data. It is an overlay of the transmission network. The management system (for example Lucent OMS) and the network elements (NEs) together are the nodes of this network.

DCC

See “[data communication channel](#)” (p. GL-2).

DCN

See “[data communication network](#)” (p. GL-2).

DFI

See “[DSP format identifier](#)” (p. GL-3).

DNI

See “[dual node ring interworking](#)” (p. GL-3).

DNU

See “[do not use](#)” (p. GL-2).

do not use (DNU)

A synchronization quality level; *do not use* indicates that the timing signal should not be

used, since it may cause timing loops.

domain specific part (DSP)

Part of the NSAP address.

DSP

See “[domain specific part](#)” (p. GL-3).

DSP format identifier (DFI)

Part of the NSAP address specifying the DSP format.

DSwT

See “[dual stack with tunneling](#)” (p. GL-3).

dual node ring interworking (DNI)

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.

dual stack with tunneling (DSwT)

The *dual stack with tunneling (DSwT)* feature provides a way to manage IP devices through the DCN network.

E

electrostatic discharge (ESD)

The transfer of an electrostatic charge between bodies at different electrostatic potentials. *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.

electrostatic protection (ESP)

Measures taken to reduce or avert the threat of electrostatic discharge (ESD) and electrostatic fields.

end system (ES)

In the ISO-OSI network protocol, nodes behaving as *end systems (ES)* perform no forwarding of data packets. They communicate with each other on an end-to-end basis via intermediate systems.

engineering order wire (EOW)

An external orderwire system can be connected which uses an orderwire channel for transparent data transmission via the SDH transmission network. For this functionality, the E1 byte is used as orderwire channel. The RSOH byte E1 is accessible in all network element types.

EoS

See “[Ethernet over SDH](#)” (p. GL-4).

EOW

See “engineering order wire” (p. GL-3).

ES

See “end system” (p. GL-3).

ESD

See “electrostatic discharge” (p. GL-3).

ESP

See “electrostatic protection” (p. GL-3).

Ethernet over SDH (EoS)

A method to encapsulate the Ethernet frames into the SDH transmission payload.

G gateway network element (GNE)

An NE that provides gateway functionality between external interfaces to OSs (for example, LAN ports) using one protocol stack (for example TCP/IP) and internal DCC interfaces using a different protocol stack (for example, OSI).

generic framing procedure (GFP)

A method used to encapsulate the Ethernet frames into the SDH transmission payload. It has been standardized by ITU-T.

GFP

See “generic framing procedure” (p. GL-4).

GNE

See “gateway network element” (p. GL-4).

I IDI

See “initial domain identifier” (p. GL-4).

IDP

See “initial domain part” (p. GL-4).

initial domain identifier (IDI)

Part of the NSAP address specifying the country code.

initial domain part (IDP)

Part of the NSAP address.

intermediate system (IS)

In the ISO-OSI network protocol, *intermediate systems (IS)* are used for routing data between nodes and (sub) networks. A network element can act both as an end system as well as an intermediate system.

intermediate system to intermediate system (IS-IS)

The *intermediate system to intermediate system (IS-IS) protocol* is used between intermediate systems in the DCN.

IS

See “[intermediate system](#)” (p. GL-4).

IS routing information base (RIB)

The IS-IS protocol maintains the *IS routing information base (RIB)*. The information in this information base is used for the routing of management data packets in the DCN by the intermediate systems.

IS-IS

See “[intermediate system to intermediate system](#)” (p. GL-4).

L LCAS

See “[link capacity adjustment scheme](#)” (p. GL-5).

LCN

See “[local communications network](#)” (p. GL-5).

link capacity adjustment scheme (LCAS)

The *link capacity adjustment scheme (LCAS)* is an extension of virtual concatenation that allows dynamic changes in the number of channels in a connection. In case channels are added or removed by management actions, this happens without losing any customer traffic.

link state protocol data unit (LSP)

Intermediate systems exchange routing information regularly with one another as part of the IS-IS protocol by the use of *link state protocol data units (LSP)*.

The LSPs contain the information on the NSAP addresses of nodes used in the tables of the RIBs.

local communications network (LCN)

In the case where there is no DCC connectivity between nodes, a *local communications network (LCN)* can be used to connect the nodes to each other.

LSP

See “[link state protocol data unit](#)” (p. GL-5).

M management information base (MIB)

The *management information base (MIB)* is the provisioning information stored in the database of the NE. This includes the configuration of the units within the NE, the name and type of the NE, as well as addressing information and network information necessary for management.

In Lucent OMS context, the MIB is referred to as *NE database*.

manufacturers executable code (MEC)

The *manufacturers executable code (MEC)* file contains the complete software package for one NE.

MDI

See “[miscellaneous discrete input](#)” (p. GL-6).

MDO

See “[miscellaneous discrete output](#)” (p. GL-6).

MEC

See “[manufacturers executable code](#)” (p. GL-6).

MIB

See “[management information base](#)” (p. GL-5).

miscellaneous discrete input (MDI)

A *miscellaneous discrete input (MDI)* is an input to a network element for external equipment. MDIs can be monitored by the management system. An MDI can be connected to monitor a temperature sensor or a door contact, for example.

miscellaneous discrete output (MDO)

A *miscellaneous discrete output (MDO)* is an output from a network element used to drive external equipment. MDOs can be activated or deactivated by the management system. An MDO can be connected to control a fan or a generator, for example.

MS-SPRing

See “[multiplex section shared protection ring](#)” (p. GL-6).

MSP

See “[multiplex section protection](#)” (p. GL-6).

multiplex section protection (MSP)

Multiplex section protection (MSP) is used to protect the traffic in a point-to-point connection against transmission failures (MS-AIS, LOF, LOS, MS-DEG) and port equipment failures. A requirement for this kind of protection is that the transmission lines are doubled (one working line, one protection line).

A trail continues to use the working route until a fault condition occurs or an external switch request is issued to switch to the protection route.

multiplex section shared protection ring (MS-SPRing)

An SDH ring protection mechanism.

N NBMA

See “[non-broadcast multiple access](#)” (p. GL-7).

network service access point (NSAP)

A *network service access point (NSAP)* is the address of a node (for example a network element). Each node has exactly one NSAP that is unique in the entire network (usually the NSAP is even globally unique). Routing and forwarding in each node of a network is done using the target NSAP.

network service provider (NSP)

A *network service provider (NSP)* offers services that are delivered over a network, externally managed, based on a one-to-many business model, and service-fee based.

non-broadcast multiple access (NBMA)

Non-broadcast multiple access (NBMA) is a network type that support multiple access points but does not support broadcasting or in which broadcasting is not possible.

NSAP

See “[network service access point](#)” (p. GL-7).

NSP

See “[network service provider](#)” (p. GL-7).

P PDU

See “[protocol data unit](#)” (p. GL-7).

PRC

See “[primary reference clock](#)” (p. GL-7).

primary reference clock (PRC)

A synchronization quality level; *primary reference clock* indicates that the timing signal is provided by a primary reference clock.

protocol data unit (PDU)

According to ITU-T recommendation Q.921 (1997), a unit of data specified in a protocol and consisting of protocol-control-information and possibly user-data.

Q QoS

See “[quality of service](#)” (p. GL-7).

quality of service (QoS)

According to ITU-T recommendation Q.1703 (2004), the collective effect of service performance which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services,

such as bandwidth, latency, jitter, traffic loss, and so on

R RD

See “[routing domain](#)” (p. GL-8).

RDI

See “[remote defect indicator](#)” (p. GL-8).

remote defect indicator (RDI)

An indication returned to a transmitting terminal about the fact that the receiving terminal has detected an incoming section failure.

RIB

See “[IS routing information base](#)” (p. GL-5).

routing domain (RD)

Part of the NSAP address.

S SCO

See “[station clock output](#)” (p. GL-9).

SDH equipment clock (SEC)

A synchronization quality level; *SDH equipment clock* indicates that the timing signal is provided by the NE’s own internal oscillator.

SEC

See “[SDH equipment clock](#)” (p. GL-8).

SEL

See “[selector field](#)” (p. GL-8).

selector field (SEL)

Part of the NSAP address used to direct the protocol data units (PDU) to the correct destination.

SFP

See “[small form-factor pluggable optic](#)” (p. GL-8).

small form-factor pluggable optic (SFP)

Small form-factor pluggable optic (SFP) is a specification for a new generation of optical modular transceivers. The devices are designed for use with small form factor (SFF) connectors, and offer high speed and physical compactness. They are hot-swappable.

SNCP

See “[subnetwork connection protection](#)” (p. GL-9).

SNPA

See “subnetwork point of attachment” (p. GL-9).

SSM

See “synchronization status message” (p. GL-9).

SSU

See “synchronization supply unit” (p. GL-9).

SSU-L

See “synchronization supply unit local” (p. GL-9).

SSU-T

See “synchronization supply unit transit” (p. GL-9).

station clock output (SCO)

subnetwork connection protection (SNCP)

Subnetwork connection protection (SNCP) is a type of path protection that is used to protect the traffic for a pre-selected path. A working path is replaced by a protection path if the working path fails, or if its performance falls below a required level.

subnetwork point of attachment (SNPA)

According to ITU-T recommendation X.213 (2001), a point at which a real end system, interworking unit, or real subnetwork is attached to a real subnetwork, and a conceptual point at which a subnetwork service is offered within an end or intermediate system.

synchronization status message (SSM)

A *synchronization status message (SSM)* is defined for SDH/SONET transport signals, for framed 2-Mbps signals, and for DS1 ESF external timing input signals. The purpose of the SSM is to signal the reference clock quality level from NE to NE to:

- Enable the timing generator to extract the timing reference signal with the best quality.
- Make it possible to autonomously enter the holdover mode in case there is no suitable timing reference signal.
- Prevent timing loops.

synchronization supply unit (SSU)

According to ITU-T recommendation G.810 (1996), a logical function for frequency reference selection, processing and distribution, having specific frequency characteristics.

synchronization supply unit local (SSU-L)

A synchronization quality level; *synchronization supply unit local* indicates that the timing signal was derived from a local SSU.

synchronization supply unit transit (SSU-T)

A synchronization quality level; *synchronization supply unit transit* indicates that the timing signal is derived from a transit SSU.

System

See “[system identifier](#)” (p. GL-10).

system identifier (System)

Part of the NSAP address representing the node. The IEEE 802.3 MAC address is reserved and physically stored on every NE.

T TAP

See “[tunnel auto provisioning](#)” (p. GL-10).

target identifier (TID)

A parameter (provisionable using ITM-CIT) 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 (-).

TID

See “[target identifier](#)” (p. GL-10).

TIM

See “[trace identifier mismatch](#)” (p. GL-10).

trace identifier mismatch (TIM)

If the *trace identifier mismatch (TIM)* detection is enabled, traffic will be lost when a mistake in the trace string is detected.

trail termination point (TTP)

In a *trail termination point (TTP)* the path overhead bytes of a signal are terminated.

trail trace identifier (TTI)

To check whether a path is correctly provisioned a path trace can be set. A label (for example a word) is sent along the path from one termination point to the other. This label is called *trail trace identifier (TTI)*. If the TTI is a specific string, this string is called *access point identifier (API)*. If the expected API equals the accepted API, the transmission path is well provisioned.

TTI

See “[trail trace identifier](#)” (p. GL-10).

TTP

See “[trail termination point](#)” (p. GL-10).

tunnel auto provisioning (TAP)

A method developed by Lucent Technologies to simplify the provisioning of nodes in a routing table. The principle behind TAP is that IP routes known by dual stack with tunneling nodes (DSwT nodes) at the edge of the OSI network are advertised across the OSI network to the other DSwT nodes which can then insert these routes into their own routing tables.

U UITS

See [“unacknowledged information transfer service”](#) (p. GL-11).

unacknowledged information transfer service (UITS)

A LAPD mode.

In the *unacknowledged information transfer service (UITS)*, corrupted PDUs are ignored and no further actions taken. Upper layers of the OSI stack are responsible for recovery actions.

unidirectional path switched ring (UPSR)

UPSR is typically a SONET ring architecture. It provides path-level protection for STS-*N* circuits within in physical ring network.

UPSR

See [“unidirectional path switched ring”](#) (p. GL-11).

Index

Numerics

- 1+1 MSP protection groups
 - add, [11-67](#)
- 1x1 MSP protection groups
 - add, [11-69](#)
- 1+1 APS protection groups
 - add, [11-78](#)
- 1x1 APS protection groups
 - add, [11-80](#)
- 1+1 MSP protection groups
 - delete, [11-73](#)
- 1x1 MSP protection groups
 - delete, [11-73](#)
- 1+1 APS protection groups
 - delete, [11-84](#)
- 1x1 APS protection groups
 - delete, [11-84](#)
- 1+1 MSP protection groups
 - modify, [11-71](#)
- 1x1 MSP protection groups
 - modify, [11-71](#)
- 1+1 APS protection groups
 - modify, [11-82](#)
- 1x1 APS protection groups
 - modify, [11-82](#)
- 1+1 MSP
 - non-revertive mode, [10-15](#)
- 1+1 APS
 - non-revertive mode, [10-15](#)
- 1+1 MSP
 - revertive mode, [10-15](#)
- 1+1 APS
 - revertive mode, [10-15](#)
- 1:1 MSP
 - revertive mode, [10-16](#)
- 1x1 MSP protection groups
 - view list, [11-66](#)
- 1+1 MSP protection groups
 - view list, [11-66](#)
- 1x1 APS protection groups
 - view list, [11-77](#)
- 1+1 APS protection groups
 - view list, [11-77](#)
- 2-fiber MS-SPRing protection groups
 - add, [11-89](#)
- 2-fiber BLSR protection groups
 - add, [11-107](#)
- 2-fiber MS-SPRing protection groups
 - delete, [11-93](#)
- 2-fiber BLSR protection groups
 - delete, [11-111](#)
- 2-fiber MS-SPRing protection groups
 - modify, [11-91](#)
- 2-fiber BLSR protection groups
 - modify, [11-109](#)
- 2-fiber MS-SPRing protection switches
 - operate, [11-95](#)
- 2-fiber BLSR protection switches
 - operate, [11-113](#)
- 2-fiber MS-SPRing protection groups
 - view list, [11-88](#)
- 2-fiber BLSR protection groups
 - view list, [11-106](#)
- 2.5-Gbps optical port units,
 - [5-22](#)
- 4-fiber MS-SPRing protection groups
 - add, [11-98](#)
- 4-fiber BLSR protection groups
 - add, [11-116](#)
- 4-fiber MS-SPRing protection groups
 - delete, [11-102](#)

- 4-fiber BLSR protection groups
 - delete, [11-120](#)
- 4-fiber MS-SPRing protection groups
 - modify, [11-100](#)
- 4-fiber BLSR protection groups
 - modify, [11-118](#)
- 4-fiber MS-SPRing protection switches
 - operate, [11-104](#)
- 4-fiber BLSR protection switches
 - operate, [11-122](#)
- 4-fiber MS-SPRing protection groups
 - view list, [11-97](#)
- 4-fiber BLSR protection groups
 - view list, [11-115](#)
- 10-Gbps optical port units, [5-21](#)
- 155-Mbps optical port units, [5-23](#)
- 622-Mbps optical port units, [5-23](#)
-
- A** abort in-progress NE generic transfer, [13-12](#)
- accepted trace display mode, [6-19](#)
- accepted trail trace format, [6-33](#)
- acknowledged information transfer service
 - See: AITS
- activate
 - NE generic, [13-17](#)
 - NE generics, [12-3](#)
- OMS-to-NE connections, [4-15](#)
- active system timing reference, [8-30](#)
- add
 - 1+1 APS protection group, [11-78](#)
 - 1+1 MSP protection group, [11-67](#)
 - 1x1 APS protection group, [11-80](#)
 - 1x1 MSP protection group, [11-69](#)
 - 2-fiber BLSR protection group, [11-107](#)
 - 2-fiber MS-SPRing protection group, [11-89](#)
 - 4-fiber BLSR protection group, [11-116](#)
 - 4-fiber MS-SPRing protection group, [11-98](#)
 - equipment protection group, [6-59](#)
 - higher-order
 - cross-connections, [11-27](#)
 - lower-order
 - cross-connections, [11-16](#)
 - NE generic to the management system, [13-4](#)
 - OMS-to-NE connections, [4-4](#)
 - ONNS to UPSR/SNCP constructs, [11-54](#)
 - transparent DCC
 - cross-connections, [4-34](#)
- AFI, [3-13](#), [4-4](#), [4-9](#)
- AITS, [3-15](#)
- alarm profile name, [6-20](#), [6-27](#), [6-33](#)
- alarm severity assignment profile
 - See: ASAP
- alarms
 - allow, [6-40](#)
 - environmental, [5-30](#)
 - inhibit, [6-38](#)
- allow
 - autonomous messages, [6-40](#)
- APS, [10-4](#), [10-15](#), [11-77](#), [11-78](#), [11-80](#)
 - 1+1, [10-15](#)
- APS protection switches
 - operate, [11-86](#)
- area, [3-13](#), [4-4](#), [4-9](#)
- area identifier
 - See: Area
- ASAP, [6-27](#), [6-33](#), [6-52](#), [8-31](#), [9-11](#), [9-14](#)
 - assigned to an MDI, [6-54](#)
- assigned timing references, [8-30](#)
- Associate Tandem Connection
 - ONNS controlled plane, [7-47](#)
- Associated MxN Connection List
 - view for ONNS, [7-46](#)
- ASTN Capacity Utilization Query, [7-44](#)
 - View, [7-44](#)
- ASTN NE
 - definition, [7-3](#)
 - functionality, [7-3](#)
- ASTN Only Network parameter
 - PURE, [7-3](#)

- ASTN port parameters
 - provision ASTN port parameters for multiplex section network connection, [7-41](#)
 - ASTN ports
 - provision ASTN port parameters, [7-33](#)
 - ASTN propagation delay (msec), [6-25](#)
 - AU-3/AU-4 conversion
 - cross-connections, [10-10](#)
 - authority and format identifier
 - See: AFI
 - auto negotiation mode, [6-26](#)
 - autonomous messages
 - allow, [6-40](#)
 - inhibit, [6-38](#)
-
- B** backup
 - NE database versions onto the management system, [13-32](#)
 - BLSR, [10-4](#), [10-17](#), [11-106](#), [11-107](#), [11-115](#)
 - self healing rings, [10-19](#)
 - bursty error threshold (%), [6-20](#), [6-34](#)
 - bursty interval (sec), [6-20](#), [6-34](#)
-
- C** Cancel Group for MxN
 - Connection Group
 - ONNS, [7-92](#)
 - change
 - higher-order cross-connection from ONNS to traditional mode, [11-41](#)
 - clear
 - equipment protection switch requests, [6-63](#)
 - commit an NE generic on an NE, [13-20](#)
 - communications interfaces
 - OSI, [3-19](#)
 - TCP/IP, [3-19](#)
 - CompactFlash*[®] card, [5-11](#), [5-11](#)
 - Connection Group page, [7-20](#)
 - Connection provisioning
 - ONNS, [7-11](#), [7-13](#), [7-19](#), [7-24](#)
 - consequent action mode, [6-31](#)
 - consequent action on trail trace mismatch, [6-19](#), [6-33](#)
 - Control plane path state, [7-28](#)
 - Controlled plane service connections
 - provision, [7-48](#), [7-93](#)
 - controller variants, [5-33](#)
 - Conversion cross-connections, [10-10](#)
 - cooling, [5-6](#)
 - cost, [6-25](#)
 - create
 - users, [2-20](#)
 - Creating a AU-3/AU-4 conversion cross-connection, [11-19](#), [11-23](#)
 - cross-connect units, [5-21](#)
 - cross-connection levels, [10-5](#)
 - Cross-connection wizard, [11-19](#), [11-23](#)
 - cross-connections
 - add-drop (bi), [10-2](#)
 - add-drop A (uni), [10-2](#)
 - add-drop Z (uni), [10-2](#)
 - delete, [11-49](#)
 - double add-drop (bi), [10-2](#)
 - interconnect-P (bi), [10-2](#)
 - interconnect-W (bi), [10-2](#)
 - lower-order, [10-8](#)
 - modify parameters, [11-38](#)
 - output mode, [10-6](#)
 - shape, [10-2](#)
 - simple (bi), [10-2](#)
 - simple (uni), [10-2](#)
 - view, [11-4](#)
- CTL equipment protection, [5-32](#)
 - current user's password
 - modify, [2-16](#)
 - current user's security information
 - modify, [2-9](#)
-
- D** data communication channel
 - See: DCC
 - data communication network
 - See: DCN
 - Database synchronization
 - ONNS, [7-30](#)
 - partial synchronization, [7-101](#)
 - date
 - modify, [4-40](#)
 - view, [4-38](#)
 - DB Delete Group for MxN Connection Group
 - ONNS, [7-91](#)

DCC, 3-2, 3-14
 channel selection, 3-14
 controller, 3-3
 cross-connections, 3-14
 transparent
 cross-connections, 3-14,
 4-32, 4-34, 4-36

DCC in MSP mode, 3-16

DCC related parameters
 modify, 4-26
 retrieve, 4-23

DCC/EOW status information
 modify, 4-30
 retrieve, 4-28

DCN, 3-2, 3-14
 area-divisioning, 3-5
 communication protocols,
 3-3

deactivate
 OMS-to-NE connections,
 4-13

default user priority, 6-26, 6-31

delete
 1+1 APS protection group,
 11-84
 1+1 MSP protection group,
 11-73
 1x1 APS protection group,
 11-84
 1x1 MSP protection group,
 11-73
 2-fiber BLSR protection
 group, 11-111
 2-fiber MS-SPRing
 protection group, 11-93
 4-fiber BLSR protection
 group, 11-120

4-fiber MS-SPRing
 protection group, 11-102

cross-connections, 11-49

NE, 4-19

NE generic from the
 management system, 13-5

OMS-to-NE connections,
 4-17

ONNS to UPSR/SNCP
 constructs, 11-56

transparent DCC
 cross-connections, 4-36

users, 2-23

Delete Group for MxN
 Connection Group
 ONNS, 7-90

deprovision
 loopback on a port, 6-7

derived output timing, 8-26

DFI, 3-13

DIX frames, 10-23

DNI, 10-22

domain specific part
 See: DSP

Domain type, 7-8

double tagging, 10-29

DRI, 10-22

drop and continue, 10-22

DS3 violation monitoring
 mode, 6-15

DS3/EC-1 equipment
 protection, 5-47

DSP, 3-13

DSP format identifier
 See: DFI

duplex control, 5-32

DUR shelf, 5-2

.....

E E1 byte, 3-23

E2 byte, 3-23

ECI, 5-40, 5-42, 5-48
 ECI/155ME8, 5-41
 ECI/155MP8, 5-41
 ECI51/MP72, 5-48

electrical connection interface
 See: ECI

electrical interface type, 6-11

electrical interfaces, 5-2

electrical port units, 5-24

end system
 See: ES

ENNI Associated ASTN
 Connection List
 view for ONNS, 7-100

ENNI ONNS
 provision controlled plane
 service connections, 7-93

environmental alarms, 5-30

EP155 port units, 5-40, 5-43

EP51 port units, 5-47, 5-50

equipment protection
 CTL, 5-32
 DS3/EC-1, 5-47
 LOXC, 5-55
 STM-1E, 5-40, 5-42
 XC, 5-37

equipment protection group
 add, 6-59

equipment protection group
 information
 operate, 6-65
 retrieve, 6-56

- switch, [6-65](#)
- equipment protection groups
 - operate, [6-61](#)
 - release, [6-63](#)
 - switch, [6-61](#)
- equipment protection switch requests
 - clear, [6-63](#)
- ES, [3-2](#)
- Ethernet, [10-23](#)
 - Also see: *TransLAN*®
- Ethernet II, [10-23](#)
- expected trace display mode, [6-19](#), [6-33](#)
- expected trail trace format, [6-19](#), [6-32](#)
- expected trail trace out format, [6-17](#)
- expected trail trace out value, [6-17](#)
- expected trail trace value, [6-19](#), [6-32](#)
- external timing input, [8-2](#), [8-6](#), [8-23](#)
- external timing output, [8-2](#), [8-7](#)
- external timing output ports, [8-25](#)
- external timing references, [8-9](#), [8-30](#), [8-31](#)

F F1 byte, [3-23](#)

- far-end incoming path PM enable, [6-22](#)
- far-end line/MS PM enable, [6-22](#)
- far-end outgoing path PM enable, [6-22](#)

- far-end outgoing path SES PM threshold, [6-23](#)
- far-end path SES threshold, [6-23](#), [6-23](#), [6-35](#)
- far-end PM, [6-22](#), [6-27](#), [6-35](#)
- far-end VCG PM, [6-35](#)
- far-end vcg SES threshold, [6-35](#)
- FEC, [6-21](#)
- FEC type, [6-11](#)
- File Transfer, Access and Management (FTAM), [3-10](#)
- Filtering
 - filter ONNS NEs on Network Map, [7-32](#)
- fixed 20-byte NSAP address structure, [3-12](#)
- flexible part, [4-4](#), [4-9](#)
- ForceDNU, [6-20](#)
- forward error correction, [6-21](#)
- forward error correction scrambling polynomial, [6-21](#)
- frame format, [6-15](#)
- Free-running mode, [8-18](#)
- FTP/FTAM gateway, [3-20](#)

G G.703 interfaces, [3-23](#)

- gateway NE
 - See: GNE
- gateway network element
 - See: GNE
- generic framing procedure
 - See: GFP
- GFP, [10-23](#)
- Gigabit Ethernet port units, [5-24](#)
- GNE, [3-2](#), [3-19](#)

- Graphical layout
 - ONNS, [7-28](#)
 - GVRP, [10-30](#)

H hardware upgrade, [5-39](#)

- hazard statements
 - symbols, [1-7](#)
- higher-order cross-connections
 - add, [11-27](#)
 - change from ONNS to traditional mode, [11-41](#)
 - modify topology, [11-34](#)
 - roll, [11-46](#)
 - view, [11-12](#)
- holdover mode, [8-11](#), [8-18](#), [8-21](#)

I IDI, [3-13](#)

- IDP, [3-13](#)
- IEEE 802.3 MAC address, [3-13](#)
- in-progress transfers of NE generics
 - view list, [13-11](#)
- in-service hardware upgrade, [5-39](#)
- incoming line PM enable, [6-22](#)
- incoming line SES threshold, [6-23](#)
- incoming path SES threshold, [6-23](#)
- incoming PM enable, [6-22](#)
- inhibit
 - autonomous messages, [6-38](#)
- initial domain identifier
 - See: IDI

- initial domain part
 - See: IDP
- inloop, [5-29](#)
- inloop/facility loopback, [6-11](#)
- input membership, [6-30](#)
- interfaces
 - electrical, [5-2](#)
 - optical, [5-2](#)
- intermediate system
 - See: IS
- intermediate system to intermediate system
 - See: IS-IS
- IS, [3-2](#)
- IS routing information base
 - See: RIB
- IS-IS, [3-2](#)
- ISO DCC NSAP address
 - format, [3-12](#)
-
- L** LAN connectors, [3-17](#)
- LAN I/O-Panel, [3-17](#)
- LAPD
 - network_side mode, [3-15](#)
 - user_side mode, [3-15](#)
- LCAS hold-off time (ms), [6-30](#)
- LCAS mode, [6-30](#)
- LCAS wait to restore time (min), [6-31](#)
- LCN, [3-2](#)
- line build out, [6-15](#)
- line timing references, [8-10](#), [8-30](#), [8-30](#)
- link pass thru mode, [6-26](#)
- link state protocol data unit
 - See: LSP
- local communications network
 - See: LCN
- local cross-connect
 - See: LXC
- Locked mode, [8-18](#)
- login security information
 - modify, [2-9](#)
 - retrieve, [2-2](#)
- logins
 - create, [2-20](#)
 - delete, [2-23](#)
- loop, [6-6](#)
- loopback ports
 - view a list of loopback-enabled ports, [6-6](#)
- lower order cross-connection unit
 - See: LOXC
- lower order tributaries, [5-55](#)
- lower-order cross-connections
 - See: LOXC
 - add, [11-16](#)
 - modify topology, [11-30](#)
 - roll, [11-43](#)
 - view, [11-8](#)
- LOXC, [5-55](#), [5-55](#), [10-8](#)
 - equipment protection switching, [5-60](#)
- LOXC equipment protection, [5-55](#)
- LSP, [3-2](#)
- LXC, [5-2](#)
-
- M** MAC, [10-27](#)
- manage
 - NE database on management system, [12-3](#)
 - NE database on NE, [12-4](#)
 - NE generics on management system, [12-2](#)
 - NE generics on NEs, [12-2](#)
- manufacturers executable code
 - See: MEC
- master timing generator, [8-18](#)
- maximum NN crossconnect rate, [6-25](#)
- maximum switch capacity, [5-6](#)
- MDI, [5-30](#)
- MDI configuration
 - retrieve, [6-52](#)
 - set, [6-54](#)
- MDO, [5-30](#)
 - operate, [6-46](#)
 - release, [6-48](#)
 - switch off, [6-48](#)
 - switch on, [6-46](#)
- MDO configuration
 - retrieve, [6-42](#)
 - set, [6-44](#)
- MDO state
 - retrieve, [6-50](#)
- MEC, [12-5](#)
- memory stores, [12-5](#)
- MIB, [12-2](#)
 - clear, [12-3](#)
 - view list of backups stored on the management system, [13-28](#)
- minimum NN crossconnect rate, [6-25](#)

- miscellaneous discrete input
 - See: MDI
 - miscellaneous discrete output
 - See: MDO
 - Mixed plane service connections
 - provision, [7-56](#)
 - modify
 - 1+1 APS protection group, [11-82](#)
 - 1+1 MSP protection group, [11-71](#)
 - 1x1 APS protection group, [11-82](#)
 - 1x1 MSP protection group, [11-71](#)
 - 2-fiber BLSR protection group, [11-109](#)
 - 2-fiber MS-SPRing protection group, [11-91](#)
 - 4-fiber BLSR protection group, [11-118](#)
 - 4-fiber MS-SPRing protection group, [11-100](#)
 - cross-connection parameters, [11-38](#)
 - current user's password, [2-16](#)
 - current user's security information, [2-9](#)
 - DCC related parameters, [4-26](#)
 - DCC/EOW status information, [4-30](#)
 - higher-order cross-connection topology, [11-34](#)
 - lower-order cross-connection topology, [11-30](#)
 - NE date and time, [4-40](#)
 - OMS-to-NE connections, [4-9](#)
 - path protection group, [11-60](#)
 - port parameters, [6-9](#)
 - SNCP protection group, [11-60](#)
 - UPSR protection group, [11-60](#)
 - user security information, [2-12](#)
 - Modify Route
 - Concepts for ONNS, [7-26](#)
 - Modify route
 - ONNS connections, [7-85](#)
 - MS-SPRing, [10-17](#), [11-88](#), [11-89](#), [11-97](#)
 - LO-VC access, [10-9](#)
 - self healing rings, [10-19](#)
 - transoceanic protocol, [10-4](#)
 - MSP, [10-4](#), [10-15](#), [11-66](#), [11-67](#), [11-69](#)
 - 1+1, [10-15](#)
 - 1:1, [10-15](#)
 - MSP protection switches
 - operate, [11-75](#)
 - Multiplex section network connections
 - provision ASTN port parameters, [7-41](#)
 - multipoint mode, [10-27](#)
 - MxN Connection Group
 - adding connections to an existing, [7-21](#)
 - deleting connections to an existing, [7-22](#)
 - MxN Connections
 - add to existing MxN Connection Group, [7-79](#)
 - Associate with Controlled planes, [7-23](#)
 - MxN protected
 - database maintenance, [7-20](#)
 - MxN protection
 - connection discovery, [7-20](#)
 - Connection Group page, [7-20](#)
 - MxN Service Group network connections
 - add ONNS, [7-72](#)
-
- N** name to address translation, [3-18](#)
 - NE
 - DCC channel selection, [3-14](#)
 - delete, [4-19](#)
 - name, [3-3](#), [4-4](#)
 - type, [4-4](#)
 - NE database, [12-2](#)
 - Also see: MIB
 - backup onto the management system, [13-37](#)
 - manage on management system, [12-3](#)
 - manage on NE, [12-4](#)
 - restore from management system to an NE, [13-39](#)
 - view list of versions stored on the management system, [13-28](#)
 - NE database versions
 - view list of versions stored on an NE, [13-31](#)

- NE database versions stored on the management system
 - view list, [13-28](#)
- NE date
 - modify, [4-40](#)
 - view, [4-38](#)
- NE generics
 - abort in progress transfer, [13-12](#)
 - activate, [12-3](#), [13-17](#)
 - add to the management system, [13-4](#)
 - commit, [12-3](#), [13-20](#)
 - delete from the management system, [13-5](#)
 - manage on management system, [12-2](#)
 - manage on NE, [12-2](#)
 - revert, [12-3](#), [13-22](#)
 - schedule activation, [13-24](#)
 - schedule transfer from management system to NE, [13-8](#)
 - transfer from the management system to an NE, [13-6](#)
 - view list of in-progress transfers, [13-11](#)
- NE generics stored on an NE
 - view list, [13-15](#)
- NE generics stored on the management system
 - view list, [13-3](#)
- NE management
 - ONNS, [7-6](#)
- NE name, [4-4](#)
- NE software
 - generics, [12-2](#)
 - management, [12-2](#)
 - upgrade, [12-5](#)
- NE time
 - modify, [4-40](#)
 - view, [4-38](#)
- NE type, [4-4](#)
- near-end line/MS PM, [6-22](#)
- near-end line/MS SES threshold, [6-23](#)
- near-end path SES threshold, [6-22](#), [6-35](#)
- near-end PM, [6-22](#), [6-27](#), [6-35](#)
- near-end VCG PM, [6-35](#)
- near-end vcg SES threshold, [6-35](#)
- NET, [3-3](#), [3-12](#)
- Net Comm Grp, [4-4](#), [4-9](#)
- Network Connections
 - partial database synchronization, [7-101](#)
- Network elements (NEs)
 - database synchronization, [7-101](#)
- network entity title
 - See: NET
- network interface, [6-24](#), [6-36](#)
- Network interface type, [7-8](#)
- network service access point
 - See: NSAP
- network service provider
 - See: NSP
- NSAP, [3-2](#), [3-3](#), [3-4](#), [4-4](#)
 - address structures, [3-12](#)
 - fixed 20-byte address structure, [3-12](#)
 - formats, [3-12](#)
- NSAP address, [4-4](#), [4-9](#)
- NSP, [3-13](#)
-
- O Ch, [6-14](#)
- OMS to NE communications
 - ONNS, [7-6](#)
- OMS-to-NE connections, [3-19](#)
 - activate, [4-15](#)
 - add, [4-4](#)
 - deactivate, [4-13](#)
 - definition, [3-19](#)
 - delete, [4-17](#)
 - modify, [4-9](#)
 - view list, [4-3](#)
- ONNS, [7-13](#), [7-19](#), [7-24](#), [11-41](#)
 - Cancel Group for MxN Connection Group, [7-92](#)
 - category, [7-13](#), [7-19](#), [7-24](#)
 - concepts, [7-3](#)
 - connection parameters, [7-11](#)
 - control plan path state, [7-28](#)
 - database synchronization, [7-30](#)
 - DB Delete Group for MxN Connection Group, [7-91](#)
 - definition, [7-3](#)
 - Delete Group for MxN Connection Group, [7-90](#)
 - filter NEs on the Network Map, [7-32](#)
 - graphical layout, [7-28](#)
 - managing path states, [7-28](#)
 - Modify Route Concepts, [7-26](#)

- NE icon, [7-7](#)
- NE management, [7-6](#)
- NOCON&SETUPFL state, [7-5](#)
- OMS to NE communications, [7-6](#)
- OUC provisioning, [7-15](#)
- port provisioning, [7-8](#)
- Provision, [7-1](#)
- provision controlled plane service connections, [7-48](#)
- provision controlled plane service connections for OUC Planned or Local Design Step, [7-48](#)
- provision mixed plane service connections, [7-56](#)
- provision mixed plane service connections for OUC Planned or Local Design Step, [7-56](#)
- provision OUC connections for In Effect steps, [7-64](#)
- query ASTN Capacity Utilization, [7-44](#)
- Rearrange, [7-26](#)
- rearranged connections on graphical layout, [7-29](#)
- route discovery on graphical layout, [7-29](#)
- routing constraints, [7-15](#), [7-20](#), [7-25](#)
- routing modes, [7-20](#)
- supported rates, [7-11](#)
- tandem connections on graphical layout, [7-29](#)
- view ASTN Capacity Utilization, [7-44](#)
- ONNS connection groups
 - view, [7-43](#)
- ONNS connection parameters, [7-11](#)
 - category, [7-13](#), [7-19](#), [7-24](#)
- ONNS Connections
 - adding OUC to existing connection, [7-85](#)
 - modify route, [7-85](#)
 - rearrange, [7-85](#)
- ONNS Infrastructure connection provisioning, [7-24](#)
- ONNS multiplex section connection provisioning, [7-11](#)
- ONNS multiplex section connections, [7-35](#)
- ONNS MxN Connection Group
 - add another MxN connection, [7-79](#)
- ONNS MxN Connection Protection Group, [7-4](#)
- ONNS MxN Service Group connection provisioning, [7-19](#)
- ONNS MxN Service Group Network Connections
 - add, [7-72](#)
- ONNS NE icon, [7-7](#)
- ONNS NEs
 - filter on Network Map, [7-32](#)
- ONNS port parameters
 - domain type, [7-8](#)
 - network interface type, [7-8](#)
- ONNS service connection provisioning, [7-13](#)
- ONNS to UPSR/SNCP constructs
 - add, [11-54](#)
- delete, [11-56](#)
- retrieve, [11-52](#)
- operate
 - 2-fiber BLSR protection switch, [11-113](#)
 - 2-fiber MS-SPRing protection switch, [11-95](#)
 - 4-fiber BLSR protection switch, [11-122](#)
 - 4-fiber MS-SPRing protection switch, [11-104](#)
 - APS protection switch, [11-86](#)
 - equipment protection group, [6-61](#)
 - equipment protection group information, [6-65](#)
 - MDO, [6-46](#)
 - MSP protection switch, [11-75](#)
 - path protection group switch, [11-62](#)
 - SNCP protection group switch, [11-62](#)
 - SNCP VC-4 protection group switch, [11-64](#)
 - synchronization switch (MOD), [9-20](#)
 - synchronization switch (OUTREF), [9-26](#)
 - synchronization switch (REF), [9-24](#)
 - UPSR protection group switch, [11-62](#)
- Operator ID, [3-13](#)
- OPLB parent board, [5-18](#)
- optical interface modules, [5-12](#), [5-22](#), [5-23](#), [5-23](#), [5-23](#), [5-23](#)
- optical interfaces, [5-2](#), [10-4](#)

- optical output enable, [6-14](#)
 - orderwire, [3-23](#)
 - OSI protocol stack, [3-10](#)
 - OSI-DCN network, [3-6](#)
 - OTN client port, [6-14](#)
 - OUC
 - adding to existing ONNS connection, [7-85](#)
 - ONNS provisioning, [7-15](#)
 - OUC connection
 - provision for connections In Effect, [7-64](#)
 - OUC provisioning
 - for Planned and Local Design Steps, [7-48](#), [7-56](#)
 - outgoing path SES PM threshold, [6-23](#)
 - outgoing PM enable, [6-22](#)
 - outgoing Z0 byte, [6-14](#)
 - outloop, [5-29](#)
 - outloop/terminal loopback, [6-12](#)
 - output membership, [6-30](#)
-
- P** password (current user)
 - modify, [2-16](#)
 - path protection, [10-13](#)
 - path protection groups
 - modify, [11-60](#)
 - operate switch, [11-62](#)
 - view list, [11-58](#)
 - Path state
 - ONNS, [7-28](#)
 - PDI-P switching, [6-15](#)
 - PDU, [3-13](#)
 - performance monitoring, [6-27](#), [6-35](#)
 - physical TCA profile name, [6-24](#)
 - PM line/MS far-end SES threshold, [6-23](#)
 - PM section/RS near-end out SES threshold, [6-23](#)
 - PM section/RS near-end SES threshold, [6-23](#)
 - pointer justification event PM enable, [6-22](#)
 - port address/port alias tool, [5-28](#)
 - port mode, [6-11](#), [6-26](#), [6-30](#)
 - Port Parameter Provisioning
 - ONNS, [7-8](#)
 - Port parameters
 - domain type, [7-8](#)
 - network interface type, [7-8](#)
 - Port path cost, [6-28](#)
 - port path cost, [6-37](#)
 - Port provisioning
 - ONNS, [7-8](#)
 - port translation, [5-28](#)
 - port units
 - electrical, [5-24](#)
 - Gigabit Ethernet, [5-24](#)
 - optical, 10-Gbps, [5-21](#)
 - optical, 155-Mbps, [5-23](#)
 - optical, 2.5-Gbps, [5-22](#)
 - optical, 622-Mbps, [5-23](#)
 - ports
 - add, [5-26](#)
 - definition, [5-26](#)
 - delete, [5-26](#)
 - deprovision loopback, [6-7](#)
 - external timing output, [8-25](#)
 - ID format, [5-28](#)
 - logical, [5-26](#)
 - modify DCC/EOW status information, [4-30](#)
 - modify parameters, [6-9](#)
 - names, [5-27](#)
 - Ports
 - ONNS port provisioning, [7-8](#)
 - ONNS ports, [7-8](#)
 - ports
 - physical, [5-26](#)
 - port address/port alias tool, [5-28](#)
 - provision loopback, [6-7](#)
 - rates, [5-26](#)
 - retrieve DCC/EOW status information, [4-28](#)
 - supported rates, [5-26](#)
 - supported types, [5-26](#)
 - types, [5-26](#)
 - view a list of logical ports, [6-5](#)
 - view a list of loopback-enabled ports, [6-6](#)
 - view a list of physical ports, [6-4](#)
 - preemptible protection access, [10-15](#)
 - probable causes
 - assigned to an MDO, [6-42](#), [6-44](#)
-

assigned to set
synchronization - aexternal
timing input, [9-9](#)

assigned to set
synchronization - assigned
timing reference, [9-7](#)

assigned to set
synchronization - external
timing output, [9-11](#)

assigned to set
synchronization - system
timing, [9-14](#)

assigned to synchronization,
[9-2](#)

assigned to synchronization
switch (MOD), [9-18](#), [9-20](#)

assigned to synchronization
switch (OUTREF), [9-22](#),
[9-26](#)

assigned to synchronization
switch (REF), [9-16](#), [9-24](#)

protection types, [7-13](#), [7-19](#),
[7-24](#)

Protection types
ONNS, [7-13](#), [7-19](#), [7-24](#)

protocol data units
See: PDU

Protocol stacks, [3-10](#)

Provision
controlled plane service
connection, [7-48](#), [7-93](#)

provision
loopback on a port, [6-7](#)

Provision
Mixed plane service
connection, [7-56](#)

OUC connection for in
Effect steps, [7-64](#)

Provision ASTN port
parameters, [7-33](#)

Provision ONNS multiplex
section connection, [7-35](#)

provisioned flow control mode,
[6-26](#)

provisioned pause mode, [6-26](#)

.....

R RD, [3-13](#)

Rearrange
ONNS, [7-26](#)
ONNS connections, [7-85](#)

REI mode, [6-21](#)

release
equipment protection group,
[6-63](#)
MDO, [6-48](#)
synchronization switch
(MOD), [9-18](#)
synchronization switch
(OUTREF), [9-22](#)
synchronization switch
(REF), [9-16](#)

remote NE
See: RNE

reported payload type, [6-24](#)

restore
NE database version from
the management system to
an NE, [13-39](#)

retrieve
current user's security
information, [2-2](#)
DCC related parameters,
[4-23](#)
DCC/EOW status
information, [4-28](#)
equipment protection group
information, [6-56](#)

login security information,
[2-2](#)

MDI configuration, [6-52](#)

MDO configuration, [6-42](#)

MDO state, [6-50](#)

ONNS to UPSR/SNCP
constructs, [11-52](#)
synchronization, [9-2](#)
user security information,
[2-5](#)

revert an NE generic on an NE,
[13-22](#)

revertive mode, [8-21](#)

RIB, [3-2](#)

ring A node ID, [6-15](#)

ring Z node ID, [6-15](#)

RNE, [3-19](#)

roll
higher-order
cross-connection, [11-46](#)
lower-order
cross-connection, [11-43](#)

Routing constraints
ONNS, [7-15](#), [7-20](#), [7-25](#)

routing domain
See: RD

Routing modes
ONNS, [7-20](#)

routing table, [3-18](#)

rSTP, [10-30](#)

.....

S Sa bit location, [8-23](#)

schedule
backup NE database
versions onto the
management system, [13-37](#)

- NE generic activation, [13-24](#)
- transfer of an NE generic from management system to an NE, [13-8](#)
- scheduled tasks
 - software management, [12-4](#)
- section/RS out PM enable, [6-22](#)
- section/RS PM enable, [6-22](#)
- SEL, [3-13](#)
- selector field
 - See: SEL
- service condition, [6-12](#), [6-26](#)
- set
 - MDI configuration, [6-54](#)
 - MDO configuration, [6-44](#)
 - synchronization - assigned timing reference, [9-7](#)
 - synchronization - external timing input, [9-9](#)
 - synchronization - external timing output, [9-11](#)
 - synchronization - system timing, [9-14](#)
- shared risk link group, [6-25](#)
- shortest path first algorithm, [3-4](#)
- signal degrade threshold, [6-21](#), [6-27](#), [6-34](#)
- signal degrade/signal fail mode, [6-20](#), [6-34](#)
- signal fail threshold, [6-21](#), [6-27](#), [6-34](#)
- signal label mismatch detection mode, [6-19](#)
- simplex control, [5-32](#)
- slave timing generator, [8-18](#)
- slots
 - universal, [5-3](#)
 - view list, [6-3](#)
- SNC/I, [10-13](#)
- SNC/N, [10-13](#)
- SNCP, [11-58](#)
 - SNC/I, [10-13](#)
 - SNC/N, [10-13](#)
- SNCP protection groups
 - modify, [11-60](#)
 - operate switch, [11-62](#)
 - view list, [11-58](#)
- SNCP VC-4 protection groups
 - operate switch, [11-64](#)
 - view, [11-64](#)
- software
 - trial phase, [12-3](#), [13-20](#), [13-22](#)
- Software download, [3-10](#)
- software management, [12-2](#)
- software management tasks
 - schedule, [12-4](#)
- SSM, [8-2](#), [8-20](#), [8-23](#), [8-28](#)
- static routing table, [3-18](#)
- station clock input, [8-2](#), [8-6](#)
- station clock output, [8-2](#), [8-7](#)
- STM-1E equipment protection, [5-40](#), [5-42](#)
- STP, [10-30](#)
- STP port priority, [6-28](#), [6-37](#)
- supported ports, [5-26](#)
- switch
 - equipment protection group, [6-61](#)
 - equipment protection group information, [6-65](#)
 - switch off
 - MDO, [6-48](#)
 - switch on
 - MDO, [6-46](#)
 - symbols
 - in hazard statements, [1-7](#)
 - synchronization
 - retrieve, [9-2](#)
 - synchronization - assigned timing reference
 - set, [9-7](#)
 - synchronization - external timing input
 - set, [9-9](#)
 - synchronization - external timing output
 - set, [9-11](#)
 - synchronization - system timing
 - set, [9-14](#)
 - synchronization status message (SSM), [8-6](#)
 - synchronization switch (MOD)
 - operate, [9-20](#)
 - release, [9-18](#)
 - synchronization switch (OUTREF)
 - operate, [9-26](#)
 - release, [9-16](#), [9-22](#)
 - synchronization switch (REF)
 - operate, [9-24](#)
 - system configurations, [5-2](#)
 - system ID, [3-13](#)
 - System ID, [4-4](#)
 - system ID, [4-9](#)

- system identifier
 - See: system ID
- system timing, [8-35](#), [8-35](#)
- system timing operational modes, [8-18](#)
- system timing reference, [8-30](#)
-
- T** Tandem Connection
 - Associate with ONNS controlled plane, [7-47](#)
- Tandem network connections, [7-21](#)
 - on graphical layout, [7-29](#)
- Tandem Network Connections
 - ONNS, [7-4](#)
- target identifier
 - See: TID
- TARP, [3-18](#)
- TCA profile name, [6-24](#), [6-28](#), [6-36](#)
- TCA reset mode, [6-22](#), [6-27](#), [6-35](#)
- terminate
 - user sessions, [2-18](#)
- test loops, [5-29](#)
- TID, [3-3](#), [3-18](#), [4-4](#)
- TID to NSAP address translation, [3-18](#)
- time
 - modify, [4-40](#)
 - view, [4-38](#)
- timing generator, [8-11](#), [8-18](#), [8-21](#)
- timing input signal format, [8-23](#)
- timing operational modes, [8-18](#)
- timing protection, [8-21](#)
- timing reference protection switching, [8-21](#)
- timing references, [8-9](#)
- timing units, [5-21](#)
- TL1, [3-4](#)
- trail trace mismatch detection mode, [6-19](#), [6-33](#)
- trail trace out mismatch detection mode, [6-17](#)
- transaction language 1
 - See: TL1
- transfer an NE generic from the management system to an NE, [13-6](#)
- TransLAN*[®]
 - overview, [10-23](#)
- transmission interfaces, [10-4](#)
- transmitted interface standard, [6-11](#)
- transmitted trace display mode, [6-18](#), [6-32](#)
- transmitted trail trace format, [6-18](#), [6-31](#)
- transmitted trail trace value, [6-18](#), [6-32](#)
- transparent alarm profile name, [6-34](#)
- transparent DCC
 - cross-connections, [3-14](#)
 - delete, [4-36](#)
 - view list, [4-32](#)
- transparent DDcross-connections
 - add, [4-34](#)
- tributary input signal rate, [6-14](#)
- tributary mode, [6-13](#)
- tributary output signal rate, [6-14](#)
- trunking, [10-27](#)
-
- U** UITS, [3-15](#)
- unacknowledged information transfer service
 - See: UITS
- unconnected output
 - maintenance signal, [6-15](#)
- UNI client node identity, [6-25](#), [6-37](#)
- UNI network logical port identifier, [6-25](#), [6-37](#)
- UNI network TNA address, [6-25](#), [6-37](#)
- UNI network TNA type, [6-25](#), [6-36](#)
- universal slots, [5-3](#)
- upgrade
 - NE software, [12-5](#)
- UPSR, [10-13](#), [11-58](#)
- UPSR protection groups
 - modify, [11-60](#)
 - operate switch, [11-62](#)
 - view list, [11-58](#)
- user bytes, [3-23](#)
- User Network Interface
 - ONNS network interface type, [7-8](#)
- user security information
 - modify, [2-12](#)
 - retrieve, [2-5](#)
- user sessions
 - terminate, [2-18](#)
- USERBIO1 ... USERBIO6, [3-23](#)
- users
 - create, [2-20](#)

- delete, [2-23](#)
-
- V** V.11 interfaces, [3-23](#)
- VCG, [10-27](#)
- view
 - cross-connections, [11-4](#)
 - higher-order
 - cross-connections, [11-12](#)
 - list of 1+1 APS protection groups, [11-77](#)
 - list of 1+1 MSP protection groups, [11-66](#)
 - list of 1x1 APS protection groups, [11-77](#)
 - list of 1x1 MSP protection groups, [11-66](#)
 - list of 2-fiber BLSR protection groups, [11-106](#)
 - list of 2-fiber MS-SPRing protection groups, [11-88](#)
 - list of 4-fiber BLSR protection groups, [11-115](#)
 - list of 4-fiber MS-SPRing protection groups, [11-97](#)
 - list of in-progress transfers of NE generics, [13-11](#)
 - list of MIB backups stored on the management system, [13-28](#)
 - list of NE database versions stored on an NE, [13-31](#)
 - list of NE database versions stored on the management system, [13-28](#)
 - list of NE generics stored on an NE, [13-15](#)
 - list of NE generics stored on the management system, [13-3](#)
 - list of OMS-to-NE connections, [4-3](#)
 - list of path protection groups, [11-58](#)
 - list of slots, [6-3](#)
 - list of SNCP protection groups, [11-58](#)
 - list of transparent DCC cross-connections, [4-32](#)
 - list of UPSR protection groups, [11-58](#)
 - lower-order
 - cross-connections, [11-8](#)
 - NE date and time, [4-38](#)
 - SNCP VC-4 protection group, [11-64](#)
- View Associated MxN Connection List
 - ONNS, [7-46](#)
- View ENNI Associated ASTN Connection List
 - ONNS, [7-100](#)
- View ONNS Connections Groups, [7-43](#)
- VLAN, [10-27](#)
- VLAN tagging, [10-27](#)
- VLAN trunking, [10-27](#)
- VPN tagging, [10-29](#)
-
- W** wait-to-restore time
 - See: WTR
- WAN, [10-27](#)
- WTR, [8-21](#), [8-35](#)
-
- X** XC equipment protection, [5-37](#)
- XC equipment protection switching, [5-38](#)