LambdaUnite™ **MultiService Switch (MSS)**

Release 2.0

Alarm Messages and Trouble Clearing Guide

Notice

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

Mandatory customer information

Trademarks

These trademarks are used in this manual:

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

CompactFlash is a trademark of SanDisk Corporation

LambdaUnite is a trademark of Lucent Technologies.

Navis is a trademark of Lucent Technologies.

SanDisk is a registered trademark of SanDisk Corporation

WaveStar is a registered trademark of Lucent Technologies.

Windows is a registered trademark of Microsoft Corporation

Ordering information

The order number of this document is 365-374-057 (Issue a).

Support

Technical support

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

Information product support

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

Lucent Technologies

Lucent Technologies values your comments!

Lucent Technologies Bell Labs Innovations

LambdaUnite™ MultiService Switch (MSS)
Release 2.0
Alarm Messages and Trouble Clearing Guide
365-374-057   Issue a   January 2002

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

1.   Was the information product:

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

Please provide any additional comments:

_____
_____

2.   Please rate the effectiveness of this information product:

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

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

_____
_____

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

_____
_____

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

_____
_____

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

Name: _____   Date: _____

Company/organization: _____   Telephone number: _____

Address: _____

Email address: _____   Job function: _____

If you choose to complete this form online, go to http://www.lucent-info.com/comments
Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

LambdaUnite™ MultiService Switch (MSS)
Release 2.0
Alarm Messages and Trouble Clearing Guide
365-374-057   Issue a   January 2002

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

1.   Was the information product:

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

Please provide any additional comments:

_____
_____

2.   Please rate the effectiveness of this information product:

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

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

_____
_____

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

_____
_____

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

_____
_____

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

Name: _____   Date: _____

Company/organization: _____   Telephone number: _____

Address: _____

Email address: _____   Job function: _____

If you choose to complete this form online, go to http://www.lucent-info.com/comments
Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com

Contents

2   Alarm messages

Equipment alarms

Ethernet alarms

Linear protection switching alarms

Path-related transmission alarms

3   Trouble clearing

4   Supporting procedures

About this information product

Purpose   This *Alarm Messages and Trouble Clearing Guide* (AMTCG) provides information on the alarm messages which can be generated by the *LambdaUnite*™ MSS network elements. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.

Reason for reissue   This is the first issue of the *LambdaUnite MSS Alarm Messages and Trouble Clearing Guide*.

Safety labels   Please refer to chapter 1 ("Safety").

Intended audience   The intended audience of this *Alarm Messages and Trouble Clearing Guide* primarily consists of people who are responsible for the maintenance of network elements and for the supervision of transmission operation.

Training of personnel

Working on the complex equipments and systems described in this guide requires special training of the personnel. For more information, please also read chapter 1 ("Safety").

**How to use this
information product**

Each chapter of this manual treats a specific aspect of the system and can be regarded as an independent description. This ensures that the reader can inform himself according to his special needs. This also means that the manual provides more information than needed by many of the readers. Before you start reading the manual, it is therefore necessary to assess which aspects or chapters will cover the individual area of interest.

The following table briefly describes the type of information found in each chapter.

Chapter	Title	Description
Preface	About this information product	This chapter • describes the guide's purpose, intended audience, and organization • lists related documentation • explains how to comment on this document
1	Safety	This chapter contains a series of very important safety instructions concerning the handling of *LambdaUnite* MSS network elements.
2	Alarm messages	This chapter contains descriptions of the alarms which can be generated by the *LambdaUnite* MSS network elements.
3	Trouble clearing	This chapter describes the measures to be taken for localising and clearing faults on the *LambdaUnite* MSS network elements. It is based on the network element alarms that can be generated.
4	Supporting procedures	This chapter
5	Glossary	Defines telecommunication terms and expands common telecommunication abbreviations and acronyms
6	Index	Lists specific subjects and their corresponding page numbers

Conventions used

The following conventions are used throughout this *Alarm Messages and Trouble Clearing Guide*:

Numbering

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

Cross references

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

Keyword blocks

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

Typographical conventions

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

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

  - **Provision…**, **Delete**, **Apply**, **Close**, *OK* (pushbuttons)

  - **Provision Timing/Sync** (window title)

  - **View Equipment Details…** (menu option)

  - **Administration** → **Security** → **User Provisioning…** (path for invoking a window)

- Filenames and system path information
  These are examples of filenames and system path information:

  - *setup.exe*

  - *C:\Program Files\Lucent Technologies*

- Keyboard entries
  These are examples of keyboard entries:

  - **F1**, **Esc X**, **Alt-F**, **Ctrl-D**, **Ctrl-Alt-Del** (simple keyboard entries)

A hyphen between two keys means that both keys have to be pressed simultaneously. Otherwise, a single key has to be pressed, or several keys have to be pressed in sequence.

- `copy abc xyz` (command)
  A complete command has to be entered.

- Alarms and error messages
  These are examples of alarms and error messages:

  - `Loss of Signal`

  - `Circuit Pack Failure`

  - `Ring Incomplete`

Abbreviations

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

Related documentation

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

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

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

- User Operations Guide
  The *LambdaUnite* MSS User Operations Guide (UOG) 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 ManualProduct CIT.

- Alarm Messages and Trouble Clearing Guide

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

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

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

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

Document Number	Title
109149849 (365-371-026)	*LambdaUnite* MultiService Switch (MSS) Release 1.0 Safety Guide
109192385 (365-374-053)	*LambdaUnite* MultiService Switch (MSS) Release 2.0 Applications, Planning, and Ordering Guide
109192393 (365-374-055)	*LambdaUnite* MultiService Switch (MSS) Release 2.0 User Operations Guide
109192377 (365-374-057)	*LambdaUnite* MultiService Switch (MSS) Release 2.0 Alarm Messages and Trouble Clearing Guide
109192401 (365-374-059)	*LambdaUnite* MultiService Switch (MSS) Release 2.0 Installation Guide

Document Number	Title
109192419 (365-374-061)	*LambdaUnite* MultiService Switch (MSS) Release 2.0 Operations System Engineering Guide
109192369 (365-374-063)	*Navis*™ Optical Element Management System (EMS) Release 7.0 Provisioning Guide for *LambdaUnite* MSS
109088666 (365-374-066)	CD-ROM Documentation *LambdaUnite* MultiService Switch (MSS) Release 2.0 (all manuals on one CD-ROM)

The following additional documents can be helpful for planning and ordering:

- Ordering & Information Drawings (ED8C933–10)
- Cable Ordering & Information Drawings (ED8C933–11)

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

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

Customer comment form

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

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

Lucent Technologies Network Systems GmbH

Customer Training and Information Products (CTIP-SDH)

Lucent Technologies

Thurn- und-Taxis-Str. 10

90327 Nürnberg, Germany

Fax: +49 911 526 3545

1 Safety

Overview

Purpose

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

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

Potential sources of danger

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

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

- opening of housings or equipment covers,

- manipulation of any kind within the equipment, even if it has been disconnected from the power supply,

- disconnection of optical or electrical connections,

through possible contact with the following:

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

Contents

General notes on safety

Overview

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

Contents

Structure of safety instructions

General structure   All safety instructions include a ***warning symbol*** and a ***signal word*** that classify the danger, and a ***text block*** that contains descriptions of the type and cause of the danger, the consequences of ignoring the safety instruction and the measures that can be taken to minimise the danger.

Example:

⚠ **DANGER**

Arcing on removing or inserting a live power supply plug.

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

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

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

DANGER   Serious injury is definite or likely.

WARNING   Serious injury is possible.

CAUTION   Minor injury is definite, likely or possible, or material damage to the product or in the product environment is definite or likely.

Warning symbols   These warning symbols are defined for safety instructions:

1	2	3	4	5	6

7	8	9	10	11	12
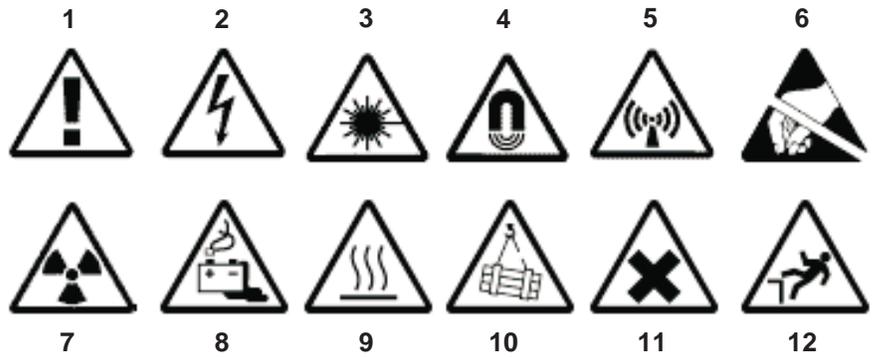
Legend:

1   General warning of danger

2   Electric shock

3   Hazard of laser radiation

4   Magnetic hazard

5   Electromagnetic radiation

6   Components sensitive to electrostatic discharge (ESD)

7   Radioactivity

8   Hazard caused by batteries

9   Hot surface

10   Heavy load

11   Unhealthy, irritating substance

12   Hazard of falling

Basic safety aspects

General safety requirements

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

- Transport, storage and operation of the system must be under the *permissible conditions only*.
  See accompanying documentation and information on the system.

- Installation, configuration and disassembly must be carried out only by *expert personnel* and *with reference to the respective documentation*.
  Due to the complexity of the system, the personnel requires *special training*.

- The system must be operated by *expert and authorised users only*.
  The user must operate the system only after having *read and understood* this chapter on safety and the parts of the documentation relevant to operation. For complex systems, additional training is recommended. Any obligatory training for operating and service personnel must be carried out and documented.

- The system must not be operated unless it is in perfect working order.
  Any faults and errors that might affect safety must be reported *immediately* by the user to a person in responsibility.

- The system must be operated only with the connections and under the environmental conditions as described in the documentation.

- Any conversions or changes to the system or parts of the system (including the software) must be carried out by qualified Lucent Technologies personnel or by expert personnel authorised by Lucent Technologies.
  All changes carried out by other persons lead to a *complete exemption from liability*.
  No components/spare parts must be used other than those recommended by the manufacturer and those listed in the procurement documents.

- The removal or disabling of safety facilities, the clearing of faults and errors, and the maintenance of the equipment must be carried out by *specially qualified personnel only*.

The respective parts of the documentation must be strictly observed. The documentation must also be consulted during the selection of measuring and test equipment.

- Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived.

- Non-system software is used at one's **own risk**. The use/installation of non-system software can adversely affect the normal functioning of the system.

- Only use **tested and virus-free** data carriers (floppy disks, streamer tapes, …).

Summary of important safety instructions

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

- This equipment is to be installed only in **Restricted Access Areas** in business and customer premises.
  Applications in accordance with Articles 110-16, 110-17 and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other installations exempt from the enforcement of the National Electrical Code may be engineered according to the accepted practices of the local telecommunications utility.

- This product should only be operated from the type of power source indicated on the marking label.

- This equipment must be provided with a readily accessible disconnect device as part of the building installation.

- Disconnect up to four (4) power supply connections when removing power from the system.

- Installation must include an independent frame ground drop to the building ground. Refer to the *LambdaUnite MSS Installation Guide*.

- For information on proper mounting instructions, consult the *LambdaUnite MSS Installation Guide*.

- Install only equipment identified in the *LambdaUnite MSS Installation Guide* provided with this product. Use of other equipment may result in improper connection of circuitry leading to fire or injury to persons.

- To reduce the risk of electrical shock, do not disassemble this product. Installation and service should be performed by trained personnel only. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electrical shock when the unit is subsequently used.

- Slots and openings in this product are provided for ventilation. To protect the product from overheating, these openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.

- Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short-out parts that could result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.

- CAUTION: This equipment is designed to permit the connection of the grounded conductor of the DC supply circuit to the grounding conductor at the equipment.

  1. This equipment shall be connected directly to the DC supply system grounding electrode conductor or to a bonding jumper from a grounding terminal bar or bus to which the DC supply system grounding electrode conductor is connected.

  2. This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system shall not be grounded elsewhere.

  3. The DC supply source is to be located within the same premises as this equipment.

  4. There shall be no switching or disconnection devices in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.

CAUTION

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

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

□

Specific safety areas

Overview

....

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

Contents

□

....

Laser safety

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

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

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

⚠ **DANGER**

INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.
Avoid direct exposure to beam.
Do not view beam directly with optical instruments.

CAUTION

INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.
Do not stare into the beam or view directly with optical instruments.

Class 1 Laser Product

⚠ DANGER
INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED
Avoid direct exposure to beam
Do not view beam directly with optical instruments

CAUTION
INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED
Do not stare into the beam or view directly with optical instruments.

Class 1 Laser Product

Potential sources of danger

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

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

Laser classes

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

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

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

Laser safety instructions

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

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

- Ensure that the optical source is switched off before disconnecting optical fiber connectors.

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

⚠ CAUTION

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

☐

Optical circuit pack specifications

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

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

Notes:

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

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

☐

Laser product classification

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

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

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

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

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

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

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

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

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

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

---

3.   Class 3B requires strict engineering controls.

4.   Classification is under single fault conditions.

FDA/CDRH laser classification

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

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

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

IEC laser classification

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

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

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

Hazard level assignment

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

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

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

Classification of optical telecommunication equipment

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

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

Electrostatic discharge

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

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

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

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

- Wear working garment made of 100% cotton to avoid
  electrostatic charging.

- Touch the circuit packs at the edges or the insertion and removal
  facilities only.

- Ensure that the rack is grounded.

- Wear conductively connected wrist straps and connect them to
  the rack ESP bonding point.

- Work in an area which is protected against electrostatic
  discharge. Use conducting floor and bench mats which are
  conductively connected to the rack ESP bonding point.

- Conductively connect all test equipment and trolleys to the rack
  ESP bonding point.

- Store and ship circuit packs and components in their shipping packing. Circuit packs and components must be packed and unpacked only at workplaces suitably protected against build-up of charge.

- Whenever possible, maintain the relative humidity of air above 20%.

□

Safety requirements in specific deployment phases

Overview

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

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

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

☐

Lucent Technologies

Transportation

Weight

⚠️ **WARNING**

Risk of injury due to unsecured shelf.

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

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

Packaging

⚠️ **CAUTION**

Adverse effect on operation due to incorrect packaging.

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

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

Climatic conditions

⚠ **CAUTION**

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

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

Climatic limits for transportation and storage

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

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

The following climatogram visualizes these climatic limits:
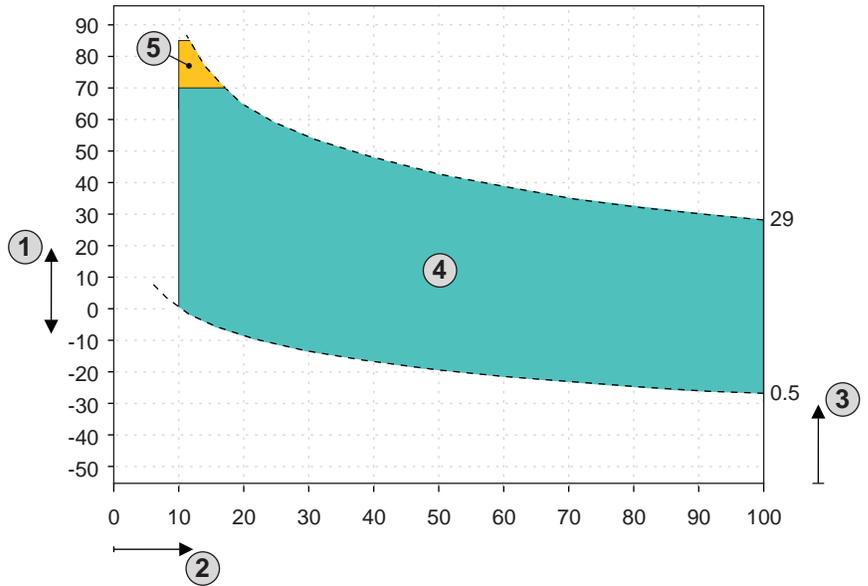
Legend:

1   Air temperature [°C]

2   Relative humidity [%]

3   Absolute humidity [g/m^3]. The dashed curves specify a constant
     absolute humidity of 0.5 g/m^3 or 29 g/m^3, respectively.

4   Permissible range for transportation and storage of *LambdaUnite*
     MSS systems.

5   Exceptional conditions, permissible for a short duration only.

□

Storage

....

Weight

⚠️ **WARNING**

Risk of injury due to unsecured shelf.

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

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

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Packaging

....

1 - 2 4   **Lucent Technologies**   365-374-057
Issue a, January 2002

⚠ **CAUTION**

Adverse effect on operation due to incorrect packaging.

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

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

Climatic conditions

⚠ **CAUTION**

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

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

□

....

365-374-057   **Lucent Technologies**   1 - 2 5
Issue a, January 2002

Installation

....

Weight

⚠ **WARNING**

Risk of injury due to unsecured shelf.

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

At least two persons are required for lifting the shelf.

Laser warning labels

⚠ **WARNING**

Ineffectiveness of laser warning labels if removed or concealed.

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

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

Electrostatic discharge (ESD)

....

1 - 2 6   **Lucent Technologies**   365-374-057
Issue a, January 2002

 CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Overheating

 CAUTION

Risk of fire due to overheating.

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

You must therefore ensure that

* *the fan unit is installed,*

* *the individual fans are not obstructed,*

* *the minimum separation is maintained between two shelves in a rack (follow the installation instructions given in the LambdaUnite™ MSS Installation Guide).*

Detector diodes

....
365-374-057
Issue a, January 2002

Lucent Technologies

1 - 2 7

⚠ **CAUTION**

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

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

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

☐

Taking into operation

Invisible laser radiation

 DANGER

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

 DANGER

Arcing on removing or inserting a live power supply plug.

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

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

Supply voltage

⚠ **CAUTION**

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

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

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

Fusing

⚠ **CAUTION**

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

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

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

Condensation

⚠ **CAUTION**

Condensation causes malfunctioning

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

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

□

Operation and maintenance

....

Invisible laser radiation

 DANGER

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

 DANGER

Arcing on removing or inserting a live power supply plug.

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

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

Laser warning labels

....

Safety requirements in specific deployment
phases
Operation and maintenance

Safety

WARNING

Ineffectiveness of laser warning labels if removed or concealed.

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

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

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Overheating

Safety requirements in specific deployment
phases
Operation and maintenance

Safety

⚠ **CAUTION**

Risk of fire due to overheating.

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

You must therefore ensure that

- *the fan unit is installed,*

- *the individual fans are not obstructed,*

- *the minimum separation is maintained between two shelves in a rack (follow the installation instructions given in the LambdaUnite MSS Installation Guide).*

Detector diodes

⚠ **CAUTION**

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

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

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

Short-circuit

Safety requirements in specific deployment
phases
Operation and maintenance

Safety

⚠ **CAUTION**

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

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

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

Test voltage

⚠ **CAUTION**

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

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

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

Climatic conditions

⚠ **CAUTION**

**Damage to system components under extreme
environmental conditions.**

*Extreme environmental conditions can damage system
components and cause malfunctioning.*

Ensure that the <u>*"Climatic limits for the operation of
LambdaUnite MSS equipment" (1-35)*</u> *are complied with
during operation.*

Safety requirements in specific deployment
phases
Operation and maintenance

Safety

Climatic limits for the operation of *LambdaUnite* MSS equipment

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

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

The following climatogram visualizes these climatic limits:
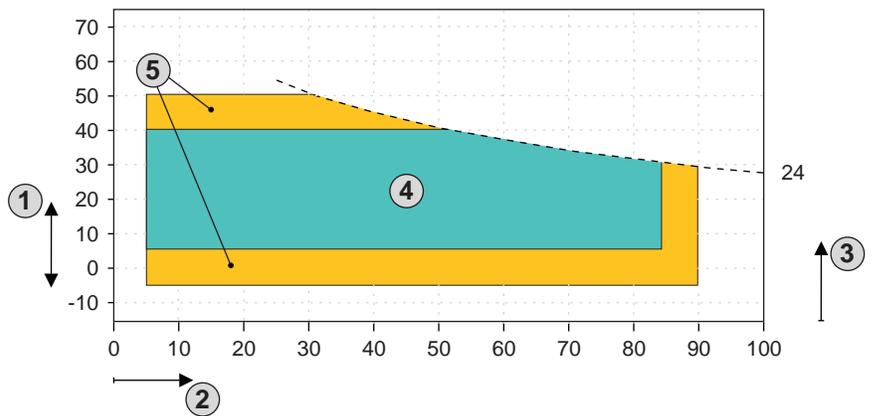
Legend:

1   Air temperature [°C]

2   Relative humidity [%]

3   Absolute humidity [g water/kg dry air]. The dashed curve specifies a constant absolute humidity of 24 g water per kg dry air.

4   Permissible range for the operation of *LambdaUnite* MSS systems.

5   Exceptional conditions, permissible for a short duration only.

□

....

365-374-057
Issue a, January 2002

Lucent Technologies

1 - 3 5

Taking out of operation

Invisible laser radiation

⚠ **DANGER**

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

⚠ **DANGER**

Arcing on removing or inserting a live power supply plug.

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

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

Weight

Safety requirements in specific deployment
phases
Taking out of operation

Safety

 WARNING

Risk of injury due to unsecured shelf.

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

At least two persons are required for lifting the shelf.

Electrostatic discharge (ESD)

 CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

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

□

....
365-374-057
Issue a, January 2002

Lucent Technologies

1 - 3 7

2   Alarm messages

Overview

Purpose   The present chapter contains information about the alarm messages that can be reported by *LambdaUnite*™ MultiService Switch (MSS) network elements.

Introduction   This chapter on network element (NE) alarm messages is divided thematically into the following sections:

- "DCN alarms" (2-8)
- "Equipment alarms" (2-17)
- "Ethernet alarms" (2-40)
- "Linear protection switching alarms" (2-47)
- "Path-related transmission alarms" (2-49)
- "Port-related transmission alarms" (2-73)
- "Ring protection switching alarms" (2-86)
- "Synchronisation alarms" (2-105)
- "Additional alarm-related information" (2-113)

The alarm descriptions are alphabetically ordered within each section according to the alarm text displayed in the **Description** column of the *WaveStar*® CIT **NE Alarm List**.

The information provided for each alarm includes the meaning of the alarm, the alarm's short designation (alarm identifier, "probable

cause"), the alarm category, the type of alarm severity assignment profile (ASAP) the alarm belongs to, the alarm's default severity etc.

Local indications via the red "FAULT" LED on the circuit pack faceplate, additional alarm-related information, consequent actions, and how protection switching is influenced by the corresponding alarm, are described, if appropriate.

Furthermore, a reference to the corresponding trouble clearing procedure is provided.

General alarm information   Each NE alarm description contains a brief tabular overview of the main alarm characteristics:

Alarm identifier (**Probable cause**)	"LOS", "LOF" or "DUPL-RNG" for example
ASAP type	"System Timing" for example
Alarm category	"Equipment" for example
Alarm severity (default setting)	"Critical" for example
Alarm source	"Circuit pack" or "STS-12C" for example.

In the following, the general meaning of these characteristics will be desribed in more detail.

Probable cause (alarm identifier)   The "Alarm identifier (**Probable Cause**)" entry in the alarm overview table gives the alarm short designation as displayed in the **Probable Cause** column of the *WaveStar* CIT **NE Alarm List** or the *WaveStar* SNMS **Alarm List**.

Please notice that the alarm short designations displayed when provisioning ASAPs by using the *WaveStar* SNMS are different to those displayed in the alarm lists. For ASAP provisioning purposes the *WaveStar* SNMS alarm short designations are preceded by "SA_" or "NSA_" ("SA_LOS" and "NSA_LOS" for example) to make a distinction concerning the alarm's affect-on-service attribute. The preceding "SA_" or "NSA_" attribute is ommitted in the brief alarm overview table.

Alphabetical index

Please refer to the alphabetical index provided with this information product to find information concerning alarms of which you only know the alarm short designation.

Alarm category The "Alarm category" entry in the alarm overview table indicates the functional area to which the relevant alarm belongs.

The NE alarms are assigned to the following alarm categories:

- Communication
  This alarm category comprises DCN, synchronisation and transmission alarms. Therefore, the "Communication" alarm category is further divided into:

  - Communication (DCN)

  - Communication (Synchronisation)

  - Communication (Transport)

- Equipment
  This alarm category is used for hardware- and configuration-related alarms and alarms concerning the internal communication.

- Processing error
  This alarm category is used for alarms related to problems or failures of the control system software, due to overload situations for example.

ASAP type The "ASAP type" entry in the alarm overview table indicates the type of alarm severity assignment profile (ASAP) to which the corresponding alarm belongs.

Please refer to the *LambdaUnite MultiService Switch (MSS) User Operations Guide* for information about the available ASAP types.

Default alarm severity The "Alarm severity (default setting)" entry in the alarm overview table indicates the factory settings of the corresponding alarm's severity.

Alarm severities can be assigned by means of alarm severity assignment profiles (ASAPs). The default alarm severity is the alarm severity as originally specified in the ASAPs named "Default".

Please refer to the *LambdaUnite MultiService Switch (MSS) User Operations Guide* for information about the available ASAP types, and how alarm severities can be assigned.

....

Alarm source   The "Alarm source" entry in the alarm overview table specifies the alarm origination point, i.e. the system component where the alarm has been detected or the affected signal level in case of transmission alarms.

Local indications   Local indications are indications via the circuit pack faceplate LEDs, especially via the red "FAULT" LED.

Please note that the signalling of alarms by means of the user panel LEDs or the office alarm interfaces cannot be taken into consideration in this *Alarm Messages and Trouble Clearing Guide* because the signalling of alarms depends on the actual value of the alarm severity assigned.

Please refer to the *LambdaUnite MultiService Switch (MSS) User Operations Guide* for further information.

Consequent actions   Consequent actions mean the autonomous insertion of maintenance signals as the consequence of a detected defect.

Contents

DCN alarms

Overview

Purpose   In the following, alarm descriptions are given for the alarms related to the Data Communication Network (DCN) that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

Address List Overflow

....

Meaning of the alarm One or more computed area addresses have been dropped, because the maximum capacity of the computed area address list is exceeded.

Brief alarm overview The following tabular overview summarizes important information concerning the `Address List Overflow` alarm:

Alarm identifier (**Probable cause**)	ADDRO
ASAP type	DCN
Alarm category	Communication (DCN)
Alarm severity (default setting)	Major
Alarm source	DCN

Related information Please also refer to the *LambdaUnite*™ *MultiService Switch (MSS) User Operations Guide*.

Trouble clearing For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

....

DCC Failure

Meaning of the alarm   No connection could be established on an enabled DCC link provisioned for the Acknowledged Information Transfer Service (AITS).

Brief alarm overview   The following tabular overview summarizes important information concerning the `DCC Failure` alarm:

Alarm identifier (**Probable cause**)	DCCRSF or DCCMSF, depending on which type of DCC link is affected:	
	DCCRSF – Section DCC, RS-DDC	
	DCCMSF – Line DCC, MS-DDC	
ASAP type	Port	
Alarm category	Communication (DCN)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	– (not applicable)
	NSA	Major
Alarm source	DCC	

Local indications   The red "FAULT" LED on the faceplate of the circuit pack where the respective port resides is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Related information   Please also refer to the *LambdaUnite™ MultiService Switch (MSS) User Operations Guide*.

Trouble clearing   For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

DCN Provisioning Not Valid

Meaning of the alarm The network element is not in a position to retrieve valid parameter values for the IS-IS protocol (e.g. during protocol restart) from the NE database.

Brief alarm overview The following tabular overview summarizes important information concerning the DCN Provisioning Not Valid alarm:

Alarm identifier (**Probable cause**)	PROVINVAL
ASAP type	DCN
Alarm category	Communication (DCN)
Alarm severity (default setting)	Major
Alarm source	DCN

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Partitioned Area Repair

....

Meaning of the alarm   A partition repair path ("partition repair tunnel") has been established in order to repair a partitioned area using connections via nodes outside the area.

The `Partitioned Area Repair` alarm is reported by the end nodes of a partition repair tunnel.

Important! Do not start a software upgrade of network elements or a software download, while a partition repair is active in the destination area.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Partitioned Area Repair` alarm:

Alarm identifier (**Probable cause**)	PARARREP
ASAP type	DCN
Alarm category	Communication (DCN)
Alarm severity (default setting)	Minor
Alarm source	DCN

Partitioning of an area   The following situations may lead to the partitioning of an area:

- The design of the DCN is not correct (the DCN has not a ring or meshed structure within the area for example).

- The provisioning of the DCN is not correct (a DCC may be unintentionally disabled for example).

- A node failure or fiber cut. Such failures would result in a `DCC Failure` alarm to be reported, possibly in connection with `Loss of Signal` or `Loss of Frame` for example.

....

Partition repair   Partition repair provides a way to enhance the robustness of the DCN by providing the capability to repair intra-area routing using connections via nodes outside the area. This is done by creating a path through the level-2 subdomain outside the area, between two level-2 nodes (which must be provisioned to be partition repair capable level-2 nodes), belonging to distinct partitions of the same IS-IS area. Level-1 IS-IS/CLNP PDU's are encapsulated and transferred over that path. This is also referred to as tunnelling.

Related information

Please also refer to the *LambdaUnite*™ *MultiService Switch (MSS) User Operations Guide*.

Trouble clearing   For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Protocol Version Mismatch

....

Meaning of the alarm	The automatic exchange of link ID information between two adjacent end nodes of an enabled DCC link is not possible because the version numbers of their link ID protocols or the protocol types or version numbers of their network address protocols are incompatible.
Brief alarm overview	The following tabular overview summarizes important information concerning the `Protocol Version Mismatch` alarm:

Alarm identifier (**Probable cause**)	LIDRSM or LIDMSM, depending on which type of DCC link is affected: LIDRSM – Section DCC, RS-DDC LIDMSM – Line DCC, MS-DDC	
ASAP type	Port	
Alarm category	Communication (DCN)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	not applicable
	NSA	Major
Alarm source	Optical interface port	

Local indications	The red "FAULT" LED on the faceplate of the circuit pack where the respective port resides is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).
Effect on protection switching	BLSR/MS-SPRing ring interworking, and thus ring protection switching is not possible between the concerning network elements.
Automatic exchange of link ID information	*LambdaUnite*™ MSS network elements autonomously exchange link identification (link ID) information via the so-called "link ID protocol" between two adjacent end nodes of enabled DCC links.

The link ID information is discovered upon initial link start-up and upon dynamic changes to the link ID information. The network elements determine bidirectional connectivity with their neighbours |

....

via the LAPD datalink service and determine the link ID information of the neighbour via a message exchange over that LAPD datalink service. The link ID information is used as an additional means to automatically and unambiguously discover the BLSR/MS-SPRing topology (please also refer to "Automatic discovery of the ring topology" (2-117)).

The link ID information includes:

- Link ID protocol version number
  The version number specifies which version of the link ID protocol is running at the end node. For *LambdaUnite* MSS network elements only the version number "2" is supported.

- NE name
  The NE name, also referred to as the NE's target identifier (TID), is an alphanumeric string of up to 20 characters, used to uniquely identify a network element within the network.

- Port information
  The access identifier (AID) of the port where the DCC link is terminated.

- Network address
  The node's NSAP address.
  The NSAP information is transported in the so-called "Network address protocol" which is nested in the link ID protocol. The NSAP address is used to set up an OSI association between adjacent ring nodes to support the distribution of BLSR/MS-SPRing related information for the automatic discovery of ring topology, for the automatic allocation of the node IDs and for the distribution of cross connection information in the ring.
  The network address information includes:

  - Protocol type
    "OSI" for *LambdaUnite* MSS network elements.

  - Network address protocol version number, indicating the supported OSI presentation context.
    "1" or "3" for *LambdaUnite* MSS network elements.

  - Length of the NSAP address

  - Value of the NSAP address

Trouble clearing   Please refer to "Clearing Protocol Version Mismatch" (3-71).

☐

Equipment alarms

Overview

Purpose   In the following, alarm descriptions are given for the equipment alarms that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

Backplane Read Failure

Meaning of the alarm   The backplane EEPROM cannot be accessed by the Controller (CTL). Reading from or writing to the EEPROM is not possible. This means that the EEPROM is either not or not correctly partitioned, does not hold data, or that the hardware is defective.

The backplane EEPROM contains factory and application specific data and the electronic type label.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Backplane Read Failure` alarm:

Alarm identifier (**Probable cause**)	BPEF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Major
Alarm source	Shelf

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing Backplane Read Failure" (3-6).

CICTL Comm Failure

| **Meaning of the alarm** | The internal communication between the CI-CTL (Connection Interface of the Controller) and the Controller (CTL) is disturbed. |

| **Brief alarm overview** | The following tabular overview summarizes important information concerning the `CICTL Comm Failure` alarm: |

Alarm identifier (**Probable cause**)	CICOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

| **Local indications** | There are no specific local indications. |

| **Inventory EEPROM** | The inventory EEPROM is used to store fixed circuit pack parameters that are written during the manufacturing of the circuit pack. |

| **Trouble clearing** | Please refer to "Clearing CICTL Comm Failure" (3-8). |

CICTL not Present

Meaning of the alarm   The CI-CTL (Connection Interface of the Controller) cannot be detected by the Controller (CTL). Either there is no CI-CTL plugged in slot 51 on the rear side of the shelf, or the CTL is defective.

Brief alarm overview   The following tabular overview summarizes important information concerning the CICTL not Present alarm:

Alarm identifier (**Probable cause**)	CIMISS
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Slot

Trouble clearing   Please refer to "Clearing CICTL not Present" (3-12).

☐

Circuit Pack Comm Failure

....

Meaning of the alarm A protocol failure occurred in the internal data communication between the circuit pack reporting the `Circuit Pack Comm Failure` alarm and the Controller (CTL).

Brief alarm overview The following tabular overview summarizes important information concerning the `Circuit Pack Comm Failure` alarm:

Alarm identifier (**Probable cause**)	CPCOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications There are no specific local indications.

Trouble clearing Please refer to "Clearing Circuit Pack Comm Failure" (3-15).

☐

....

Circuit Pack Failure

Meaning of the alarm   One of the following failure conditions exists on the circuit pack for which the alarm is reported:

- An error occurred during the initialization of the circuit pack.
- There is a hardware error on the circuit pack.
- One of the local circuit pack voltages is out of range.

In the case of an XC320 switch unit, the `Circuit Pack Failure` alarm may also indicate a failure of the system timing function.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Circuit Pack Failure` alarm:

Alarm identifier (**Probable cause**)	CPFAIL	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Circuit pack	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is constantly lit.

Trouble clearing   Please refer to "Clearing Circuit Pack Failure" (3-22).

☐

Circuit Pack not Present

Meaning of the alarm   Although previously provisioned, no circuit pack can be detected by the Controller (CTL) in the slot for which the `Circuit Pack not Present` alarm is reported. Either there is no circuit pack plugged in the corresponding slot, or the CTL is defective.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Circuit Pack not Present` alarm:

Alarm identifier (**Probable cause**)	REPLUNITMISS	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Slot	

Trouble clearing   Please refer to "Clearing Circuit Pack not Present" (3-19).

☐

Circuit Pack Type Mismatch

Meaning of the alarm   There is an unexpected circuit pack present in the slot for which the `Circuit Pack Type Mismatch` alarm is reported. Although the circuit pack may in principle be permitted, a different type of circuit pack had previously been provisioned for that slot. Furthermore, a `Circuit Pack Type Mismatch` alarm will also be reported if the circuit pack latches are not closed.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Circuit Pack Type Mismatch` alarm:

Alarm identifier (**Probable cause**)	PRCDRERR	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Slot	

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing Circuit Pack Type Mismatch" (3-20).

☐

Comm Channel Failure

Meaning of the alarm
A protocol failure occurred in the internal data communication between the XC320 switch unit and the Controller (CTL).

Brief alarm overview
The following tabular overview summarizes important information concerning the `Comm Channel Failure` alarm:

Alarm identifier (**Probable cause**)	SYSCOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Major
Alarm source	System

Local indications
The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing
Please refer to "Clearing Comm Channel Failure" (3-23).

☐

CTL Comm Failure

....

Meaning of the alarm   The `CTL Comm Failure` alarm may have different causes:

- The inventory data of the Controller (CTL) cannot be accessed, or

- one of the internal selftests failed, or

- the ONI communication between the DCC controller function and the system controller function (both are realized on the CTL) is disturbed.

Brief alarm overview   The following tabular overview summarizes important information concerning the `CTL Comm Failure` alarm:

Alarm identifier (**Probable cause**)	CTLCOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing CTL Comm Failure" (3-26).

☐

....

Fan Failure

Meaning of the alarm One or more fans have failed.

Brief alarm overview The following tabular overview summarizes important information concerning the `Fan Failure` alarm:

Alarm identifier (**Probable cause**)	FANF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Major
Alarm source	Fan unit

Local indications The red "FAULT" LED on the faceplate of the fan unit is constantly lit.

Trouble clearing Please refer to "Clearing Fan Failure" (3-33).

□

Fan Unit Comm Failure

Meaning of the alarm A failure occurred in the internal communication between the fan unit, the CI-CTL (Connection Interface of the Controller) and the Controller (CTL), or no fan unit is installed .

Brief alarm overview The following tabular overview summarizes important information concerning the `Fan Unit Comm Failure` alarm:

Alarm identifier (**Probable cause**)	FANUNITCOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Fan unit

Local indications There are no specific local indications.

Trouble clearing Please refer to "Clearing Fan Unit Comm Failure" (3-36).

☐

Fan Unit Failure

Meaning of the alarm   The fan unit has no power supply.

Brief alarm overview   The following tabular overview summarizes important information
concerning the Fan Unit Failure alarm:

Alarm identifier (**Probable cause**)	FANUNITF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	Fan unit

Local indications   Both LEDs on the fan unit faceplate are off.

Trouble clearing   Please refer to "Clearing Fan Unit Failure" (3-40).

☐

Fan Voltage Feed A Failure

Meaning of the alarm   There is no voltage supply at the "Power Input A" of the fan unit, or the voltage is too low.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Fan Voltage Feed A Failure` alarm:

Alarm identifier (**Probable cause**)	FEEDAF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Fan unit

Local indications   The red "FAULT" LED on the faceplate of the fan unit is constantly lit.

Trouble clearing   Please refer to "Clearing Fan Voltage Feed A Failure" (3-44).

□

Fan Voltage Feed B Failure

Meaning of the alarm There is no voltage supply at the "Power Input B" of the fan unit, or the voltage is too low.

Brief alarm overview The following tabular overview summarizes important information concerning the Fan Voltage Feed B Failure alarm:

Alarm identifier (**Probable cause**)	FEEDBF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Fan unit

Local indications The red "FAULT" LED on the faceplate of the fan unit is constantly lit.

Trouble clearing Please refer to "Clearing Fan Voltage Feed B Failure" (3-47).

☐

ONI Failure

....

Meaning of the alarm   The internal communication between circuit packs via their Operations Network Interface (ONI) failed. This may have an impact on the overhead information communicated between circuit packs.

Brief alarm overview   The following tabular overview summarizes important information concerning the `ONI Failure` alarm:

Alarm identifier (**Probable cause**)	ONIF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing   Please refer to "Clearing ONI Failure" (3-62).

....

2 - 3 2   **Lucent Technologies**   365-374-057
Issue a, January 2002

Power Interface not Present

Meaning of the alarm   The Power Interface (PI) is not installed.

Which of the two Power Interfaces is affected can be seen from the `Fan Voltage Feed A Failure` or `Fan Voltage Feed B Failure` alarm which will be reported at the same time (the power feeders are through-connected).

Brief alarm overview   The following tabular overview summarizes important information concerning the `Power Interface not Present` alarm:

Alarm identifier (**Probable cause**)	PIMISS	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Shelf	

Trouble clearing   Please refer to "Clearing Power Interface not Present" (3-67).

System Power Failure

....

Meaning of the alarm The supply voltage of one of the two input power feeders has dropped below 39 V DC (–39.0 ± 1.0 V DC). The second supply voltage is within the normal range.

Which system power feeder is affected can be seen from the `Fan Voltage Feed A Failure` or `Fan Voltage Feed B Failure` **alarm** which will be reported at the same time (the power feeders are through-connected), or from the green "PWR ON" LED on the respective Power Interface (PI) A or B (cf. "Local indications").

Brief alarm overview The following tabular overview summarizes important information concerning the `System Power Failure` alarm:

Alarm identifier (**Probable cause**)	POWF	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Shelf	

Trouble clearing Please refer to "Clearing System Power Failure" (3-80).

□

....

TI Mismatch

Meaning of the alarm
A second Timing Interface (TI) has been inserted into the system, and the type of this second TI does not match the type of the already plugged-in TI.

Brief alarm overview
The following tabular overview summarizes important information concerning the `TI Mismatch` alarm:

Alarm identifier (**Probable cause**)	TIMM
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications
There are no specific local indications.

Trouble clearing
Please refer to "Clearing TI Mismatch" (3-86).

□

TXI Failure

Meaning of the alarm

Frame alignment has been lost for the corresponding TXI bus line. The affected TXI bus line can be derived from the alarm identifier (**Probable cause**).

Important! If a `TXI Failure` **is reported by the currently active XC320 switch unit, then perform a manual protection switch to the standby XC320 switch unit.**

Brief alarm overview

The following tabular overview summarizes important information concerning the `TXI Failure` alarm:

Alarm identifier (**Probable cause**)	TXInF (where "n" is a number representing the affected TXI bus line)	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Circuit pack	

Local indications

The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing

For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

• Phone: +49 911 526 2846

• Fax: +49 911 526 3131

• E-mail: htransde@lucent.com

Unit Cooling Degraded

Meaning of the alarm   The operating temperature of the circuit pack reporting the alarm has exceeded a predefined limit, where the lifetime of the circuit pack will be degraded.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Unit Cooling Degraded` alarm:

Alarm identifier (**Probable cause**)	CPDEGR
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing   Please refer to "Clearing Unit Cooling Degraded" (3-87).

☐

Unit Temperature too High

Meaning of the alarm The operating temperature of the circuit pack reporting the alarm has exceeded the maximum permitted value.

Brief alarm overview The following tabular overview summarizes important information concerning the `Unit Temperature too High` alarm:

Alarm identifier (**Probable cause**)	CPTEMP	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Circuit pack	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Effect on protection switching `Unit Temperature too High` is a trigger for equipment protection switching.

Trouble clearing Please refer to "Clearing Unit Temperature too High" (3-89).

☐

User Panel Comm Failure

Meaning of the alarm   A failure occurred in the internal communication between the user panel and the Controller (CTL).

Brief alarm overview   The following tabular overview summarizes important information concerning the User Panel Comm Failure alarm:

Alarm identifier (**Probable cause**)	UPCOMF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	User panel

Trouble clearing   Please refer to "Clearing User Panel Comm Failure" (3-92).

☐

Ethernet alarms

Overview

Purpose   In the following, alarm descriptions are given for the alarms related to the Ethernet-over-SDH/SONET (EoS) functionality that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

GFP Loss of Frame

Meaning of the alarm The GFP delineation algorithm failed to recover the framestart of a GFP frame.

Brief alarm overview The following tabular overview summarizes important information concerning the GFP Loss of Frame alarm:

Alarm identifier (**Probable cause**)	GFPLOF	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Virtual Concatenated Group (VCG)	

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

LAN Loss of Signal

....

Meaning of the alarm   The receiver of the corresponding Gigabit Ethernet port has detected no optical input signal for more than one second or is not able to synchronize to the incoming signal.

Brief alarm overview   The following tabular overview summarizes important information concerning the LAN Loss of Signal alarm:

Alarm identifier (**Probable cause**)	LANLOS	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Gigabit Ethernet port	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

....

2 - 4 2   **Lucent Technologies**   365-374-057
                                                                    Issue a, January 2002

Loss of Alignment

....

Meaning of the alarm	The virtually concatenated payload cannot be aligned to a common multiframe start because the delay difference between the VC-4s in the Virtual Concatenated Group (VCG) exceeds the range that can be compensated by buffering.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Loss of Alignment` alarm:

Alarm identifier (**Probable cause**)	VCGLOA	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Virtual Concatenated Group (VCG)	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Payload realignment   The different VC-4s of a Virtual Concatenated Group (VCG) in general have different transit times when transmitted over the network. These differences have to be compensated in a realignment process by buffering the "fastest" and all subsequent VC-4s until the "slowest" VC-4 has arrived. The sequence number and the multiframe information are used to realign the virtually concatenated payload provided that no `Sequence Number Mismatch` or `Loss of Multiframe` alarm is present.

Compensation of delay is only possible in a relatively small region called the "correction range". As soon as the delay difference between the fastest and the slowest VC-4 is larger than the correction range, realignment is no longer possible and a `Loss of Alignment` alarm will be reported.

....

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Partial Transport Capacity Loss

Meaning of the alarm The transport capacity of the Virtual Concatenated Group (VCG) is partially unavailable.

Brief alarm overview The following tabular overview summarizes important information concerning the `Partial Transport Capacity Loss` alarm:

Alarm identifier (**Probable cause**)	VCGLOPC	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Virtual Concatenated Group (VCG)	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Total Transport Capacity Loss
....

Meaning of the alarm   The transport capacity of the Virtual Concatenated Group (VCG) is
completely unavailable.

Brief alarm overview   The following tabular overview summarizes important information
concerning the `Total Transport Capacity Loss` alarm:

Alarm identifier (**Probable cause**)	VCGLOTC	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Virtual Concatenated Group (VCG)	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack
is flashing (provided that no equipment alarm is present at the same
time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and
related maintenance and trouble clearing measures cannot be provided
to the full extent.

If you need technical support please contact your Lucent Technologies
Local Customer Support (LCS) team or the Lucent Technologies
Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax
or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

....

Linear protection switching alarms

Overview

Purpose   In the following, alarm descriptions are given for the alarms related to linear protection switching that can be reported by the *LambdaUnite*™ MSS network elements.

Linear protection switching includes:

- SDH:
  Multiplex Section Protection (MSP)

- SONET:
  Linear Automatic Protection Switching (Linear APS), Line Protection

Contents

Prot. Arch. Mismatch

Meaning of the alarm The protection architectures at both end nodes of the optical line do not match.

For example, for the alarm-reporting network element a 1+1 architecture might be provisioned while for the network element at the far end of the optical line a 1:1 architecture is provisioned.

In the present *LambdaUnite*™ MSS release, the protection architecture of a *LambdaUnite* MSS network element is not provisionable, but always "1+1".

Brief alarm overview The following tabular overview summarizes important information concerning the `Prot. Arch. Mismatch` (protection architecture mismatch) alarm:

Alarm identifier (**Probable cause**)	PAMARCH
ASAP type	Automatic Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	SDH: MSP (group) SONET: Line protection (group)

Protection architecture The protection architecture of the Multiplex Section Protection (MSP, SDH) or Line Protection (SONET) respectively is indicated in bit 5 of the K2 byte (K2 [5]):

- K2 [5] = 0 → 1+1 architecture
- K2 [5] = 1 → 1:1 architecture

Trouble clearing Please refer to "Clearing Prot. Arch. Mismatch" (3-68).

□

Path-related transmission alarms

Overview

Purpose   In the following, alarm descriptions are given for the path-related transmission alarms that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

Alarm Indication Signal (AIS-P)

Meaning of the alarm The Alarm Indication Signal (AIS) has been detected in the receive signal of the path. The signal cannot be used.

Brief alarm overview The following tabular overview summarizes important information concerning the `Alarm Indication Signal` alarm:

Alarm identifier (**Probable cause**)	AIS-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	Non-intrusively monitored path	

Local indications There are no specific local indications.

Consequent actions AIS (all-ones signal) on path level is inserted in the downstream direction.

RDI (Remote Defect Indication) on path level is inserted in the upstream direction.

Effect on protection switching The alarm is a trigger for UPSR and SNCP (SNC/N, but not SNC/I) automatic path protection switching.

Trouble clearing Please refer to "Clearing Alarm Indication Signal (AIS-P)" (3-5).

☐

Degraded Signal (DEG-P)

....

Meaning of the alarm	The bit error ratio (BER) in the path has exceeded the provisioned **HP Degraded Threshold**. The quality of the transmission signal is degraded.
	The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview   The following tabular overview summarizes important information concerning the Degraded Signal alarm:

Alarm identifier (**Probable cause**)	DEG-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Effect on protection switching   The alarm is a trigger for SNCP (SNC/N, but neither SNC/I nor UPSR) automatic path protection switching.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

....

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

☐

Excessive Bit Error Ratio (EXC-P)

....

Meaning of the alarm
The bit error ratio (BER) in the path, calculated using the B3 byte of the Path Overhead (POH), has exceeded the provisioned **HP DEXC Threshold**.

The **HP DEXC Threshold** can be set in terms of integer powers of ten between 10^{-3} and 10^{-5}. The default setting is 10^{-3}.

The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview
The following tabular overview summarizes important information concerning the Excessive Bit Error Ratio alarm:

Alarm identifier (**Probable cause**)	EXC-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications
The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Effect on protection switching
The alarm is a trigger for UPSR and SNCP (SNC/N, but not SNC/I) automatic path protection switching.

Trouble clearing
For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

....

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Loss of Multiframe

....

Meaning of the alarm	The receiver of the corresponding Gigabit Ethernet port has detected an unexpected, unsequential pattern in either the multiframe 1 (MF1) or multiframe 2 (MF2) of at least one VC-4 in a Virtual Concatenated Group (VCG).
Brief alarm overview	The following tabular overview summarizes important information concerning the `Loss of Multiframe` alarm:

Alarm identifier (**Probable cause**)	VCLOM	
ASAP type	Path terminating SDH	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Path termination	

Local indications	The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).
Consequent actions	AIS (all-ones signal in the affected VC-4s) is inserted in the downstream direction.
Virtual concatenation multiframe indicators	The consecutive frames of the VC-4s in a Virtual Concatenated Group (VCG) are organized into a multiframe consisting of 4096 frames by writing a 12-bit multiframe indicator into the H4 byte of the VC-4 Path Overhead (VC-4-POH). The individual bits of the 12-bit multiframe indicator are distributed to several frames to accomplish the transmission of a 12-bit multiframe indicator by using a single byte. Therefore, a 12-bit multiframe indicator consists of two parts, a multiframe 1 (MF1) and a multiframe 2 (MF2).

....

Multiframe 1 (MF1)	The four least significant bits of the 12-bit multiframe indicator are transmitted each frame in bits 5 to 8 of the H4 byte forming a multiframe 1 (MF1) which consists of 16 frames. Per MF1, the inserted bits are incremented in successive frames from "0000" to "1111". An MF1 is 2 ms long as the basic frame length is 125 µs.
Multiframe 2 (MF2)	The eigth most significant bits of the 12-bit multiframe indicator are transmitted only once per MF1, in bits 1 to 4 of the H4 byte, four bits in the first frame of MF1 and four bits in the second frame. These bits form a multiframe 2 (MF2) consisting of 256 MF1s (4096 frames). Per MF2, the inserted bits are incremented in successive MF1s from "00000000" to "11111111". An MF2 is 512 ms long.

Furthermore, bits 1 to 4 of the H4 byte are used to transmit sequence numbers associated with the VC-4s (in the last two frames of each MF1) and the Link Capacity Adjustment Scheme (LCAS) protocol, thus providing a means to clearly identify the ordering of the transmitted VC-4s, and, at the receiver, to compensate possible delay differences between the individual VC-4s of the Virtual Concatenated Group.

Effect on protection switching　The alarm is a trigger for UPSR and SNCP (SNC/N and SNC/I) automatic path protection switching.

Trouble clearing　For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Loss of Pointer

....

Meaning of the alarm	The expected signal structure cannot be found in the receive signal.	
	The alarm is detected at a non-intrusive monitoring (NIM) point.	

Brief alarm overview The following tabular overview summarizes important information concerning the `Loss of Pointer` alarm:

Alarm identifier (**Probable cause**)	LOP-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Effect on protection switching The alarm is a trigger for UPSR and SNCP (SNC/N and SNC/I) automatic path protection switching.

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

☐

....

Path Switch Denial

....

Meaning of the alarm	Although a switching criterion for automatic path protection switching has been detected (for example `Alarm Indication Signal`, `Loss of Pointer` or `Unequipped`), the protection switch has not been performed either because a path protection switch request of a higher or equal priority is active, or there is an invalid signal on the other path.

For example, a `Path Switch Denial` alarm will be reported if AIS-P is detected on the working path, and a "Forced Switch to Working" command was previously initiated for the path.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Path Switch Denial` alarm:

Alarm identifier (**Probable cause**)	FAILTOSW
ASAP type	Path Protection SNCP_UPSR
Alarm category	Communication (Transport)
Alarm severity (default setting)	Not alarmed
Alarm source	Path protection group

Local indications   There are no specific local indications.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

....

Payload Defect Indication

Meaning of the alarm   The `Payload Defect Indication` alarm is used to indicate to downstream equipment that there is a defect in one or more of the directly mapped payloads.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Payload Defect Indication` alarm:

Alarm identifier (**Probable cause**)	PDI-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications   There are no specific local indications.

Effect on protection switching   The alarm is a trigger for UPSR (not SNCP!) automatic path protection switching if correspondingly provisioned. The **PDI-P Switching Enable** parameter determines if the `Payload Defect Indication` shall contribute to automatic path protection switching or not.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Payload Mismatch

Meaning of the alarm
The received (and accepted) trail signal label (TSL) differs from the expected TSL and has a value other than ″equipped - not specified″.

A TSL is accepted after the reception of five consecutive C2 bytes with identical values.

Brief alarm overview
The following tabular overview summarizes important information concerning the `Payload Mismatch` alarm:

Alarm identifier (**Probable cause**)	THPPLM	
ASAP type	Path terminating SDH	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Payload signal	

Local indications
The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing
For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Remote Defect Indication (RFI-P)

....

Meaning of the alarm   The receive signal contains RDI.

This means that the network element at the far-end path termination (in the downstream direction) has detected a defect in the incoming signal and has inserted RDI into the outgoing signal as a consequent action.

The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Remote Defect Indication` alarm:

Alarm identifier (**Probable cause**)	RFI-P[1]	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	Non-intrusively monitored path	

Notes:

1.   In SONET standards, a distinction is made between the RDI defect and the resulting failure, which is RFI (Remote Failure Indication). Therefore, RFI is used in the probable cause definition.

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing Remote Defect Indication (RFI-P)" (3-74).

☐

....

365-374-057
Issue a, January 2002

Lucent Technologies

2 - 6 3

Sequence Number Mismatch
....

Meaning of the alarm	The accepted and the expected sequence number of at least one VC-4 in a Virtual Concatenated Group (VCG) does not match.

Brief alarm overview The following tabular overview summarizes important information concerning the `Sequence Number Mismatch` alarm:

Alarm identifier (**Probable cause**)	VCSQM	
ASAP type	Path terminating SDH	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Path termination	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Sequence numbers Sequence numbers are used to signal to the receive end in which order the VC-4s of the VC-4-Xv Virtual Concatenated Group (VCG) are filled with payload data and to check that ordering of the VC-4s inside the VC-4-Xv has not been altered during transport.

Each VC-4 inside a VCG carries a sequence number in the last two frames of multiframe 1 (MF1). A received sequence number is considered an "accepted" sequence number, if it is identical in three consecutive MF1s. The accepted sequence numbers can be useful when corrective actions are necessary, for example to find misconnections in other network elements.

Sequence numbers are not evaluated when the Link Capacity Adjustment Scheme (LCAS) protocol is active.

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

....

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Server Signal Fail (SSF-P)

....

Meaning of the alarm   The payload signal is unusable and has been replaced by AIS (all-ones signal) due to a failure that occurred in the upstream direction.

The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Server Signal Fail` alarm:

Alarm identifier (**Probable cause**)	SSF-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	Non-intrusively monitored path	

Local indications   There are no specific local indications.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

....

Signal Rate Mismatch

....

Meaning of the alarm   The `Signal Rate Mismatch` alarm is reported whenever one of the following two situations occur:

- The constituent signal rate for a certain set of tributaries is larger than the rate of a cross connection configured for these tributaries.

- There is a mismatch between the received and the expected signal structure in a port working in adaptive-rate tributary mode but which tries to approximate the fixed-rate mode. In this case, the `Signal Rate Mismatch` alarm is reported instead of the `Loss of Pointer` alarm that a normal fixed-rate port would have issued.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Signal Rate Mismatch` alarm:

Alarm identifier (**Probable cause**)	SRM-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications   There are no specific local indications.

Effect on protection switching   The alarm is a trigger for UPSR and SNCP (SNC/N and SNC/I) automatic path protection switching.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

....

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Trace Identifier Mismatch (TIM-P)

....

Meaning of the alarm   The received path trace identifier in the J1 byte of the VC-n or STS-m Path Overhead (POH) does not match the expected path trace identifier.

The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Trace Identifier Mismatch` **alarm:**

Alarm identifier (**Probable cause**)	TIM-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Related information   Please also refer to the *LambdaUnite™ MultiService Switch (MSS) User Operations Guide*.

Consequent actions   AIS (all-ones signal) is inserted in the downstream direction.

HP-RDI is inserted in the upstream (opposite) direction.

Effect on protection switching   The alarm is a trigger for UPSR and SNCP (SNC/N and SNC/I) automatic path protection switching.

Trouble clearing   For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

....

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

Unequipped

Meaning of the alarm	The corresponding tributary channel in the receive signal is not in use. Possibly, the cross connections are not consistently defined at both sides of a line (e. g. at the local and remote station).
	The alarm is detected at a non-intrusive monitoring (NIM) point.

Brief alarm overview The following tabular overview summarizes important information concerning the Unequipped alarm:

Alarm identifier (**Probable cause**)	UNEQ-P	
ASAP type	MSA/NIM	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Non-intrusively monitored path	

Local indications	The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction.
	HP-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	The alarm is a trigger for UPSR and SNCP (SNC/N, but not SNC/I) automatic path protection switching.
Trouble clearing	For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.
	If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

....

2 - 7 2   **Lucent Technologies**   365-374-057
Issue a, January 2002

Port-related transmission alarms

Overview

Purpose In the following, alarm descriptions are given for the port-related transmission alarms that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

□

Alarm Indication Signal (AIS-L)

Meaning of the alarm   The receive signal contains MS-AIS or Line AIS respectively.

MS-AIS or Line AIS respectively is an indication that `Loss of Signal` or `Loss of Frame` has been detected in the upstream equipment.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Alarm Indication Signal` alarm:

Alarm identifier (**Probable cause**)	AIS-L	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	SDH/SONET optical interface port	

Local indications   There are no specific local indications.

Consequent actions   AIS (all-ones signal) is inserted in the downstream direction.

RDI is inserted in the upstream (opposite) direction.

Effect on protection switching   The alarm is a trigger for BLSR/MS-SPRing protection switching.

Trouble clearing   Please refer to "Clearing Alarm Indication Signal (AIS-L)" (3-4).

□

Degraded Signal

Meaning of the alarm	The bit error ratio (BER) in the Multiplex Section (MS) or Line respectively has exceeded the provisioned **MS Degrade Threshold** or **Optical Line BER Threshold** respectively. The quality of the transmission signal is degraded.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Degraded Signal` alarm:

Alarm identifier (**Probable cause**)	MSDEG	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications	The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).
Effect on protection switching	The alarm is a trigger for BLSR/MS-SPRing protection switching.
Trouble clearing	For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Excessive Bit Error Ratio

Meaning of the alarm   The bit error ratio (BER) in the Multiplex Section (MS) or Line respectively, calculated using the B2 bytes of the Multiplex Section (MS) or Line Overhead, has exceeded the provisioned **MS DEXC Threshold** or **Optical Line EBER Threshold** respectively.

The **MS DEXC Threshold** or **Optical Line EBER Threshold** can be set in terms of integer powers of ten between 10^{-3} and 10^{-5}. The default setting is 10^{-3}.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Excessive Bit Error Ratio` alarm:

Alarm identifier (**Probable cause**)	MSEXC	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Effect on protection switching   The alarm is a trigger for BLSR/MS-SPRing protection switching.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Loss of Frame

| **Meaning of the alarm** | The position of the frame alignment bytes (A1/A2 bytes) cannot be detected correctly in the receive signal. |

Brief alarm overview   The following tabular overview summarizes important information concerning the `Loss of Frame` alarm:

Alarm identifier (**Probable cause**)	LOF	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Consequent actions   AIS (all-ones signal) is inserted in the downstream direction.

RDI is inserted in the upstream (opposite) direction.

Effect on protection switching   `Loss of Frame` is a trigger for line protection switching (MSP, linear APS) and ring protection switching (MS-SPRing, BLSR).

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Loss of Signal

Meaning of the alarm   The optical input power at the corresponding port is too low. Frame alignment and synchronisation to the receive signal is not possible.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Loss of Signal` alarm:

Alarm identifier (**Probable cause**)	LOS	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Consequent actions   AIS (all-ones signal) is inserted in the downstream direction.

RDI is inserted in the upstream (opposite) direction.

Effect on protection switching   `Loss of Signal` is a trigger for line protection switching (MSP, linear APS) and ring protection switching (MS-SPRing, BLSR).

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

OCh Loss of Frame

Meaning of the alarm The position of the frame alignment bytes (OA1/OA2 bytes) cannot be detected correctly in the receive signal.

Brief alarm overview The following tabular overview summarizes important information concerning the `OCh Loss of Frame` alarm:

Alarm identifier (**Probable cause**)	OCHLOF	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Remote Defect Indication (RFI-L)

Meaning of the alarm   The receive signal contains RDI.

The network element at the far end of the Multiplex Section or Line respectively (in the downstream direction) has detected an error in the incoming signal and, as a consequent action, has inserted RDI ("110" in bits 6, 7 and 8 of the K2 byte) into the outgoing signal in the upstream direction.

Brief alarm overview   The following tabular overview summarizes important information concerning the Remote Defect Indication alarm:

Alarm identifier (**Probable cause**)	RFI-L[1]	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	SDH/SONET optical interface port	

Notes:

1. In SONET standards, a distinction is made between the RDI defect and the resulting failure, which is RFI (Remote Failure Indication). Therefore, RFI is used in the probable cause definition.

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing   Please refer to "Clearing Remote Defect Indication (RFI-L)" (3-73).

☐

Server Signal Fail (MSSSF)

Meaning of the alarm   The receive signal contains AIS (all-ones signal) due to a signal failure that occurred in the upstream direction.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Server Signal Fail` alarm:

Alarm identifier (**Probable cause**)	MSSSF	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	SDH/SONET optical interface port	

Local indications   There are no specific local indications.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Trace Identifier Mismatch (RSTIM)

....

Meaning of the alarm The received section trace identifier in the J0 byte of the STM-n or OC-m Section Overhead (SOH) does not match the expected section trace identifier.

Brief alarm overview The following tabular overview summarizes important information concerning the `Trace Identifier Mismatch` alarm:

Alarm identifier (**Probable cause**)	RSTIM	
ASAP type	Port	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	SDH/SONET optical interface port	

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

....

Ring protection switching alarms

Overview

Purpose   In the following, alarm descriptions are given for the alarms related to ring protection switching that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

Default K-bytes
....

Meaning of the alarm The source node and destination node identifiers in the received APS bytes (K1 and K2) have equal values.

Default K1/K2 bytes

The K1/K2 bytes in the SDH Multiplex Section Overhead (MSOH) or SONET Line Overhead (LOH) respectively are used to transport the BLSR/MS-SPRing automatic protection switching (APS) protocol. Default K1/K2 bytes with identical source node and destination node identifiers are inserted when a ring node is not in a position to properly signal the BLSR/MS-SPRing protection switching protocol, and therefore cannot properly execute BLSR/MS-SPRing protection switching.

Brief alarm overview The following tabular overview summarizes important information concerning the Default K-bytes alarm:

Alarm identifier (**Probable cause**)	DKB
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications There are no specific local indications.

Effect on protection switching BLSR/MS-SPRing protection switching is not possible.

Trouble clearing Please refer to "Clearing Default K-bytes" (3-28).

☐

....

Duplicate Ring Node

....

Meaning of the alarm The `Duplicate Ring Node` alarm is reported by all the nodes in a ring if an erroneous BLSR/MS-SPRing configuration (cf. "Erroneous BLSR/MS-SPRing configurations" (2-89)) has been detected.

Brief alarm overview The following tabular overview summarizes important information concerning the `Duplicate Ring Node` alarm:

Alarm identifier (**Probable cause**)	DUPL-RNG
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications There are no specific local indications.

Effect on protection switching Ring protection switching is suspended (disabled) as long as a `Duplicate Ring Node` alarm is present.

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

....

Erroneous BLSR/MS-SPRing configurations

The following BLSR/MS-SPRing configurations are ***not allowed***:

- Multiple ring nodes from the same *LambdaUnite* MSS NE on the same ring.
- More than 16 nodes in a ring.

Therefore, a `Duplicate Ring Node` alarm will be reported if one of the following erroneous BLSR/MS-SPRing configurations has been detected:

1. Duplicate TIDs (NE names)
   In the same ring there are

   - multiple ring nodes from the same NE, or
   - multiple NEs with the same TID.

2. Duplicate NSAP addresses
   In the same ring there are

   - multiple ring nodes from the same NE, or
   - multiple NEs with the same system identifier.

3. Duplicate node IDs
   There are more than 16 nodes in the ring.

Related information

Please also refer to "Automatic node ID allocation" (2-121).

☐

Improper APS Codes

....

Meaning of the alarm   An `Improper APS Codes` alarm is reported

- if an expected request code in the K1byte (bits 1 to 4) is not received within a predefined time limit of two seconds, or

- when invalid K1/K2 bytes are received:

    - APS bytes with an unused channel status code in the K2 byte (bits 6 to 8),

    - APS bytes with an invalid request code in the K1 byte (bits 1 to 4).

Brief alarm overview   The following tabular overview summarizes important information concerning the `Improper APS Codes` alarm:

Alarm identifier (**Probable cause**)	IMAPS
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications   There are no specific local indications.

Effect on protection switching   An existing ring protection switch will be released when the `Improper APS Codes` alarm condition is received on the long path.

Meaning of "short path" and "long path"

In a typical 2-fiber BLSR/MS-SPRing configuration the working traffic will usually be routed the short way around the ring ("short path") as long as no ring protection switching conditions are present. After a ring protection switch due to a failure on the short path the traffic will be routed in the opposite direction, the long way around the ring ("long path").

Trouble clearing   Please refer to "Clearing Improper APS Codes" (3-50).

☐

....

Inconsistent APS Codes

....

Meaning of the alarm	The values of the APS bytes (K1/K2 bytes in the SDH Multiplex Section Overhead (MSOH) or SONET Line Overhead respectively) are not stable, i.e. change too frequently.
	In the twelve frames starting with the last frame containing previously consistent APS bytes, there are not three consecutive frames containing identical K1 and K2 bytes.
Brief alarm overview	The following tabular overview summarizes important information concerning the `Inconsistent APS Codes` alarm:

Alarm identifier (**Probable cause**)	APSC
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications	There are no specific local indications.
Effect on protection switching	An existing ring protection switch will be released when the `Inconsistent APS Codes` alarm condition is received on the long path.

Meaning of "short path" and "long path"

In a typical 2-fiber BLSR/MS-SPRing configuration the working traffic will usually be routed the short way around the ring ("short path") as long as no ring protection switching conditions are present. After a ring protection switch due to a failure on the short path the traffic will be routed in the opposite direction, the long way around the ring ("long path").

Trouble clearing	Please refer to "Clearing Inconsistent APS Codes" (3-55).

☐

....

Inconsistent Ring Protection Mode

Meaning of the alarm   The protection mode is not consistently provisioned for all ring nodes.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Inconsistent Ring Protection Mode` alarm:

Alarm identifier (**Probable cause**)	RNG-IRPM
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications   There are no specific local indications.

Related information   Please also refer to "Automatic discovery of the ring type" (2-122).

Effect on protection switching   BLSR/MS-SPRing protection switching is not possible.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Local Squelch Map Conflict
....

Meaning of the alarm		The ring node's local squelch map contains invalid values for the source and destination nodes of a ring circuit.

Brief alarm overview The following tabular overview summarizes important information concerning the `Local Squelch Map Conflict` alarm:

Alarm identifier (**Probable cause**)	SQMAP-CONFL
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications There are no specific local indications.

Related information Please refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide* for a general description of BLSR/MS-SPRing protection switching.

Ring circuits

A ring circuit is a provisioned path within a ring which can be carrying service or extra traffic.

A ring circuit enters a ring at one or more "source" nodes, continues on the same or on a different tributary within the ring, and is dropped from the ring at one or more "destination" nodes.

Local squelch map

Each NE internally maintains a local view of the source and destination nodes of the ring circuits and the local cross connection information in its local squelch map.

The local squelch map is used by a ring node adjacent to a failed link or failed node to determine which tributary channels between itself and the adjacent node can be protected and which need to be squelched via the insertion of AIS.

....

Trouble clearing   For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

□

Node ID Mismatch

....

Meaning of the alarm	The node IDs in the received APS bytes (K1/K2 bytes in the SDH Multiplex Section Overhead (MSOH) or SONET Line Overhead (LOH) respectively are inconsistent with the ring topology data stored in the node's ring map.

A `Node ID Mismatch` condition causes a ring topology discovery.

Brief alarm overview	The following tabular overview summarizes important information concerning the `Node ID Mismatch` alarm:

Alarm identifier (**Probable cause**)	NID-CONFL
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications	There are no specific local indications.

Trouble clearing	For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

....

Open Ring

....

Meaning of the alarm During a ring topology discovery, an open ring configuration has been detected.

Brief alarm overview The following tabular overview summarizes important information concerning the Open Ring alarm:

Alarm identifier (**Probable cause**)	RNG-OPEN
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications There are no specific local indications.

Trouble clearing For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

....

Ring Discovery in Progress

Meaning of the alarm

A ring topology discovery is currently in progress.

The `Ring Discovery in Progress` alarm is a temporary indication, it is to be understood as an information rather than as an alarm.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Ring Discovery in Progress` alarm:

Alarm identifier (**Probable cause**)	RNG-DSCVY
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Not alarmed
Alarm source	BLSR/MS-SPRing protection group

Local indications

There are no specific local indications.

Ring topology discovery

Please refer to "Automatic discovery of the ring topology" (2-117).

Effect on protection switching

BLSR/MS-SPRing protection switching is temporarily not possible.

Trouble clearing

In the normal case there are no specific trouble clearing measures required for the `Ring Discovery in Progress` alarm, the alarm will be cleared as soon as the ring topology discovery has finished.

If the alarm persists for longer than approximately ten minutes, please refer to "Clearing Ring Discovery in Progress" (3-75).

□

Ring Incomplete

Meaning of the alarm   A `Ring Incomplete` alarm is reported if no correct ring topology can be discovered.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Ring Incomplete` alarm:

Alarm identifier (**Probable cause**)	RNG-INC
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications   There are no specific local indications.

Related information   Please also refer to "Automatic discovery of the ring topology" (2-117).

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846
- Fax: +49 911 526 3131
- E-mail: htransde@lucent.com

Ring Protection Switch Suspended

Meaning of the alarm	MS-SPRing protection switching is suspended. No further MS-SPRing protection switching requests will be processed.
	Protection switching is suspended by a ring node if the node's ring map is invalid or the node does not yet have a node ID. This alarm is typically reported when a new node is added to a ring and does not have a ring map, or if the ring map is invalid.
	The `Ring Protection Switch Suspended` alarm will be cleared as soon as the ring node has a valid node ID and ring map.
Brief alarm overview	The following tabular overview summarizes important information concerning the `Ring Protection Switch Suspended` alarm:

Alarm identifier (**Probable cause**)	RNG-PSS
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications	There are no specific local indications.
Trouble clearing	Please refer to "Clearing Ring Protection Switch Suspended" (3-77).

□

Traffic Squelched

Meaning of the alarm The `Traffic Squelched` alarm is reported by a ring node for each channel on which the traffic has been squelched.

Brief alarm overview The following tabular overview summarizes important information concerning the `Traffic Squelched` alarm:

Alarm identifier (**Probable cause**)	TS
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	BLSR/MS-SPRing protection group

Local indications There are no specific local indications.

Related information Please refer to the *LambdaUnite*™ *MSS User Operations Guide* for a general description of BLSR/MS-SPRing protection switching.

Misconnected traffic

Because the protection channels are shared amongst each span of the ring and may carry extra traffic, each channel is subject to use by multiple services. With no extra traffic on the ring, under certain multiple point failures, such as those that cause the isolation of nodes, services may contend for access to the same protection channel. With extra traffic on the ring, even under single point failures, service on the working channels may contend for access to the same protection channel. These cases yield the potential for misconnected traffic. Therefore, a mechanism to prevent traffic misconnection is provided.

Prevention of traffic misconnection

A potential traffic misconnection is determined by identifying the nodes that will act as the switching nodes for a protection switching bridge request and how the nodes are interconnected (by means of the ring map), and by examining the traffic that will be affected by the switch.

Traffic squelching

Squelching means replacing a potentially misconnected signal by an all-ones signal (Alarm Indication Signal, AIS). In the case of a *LambdaUnite* MSS system, the traffic that cannot be protected will be squelched by replacing the payload signal with AIS (all-ones signal).

Specifically, the traffic that is sourced or dropped at the nodes isolated from the ring by a failure is squelched. In addition, extra traffic circuits that have their source removed due to preemption are squelched.

The following figure provides an example of the squelching functional principle:

1. In a ring consisting of five nodes (A, B, C, D, E), a bidirectional Signal Fail (SF) condition, a "Loss of Signal" for example, occurs between the nodes E and D. This SF condition is protected by a ring protection switch.

2. Afterwards, a second bidirectional SF condition occurs between the nodes B and C.

——————— Working channels

- - - - - - - - - - - Protection channels
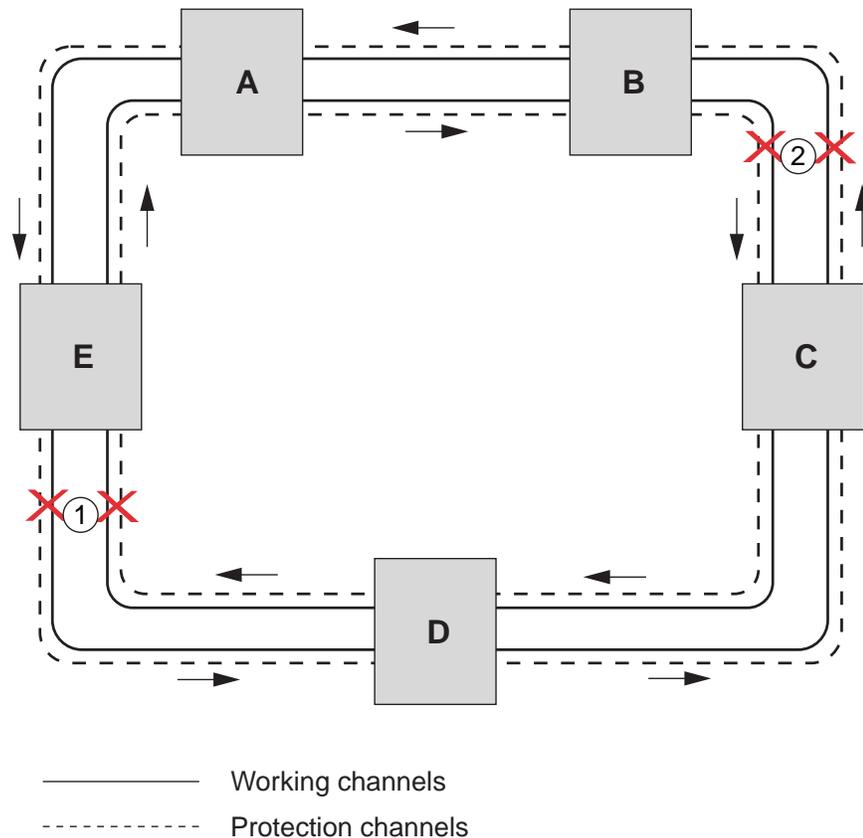
The following squelching occurs:

- Node B
  Any traffic is squelched that

  -   was being transmitted towards node C with C or D as the destination node,

  -   was being received from node C with C or D as the source node.

- Node C
  Any traffic is squelched that

  -   was being transmitted towards node B with A, B or E as the destination node,

  -   was being received from node B with A, B or E as the source node.

- Node D
  Any traffic is squelched that

  - was being transmitted towards node E with A, B or E as the destination node,

  - was being received from node E with A, B or E as the source node.

- Node E
  Any traffic is squelched that

  - was being transmitted towards node D with C or D as the destination node,

  - was being received from node D with C or D as the source node.

Trouble clearing   For the present *LambdaUnite* MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

□

....
365-374-057
Issue a, January 2002

Lucent Technologies

2 - 1 0 3

Unknown Ring Type

Meaning of the alarm   During an automatic discovery of the ring type, the ring type could not be determined.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Unknown Ring Type` alarm:

Alarm identifier (**Probable cause**)	RNG-URT
ASAP type	BLSR/MS SPRing Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Not alarmed
Alarm source	BLSR/MS-SPRing protection group

Local indications   There are no specific local indications.

Related information   Please refer to "Automatic discovery of the ring type" (2-122).

Effect on protection switching   BLSR/MS-SPRing protection switching is not possible.

Trouble clearing   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extent.

If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

Synchronisation alarms

Overview

Purpose   In the following, alarm descriptions are given for the alarms related to the network element synchronisation that can be reported by the *LambdaUnite*™ MSS network elements.

Contents

☐

Circuit Pack Clock Failure

Meaning of the alarm   The circuit pack reporting the alarm is either unable to process the internal system clock signals or is not receiving any clock signals from the system timing function.

Please note that if the `Circuit Pack Clock Failure` condition is present for ***all*** circuit packs of the *LambdaUnite*™ MSS network element an `NE Clock Failure` alarm (cf. "NE Clock Failure" (2-108)) will be reported for the complete system instead of a separate `Circuit Pack Clock Failure` alarm for each circuit pack.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Circuit Pack Clock Failure` alarm:

Alarm identifier (**Probable cause**)	EQPT	
ASAP type	Equipment with SA/NSA	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Circuit pack	

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing Circuit Pack Clock Failure" (3-13).

☐

Loss of Synchronisation

....

Meaning of the alarm   The internal system clock generator is not synchronised externally because ***all*** assigned timing references have failed. Therefore, the internal timing generator has autonomously entered the holdover mode.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Loss of Synchronisation` alarm:

Alarm identifier (**Probable cause**)	SYNCLOSS
ASAP type	System Timing
Alarm category	Communication (Synchronisation)
Alarm severity (default setting)	Major
Alarm source	System

Related information   Please also refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide* for information about timing provisioning.

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing Loss of Synchronisation" (3-60).

◻

....

NE Clock Failure

Meaning of the alarm   A `Circuit Pack Clock Failure` condition is present for ***all*** circuit packs of the *LambdaUnite*™ MSS network element.

Note

In the case of an XC320 switch unit a Circuit Pack Clock Failure condition causes a Circuit Pack Failure alarm to be reported.

Brief alarm overview   The following tabular overview summarizes important information concerning the `NE Clock Failure` alarm:

Alarm identifier (**Probable cause**)	SYNCCLK
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	System

Local indications   The red "FAULT" LED on the faceplate of the XC320 switch unit(s) is constantly lit.

Trouble clearing   Please refer to "Clearing NE Clock Failure" (3-61).

Protection Clock Input Fail

Meaning of the alarm There is either no clock signal available at the protection timing reference input of the respective circuit pack, or the available clock signal is not suitable for synchronisation.

Brief alarm overview The following tabular overview summarizes important information concerning the `Protection Clock Input Fail` alarm:

Alarm identifier (**Probable cause**)	CSDPF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Clock and synchronisa-tion distribution The clock and synchronisation distribution function (CSD function, located on each circuit pack) is supplied with a working and a protection timing reference from the system timing function (located on the working or protection XC320 circuit pack, respectively). In addition, an internal oscillator is available on each circuit pack which serves as the timing reference when both timing references from the system timing function are unavailable or not suitable for synchronisation.

Trouble clearing Please refer to "Clearing Protection Clock Input Fail" (3-69).

☐

T4 quality unsufficient

Meaning of the alarm   The quality of the relevant timing reference for the external timing output (T4 timing output) is insufficient. The external timing output has been switched off ("squelched").

Brief alarm overview   The following tabular overview summarizes important information concerning the T4 quality unsufficient alarm:

Alarm identifier (**Probable cause**)	SYNCT4OUT
ASAP type	System Timing
Alarm category	Communication (Synchronisation)
Alarm severity (default setting)	Major
Alarm source	External timing output

Local indications   There are no specific local indications.

Trouble clearing   Please refer to "Clearing T4 quality unsufficient" (3-81).

☐

Timing Reference Failure

Meaning of the alarm There is no clock source connected to an external or line timing input that is assigned as a timing reference, or the signal connected is not suitable for synchronisation.

Brief alarm overview The following tabular overview summarizes important information concerning the `Timing Reference Failure` alarm:

Alarm identifier (**Probable cause**)	SYNCRF
ASAP type	System Timing
Alarm category	Communication (Synchronisation)
Alarm severity (default setting)	Major
Alarm source	External or line timing reference

Local indications There are no specific local indications.

Trouble clearing Please refer to "Clearing Timing Reference Failure" (3-83).

☐

Worker Clock Input Fail

Meaning of the alarm   There is either no clock signal available at the working timing reference input of the respective circuit pack, or the available clock signal is not suitable for synchronisation.

Brief alarm overview   The following tabular overview summarizes important information concerning the `Worker Clock Input Fail` alarm:

Alarm identifier (**Probable cause**)	CSDWF
ASAP type	Equipment without SA/NSA
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

Local indications   The red "FAULT" LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red "FAULT" LED to be constantly lit).

Clock and synchronisation distribution   The clock and synchronisation distribution function (CSD function, located on each circuit pack) receives a working and a protection timing reference from the system timing function (located on the working or protection XC320 circuit pack, respectively). In addition, an internal oscillator is available on each circuit pack which serves as the timing reference when both timing references from the system timing function are unavailable or not suitable for synchronisation.

Trouble clearing   Please refer to "Clearing Worker Clock Input Fail" (3-96).

☐

Additional alarm-related information

Overview

Purpose   This chapter provides additional information for network element alarms that might be useful to understand the meaning of alarms and to locate their origin.

Contents

BLSR/MS-SPRing management information

Terms and definitions   Please refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide* for a general description of BLSR/MS-SPRing protection switching.

Ring node

A BLSR/MS-SPRing consists of at least two and at most 16 nodes (cf. <u>"Maximum number of ring nodes" (2-121)</u>).

Each ring node is characterized by the NE name (TID), the protection group AID, the East (E) and West (W) interface port information, the node ID, and the associated ring ID.

Multiple ring nodes from the same NE on the same ring are not allowed. If such a situation occurs a `Duplicate Ring Node` alarm will be generated.

NE name (TID)

The NE name, also referred to as the NE's target identifier (TID), is an alphanumeric string of up to 20 characters, used to uniquely identify a network element within the network.

Important!

Protection group AID

The protection group AID is the port AID associated with a port protection group. It is unique within an NE and used to distinguish the different port protection groups. Each ring node in a network is uniquely identified by the NE name (TID) in connection with the protection group AID.

East/West interface ports

The east (E) and west (W) interface port information is required to determine the directionality of a link within a ring circuit.

Node ID

Each node within a ring is automatically allocated a node identifier (node ID) which is used to uniquely identify a ring node within a ring. The node ID value may range from 0 to 15.

Ring ID

To uniquely identify rings within a network, each ring can be assigned a ring identifier (ring ID, an alphanumeric string of up to 15

characters) when a port protection group is configured for a ring node. All ring nodes in the same ring have the same ring ID.

Link ID

To support ring protection switching and the display of ring configuration information on graphical user interfaces, each ring node maintains the following information for each link to a neighbouring ring node:

- the local NE name (TID), port ID and the east (E) and west (W) interface port information of the local end of the link,

- the ring neighbour's NE name (TID), port ID and the east (E) and west (W) interface port information of the remote end of the link.

The link ID information is required to discover a given ring topology. The link ID information is discovered upon initial link startup and is modified dynamically when changes to the link ID information occur (for example, when the name of a neighbouring NE is changed, or a node is added to or removed from a ring). After the links are discovered, the sequence of links around the ring is determined. This information is used to assign node IDs to each node of the ring and to create a ring map. Please also refer to "Automatic discovery of the ring topology" (2-117).

Link map

The link map contains a list of link IDs, starting with the local node's east link and ordered by their sequence in the ring.

Ring map

Each NE internally maintains a ring map in its non-volatile memory (NVM). The ring map serves to identify the relative position of all nodes within a ring.

The ring map contains the ring ID assigned to the ring and a list of all ring nodes, identified by their node IDs and ordered by their sequence of occurrence in the ring. Because the list does not necessarily start with the local node, the ring map also contains the node ID of the local node, and because the ring protection switching signalling requires node IDs instead of TIDs, the ring map additionally contains a mapping of TIDs to node IDs.

Please also refer to "Automatic discovery of the ring topology" (2-117).

....
365-374-057
Issue a, January 2002

Lucent Technologies

2 - 1 1 5

Ring circuits

A ring circuit is a provisioned path within a ring which can be carrying service or extra traffic.

A ring circuit enters a ring at one or more "source" nodes, continues on the same or on a different tributary within the ring, and is dropped from the ring at one or more "destination" nodes.

Local squelch map

Each NE internally maintains a local view of the source and destination nodes of the ring circuits and the local cross connection information in its local squelch map.

The local squelch map is used by a ring node adjacent to a failed link or failed node to determine which tributary channels between itself and the adjacent node can be protected and which need to be squelched via the insertion of AU-AIS.

□

Automatic discovery of the ring topology

Introduction   As a prerequisite for BLSR/MS-SPRing protection switching the topology of the ring must be known at each ring node. *LambdaUnite*™ MSS network elements have a proprietary algorithm implemented to discover the ring topology automatically.

Closed ring

A closed ring consists of network elements which are all equipped and cabled with optical interface circuit packs for both the east (E) and west (W) directions.

Example of a closed ring:
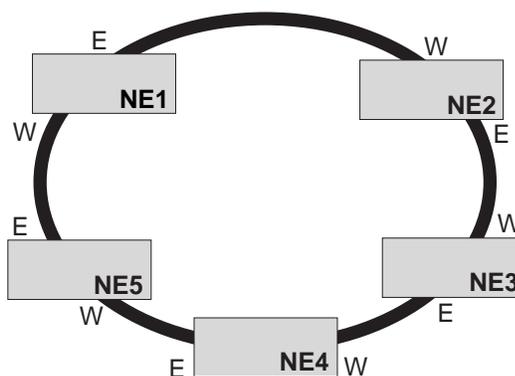
Open ring

An open ring is a linear configuration of network elements where the two end nodes are equipped and/or cabled with optical interface circuit packs for only one direction.

Example of an open ring:
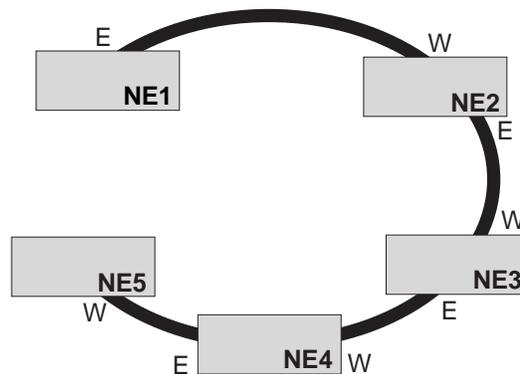
In a 2-fiber BLSR/MS-SPRing, an open ring configuration will automatically be detected by the *LambdaUnite* MSS network elements, and an Open Ring alarm will be reported in that case.

Ring topology data   Each ring node inserts or appends the following ring topology data (ring data) to a message which it sends or forwards over a DCN association to its neighbour on the ring:

- Its own NSAP address and TID.
  The system identifier in the NSAP address is also used for automatic allocation of the node ID (cf. "Automatic node ID allocation" (2-121)).

- The interface port identification and the east/west (E/W) directionality information of the link to its neighbour.

This way, at each ring node sufficient information is available to form a ring map representing the ring topology.

Trigger for the topology discovery   The discovery of the ring topology is initiated by a ring node when the ring node is first created by the provisioning of an BLSR/MS-SPRing port protection group, or when the DCC controller on the Controller (CTL) is re-initialized.

Discovery of a closed ring topology

The ring topology data (ring data) "circles" once around the ring until the node that initiated the ring topology discovery again receives a corresponding message. The following figure shows the ring topology discovery for a ring of five nodes as an example.
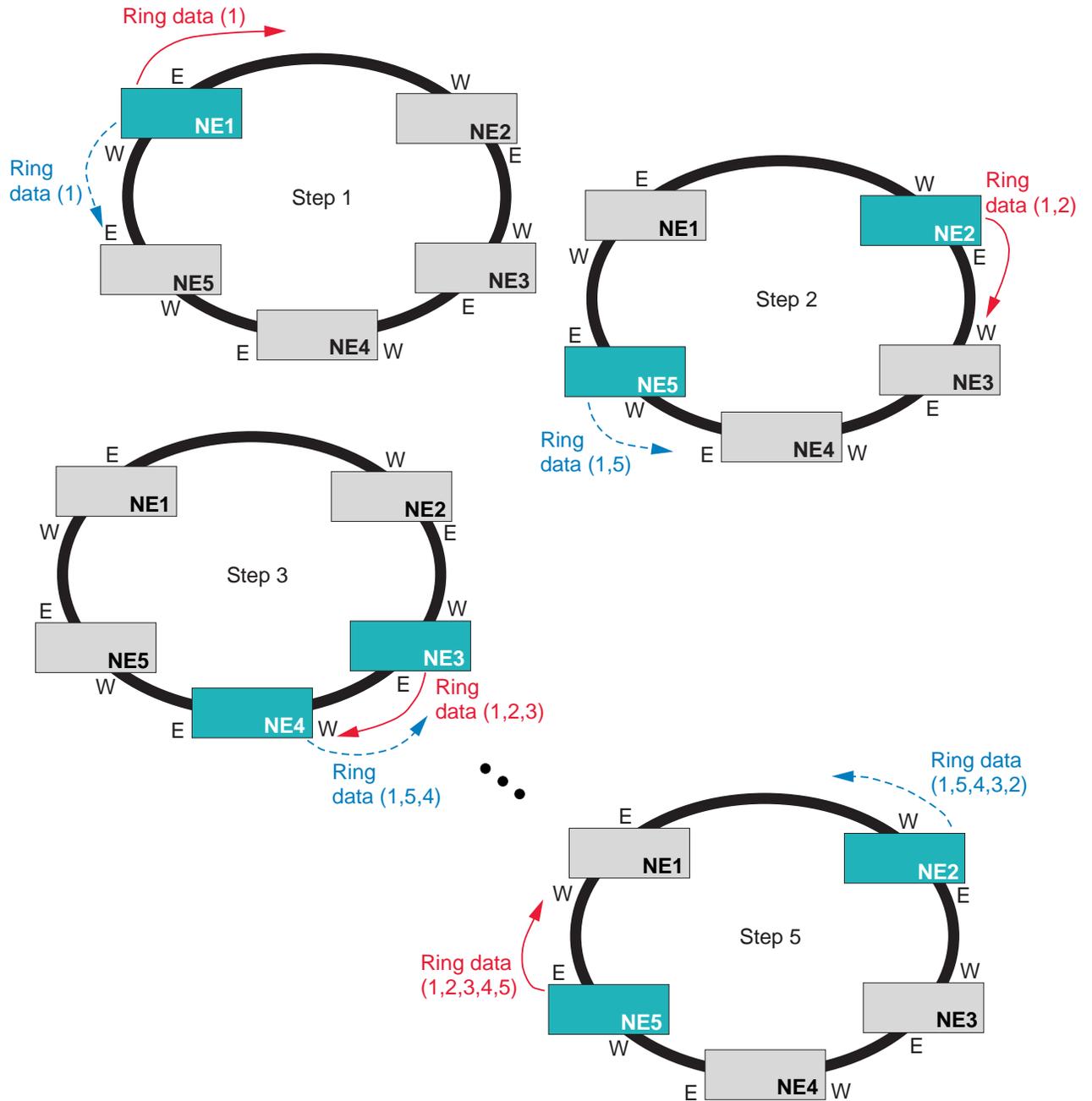
Related alarms   These alarms are related to the ring topology discovery:

- Ring Discovery in Progress
- Ring Incomplete
- Open Ring

☐

Automatic node ID allocation
....

Node identifier (node ID)   Each node within a ring is automatically allocated a node identifier (node ID). The node ID is a 4-bit address used in the BLSR/MS-SPRing protection switching protocol to uniquely identify a ring node within a ring.

Principle of node ID allocation   All nodes of a ring are ordered according to their system identifier, the IEEE 802.3 MAC address in the "SYSTEM" field of the NSAP address. For this purpose, the ring nodes distribute their system identifier values over the ring to every other node on the ring.

The ring node with the lowest system identifier value is allocated a node ID of "0". The remaining node IDs are allocated in ascending order in accordance with the value of their system identifier. The following table shows an example for a ring of five nodes.

NE name (TID)	System Identifier (in hexadecimal-representation)	Node ID
NE3	00 00 00 01 20 40	0
NE1	00 00 00 45 A3 21	1
NE4	00 00 00 80 0B 54	2
NE5	00 00 03 76 D0 88	3
NE2	00 00 09 9C 99 32	4

Re-allocation of node IDs   Node IDs may change in value, they will be re-allocated when:

•   a node is added to the ring,

•   a node is deleted from the ring, or

•   the Controller (CTL) is re-initialized.

Maximum number of ring nodes   As the node ID is a 4-bit address, its value may vary from 0 to 15, thus the maximum number of nodes in a ring is restricted to 16.

☐

....

Automatic discovery of the ring type

Introduction In parallel to the discovery of the ring topology (cf "Automatic discovery of the ring topology" (2-117)), a discovery of the ring type takes place. This means that the type of network elements involved in the ring is evaluated. The discovery of the ring type also includes the evaluation of the signal level (port type) and the ring protection mode used.

Ring type discovery *LambdaUnite*™ MSS network elements have a proprietary algorithm implemented to automatically discover the ring type of other nodes in the ring. The discovery of the ring type is required to determine the compatibility of the nodes in the ring and to derive information specific to ring interworking.

The information exchanged during the discovery of the ring type includes:

- NE type
  NE types that are "known" to *LambdaUnite* MSS network elements are:

  - *WaveStar*® BandWidth Manager,

  - *WaveStar* TDM 2.5G (OC-48 2F),

  - *WaveStar* TDM 10G (OC-192 2F),

  - *WaveStar* TDM 10G (STM-64),

  - FT-2000 OC-48 Lightwave System,

  - *WaveStar* ADM 16/1,

  - *WaveStar* LambdaChameleon,

  - *LambdaUnite* MSS.

- Port type
  Possible port types are STM-16, STM-64, STM-256, OC-48, OC-192 or OC-768 (STM-256 and OC-768 are not supported in *LambdaUnite* MSS Release 1.0).

- Ring protection mode
  Possible ring protection modes are BLSR, MS-SPRing, BCSR or BCSR_restPA (BCSR and BCSR_restPA are not supported in *LambdaUnite* MSS Release 1.0).

Ring types   Based on the information exchanged during the discovery of the ring type, the following ring types can be determined by a *LambdaUnite* MSS ring node:

- Lucent Technologies SONET ring

  - NE type
    WaveStar BandWidth Manager, *WaveStar* TDM 2.5G (OC-48 2F), *WaveStar* TDM 10G (OC-192 2F) or *LambdaUnite* MSS.

  - Port type
    OC-48, OC-192 or OC-768 (OC-768 ports are not supported in *LambdaUnite* MSS Release 1.0).

  - Ring protection mode
    BLSR

- Lucent Technologies SDH ring

  - NE type
    WaveStar BandWidth Manager, *WaveStar* TDM 10G (STM-64), *WaveStar* LambdaChameleon or *LambdaUnite* MSS.

  - Port type
    STM-16, STM-64 or STM-256 (STM-256 interface ports are not supported in *LambdaUnite* MSS Release 1.0).

  - Ring protection mode
    MS-SPRing, BCSR or BCSR_restPA.

- Unknown ring type
  A ring is considered to be of an unknown ring type if the combinations of NE type, port type and ring protection mode are not in one of the above categories, or if the information for discovering the ring type is not available after a predefined time interval (timeout).

☐

....

365-374-057
Issue a, January 2002

Lucent Technologies

2 - 1 2 3

3   Trouble clearing

Overview

Purpose   The present chapter provides step-by-step procedures to localize and clear network element alarms.

Support   For the present *LambdaUnite*™ MSS release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extend. If you need technical support please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

- Phone: +49 911 526 2846

- Fax: +49 911 526 3131

- E-mail: htransde@lucent.com

Contents

Clearing Alarm Indication Signal (AIS-L)

Purpose   Use this procedure to clear an `Alarm Indication Signal` (AIS-L) alarm.

Related information

Please also refer to the corresponding alarm description → "Alarm Indication Signal (AIS-L)" (2-74).

Instructions   Proceed as follows to clear an `Alarm Indication Signal` (AIS-L) alarm.

1   Analyze the alarm state of the upstream equipment and take appropriate measures.

E N D   O F   S T E P S

□

Clearing Alarm Indication Signal (AIS-P)

Purpose   Use this procedure to clear an `Alarm Indication Signal` (AIS-P) alarm.

Related information

Please also refer to the corresponding alarm description → "Alarm Indication Signal (AIS-P)" (2-50).

Instructions   Proceed as follows to clear an `Alarm Indication Signal` (AIS-P) alarm.

1   Analyze the alarm state of the upstream equipment and take appropriate measures.

E ND   OF   S TEPS

□

Clearing Backplane Read Failure

Purpose   Use this procedure to clear a `Backplane Read Failure` alarm.

Related information

Please also refer to the corresponding alarm description →
"Backplane Read Failure" (2-18).

Before you begin   You or a service technician should be on-site at the NE to clear a
`Backplane Read Failure` alarm.

Prior to performing the following trouble clearing procedure, you
must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the
  alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement Controller (CTL)

Trouble clearing procedure   Proceed as follows to clear a `Backplane Read Failure` alarm:

1   Perform a controller reset of the CTL.

   Reference: Please refer to:

   - "Initiating a circuit pack reset" (4-47)

2   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
     alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3   Perform a full reset of the CTL, and wait for the system to
     re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
  - SDH: Multiplex Section Protection (MSP) and MS-SPRing
  - SONET: Line Protection and BLSR

  Reference: Please refer to:

  - "Initiating a circuit pack reset" (4-47)

....

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Replace the Controller (CTL).

  Reference: Please refer to:

  - "Replacing the Controller (CTL)" (4-42)

....

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing CICTL Comm Failure

....

Purpose Use this procedure to clear a `CICTL Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "CICTL Comm Failure" (2-19).

Before you begin You or a service technician must be on-site at the NE to clear a `CICTL Comm Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

* have a valid user login and password for the *WaveStar*® CIT, and
* have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

* *WaveStar* CIT
* A replacement CI-CTL (Connection Interface of the Controller)

Trouble clearing procedure Proceed as follows to clear a `CICTL Comm Failure` alarm:
....

1 At the CI-CTL and at the fan unit, check the connectors of the fan unit control cable.

If …	then …
both connectors are connected properly	proceed with the next step.
any of the connectors is not properly connected	connect the respective connector(s) properly, and then proceed with the next step.

....

2 Perform a controller reset of the CTL.

Reference: Please refer to:

* "Initiating a circuit pack reset" (4-47)

....
Lucent Technologies

....

3   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

4   Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and

- Automatic Protection Switching (APS) on MS/Line level

    - SDH: Multiplex Section Protection (MSP) and MS-SPRing

    - SONET: Line Protection and BLSR

    Reference: Please refer to:

    - "Initiating a circuit pack reset" (4-47)

....

5   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

6   Replace the CI-CTL.

....

7   Perform a full reset of the CTL, and wait for the system to re-initialize.

....

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and

- Automatic Protection Switching (APS) on MS/Line level

    - SDH: Multiplex Section Protection (MSP) and MS-SPRing

    - SONET: Line Protection and BLSR

    Reference: Please refer to:

    - "Initiating a circuit pack reset" (4-47)

....

8   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

9   Replace the fan unit control cable, and then perform a controller reset of the CTL.

    Reference: Please refer to:

    - "Initiating a circuit pack reset" (4-47)

....

10   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

11   Replace the fan unit, and then perform a controller reset of the CTL.

    Reference: Please refer to:

    - "Replacing the fan unit" (4-15)

    - "Initiating a circuit pack reset" (4-47)

....

....

12   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

□

....

365-374-057
Issue a, January 2002

Lucent Technologies

3 - 1 1

Clearing CICTL not Present

....

Purpose Use this procedure to clear a `CICTL not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "CICTL not Present" (2-20).

Before you begin You or a service technician must be on-site at the NE to clear a `CICTL not Present` alarm.

Required equipment

Make sure that the following equipment is available:

- A replacement Controller (CTL)

Trouble clearing procedure Proceed as follows to clear a `CICTL not Present` alarm:

....

1 Check if the CI-CTL (Connection Interface of the Controller) is plugged in slot 51 on the rear side of the shelf.

If …	then …
the CI-CTL is plugged	replace the CTL. **Reference:** Please refer to: • "Replacing the Controller (CTL)" (4-42)
the CI-CTL is not plugged	insert the CI-CTL.

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

☐

Lucent Technologies

Clearing Circuit Pack Clock Failure

Purpose   Use this procedure to clear a `Circuit Pack Clock Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Circuit Pack Clock Failure" (2-106).

Before you begin   You or a service technician must be on-site at the NE to clear a `Circuit Pack Clock Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement circuit pack for the circuit pack reporting the alarm
- A replacement XC320 switch unit

Trouble clearing procedure   Proceed as follows to clear a `Circuit Pack Clock Failure` alarm:

1   Depending on whether one or more circuit packs report the alarm:

If …	then …
the alarm is reported by only one circuit pack	replace the circuit pack reporting the alarm. **Reference:** Please refer to: - "Replacing a circuit pack by a circuit pack of the same type" (4-39)

If …	then …
the alarm is reported by several circuit packs	replace the XC320 switch unit (replacing the standby circuit pack is sufficient). **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-39)

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E ND OF S TEPS

□

Clearing Circuit Pack Comm Failure

Purpose   Use this procedure to clear a `Circuit Pack Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Circuit Pack Comm Failure" (2-21).

Before you begin   You or a service technician should be on-site at the NE to clear a `Circuit Pack Comm Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement circuit pack for the circuit pack reporting the alarm
- A replacement Controller (CTL)

Trouble clearing procedure   Proceed as follows to clear a `Circuit Pack Comm Failure` alarm:

1   Perform a controller reset of the circuit pack reporting the alarm.

   Reference: Please refer to:

   - "Initiating a circuit pack reset" (4-47)

2   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3   Perform a controller reset of the CTL.

> **Reference:** Please refer to:
> - "Initiating a circuit pack reset" (4-47)

4   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

5   Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
  - SDH: Multiplex Section Protection (MSP) and MS-SPRing
  - SONET: Line Protection and BLSR

> **Reference:** Please refer to:
> - "Initiating a circuit pack reset" (4-47)

6   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

7   Perform a full reset of the circuit pack reporting the alarm.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-47)

....

8 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

9 Replace the Controller (CTL).

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-42)

....

10 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

11 Replace the circuit pack reporting the alarm.

....

12 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.

....

If …	then …
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

END OF STEPS

Clearing Circuit Pack not Present

Purpose Use this procedure to clear a `Circuit Pack not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "Circuit Pack not Present" (2-23).

Before you begin You or a service technician must be on-site at the NE to clear a `Circuit Pack not Present` alarm.

Required equipment

Make sure that the following equipment is available:

- A replacement circuit pack of the correct type

Trouble clearing procedure Proceed as follows to clear a `Circuit Pack not Present` alarm:

1 Check if a circuit pack is plugged in the slot for which the `Circuit Pack not Present` alarm is reported.

If …	then …
a circuit pack is plugged	replace the CTL. **Reference:** Please refer to: - "Replacing the Controller (CTL)" (4-42)
no circuit pack is plugged	insert a circuit pack of the correct type (acc. to the actual provisioning).

E N D   O F   S T E P S

☐

Clearing Circuit Pack Type Mismatch

Purpose Use this procedure to clear a `Circuit Pack Type Mismatch` alarm.

Related information

Please also refer to the corresponding alarm description → "Circuit Pack Type Mismatch" (2-24).

Before you begin You or a service technician must be on-site at the NE to clear a `Circuit Pack Type Mismatch` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement circuit pack of the correct type

Trouble clearing procedure Proceed as follows to clear a `Circuit Pack Type Mismatch` alarm:

1 Check if the latches of the circuit pack are closed.

If …	then …
the latches are closed	proceed with the next step.
the latches are not closed	close the latches, and then proceed with the next step.

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.

If …	then …
the alarm persists	proceed with the next step.

3   Verify that the provisioning for the slot, for which the `Circuit Pack Type Mismatch` alarm is reported, is according to your needs.

If …	then …
the provisioning is correct	replace the affected circuit pack. The circuit pack EEPROM seems to be defective.
the provisioning is not correct	correct the provisioning.

E N D   O F   S T E P S

☐

Clearing Circuit Pack Failure

....

Purpose   Use this procedure to clear a `Circuit Pack Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Circuit Pack Failure" (2-22).

Before you begin   You or a service technician should be on-site at the NE to clear a `Circuit Pack Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement circuit pack of the same type

Trouble clearing procedure   Proceed as follows to clear a `Circuit Pack Failure` alarm:

....

1   Replace the faulty circuit pack with a circuit pack of the same type.

       Reference: Please refer to:

- "Replacing a circuit pack by a circuit pack of the same type" (4-39)

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

□

....

Clearing Comm Channel Failure

....

Purpose Use this procedure to clear a `Comm Channel Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Comm Channel Failure" (2-25).

Before you begin You or a service technician must be on-site at the NE to clear a `Comm Channel Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement Controller (CTL)
- A replacement XC320 switch unit

Trouble clearing procedure Proceed as follows to clear a `Comm Channel Failure` alarm:
....

1 Perform a full reset of the XC320 switch unit.

 Reference: Please refer to:

 - "Initiating a circuit pack reset" (4-47)

....

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

365-374-057
Issue a, January 2002

Lucent Technologies

3 - 2 3

....

3 Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and

- Automatic Protection Switching (APS) on MS/Line level

   - SDH: Multiplex Section Protection (MSP) and MS-SPRing

   - SONET: Line Protection and BLSR

   Reference: Please refer to:

   - "Initiating a circuit pack reset" (4-47)

....

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Replace the CTL.

   Reference: Please refer to:

   - "Replacing the Controller (CTL)" (4-42)

....

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

7 Replace the XC320 switch unit.

....

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-42)

....

8 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E ND OF S TEPS

☐

Clearing CTL Comm Failure

....

Purpose Use this procedure to clear a `CTL Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "CTL Comm Failure" (2-26).

Before you begin You or a service technician should be on-site at the NE to clear a `CTL Comm Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement Controller (CTL)

Trouble clearing procedure Proceed as follows to clear a `CTL Comm Failure` alarm:

....

1 Perform a controller reset of the CTL.

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

....

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

3 Perform a full reset of the CTL, and wait for the system to re-initialize.

....

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
    - SDH: Multiplex Section Protection (MSP) and MS-SPRing
    - SONET: Line Protection and BLSR

    Reference: Please refer to:

    - "Initiating a circuit pack reset" (4-47)

....

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Replace the CTL.

    Reference: Please refer to:

    - "Replacing the Controller (CTL)" (4-42)

....

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing Default K-bytes

....

Purpose Use this procedure to clear a `Default K-bytes` alarm.

Related information

Please also refer to the corresponding alarm description → "Default K-bytes" (2-87).

Before you begin You or a service technician must be on-site at the NE to clear a `Default K-bytes` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

The following equipment is required:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear a `Default K-bytes` alarm.

....

1 At the *WaveStar* CIT, open the alarm list.

....

2 Determine the port AID for which the alarm is reported from the **AID** column of the *WaveStar* CIT **NE Alarm List**.

....

3 Are other alarms, related to BLSR/MS-SPRing protection switching (for example `Ring Incomplete`, `Ring Discovery in Progress` (persistently) or `Ring Protection Switch Suspended`), reported at the same time for the same port?

If …	then …
other BLSR/MS-SPRing alarms are reported	clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.

....

Lucent Technologies

If …	then …
no other BLSR/MS-SPRing alarms are reported	proceed with Step 5.

....

4 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Are other transmission alarms (SD/SF conditions) reported at the same time for the same port?

If …	then …
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
No	proceed with Step 7

....

6 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

7 Determine the AIDs of the two network elements involved.

....

365-374-057
Issue a, January 2002

Lucent Technologies

3 - 2 9

Refer to the following figure for clarification and further reference. The `Default K-bytes` alarm is reported on node A, port q.

....

8   Perform a Forced Switch (FS-R) at the transmitter (node B, port p).

....

9   Check the switch status of the network elements.

If …	then …
the Forced Switch has been executed correctly	remove and re-insert the transmitter circuit pack (node B, port p), and then proceed with the next step.
the Forced Switch has *not* been executed correctly	clear the Forced Switch and abort the procedure.

....

10   Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

11   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 18.
the alarm persists	proceed with the next step.

....

12   Replace the transmitter circuit pack (node B, port p) with a circuit pack of the same type.

> **Reference:** Please refer to:
> - "Replacing a circuit pack by a circuit pack of the same type" (4-39)

....

Lucent Technologies

....

13 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

14 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 18.
the alarm persists	proceed with the next step.

....

15 Replace the alarm-reporting circuit pack (node A, port q) with a circuit pack of the same type.

> **Reference:** Please refer to:
> * "Replacing a circuit pack by a circuit pack of the same type" (4-39)

....

16 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

17 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

If …	then …
the alarm has cleared	proceed with the next step.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	• Phone: +49 911 526 2846
	• Fax: +49 911 526 3131
	• E-mail: htransde@lucent.com

....

18 Clear the Forced Switch at the transmitter (node B, port p).

....

19 Check the switch status of the network elements, and determine if the Forced Switch has been cleared.

20 If you need further support, please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

Phone   +49 911 526 2846

Fax   +49 911 526 3131

E-mail   htransde@lucent.com

E ND OF S TEPS

□

Clearing Fan Failure

Purpose Use this procedure to clear a `Fan Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Fan Failure" (2-27).

Before you begin You or a service technician must be on-site at the NE to clear a `Fan Failure` alarm.

Required equipment

Make sure that the following equipment is available:

• A fully functional fan unit

Fan speed The information that a fan has failed is derived from the fan speed. If the fan speed drops below a certain value, then the fan is likely to be faulty.

Opening angle of the non-return valves

In normal operation the fan speed may vary between 2000 and 4400 RPM (rotations per minute) in steps of 400 RPM. An operational fan produces an airflow which opens the non-return valves. The opening angle of the non-return valves depends on the amount of airflow passing through. Thus, the opening angle of the non-return valves can be used to make a rough estimate of the fan speed.

To give you a clue, the following figure shows the non-return valves
at three different fan speeds.
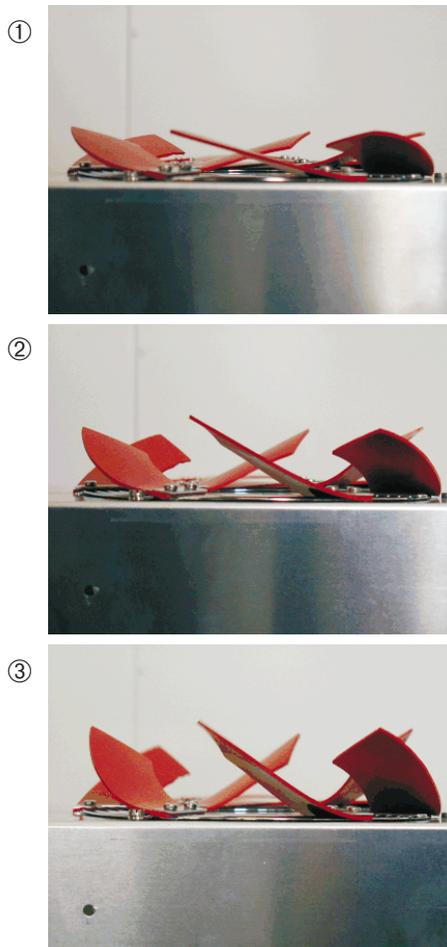
Legend:

1   2000 RPM, opening angle approx. 16°

2   3200 RPM, opening angle approx. 30°

3   4400 RPM, opening angle approx. 35°

Trouble clearing procedure   Proceed as follows to clear a `Fan Failure` alarm:

1   Replace the fan unit.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)

E N D   O F   S T E P S

□

Clearing Fan Unit Comm Failure

....

Purpose   Use this procedure to clear a `Fan Unit Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → <u>"Fan Unit Comm Failure" (2-28)</u>.

Before you begin   You or a service technician must be on-site at the NE to clear a `Fan Unit Comm Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement fan unit control cable

- A replacement CI-CTL (Connection Interface of the Controller)

Trouble clearing procedure   Proceed as follows to clear a `Fan Unit Comm Failure` alarm:
....

1   At the CI-CTL and at the fan unit, check the connectors of the fan unit control cable.

If …	then …
both connectors are connected properly	proceed with the next step.
any of the connectors is not properly connected	connect the respective connector(s) properly, and then proceed with the next step.

....

2   Perform a controller reset of the CTL.

Reference: Please refer to:

- <u>"Initiating a circuit pack reset" (4-47)</u>

....

3   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

4   Replace the fan unit control cable.

5   Perform a controller reset of the CTL.

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

6   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

7   Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
    - SDH: Multiplex Section Protection (MSP) and MS-SPRing
    - SONET: Line Protection and BLSR

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

....

8   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

9   Replace the CI-CTL.

....

10   Perform a full reset of the CTL, and wait for the system to
re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL
affects

- MS/Line performance monitoring, and

- Automatic Protection Switching (APS) on MS/Line level

  - SDH: Multiplex Section Protection (MSP) and MS-SPRing

  - SONET: Line Protection and BLSR

  Reference: Please refer to:

  - "Initiating a circuit pack reset" (4-47)

....

11   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

12   Replace the fan unit control cable, and then perform a controller reset
of the CTL.

  Reference: Please refer to:

  - "Initiating a circuit pack reset" (4-47)

....

13   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

14   Replace the fan unit, and then perform a controller reset of the CTL.

>   **Reference:** Please refer to:
>   - "Replacing the fan unit" (4-15)
>   - "Initiating a circuit pack reset" (4-47)

15   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing Fan Unit Failure

....

Purpose   Use this procedure to clear a `Fan Unit Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Fan Unit Failure" (2-29).

Before you begin   You or a service technician must be on-site at the NE to clear a `Fan Unit Failure` alarm.

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A fully functional fan unit

- Two replacement fan unit power cables

- Two replacement Power Interfaces

Trouble clearing procedure

⚠️ **CAUTION**

A network element may fail without proper cooling.

A network element which is operated without a functional fan unit for more than two minutes may fail due to overheating.

Therefore, do not operate a network element without a functional fan unit.

....

Lucent Technologies

Proceed as follows to clear a `Fan Unit Failure` alarm:

1 Replace the fan unit.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3 During the following steps, refresh and check the alarm list *in regular intervals*. If a `Unit Temperature too High` alarm should be reported, refer to "Unit Temperature too High in combination with Fan Unit Failure" (3-43) .

4 Are both the fan unit power connectors ("Power Input A/B") and the corresponding Power Interface (PI) connectors "(FAN output)" connected properly?

If …	then …
yes	proceed with Step 6.
no	connect the connectors properly, and then proceed with the next step.

5 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

6   Successively replace both fan unit power cables.

....

7   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

8   Replace PI A.

....

9   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

10   Replace PI B.

....

11   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.

....

If …	then …
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	• Phone: +49 911 526 2846
	• Fax: +49 911 526 3131
	• E-mail: htransde@lucent.com

E N D   O F   S T E P S

Unit Temperature too High **in combination with** Fan Unit Failure

If a Unit Temperature too High alarm is reported while a Fan Unit Failure alarm is present, then it is up to your discretion how to proceed. You may take one of the following actions:

Possible action	Consequences
You may switch off the NE to prevent circuit packs from being seriously damaged due to overheating.	All traffic managed by the respective NE will be interrupted. However, it might be an option to wait a while (at least ten minutes) to let the circuit packs cool off, switch on the NE again, and then proceed with the trouble clearing procedure. *Important:* Before switching off the NE, follow the instructions given in Step 1 of the procedure "Replacing the Controller (CTL)" (4-42) to remove the Controller (CTL) from its slot.
You may remove the affected circuit pack from the system to prevent it from being seriously damaged due to overheating.	The traffic managed by the respective circuit pack will be interrupted. The circuit pack can be re-inserted after the Fan Unit Failure alarm is cleared.
You might ignore the Unit Temperature too High alarm.	There is a **high risk** of seriously damaging circuit packs due to overheating.

Clearing Fan Voltage Feed A Failure

....

Purpose Use this procedure to clear a `Fan Voltage Feed A Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "Fan Voltage Feed A Failure" (2-30).

Before you begin You or a service technician must be on-site at the NE to clear a `Fan Voltage Feed A Failure` alarm.

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement fan unit power cable

- A replacement Power Interface (PI)

Trouble clearing procedure Proceed as follows to clear a `Fan Voltage Feed A Failure` alarm:

....

1 Is a fan unit power cable installed between "Power Input A" of the fan unit and the "FAN output" of the Power Interface A (PI A)?

If …	then …
yes	proceed with Step 3.
no	install a fan unit power cable between "Power Input A" of the fan unit and the "FAN output" of the PI A, and then proceed with the next step.

....

Lucent Technologies

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3 Are the connectors of the power cable connected properly at both the "Power Input A" of the fan unit and the "FAN output" of the PI A?

If …	then …
yes	proceed with Step 7.
no	connect the connectors properly, and then proceed with the next step.

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

5 At the *WaveStar* CIT, check the **NE Alarm List**.

If …	then …
a System Power Failure alarm is reported at the same time	clear this alarm first (cf. "Clearing System Power Failure" (3-80)), and then proceed with the next step.
no System Power Failure alarm is reported	close the circuit breaker on the PI A.

....

6   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

7   Replace the fan unit power cable between "Power Input A" of the fan unit and the "FAN output" of the PI A.

....

8   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

9   Replace PI A.

....

10   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

END OF STEPS

....

Clearing Fan Voltage Feed B Failure

Purpose   Use this procedure to clear a `Fan Voltage Feed B Failure` alarm.

Related information

Please also refer to the corresponding alarm description → <u>"Fan Voltage Feed B Failure" (2-31)</u>.

Before you begin   You or a service technician must be on-site at the NE to clear a `Fan Voltage Feed B Failure` alarm.

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement fan unit power cable
- A replacement Power Interface (PI)

Trouble clearing procedure   Proceed as follows to clear a `Fan Voltage Feed B Failure` alarm:

1   Is a fan unit power cable installed between "Power Input B" of the fan unit and the "FAN output" of the Power Interface B (PI B)?

If …	then …
yes	proceed with <u>Step 3</u>.
no	install a fan unit power cable between "Power Input B" of the fan unit and the "FAN output" of the PI B, and then proceed with the next step.

....

2   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

3   Are the connectors of the power cable connected properly at both the
"Power Input B" of the fan unit and the "FAN output" of the PI B?

If …	then …
yes	proceed with Step 7.
no	connect the connectors properly, and then proceed with the next step.

....

4   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5   At the *WaveStar* CIT, check the **NE Alarm List**.

If …	then …
a System Power Failure alarm is reported at the same time	clear this alarm first (cf. "Clearing System Power Failure" (3-80)), and then proceed with the next step.
no System Power Failure alarm is reported	close the circuit breaker on the PI B.

....

3 - 4 8   **Lucent Technologies**   365-374-057
                                                                           Issue a, January 2002

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

7 Replace the fan unit power cable between "Power Input B" of the fan unit and the "FAN output" of the PI B.

8 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

9 Replace PI B.

10 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing Improper APS Codes

<div style="text-align:right">

Purpose Use this procedure to clear an `Improper APS Codes` alarm.

</div>

Related information

Please also refer to the corresponding alarm description → "Improper APS Codes" (2-90).

Before you begin You or a service technician must be on-site at the NE to clear an `Improper APS Codes` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

The following equipment is required:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear an `Improper APS Codes` alarm:

1 At the *WaveStar* CIT, open the alarm list.

2 Determine the port AID for which the alarm is reported from the **AID** column of the *WaveStar* CIT **NE Alarm List**.

3 Are other transmission transmission alarms (SD/SF conditions) reported at the same time for the same port?

If …	then …
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
No	proceed with Step 5.

4   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

5   Check the switch status of the network elements. Are there any switch requests in the network?

If …	then …
there are other switch requests	abort the procedure.
there are no other switch requests	proceed with the next step.

6   Determine the AIDs of the two network elements involved.

Refer to the following figure for clarification and further reference. The `Improper APS Codes` alarm is reported on node A, port q.

7   Perform a Forced Switch (FS-R) at the transmitter (node B, port p).

8   Check the switch status of the network elements.

If …	then …
the Forced Switch has been executed correctly	remove and re-insert the transmitter circuit pack (node B, port p), and then proceed with the next step.
the Forced Switch has *not* been executed correctly	clear the Forced Switch and abort the procedure.

9 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

10 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 17.
the alarm persists	proceed with the next step.

11 Replace the transmitter circuit pack (node B, port p) with a circuit pack of the same type.

> **Reference:** Please refer to:
>
> - "Replacing a circuit pack by a circuit pack of the same type" (4-39)

12 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

13 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 17.
the alarm persists	proceed with the next step.

....

14   Replace the alarm-reporting circuit pack (node A, port q) with a circuit pack of the same type.

Reference: Please refer to:

- "Replacing a circuit pack by a circuit pack of the same type" (4-39)

....

15   Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

16   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with the next step.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	• Phone: +49 911 526 2846
	• Fax: +49 911 526 3131
	• E-mail: htransde@lucent.com

....

17   Clear the Forced Switch at the transmitter (node B, port p).

....

18   Check the switch status of the network elements, and determine if the Forced Switch has been cleared.

....

19   If you need further support, please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

Phone   +49 911 526 2846

....

Fax   +49 911 526 3131

E-mail   htransde@lucent.com

E N D   O F   S T E P S

□

Clearing Inconsistent APS Codes

Purpose   Use this procedure to clear an `Inconsistent APS Codes` alarm.

Related information

Please also refer to the corresponding alarm description → "Improper APS Codes" (2-90).

Before you begin   You or a service technician must be on-site at the NE to clear an `Inconsistent APS Codes` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

The following equipment is required:

- *WaveStar* CIT

Trouble clearing procedure   Proceed as follows to clear an `Inconsistent APS Codes` alarm.

1   At the *WaveStar* CIT, open the alarm list.

2   Determine the port AID for which the alarm is reported from the **AID** column of the *WaveStar* CIT **NE Alarm List**.

3   Are other alarms, related to BLSR/MS-SPRing protection switching, reported at the same time for the same port?

If …	then …
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
No	proceed with Step 5.

....

4 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

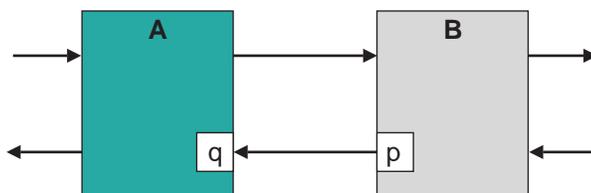| If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Are other transmission transmission alarms (SD/SF conditions) reported at the same time for the same port?

If …	then …
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
No	proceed with Step 7

....

6 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

7 Determine the AIDs of the two network elements involved.

....

Lucent Technologies

Refer to the following figure for clarification and further reference. The `Inconsistent APS Codes` alarm is reported on node A, port q.

....

8   Perform a Forced Switch (FS-R) at the transmitter (node B, port p).

....

9   Check the switch status of the network elements.

If …	then …
the Forced Switch has been executed correctly	remove and re-insert the transmitter circuit pack (node B, port p), and then proceed with the next step.
the Forced Switch has ***not*** been executed correctly	clear the Forced Switch and abort the procedure.

....

10   Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

11   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 18.
the alarm persists	proceed with the next step.

....

12   Replace the transmitter circuit pack (node B, port p) with a circuit pack of the same type.

> **Reference:** Please refer to:
> • "Replacing a circuit pack by a circuit pack of the same type" (4-39)

....

....

13 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....

14 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	proceed with Step 18.
the alarm persists	proceed with the next step.

....

15 Replace the alarm-reporting circuit pack (node A, port q) with a circuit pack of the same type.

> **Reference:** Please refer to:
> * "Replacing a circuit pack by a circuit pack of the same type" (4-39)

....

16 Wait until the green "ACTIVE" LED on the faceplate of the circuit pack is constantly lit.

....
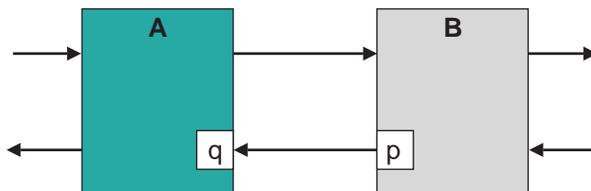
17 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

If …	then …
the alarm has cleared	proceed with the next step.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	• Phone: +49 911 526 2846
	• Fax: +49 911 526 3131
	• E-mail: htransde@lucent.com

....

18 Clear the Forced Switch at the transmitter (node B, port p).

....

....

19   Check the switch status of the network elements, and determine if the Forced Switch has been cleared.

....

20   If you need further support, please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.

You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:

Phone   +49 911 526 2846

Fax   +49 911 526 3131

E-mail   htransde@lucent.com

E ND OF S TEPS
....

☐

....

365-374-057
Issue a, January 2002   **Lucent Technologies**   3 - 5 9

Clearing Loss of Synchronisation

....

Purpose Use this procedure to clear a `Loss of Synchronisation` alarm.

Related information

Please also refer to the corresponding alarm description → "Loss of Synchronisation" (2-107).

Before you begin You or a service technician must be on-site at the NE to clear a `Loss of Synchronisation` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- An oscilloscope or frequency analyzer

- An STM analyzer

Related information

Please also refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide*.

Trouble clearing procedure Proceed as follows to clear a `Loss of Synchronisation` alarm:

....

1 Verify the quality of *all* assigned timing references starting with the timing reference with the highest priority.

    Reference: Please refer to:

- "Checking external timing references" (3-84)
  to check the quality of an external timing reference.

- "Checking line timing references" (3-85)
  to check the quality of a line timing reference.

E N D   O F   S T E P S

....

□

Clearing NE Clock Failure

Purpose Use this procedure to clear a NE Clock Failure alarm.

Related information

Please also refer to the corresponding alarm description → "NE Clock Failure" (2-108).

Before you begin You or a service technician must be on-site at the NE to clear a NE Clock Failure alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement XC320 switch unit

Trouble clearing procedure Proceed as follows to clear a NE Clock Failure alarm:

1 Replace the XC320 switch unit (replacing the standby circuit pack is sufficient).

Important! To clear the alarm, it is sufficient to replace the standby circuit pack. However, *both* XC320 switch units are defective.

    Reference: Please refer to:

- "Replacing a circuit pack by a circuit pack of the same type" (4-39)

E ND OF S TEPS

□

Clearing ONI Failure

Purpose Use this procedure to clear an ONI Failure alarm.

Related information

Please also refer to the corresponding alarm description → <u>"ONI Failure" (2-32)</u>.

Before you begin You or a service technician should be on-site at the NE to clear an ONI Failure alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement circuit pack for the circuit pack reporting the alarm

- A replacement Controller (CTL)

Trouble clearing procedure Proceed as follows to clear an ONI Failure alarm:

1 Perform a controller reset of the circuit pack reporting the alarm.

   Reference: Please refer to:

   - <u>"Initiating a circuit pack reset" (4-47)</u>

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

3 Perform a controller reset of the CTL.

> **Reference:** Please refer to:
>
> • "Initiating a circuit pack reset" (4-47)

....

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

5 Perform a full reset of the circuit pack reporting the alarm.

> **Reference:** Please refer to:
>
> • "Initiating a circuit pack reset" (4-47)

....

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

7 Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

• MS/Line performance monitoring, and

• Automatic Protection Switching (APS) on MS/Line level

- SDH: Multiplex Section Protection (MSP) and MS-SPRing

- SONET: Line Protection and BLSR

....

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-47)

....

8   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

9   Replace the circuit pack reporting the alarm.

....

10   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

11   Replace the Controller (CTL).

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-42)

....

12   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.

....

3 - 6 4   **Lucent Technologies**   365-374-057
Issue a, January 2002

If …	then …
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E ND OF S TEPS

Clearing Partitioned Area Repair

Purpose   Use this procedure to clear a `Partitioned Area Repair` alarm.

Related information

Please also refer to the corresponding alarm description →
"Partitioned Area Repair" (2-13).

Before you begin

Required equipment

The following equipment is required to complete this procedure:

*   *WaveStar*® CIT or *Navis*™ Optical EMS to check the alarm state of the network

Trouble clearing procedure   Proceed as follows to clear a `Partitioned Area Repair` alarm:

1   Locate and clear the failure in the network that caused the partion repair.

Please refer to "Partitioning of an area" (2-13).

E N D   O F   S T E P S

☐

Clearing Power Interface not Present

Purpose   Use this procedure to clear a `Power Interface not Present` alarm.

Related information

Please also refer to

- the corresponding alarm description → <u>"Power Interface not Present" (2-33)</u>

- <u>"Configuration rules" (4-44)</u>

Before you begin   You or a service technician must be on-site at the NE to clear a `Power Interface not Present` alarm.

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

Trouble clearing procedure   Proceed as follows to clear a `Power Interface not Present` alarm:

1   Install the missing Power Interface (PI).

E ND OF S TEPS

☐

Clearing Prot. Arch. Mismatch

Purpose   Use this procedure to clear a `Prot. Arch. Mismatch` alarm.

Related information

Please also refer to the corresponding alarm description → "Prot. Arch. Mismatch" (2-48).

Instructions   Proceed as follows to clear a `Prot. Arch. Mismatch` alarm.

1   Define the protection architecture consistently at both ends of the protection line.

E N D   O F   S T E P S

□

Clearing Protection Clock Input Fail

Purpose   Use this procedure to clear a `Protection Clock Input Fail` alarm.

Related information

Please also refer to the corresponding alarm description → "Protection Clock Input Fail" (2-109).

Before you begin   You or a service technician must be on-site at the NE to clear a `Protection Clock Input Fail` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT
- A replacement circuit pack for the circuit pack reporting the alarm
- A replacement XC320 switch unit

Trouble clearing procedure   Proceed as follows to clear a `Protection Clock Input Fail` alarm:

1   Depending on whether one or more circuit packs report the alarm:

If …	then …
the alarm is reported by only one circuit pack	replace the circuit pack reporting the alarm. **Reference:** Please refer to: - "Replacing a circuit pack by a circuit pack of the same type" (4-39)

If …	then …
the alarm is reported by several circuit packs	replace the XC320 switch unit in the protection slot (slot 10, cf. "Configuration rules" (4-44)). **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-39)

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing Protocol Version Mismatch

Purpose Use this procedure to clear a `Protocol Version Mismatch` alarm.

Related information

Please also refer to the corresponding alarm description → "Protocol Version Mismatch" (2-15).

Before you begin Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required privilege

You must have at least a privilege code of *S4*.

Required equipment

The following equipment is required:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear a `Protocol Version Mismatch` alarm:

1 Perform a software download at the neighboring NE to adjust the supported protocol versions at both NEs.

Please refer to the *LambdaUnite*™ *MSS User Operations Guide* for information how to perform a software download for upgrade purposes.

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.

If …	then …
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	• Phone: +49 911 526 2846
	• Fax: +49 911 526 3131
	• E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing Remote Defect Indication (RFI-L)

Purpose Use this procedure to clear an `Remote Defect Indication` (RFI-L) alarm.

Related information

Please also refer to the corresponding alarm description → <u>"Remote Defect Indication (RFI-L)" (2-83)</u>.

Instructions Proceed as follows to clear an `Remote Defect Indication` (RFI-L) alarm.

....

1 Analyse the alarm state at the far end of the Multiplex Section or Line respectively and take appropriate measures.

E N D   O F   S T E P S

□

Clearing Remote Defect Indication (RFI-P)

Purpose   Use this procedure to clear an `Remote Defect Indication` (RFI-P) alarm.

Related information

Please also refer to the corresponding alarm description → "Remote Defect Indication (RFI-P)" (2-63).

Instructions   Proceed as follows to clear an `Remote Defect Indication` (RFI-P) alarm.

1   Analyse the alarm state at the far end of the path (in the downstream direction) and take appropriate measures.

E N D   O F   S T E P S

☐

Clearing Ring Discovery in Progress

Purpose Use this procedure to clear a ***persistent*** Ring Discovery in Progress alarm. "Persistent" means that the alarm is present for longer than approximately ten minutes.

Related information

Please also refer to the corresponding alarm description → "Ring Discovery in Progress" (2-97).

Before you begin Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear a persistent Ring Discovery in Progress alarm:

1 Perform a controller reset of the CTL.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-47)

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3 Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and

- Automatic Protection Switching (APS) on MS/Line level

  - SDH: Multiplex Section Protection (MSP) and MS-SPRing

  - SONET: Line Protection and BLSR

  Reference: Please refer to:

  - "Initiating a circuit pack reset" (4-47)

....

4   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline.
	You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail:
	- Phone: +49 911 526 2846
	- Fax: +49 911 526 3131
	- E-mail: htransde@lucent.com

E N D   O F   S T E P S

□

Clearing Ring Protection Switch Suspended

Purpose Use this procedure to clear a `Ring Protection Switch Suspended` alarm.

Related information

Please also refer to the corresponding alarm description → "Ring Protection Switch Suspended" (2-99).

Before you begin Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and
- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear a `Ring Protection Switch Suspended` alarm:

1 At the *WaveStar* CIT, open the **NE Alarm List**, and check if other alarms, related to BLSR/MS-SPRing protection switching (for example `Ring Incomplete` or `Inconsistent Ring Protection Mode`), are being reported at the same time for the same port.

If …	then …
other BLSR/MS-SPRing alarms are reported	clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
no other BLSR/MS-SPRing alarms are reported	proceed with Step 3.

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3 Perform a controller reset of the CTL.

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

4 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

5 Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
  - SDH: Multiplex Section Protection (MSP) and MS-SPRing
  - SONET: Line Protection and BLSR

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

6 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E N D   O F   S T E P S

Clearing System Power Failure

....

Purpose   Use this procedure to clear a `System Power Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "System Power Failure" (2-34).

Before you begin   You or a service technician must be on-site at the NE to clear a `System Power Failure` alarm.

Which system power feeder is affected can be seen from the `Fan Voltage Feed A Failure` or `Fan Voltage Feed B Failure` alarm which will be reported at the same time (the power feeders are through-connected), or from the green "PWR ON" LED on the respective Power Interface (PI) A or B. The "PWR ON" LED will be off on the PI associated to the affected system power feeder.

Required equipment

Make sure that the following equipment is available:

- A volt meter
- A replacement Power Interface (PI)

Trouble clearing procedure   Proceed as follows to clear a `System Power Failure` alarm:
....

1   Measure the actual supply voltage at the affected system power feeder of the exchange battery.

If …	then …
the voltage is within the normal range ($\geq$ 38.0 V DC)	replace the associated Power Interface (PI).
the voltage is out of range	repair the exchange battery.

E N D   O F   S T E P S

□

....

Lucent Technologies

Clearing T4 quality unsufficient

Purpose Use this procedure to clear a `T4 quality unsufficient` alarm.

Related information

Please also refer to the corresponding alarm description → "T4 quality unsufficient" (2-110).

Before you begin You or a service technician must be on-site at the NE to clear a `T4 quality unsufficient` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- An oscilloscope or frequency analyzer

- A SONET/SDH Network Tester

Related information

Please also refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide* for information about timing provisioning.

Trouble clearing procedure Proceed as follows to clear a `T4 quality unsufficient` alarm:

1 Verify if other alarms are reported at the same time for the circuit pack that supplies the timing reference for the external timing output, for example `Circuit Pack Failure`, `Loss of Signal`, `Loss of Frame`, `Alarm Indication Signal` (AIS-L), `Excessive Bit Error Ratio` (MSEXC) or `Degraded Signal` (MSDEG).

If …	then …
any of these alarms is reported at the same time	clear these alarms first.

If …	then …
none of these alarms is reported at the same time	proceed with the next step.

2   Now you have the following options to choose from:

1.   Select a different timing reference (**Provisioned Derived Output Timing Source Selection**) from which the external timing signal shall be derived.

2.   Decrease the provisioned quality acceptance level for the external timing output (**Acceptance Quality Level for Output Threshold AIS**).

E N D   O F   S T E P S

☐

Clearing Timing Reference Failure

....

Purpose   Use this procedure to clear a `Timing Reference Failure` alarm.

Related information

Please also refer to the corresponding alarm description → <u>"Timing Reference Failure" (2-111)</u>.

Before you begin   You or a service technician must be on-site at the NE to clear a `Timing Reference Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

● have a valid user login and password for the *WaveStar*® CIT, and

● have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

● *WaveStar* CIT

● An oscilloscope or frequency analyzer

● A SONET/SDH Network Tester

Related information

Please also refer to the *LambdaUnite*™ MultiService Switch (MSS)*User Operations Guide*.

Nominal values of external timing input signals   The following table provides an overview of the possible external timing input signals and their characteristics.

External timing input signal	Frequency or bit rate	Signal level	Encoding
2 MHz	2048 kHz (± 20 ppm)	1.0 to 1.9 V (120 Ω balanced mode) 0.75 to 0.9 V (75 Ω unbalanced mode)	–
2 Mbit/s (framed or unframed)	2048 kbit/s (± 20 ppm)		HDB3
DS1 (SF or ESF)	1544 kbit/s (± 20 ppm)		B8ZS

....

Trouble clearing procedure

Proceed as follows to clear a `Loss of Synchronisation` **alarm:**

....

1   Verify the quality of the timing reference concerned.

> **Reference:** Please refer to:
>
> - "Checking external timing references" (3-84) to check the quality of an external timing reference.
>
> - "Checking line timing references" (3-85) to check the quality of a line timing reference.

E N D   O F   S T E P S

Checking external timing references

Perform the following procedure to verify the quality of a timing reference connected to an external timing input port.

....

1   Disconnect the clock source from the respective external timing input port.

....

2   Measure the supplied clock signal by using an oscilloscope or frequency analyzer, and compare the measurement results with the desired values given under "Nominal values of external timing input signals" (3-83).

....

3

If …	then …
the measurement results comply with the desired values	replace the Timing Interface (TI) associated to the external timing input under test.
the measurement results deviate from the desired values	repair or replace the station clock supply.

E N D   O F   S T E P S

....

Checking line timing references   Perform the following procedure to verify the quality of a timing reference connected to a line timing input port.

....

1   Verify if other alarms are reported at the same time for the corresponding line timing input port or the associated circuit pack, for example `Circuit Pack Failure`, `Loss of Signal`, `Loss of Frame`, `Alarm Indication Signal` (AIS-L), `Excessive Bit Error Ratio` (MSEXC) or `Degraded Signal` (MSDEG).

If …	then …
any of these alarms is reported at the same time	clear these alarms first.
none of these alarms is reported at the same time	proceed with the next step.

....

2   Verify the quality of the clock signal, indicated by means of the Synchronization Status Message (SSM) in bits 1 to 4 of the S1 byte (S1 [1-4]), by using a SONET/SDH Network Tester.

If …	then …
the quality of the clock signal is better than or equal to SEC (for SDH signals) or ST3 (for SONET signals)	replace the receive unit **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-39)
the quality of the clock signal is less than SEC (for SDH signals) or ST3 (for SONET signals)	check the far-end equipment. The transmit unit might be defective, or the timing provisioning might be incorrect.

E N D   O F   S T E P S

....

☐

Clearing TI Mismatch

Purpose Use this procedure to clear a `TI Mismatch` alarm.

Related information

Please also refer to the corresponding alarm description → "TI Mismatch" (2-35).

Before you begin You or a service technician must be on-site at the NE to clear a `TI Mismatch` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

Trouble clearing procedure Proceed as follows to clear a `TI Mismatch` alarm:

1 Replace the last installed Timing Interface (TI) by a model of the correct type.

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3

If …	then …

E N D   O F   S T E P S

□

Clearing Unit Cooling Degraded

....

Purpose	Use this procedure to clear a `Unit Cooling Degraded` alarm.

Related information

Please also refer to the corresponding alarm description → "Unit Cooling Degraded" (2-37).

Before you begin	You or a service technician should be on-site at the NE to clear a `Unit Cooling Degraded` alarm.

Required equipment

Make sure that the following equipment is available:

* A replacement air filter

Trouble clearing procedure   Proceed as follows to clear a `Unit Cooling Degraded` alarm:

....

1   Check the **NE Alarm List**.

If …	then …
any of the following alarms is present at the same time: `Fan Failure`, `Fan Unit Failure`, `Unit Temperature too High`.	clear these alarms first. **Reference:** Please refer to the corresponding trouble clearing procedure: • "Clearing Fan Failure " (3-33) • "Clearing Fan Unit Failure" (3-40) • "Clearing Unit Temperature too High" (3-89)
none of these alarms is present	proceed with the next step.

....

2   Check the shelf equipage (front and rear side).

If …	then …
there are empty slots which are not covered by blank faceplates	cover all empty slots by blank faceplates

....

If …	then …
all empty slots are covered by blank faceplates	proceed with the next step.

3 Ensure that a sufficient air flow through the shelf is garantueed.

If …	then …
the air inlet (air filter) or outlet (fan unit) are obstructed	provide for adequate air supply and circulation by removing the obstructing objects.
the air inlet or outlet are not obstructed by any objects	possibly, the air filter is clogged. Replace the air filter. **Reference:** Please refer to: • "Replacing the air filter" (4-17)

4 Wait a few minutes.

5 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	check if the ambient temperature is extremly high (please refer to the climatic conditions for the operation of *LambdaUnite*™ MSS network elements given in the safety guide). If the ambient temperature is extremly high, then provide cooling at least in the direct vicinity of the nework element.

E N D   O F   S T E P S

Clearing Unit Temperature too High

Purpose	Use this procedure to clear a `Unit Temperature too High` alarm.

Related information

Please also refer to the corresponding alarm description → <u>"Unit Cooling Degraded" (2-37)</u>.

Before you begin	You or a service technician should be on-site at the NE to clear a `Unit Temperature too High` alarm.

Trouble clearing procedure	Proceed as follows to clear a `Unit Temperature too High` alarm:

1 Check the **NE Alarm List**.

If …	then …

any of the following alarms is present at the same time:
`Fan Failure,`
`Fan Unit Failure.`
	clear these alarms first.**Important!** It is critical to clear these fan unit alarms quickly. If this is not possible please consider the case differentiation concerning a persistent `Unit Temperature too High` alarm given subsequent to this trouble clearing procedure.
	
	  Reference:
	  Please refer to the corresponding trouble clearing procedure:
	• <u>"Clearing Fan Failure " (3-33)</u>
	• <u>"Clearing Fan Unit Failure" (3-40)</u>

none of these alarms is present	consider the case differentiation concerning a persistent `Unit Temperature too High` alarm given subsequent to this trouble clearing procedure. Then proceed with the next step.

2 Check the shelf equipage (front and rear side).

If …	then …
there are empty slots which are not covered by blank faceplates	cover all empty slots by blank faceplates
all empty slots are covered by blank faceplates	proceed with the next step.

3 Check if the air inlet or outlet are obstructed.

If …	then …
the air inlet or outlet are obstructed	provide for adequate air supply.
the air inlet or outlet are not obstructed	check if the ambient temperature is extremly high (please refer to the climatic conditions for the operation of *LambdaUnite*™ MSS network elements given in the safety guide). If the ambient temperature is extremly high, then provide cooling at least in the direct vicinity of the nework element.

E N D   O F   S T E P S

Persistent "Unit Temperature too High" alarm If a `Unit Temperature too High` alarm persists for a longer period (more than two minutes), then it is up to your discretion how to proceed. You may take one of the following actions:

Possible action	Consequences
You may switch off the NE to prevent circuit packs from being seriously damaged due to overheating.	All traffic managed by the respective NE will be interrupted. However, it might be an option to wait a while (at least ten minutes) to let the circuit packs cool off, switch on the NE again, and then proceed with the trouble clearing procedure. ***Important:*** Before switching off the NE, follow the instructions given in Step 1 of the procedure "Replacing the Controller (CTL)" (4-42) to remove the Controller (CTL) from its slot.
You may remove the affected circuit pack from the system to prevent it from being seriously damaged due to overheating.	The traffic managed by the respective circuit pack will be interrupted. The circuit pack can be re-inserted after the Unit Temperature too High alarm has cleared.
You might ignore the Unit Temperature too High alarm.	There is a high risk of seriously damaging circuit packs due to overheating.

Clearing User Panel Comm Failure

Purpose Use this procedure to clear a `User Panel Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → ["User Panel Comm Failure" (2-39)](#).

Before you begin You or a service technician must be on-site at the NE to clear a `User Panel Comm Failure` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement user panel

- A replacement CI-CTL (Connection Interface of the Controller)

Trouble clearing procedure Proceed as follows to clear a `User Panel Comm Failure` alarm:

1 Replace the user panel.

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

3 At the CI-CTL and at the fan unit, check the connectors of the fan unit control cable.

If …	then …
both connectors are connected properly	proceed with the next step.
any of the connectors is not properly connected	connect the respective connector(s) properly, and then proceed with the next step.

....

4 Perform a controller reset of the CTL.

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

....

5 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

6 Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
  - SDH: Multiplex Section Protection (MSP) and MS-SPRing
  - SONET: Line Protection and BLSR

> **Reference:** Please refer to:
>
> - "Initiating a circuit pack reset" (4-47)

....

7 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

8   Replace the CI-CTL.

9   Perform a full reset of the CTL, and wait for the system to re-initialize.

Important! A full reset, in contrast to a controller reset, of the CTL affects

- MS/Line performance monitoring, and
- Automatic Protection Switching (APS) on MS/Line level
    - SDH: Multiplex Section Protection (MSP) and MS-SPRing
    - SONET: Line Protection and BLSR

 Reference: Please refer to:

- "Initiating a circuit pack reset" (4-47)

10   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

11   Replace the fan unit control cable, and then perform a controller reset of the CTL.

 Reference: Please refer to:

- "Initiating a circuit pack reset" (4-47)

....

12   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

....

13   Replace the fan unit, and then perform a controller reset of the CTL.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)
- "Initiating a circuit pack reset" (4-47)

....

14   At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the
alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

E ND   OF   S TEPS

....

☐

....

365-374-057
Issue a, January 2002   **Lucent Technologies**   3 - 9 5

Clearing Worker Clock Input Fail

....

Purpose   Use this procedure to clear a `Worker Clock Input Fail` alarm.

Related information

Please also refer to the corresponding alarm description → "Worker Clock Input Fail" (2-112).

Before you begin   You or a service technician must be on-site at the NE to clear a `Worker Clock Input Fail` alarm.

Prior to performing the following trouble clearing procedure, you must:

- have a valid user login and password for the *WaveStar*® CIT, and

- have established a *WaveStar* CIT connection to the alarm-reporting NE.

Required equipment

Make sure that the following equipment is available:

- *WaveStar* CIT

- A replacement circuit pack for the circuit pack reporting the alarm

- A replacement XC320 switch unit

Trouble clearing procedure   Proceed as follows to clear a `Protection Clock Input Fail` alarm:

....

1   Depending on whether one or more circuit packs report the alarm:

If …	then …
the alarm is reported by only one circuit pack	replace the circuit pack reporting the alarm. **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-39)

If …	then …
the alarm is reported by several circuit packs	replace the XC320 switch unit in the worker slot (slot 9, cf. "Configuration rules" (4-44)). **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-39)

2 At the *WaveStar* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

END OF STEPS

4   Supporting procedures

Overview

Purpose

Contents

Retrieving the *WaveStar*® CIT NE Alarm List

Purpose   Use this procedure to retrieve detailed information about the current alarm status of a *LambdaUnite*™ MSS NE by using the *WaveStar* CIT.

Related information   For related information concerning the *WaveStar* CIT and *Navis*™ Optical EMS alarm lists, please refer to

- "The *WaveStar* CIT NE Alarm List" (4-5), or

- to the *Navis Optical Element Management System (EMS) Provisioning Guide for LambdaUnite MSS*.

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

- have a valid user login and password,

- be connected to the corresponding NE, and

- have proper access privileges to perform this task.

Required privilege

You must have at least a privilege code of **M1** to retrieve the *WaveStar* CIT **NE Alarm List**.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Proceed as follows to retrieve the *WaveStar* CIT **NE Alarm List**:

1   From the *WaveStar* CIT, invoke the **NE Alarm List** by either:

- pressing the **Alarm List** button in the upper right area of the **System View** window, or

- selecting **Fault → NE Alarm List** in the **System View** main menu, or

- selecting **Reports → NE Alarm List** in the **System View** main menu.

    Result:

    The **NE Alarm List** window will be opened.

The **NE Alarm List** reflects the current alarm status at the time when it is invoked.

....

2 To make sure that the **NE Alarm List** reflects the current alarm status, click

- the **Refresh** button in the **NE Alarm List** window or

- again the **Alarm List** button

as soon as you observe changes in the alarm status display in the lower left corner of the **System View** window, or whenever you are unsure whether the alarm list is still synchronized to the current alarm status.

....

3 The following options are avaialable:

If …	then …
you want to store the currently displayed alarm list as a standard text file (ASCII format)	click the **Save As** button and specify a filename and a destination.
you want to print out the currently displayed alarm list	click the **Print** button and specify a printer.
you want to dismiss the window	click the **Close** button.
you want to update the alarm list	click the **Refresh** button or again the **Alarm List** button (cf. Step 2).
you want to get online help information	click the **Help** button.

E N D   O F   S T E P S

....

☐

The *WaveStar*® CIT NE Alarm List

....

The "NE Alarm List" window

The *WaveStar* CIT provides a list of current alarms, the **NE Alarm List**, to retrieve detailled information about the current alarm status of a *LambdaUnite*™ MSS network element (NE).

Structure of the "NE Alarm List"

The following table explains the structure of the *WaveStar* CIT **NE Alarm List**.

Column	Meaning
Alarm Level	This column indicates the alarm severity. Possible values are: • Critical/Major/Minor (**CR/MJ/MN**) or • Prompt/Deferred/Info (**PR/DF/INF**). **PR/DF/INF** is the default setting for *LambdaUnite* MSS systems.
AID	This column indicates the alarm issue point, i.e. the access identifier (AID) of the component for which an alarm is being reported ("exttmg1", "1-1-#-#-ctlw-nvm" or "1-1-#-#-12-v4" for example). Please note that a special display format is being used for SDH tributary AIDs, please refer to "Identifying SDH tributaries in alarm messages" (4-9).
Date	These two columns indicate the date and time of occurrence, i.e. the date and time the alarm was reported by the NE. The date and time format depends on the country in which the *WaveStar* CIT is being used.
Time	Please refer to the *LambdaUnite MSS User Operations Guide* for information on how to set the date and time of the system.
Affect on Service	This column indicates whether the corresponding alarm is service affecting or not. Possible values are: • service affecting (**SA**), • not service affecting (**NSA**), • not applicable (-).

....

Column	Meaning
Probable Cause	This column indicates the alarm short designation. A more detailled description of the alarm's probable cause can be found in the **Description** column.
Signal Level Affected	This column indicates the affected signal level for communication alarms or the type of alarm otherwise. Possible values are: • **COM** Common Alarms that apply to the system as a whole, processing errors for example. • **ENV** Environmental • **EQPT** Equipment • **OC-48**, **OC-192**, **OC-768** Optical transport signals (SONET): OC-48 (2.5 Gbit/s), OC-192 (10 Gbit/s) or OC-768 (40 Gbit/s) • **OUTT** Output timing • **STM-16**, **STM-64**, **STM-256** Optical transport signals (SDH): STM-16 (2.5 Gbit/s), STM-64 (10 Gbit/s) or STM-256 (40 Gbit/s) • **STS-1**, **STS-3C**, **STS-12C**, **STS-48C**, **STS-192C** Payload signals (SONET): STS-1, STS-3C, STS-12C, STS-48C or STS-192C • **SYST** System timing • **VC-3**, **VC-4**, **VC-4-4C**, **VC-4-16C**, **VC-4-64C** Payload signals (SDH): VC-3, VC-4, VC-4-4C, VC-4-16C or VC-4-64C • **1GE** 1-Gbit/s Ethernet • **VCG** Virtual concatenation group tributary

Column	Meaning
Alarm Type	This column indicates the alarm category. Possible values are: • Communications, • Environmental, • Equipment, • Processing, • Quality of service.
Description	This column describes the alarm's probable cause in more detail.

Pushbuttons   The **NE Alarm List** window provides the following pushbuttons:

1. **Save As**
   Use this button to store the currently displayed alarm list as a standard text file which may then be used for editing and further processing.

2. **Print**
   Use this button to print out the currently displayed alarm list.

3. **Close**
   Use this button to dismiss the window.

4. **Refresh**
   Clicking the **Refresh** button causes the *WaveStar* CIT to retrieve the alarm information from the NE again to update the alarm list. Notice that there is a difference between the **Refresh** button and the **Update Alarms** button beside the **Alarm List** button. The **Update Alarms** button can only be used to manually refresh the alarm status display, not the alarm list.

5. **Help**
   Use this button to get online help information specific to the **NE Alarm List** window.

□

Retrieving the *WaveStar*® CIT NE Alarm Log

Purpose Use this procedure to retrieve alarm history information by using the *WaveStar* CIT.

The *WaveStar* CIT "NE Alarm Log" The *WaveStar* CIT **NE Alarm Log** window provides a detailed alarm history for each *LambdaUnite*™ MSS NE. The most recent alarms, up to 1024 alarms ordered by their date and time of occurrence, are stored in the NE alarm log. The information contained is presented in an identical fashion as in the NE alarm list; please refer to "The *WaveStar* CIT NE Alarm List" (4-5).

The *Navis*™ Optical EMS alarm history Please refer to the *Navis Optical Element Management System (EMS) Provisioning Guide for LambdaUnite MSS* for information about the *Navis* Optical EMS alarm history ("Alarm browser").

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

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

Required privilege

You must have at least a privilege code of **M1** to retrieve the **NE Alarm Log**.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Proceed as follows to retrieve the **NE Alarm Log**:

1 From the *WaveStar* CIT, invoke the **NE Alarm Log** by either:

- selecting **Fault** → **NE Alarm Log...** in the **System View** main menu, or
- selecting **Reports** → **NE Alarm Log...** in the **System View** main menu.

  Result:

  The **NE Alarm Log** window will be opened.

  E N D   O F   S T E P S

Identifying SDH tributaries in alarm messages

Purpose Use this procedure to uniquely identify SDH tributaries in case of tributary alarms reported in the *WaveStar*® CIT **NE Alarm List** or **NE Alarm Log**.

Representation of SDH tributaries in alarm messages When tributary alarms are reported, the alarm messages in the *WaveStar* CIT **NE Alarm List** or **NE Alarm Log** contain the signal level affected, but not the port type. Therefore, a five-digit representation is used for SDH tributary AIDs to facilitate the correct identification of SDH tributaries. Please also refer to "SONET and SDH tributary numbering format" (4-11).

Each of the five digits represents a particular VC-N level:
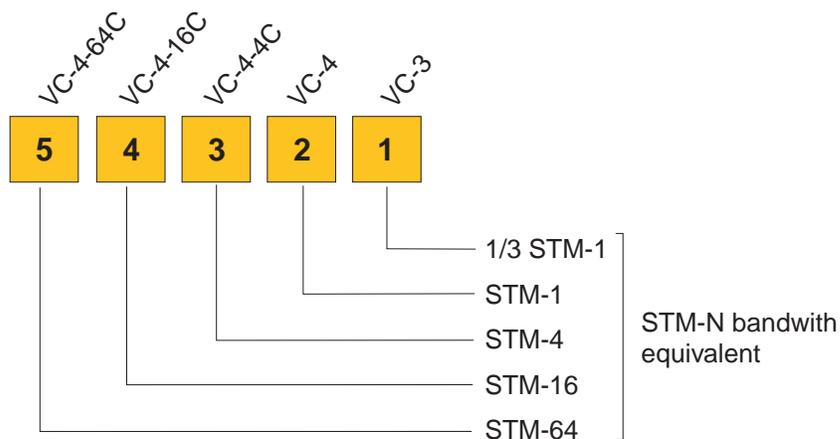
The possible values of the individual digits are as follows:

Digit	Value	Meaning
1	0	no VC-3
	1, 2 or 3	the first, second or third VC-3 within an STM-1 frame.

Digit	Value	Meaning
2	0	no VC-4
	1, 2, 3 or 4	the first, second, third or fourth VC-4 within the corresponding STM-4 frame.
	*	An asterisk represents either a "1" or a fill character which can be ignored (if the second digit is not required, in the case of an STM-1 interface port for example).
3	0	no VC-4-4C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-4C within the corresponding STM-16 frame.
	*	An asterisk represents either a "1" or a fill character which can be ignored (if the third digit is not required, in the case of an STM-1 or STM-4 interface port for example).
4	0	no VC-4-16C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-16C within the corresponding STM-64 frame.
	*	An asterisk represents either a "1" or a fill character which can be ignored (if the fourth digit is not required, in the case of an STM-1, STM-4 or STM-16 interface port for example).
5	0	no VC-4-64C
	1, 2, 3 or 4	the first, second, third or fourth VC-4-64C within the corresponding STM-256 frame.
	*	An asterisk represents either a "1" or a fill character which can be ignored (if the fifth digit is not required, in the case of an STM-1, STM-4, STM-16 or STM-64 interface port for example).

Required number of digits   Depending on the STM level of an SDH port, a different number of digits is required to uniquely identify the tributaries contained.

STM-256 interface port	All five digits are required.

STM-64 interface port	Four digits are required.
STM-16 interface port or 1-Gbit/s Ethernet port	Three digits are required.
STM-4 interface port	Two digits are required.
STM-1 interface port	Only the last digit is required.

Examples   These are examples of the *WaveStar* CIT numbering format of SDH tributaries in alarm messages:

1-3-u-#-06-1-**20   This is an STM-16 port (three digits are required): The asterisk at position 3 represents a "1", the asterisk at position 4 can be ignored. Therefore, the AID indicates a VC-4 in the second STM-1 of the first STM-4 within the STM-16 frame.

1-3-u-#-04-1-***3   This is an STM-16 port (three digits are required): The asterisks at positions 2 and 3 represent a "1", the asterisk at position 4 can be ignored. Therefore, the AID indicates the third VC-3 in the first STM-1 of the first STM-4 within the STM-16 frame.

SONET and SDH tributary numbering format   A special numbering format is used for SDH tributaries (VC-3, VC-4, VC-4-4C, VC-4-16C and VC-4-64C) whereas the SONET tributary numbering format is relatively straight-forward:

Interface port rate	Tributary rate	Tributary AID	
		SONET format	**SDH format**
OC-3/STM-1	STS-3c/VC-4	1	0
	STS-1/VC-3	1, 2, 3	1, 2, 3
OC-12/STM-4	STS-12c/VC-4-4C	1	00
	STS-3c/VC-4	1, 4, 7, 10	10, 20, 30, 40
	STS-1/VC-3	1, 2, 3, 4, … , 12	11, 12, 13, 21, 22, 23, 31, 32, 33, 41, 42, 43

Interface port rate	Tributary rate	Tributary AID	
		SONET format	**SDH format**
OC-48/STM-16	STS-48c/VC-4-16C	1	000
	STS-12c/VC-4-4C	1, 13, 25, 37	100, 200, 300, 400
	STS-3c/VC-4	1, 4, 7, 10, … , 46	110, 120, 130, 140, 210, 220, … , … , 430, 440
	STS-1/VC-3	1, 2, 3, 4, … , 48	111, 112, 113, 121, 122, 123, … , 441, 442, 443
OC-192/STM-64	STS-192c/VC-4-64C	1	0000
	STS-48c/VC-4-16C	1, 49, 97, 145	1000, 2000, 3000, 4000
	STS-12c/VC-4-4C	1, 13, 25, 37, … , 181	1100, 1200, 1300, 1400, 2100, 2200, … , … , 4300, 4400
	STS-3c/VC-4	1, 4, 7, 10, … , 190	1110, 1120, 1130, 1140, 1210, 1220, … , … , 4430, 4440
	STS-1/VC-3	1, 2, 3, 4, … , 192	1111, 1112, 1113, 1121, 1122, 1123, … , 4441, 4442, 4443

Interface port rate	Tributary rate	Tributary AID	
		SONET format	**SDH format**
OC-768/STM-256[1]	STS-768c/VC-4-256C	1	00000
	STS-192c/VC-4-64C	1, 193, 385, 577	10000, 20000, 30000, 40000
	STS-48c/VC-4-16C	1, 49, 97, 145, … , 721	11000, 12000, 13000, 14000, 21000, 22000, … , … , 43000, 44000
	STS-12c/VC-4-4C	1, 13, 25, 37, … , 757	11100, 11200, 11300, 11400, 12100, 12200, … , … , 44300, 44400
	STS-3c/VC-4	1, 4, 7, 10, … , 766	11110, 11120, 11130, 11140, 11210, 11220, … , … , 44430, 44440
	STS-1/VC-3	1, 2, 3, 4, … , 768	11111, 11112, 11113, 11121, 11122, 11123, … , 44441, 44442, 44443
1 Gbit/s (Ethernet)	STS-3c/VC-4	1, 4, 7, 10, 13, 16, 19	110, 120, 130, 140, 210, 220, 230
	STS-1/VC-3	1, 2, 3, 4, … , 24	111, 112, 113, 121, 122, 123, … , 241, 242, 243

Notes:

1. STM-256 and OC-768 ports are not supported in *LambdaUnite*™ MSS
    Release 1.0

....

365-374-057
Issue a, January 2002

Lucent Technologies

4 - 1 3

How to identify SDH tributaries in alarm messages

Proceed as follows to identify the correct tributary from the SDH tributary AID representation in the *WaveStar* CIT **NE Alarm List** or **NE Alarm Log**:

....

1 Determine the port type by means of the slot information in the AID and by using office records or the *WaveStar* CIT **System View** window for example.

....

2 Depending on the port unit type, determine the number of required digits in the tributary AID representation (cf. "Required number of digits" (4-10)).

All *required* digits with an asterisk represent "1", all other digits with an asterisk can be ignored.

Please also refer to "SONET and SDH tributary numbering format" (4-11).

E ND OF S TEPS

....

☐

....

4 - 1 4   **Lucent Technologies**   365-374-057

Issue a, January 2002

Replacing the fan unit

Purpose Use this procedure to replace the fan unit *only* when instructed to do so as part of a trouble-clearing procedure.

Before you begin Perform the following procedure from the *rear side* of the shelf.

Required equipment

The following equipment is required to perform this procedure:

* A replacement fan unit.

Instructions

⚠ **CAUTION**

A network element may fail without proper cooling.

Never remove the fan unit unless you already have a replacement fan unit in hand and immediately perform the replacement, as instructed in this procedure. Leaving the fan unit out of operation for more than two minutes may cause the respective network element to fail.

Proceed as follows to replace the fan unit.

1   At the rear side of the shelf, locate the replacement fan unit within easy reach.

⚠ **CAUTION**

A network element may fail without proper cooling.

Leaving the fan unit out of operation for more than two minutes may cause the respective network element to fail.

It is critical that you complete this procedure soon after performing this step.

2   With your fingers, loosen the screws (1) of the fan unit drawer.

Refer to the following figure for clarification and further reference.

....
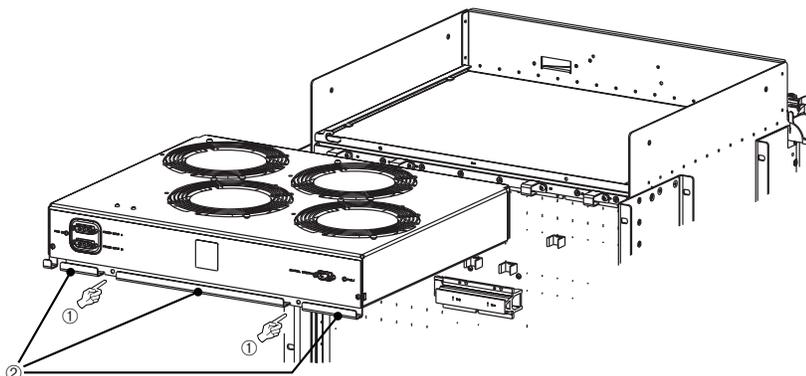
3   Disconnect the power and alarm connectors of the fan unit.

....

4   Slide the fan unit drawer from its position by using the handles (2).

....

5   Take the fan unit from the fan unit drawer.

....

6   Place the replacement fan unit into the fan unit drawer, and slide the
         fan unit drawer back into the shelf.

....

7   Re-connect the power and alarm connectors of the fan unit.

....

8   With your fingers, fasten the screws of the fan unit drawer.
         E N D   O F   S T E P S

☐

....

4 - 1 6   **Lucent Technologies**   365-374-057
                                                                               Issue a, January 2002

Replacing the air filter

When to use Use this procedure:

- Every 3 months, as a part of routine fan maintenance.

- When instructed to do so as a part of a trouble-clearing task.

Air filter position The following figure illustrates the postion of the air filter (1) in the NE rack:
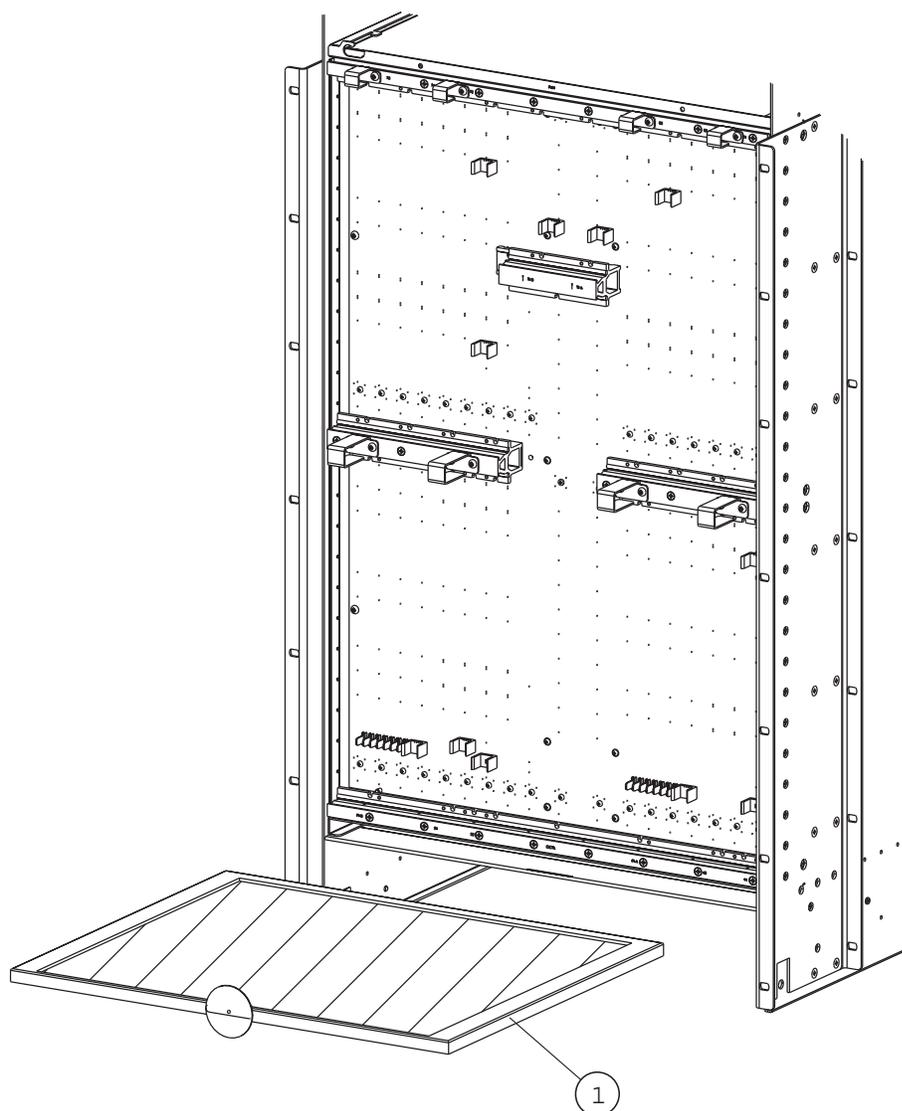
Air filter types   Two air filter types can be used

- Filter washable — DC1002025
- Filter disposable — DC1002027

Before you begin   The following equipment is required to perform this task:

- A replacement air filter (either a new or a cleaned air filter)

Instructions   Complete the following steps to replace the air filter.

....

1   Rotate the (one) locking/pull tab (in the middle of the filter) to a horizontal position.

....

2   Remove the air filter by grasping the locking/pull tab and pulling the air filter out of the subrack.

....

3   Insert the replacement air filter into the shelf so that the locking/pull tab is positioned at the rear of the subrack.

....

4   Rotate the locking/pull tab until the air filter is locked in place.

....

5   Discard or clean the dirty air filter.

There are four easy ways recommended to clean Universal's Windowpane, Quadrafoam and Uni-Foam Air Filters:

1.   Cleaning using a vacuum cleaner
A few passes of a vacuum cleaner will remove accumulated dust and dirt in seconds.

2.   Cleaning using compressed air
Point compressed air nozzle in opposite direction of operating air flow (blow from exhaust side toward intake side).

3.   Cleaning using cold water
Under normal conditions the foam media used in Universal's Windowpane, Quadrafoam and Uni-Foam filters require no oily adhesives. Collected dirt is washed away quickly and easily using just a standard hose nozzle with plain water.

4.   Cleaning using warm, soapy water

....

Where stubborn air-borne dirt is present, the filter may be dipped in a solution of warm water and mild detergent. Then simply rinse in clear water, let stand until completely dry and free of moisture, and return to service.

E ND   OF   S TEPS

☐

Cleaning optical fiber connectors

Before you begin   Make sure that the required equipment listed below is available before you begin cleaning the optical fiber connectors.

Required equipment

The following equipment is required to perform this task:

*   Isopropanol,

*   Smooth tissues,

*   Purified compressed air (optional),

*   Microscope with a magnification x 200,

*   Coupling cleaner (e.g. a cotton bud or cotton-wool swab),

*   Tape dispenser.

Instructions

⚠ DANGER

Injury to eyes caused by invisible laser radiation.

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

Never look into the end of an exposed fiber or into an open optical connector as long as the optical source is switched on. Always observe the laser warning instructions given in the safety guide.

⚠ CAUTION

Optical fiber cables will break if the bending radius is too small.

To avoid cable break ensure that the bending radius of optical fiber cables is not less than 30 mm.

Proceed as follows to clean the optical fiber connectors:

....

1 Wipe off the connector face ***lengthwise*** (not with a circular motion!) using a ***smooth*** tissue (***moistened*** with isopropanol).

....

2 Wipe off the connector face ***lengthwise*** (not with a circular motion!) using a ***dry and smooth*** tissue.

....

3 Let the connector face air-dry (the isopropanol must evaporate completely!).

As an option, purified compressed air can also be used for drying.

....

4 If necessary, the connector face can additionally be dabbed on the tape dispenser.

....

5 Check the connector face for cleanliness using the microscope.

Do ***not*** connect the optical connectors without having checked them for impurities under the microscope!

....

6 If the connector impurities were not removed completely during the first cleaning procedure, repeat the preceding steps until the result is satisfactory.

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

☐

....

365-374-057   **Lucent Technologies**   4 - 2 1
Issue a, January 2002

Cleaning optical fiber couplings

Before you begin Make sure that the required equipment listed below is available before you begin cleaning the optical fiber couplings.

Required equipment

The following equipment is required to perform this task:

- Isopropanol,
- Coupling cleaner (e.g. a cotton bud or cotton-wool swab),

Instructions

⚠ DANGER

Injury to eyes caused by invisible laser radiation.

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

Never look into the end of an exposed fiber or into an open optical connector as long as the optical source is switched on. Always observe the laser warning instructions given in the safety guide.

⚠ CAUTION

Optical fiber cables will break if the bending radius is too small.

To avoid cable break ensure that the bending radius of optical fiber cables is not less than 30 mm.

Proceed as follows to clean the optical fiber connectors:

1 Soak the coupling cleaner in isopropanol and move it back and forth in the coupling several times.

2 Let the optical fiber coupling air-dry (the isopropanol must evaporate completely!).

Important! Lightguide build-outs (LBOs) may be damaged when compressed air is used for drying. Therefore, do ***not*** use compressed air for drying LBOs.

....

3   Check the optical fiber coupling for residual impurities by holding it to the light.

The geometry of the coupling does not allow it to be checked under the microscope.

....

4   If necessary, repeat the preceding steps until the result is satisfactory.
E ND   OF   S TEPS
....

◻

....

365-374-057   **Lucent Technologies**   4 - 2 3
Issue a, January 2002

Performing facility loopbacks

Purpose   Use this procedure to operate near-side or far-side facility loopbacks.

Facility loopbacks   Facility loopbacks are loopbacks switched on whole ports. They make it possible to verify the correct system operation and may facilitate troubleshooting of problems.

There are two types of facility loopbacks:

- Near-side facility loopbacks
  The signal on the input port is looped to the corresponding output port with transpassing as few NE components as possible. Near-side facility loopbacks can be switched on all out-of-service optical interface ports.

- Far-side facility loopbacks
  The transmission signal to the output port in the NE is looped back to the corresponding input port with passing through as many equipment components as possible.
  Far-side facility loopbacks can be switched on all out-of-service optical interface ports as well as on 1-Gbit/s Ethernet ports.

Near-side facility loopbacks   Near-side facility loopbacks can be used to test the correct cabling between two network elements including the involved interface ports.

Functional principle

The following schematical diagram depicts the functional principle of near-side facility loopbacks.
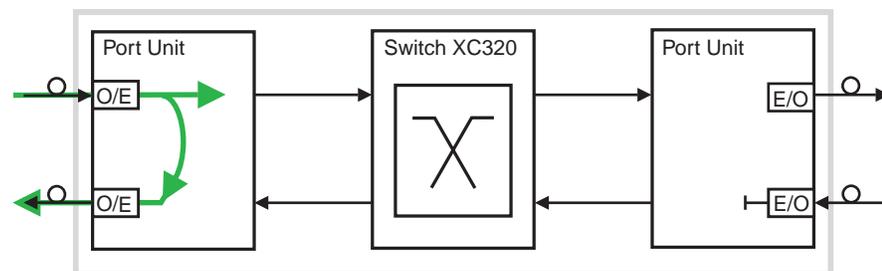
The incoming signal at the input port is, after optical-to-electrical conversion, entirely looped back to the output port.

Near-side facility loopbacks are characterized as follows:

- Near-side facility loopbacks are transparent, the signal transmitted in the downstream direction is not changed.

- The signal transmitted in the original (downstream) direction is different from the signal looped back. Particular Section/RS and Line/MS Overhead bytes, such as those used for frame alignment (A1, A2) or bit error monitoring (B1, B2) for example, are not looped back but processed. The Path Overhead (POH) and the payload signal, however, are looped back unchanged.

- The incoming signal in the upstream direction is terminated during the loopback.

Far-side facility loopbacks

Far-side facility loopbacks can be used to test signal paths through a network element.

Functional principle

The following schematical diagram depicts the functional principle of far-side facility loopbacks.
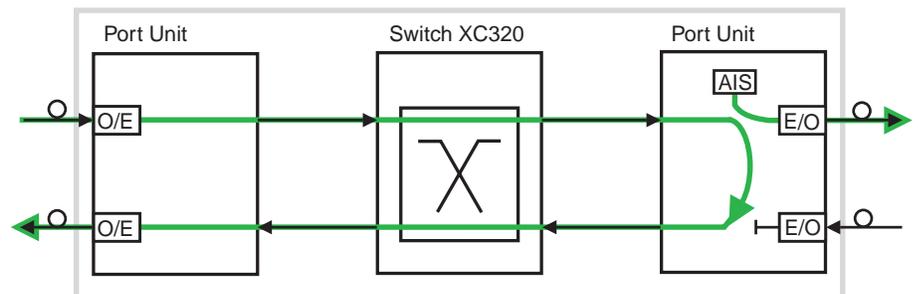
Far-side facility loopbacks are characterized as follows:

- Far-side facility loopbacks are non-transparent, the signal transmitted in the original (downstream) direction is different from the signal looped back. Line AIS (SONET) or MS-AIS (SDH) respectively is inserted into the outgoing signal in the downstream direction during the loopback.

- The signal is not changed before it is looped back.

- The incoming signal in the upstream direction is terminated during the loopback.

....

365-374-057
Issue a, January 2002

Lucent Technologies

4 - 2 5

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

- have a valid user login and password,

- be connected to the corresponding NE, and

- have proper access privileges to perform this task.

Required privilege

You must have at least privilege codes of **S1** *and* **P1** *and* **M3** to perform facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions **Important!** If you want to switch a facility loopback on a port involved in a Line/MS protection scheme (Line protection, MSP), it is highly recommended to put the corresponding protection group in the lockout or forced switch state before switching the facility loopback to avoid an unintended protection switch or failure of protocol (FOP) events.

Proceed as follows to operate a near-side or far-side facility loopback:

....

1 Make sure that the port on which you want to operate a facility loopback is *not assigned/locked as timing reference*, and that *no DCC is enabled* for that port.

....

2 By using the *WaveStar* CIT, set the port into the out-of-service state proceeding according to one of the following options:

- Option 1

    - Select **Configuration** → **Provision…** from the **System View** main menu,

    - choose the port on which you want to operate a facility loopback from the equipment selection window, and

....

4 - 2 6

Lucent Technologies

365-374-057
Issue a, January 2002

- click **Provision**.

- In the **Provision Parameters for Protection Group or Equipment** window, set the **Service Condition** to **Out Of Service**.

- Option 2

  - In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.

  - In the pop-up menu that opens, select the **Provision Port #** menu item ("#" represents the port number).

  - In the **Provision Port** window, set the **Service Condition** to **Out Of Service**.

....

3 Proceed according to one of the following options to invoke the **Facility Loopback** window from the *WaveStar* CIT:

- Option 1

  - Select **Fault → Analysis → Facility Loopback…** from the **System View** main menu,

  - choose the port on which you want to operate a facility loopback from the equipment selection window that will be opened, and

  - click **Select**.

- Option 2

  - In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.

  - In the pop-up menu that opens, select the **Facility Loopback** menu item.

....

4 By means of the read-only fields in the upper region of the window (**Port AID**, **Port Type/Rate**, **Facility Loopback Status**), verify that you selected the desired port, and that no loopback is currently active.

....

5 Select the type of facility loopback to be operated by means of the **Facility Loopback Type** checkboxes:

- **Nearside Facility** or

- **Farside Facility**.

....

....

6   Click the button in the lower left-hand-side corner of the window which may be labelled either **Operate** or **Force**.

The button will be labelled **Operate** if the corresponding port is an optical port, is protected and *not* active, and if the switch request state is "Lockout of protection". Otherwise it will be labelled **Force**.

....

Important! Operating a facility loopback may be service affecting!

7   If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window that will be opened.

E ND   OF   S TEPS
....

□

....

4 - 2 8   **Lucent Technologies**   365-374-057
                                                                                         Issue a, January 2002

Releasing a facility loopback

....

Purpose Use this procedure to dismantle (release) a facility loopback.

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

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

Required privilege

You must have at least privilege codes of **S1** *and* **P1** *and* **M3** to perform or release facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Proceed as follows to dismantle a facility loopback:

....

1 Proceed according to one of the following options to invoke the **Facility Loopback** window from the *WaveStar* CIT:

- Option 1
    - Select **Fault** → **Analysis** → **Facility Loopback…** from the **System View** main menu,
    - choose the port on which you want to dismantle a facility loopback from the equipment selection window that will be opened, and
    - click **Select**.
- Option 2
    - In the shelf display, right-click on the alarm LED of the port on which you want to dismantle a facility loopback.
    - In the pop-up menu that opens, select the **Facility Loopback** menu item.

    Result:

    The **Facility Loopback** window will be opened. The read-only fields in the upper region of the window (**Port AID**, **Port Type/Rate**, **Facility Loopback Status**) indicate the selected port

....

and whether a facility loopback is currently active. In the **Facility Loopback Type** field, the type of facility loopback currently being active is shown.

....

2   Click the **Release** button if you want to dismantle the indicated type of facility loopback on the respective port.

E ND   OF   S TEPS

□

Restoring a database to a network element

Purpose   Use this procedure to restore a previously saved database to a network element.

Before you begin   Before you begin this task:

- Obtain the work instructions for this task and note the database to be restored and the location of the most recent backup files.

- Verify that a *WaveStar*® CIT is connected and logged in to the *LambdaUnite*™ MSS network element (NE) where the database is to be restored.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Safety precautions   To assure both personal safety and the proper functioning of the *LambdaUnite* MSS system, it is imperative to review and understand these warnings and precautions prior to performing this task.

![static discharge caution symbol] **CAUTION**

Possible material damage due to electrostatic discharge

Handling circuit packs or working on a LambdaUnite MSS system can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a LambdaUnite MSS system.

Important! If provisioning changes were made after the last backup files were created, use the appropriate *WaveStar* CIT commands to manually apply the recent provisioning changes to the just-restored database.

Instructions   Complete the following steps to manually restore a database to a
network element:

....

1   From the **System View** main menu, enter the maintenance condition
via **Fault → Enter/Exit Maintenance Condition... → Enter
Maintenance Condition...**

....

2   Confirm the resulting system message by clicking **OK**.

....

3   Select **Configuration → Software → Remote Restore...** from the
System View main menu.

> **Result:**
>
> The **Restore Database** window will be opened.

....

4   Proceed as follows:

IF	THEN
you want to restore the database directly from the PC where the *WaveStar* CIT is installed,	select **CIT** in the **Restore From/Via** drop down list box. **Result:** A file selection screen appears showing that the database will back up to a specified folder under *C:\Program Files\Lucent Technologies\Wavestar CIT\....* The directory of the file selection screen is automatically pre-populated. **Reference:** Proceed with Step 5.
the connection to the NE is through a TCP/IP gateway which does *NOT* support IP tunneling,	select **FTTD** in the **Restore From/Via** drop down list box. **Reference:** Proceed with Step 6.

....

5   Select "CIT" in the **Look in** field and double click successively on *C:*,
Program Files, *Lucent Technologies*, *Wavestar CIT*, and *backups*.

Proceed Step 8.

....

Lucent Technologies

....

6   Select the **FTTD** tab and specify the **TID**, presentation selector (**Psel**), session selector (**Ssel**), transport selector (**Tsel**) and the **NSAP Address** for the FTTD information.

....

7   Select the **FTP** tab and specify the **Server** (IP address or server name), port information (optional), User name (optional) and password (optional) for the FTP information.

Proceed with <u>Step 8</u>.

....

Important! Be careful to select the correct backup files to restore to the NE.

8   Specify the path to the folder where the backup files reside.

....

9   Verify your settings and correct if necessary. Then click **Restore**.

....

10   Confirm the resulting system message by clicking **YES**.

Result:

The **NE Data Restore in Progress** window appears. When the database restore is complete, the system will perform a reset. As a consequence, the management association between the *WaveStar* CIT and the NE will be lost. After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar* CIT to the NE.

....

11   Connect to the NE again.

....

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

....

13   Confirm the resulting system message by clicking **OK**.

The *LambdaUnite* MSS NE will now perform a system reset. As a consequence, the management association between the *WaveStar* CIT and the NE will be lost. After the system reset has finished, you can

....

re-establish the management association by again connecting the *WaveStar* CIT to the NE.

E N D   O F   S T E P S

□

Replacing a defective *CompactFlash*™ card

....

Purpose   Use this procedure to replace the system's non-volatile memory (NVM, *CompactFlash* card with IDE interface) ***only*** when instructed to do so as part of a trouble clearing procedure.

Regular database backups   To make sure that the NE database (NE software and configuration data) available for restoration after the exchange of a *CompactFlash* card best represents the most recent NE configuration, it is strongly recommended to backup the NE database in regular intervals, and especially after major configuration changes.

Please refer to the *LambdaUnite*™ *MSS User Operations Guide* for further information about database backup.

***CompactFlash* card**   The *CompactFlash* card resides in a *CompactFlash* drive integrated in the CTL circuit pack.

....
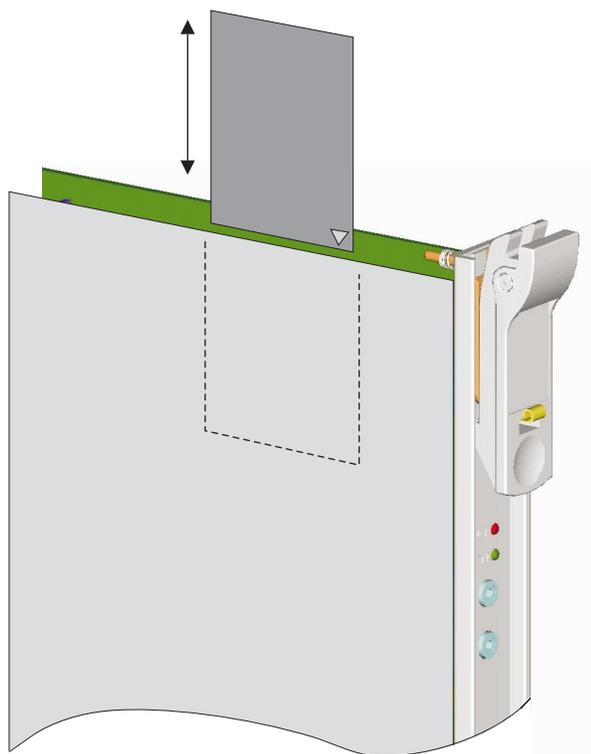
Before you begin   You or a service technician need to be on-site at the NE to replace a *CompactFlash* card.

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

Required equipment

The following equipment is required to perform this procedure:

• A replacement *CompactFlash* card.

• A PC featuring a *CompactFlash* drive. Alternatively, a PC featuring a PCMCIA drive in conjunction with a *CompactFlash* adapter (for example a *SanDisk*® CompactFlash Adapter) may be used.

Instructions

1   Insert a new *CompactFlash* card into the drive of the PC where the database backups are stored.

2   Format the *CompactFlash* card with an FAT file system.

3   By using the *Windows*® Explorer, copy the most recent database backup to the new *CompactFlash* card.

4   Unmount the *CompactFlash* card ("slot power off").

5   Eject the *CompactFlash* card from the PC drive.

6   Eject the (defective) *CompactFlash* card from the CTL *CompactFlash* drive.

7   Insert the new *CompactFlash* card into the CTL *CompactFlash* drive.
E N D   O F   S T E P S

□

Removing a circuit pack from the system

Purpose   Use this procedure to permanently remove a circuit pack from its slot.

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

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

Required equipment

The following equipment is required to perform this procedure:

- A replacement circuit pack.
- Blank faceplates to cover unequipped slots.
- *WaveStar*® CIT.

Instructions

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Proceed as follows to permanently remove a circuit pack from the shelf:

....

1   Using the *WaveStar* CIT, release all cross connections, facility loopbacks, timing reference assignments etc. which have previously been provisioned for the circuit pack to be removed.

Reference:

Please refer to "Deprovisioning a circuit pack" (4-38).

....

2   Remove the circuit pack from its slot.

....

....

3   Cover the now unequipped slot(s) with a blank faceplate (cf.
"Configuration rules" (4-44)).

Circuit packs occupying more than one slot require the corresponding
number of blank faceplates to cover the unequipped slots.

....

4   Deprovision the circuit pack by using the *WaveStar* CIT.
E N D   O F   S T E P S
....

Deprovisioning a circuit pack   These preconditions have to be fulfilled for the indicated circuit pack
before it can be deprovisioned:

- XC320 (Worker):
    - The corresponding slot is not equipped, *and*
    - there exists no port protection group, *and*
    - there exists no cross connection.
- OP… port unit:
    - The corresponding slot is not equipped, *and*
    - no port of the provisioned OP… port unit is a member of a
      port protection group, *and*
    - no port of the provisioned OP… port unit has DCC links
      enabled, *and*
    - no port of the provisioned OP… port unit is assigned as a
      timing reference, *and*
    - no port of the provisioned OP… port unit is involved in an
      orderwire connection, *and*
    - no port of the provisioned OP… port unit is involved in a
      cross connection or facility loopback, *and*
    - no tributary of the provisioned OP… port unit is involved in
      a cross connection or in a path protection.
- GE1 port unit:
    - The corresponding slot is not equipped, *and*
    - no port of the provisioned GE1 port unit is involved in a
      cross connection, *and*
    - no port of the provisioned GE1 port unit is involved in a
      facility loopback.

□

....

Replacing a circuit pack by a circuit pack of the same type

Purpose   Use the following procedure, for example during a trouble clearing procedure, to replace a circuit pack by a circuit pack of the same type.

Note that there is a specific procedure for replacing the Controller (CTL), please refer to "Replacing the Controller (CTL)" (4-42).

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

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

Required equipment

The following equipment is required to perform this procedure:

- A replacement circuit pack of the same type.

Instructions

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Proceed as follows to replace a circuit pack by a circuit pack of the same type:

....

1   Remove the circuit pack from its slot.

....

2   Within *ten* minutes (cf. "Configuration rules" (4-44)), insert the replacement circuit pack.

E ND   OF   S TEPS

☐

Replacing a circuit pack by a circuit pack of a different type

Purpose   Use this procedure, for example during a reconfiguration of a shelf, to replace a circuit pack by a circuit pack of a different type.

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

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

Required equipment

The following equipment is required to perform this procedure:

* A replacement circuit pack.
* Blank faceplates to cover unequipped slots.
* *WaveStar*® CIT.

Instructions

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

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

Proceed as follows to replace a circuit pack by a circuit pack of a different type:

1   Using the *WaveStar* CIT, release all cross connections, facility loopbacks, timing reference assignments etc. which have previously been provisioned for the circuit pack to be removed.

Reference:

Please refer to "Deprovisioning a circuit pack" (4-38).

2   Remove the circuit pack from its slot.

3   Cover the now unequipped slot(s) temporarily with a blank faceplate
(cf. "Configuration rules" (4-44)).

Circuit packs occupying more than one slot require the corresponding
number of blank faceplates to cover the unequipped slots.

4   Deprovision the circuit pack by using the *WaveStar* CIT.

5   You may now either pre-provision the circuit pack to be inserted using
the *WaveStar* CIT and then proceed with the next step, or you may
directly proceed with the next step.

6   Remove the previously inserted blank faceplates.

The number of blank faceplates to be removed depends on the
required number of slots for the circuit pack to be inserted. Do not
leave unequipped slots uncovered for more than ten minutes (cf.
"Configuration rules" (4-44)).

7   Insert the new circuit pack.

If you did not pre-provision the circuit pack, then it will now be
auto-provisioned.

E ND   OF   S TEPS

☐

Replacing the Controller (CTL)

....

Purpose Use this procedure to replace the Controller (CTL) while preserving the present NE database (NE software and configuration data).

Before you begin Make sure the required equipment listed below is available and within easy reach before you begin.

Required equipment

The following equipment is required to perform this procedure:

*   A replacement CTL circuit pack.

Instructions ....

Important! In order 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.

1 Proceed as follows:

1. Open the latches of the CTL to be replaced. *Do not remove the CTL from its slot at that time.*
    The green "ACTIVE" LED on the faceplate of the CTL starts flashing.

2. Wait until the "ACTIVE" LED has stopped flashing (about five seconds).

3. Remove the CTL from its slot.

....

2 Eject the *CompactFlash* card from the *CompactFlash* drive of the CTL circuit pack to be replaced.

....

3 Insert the *CompactFlash* card into the *CompactFlash* drive of the CTL circuit pack to be inserted.

....

4 Insert the new CTL circuit pack into its designated slot and close the latches.

Result:

The serial number stored in the backplane EEPROM will now be compared with the serial number stored on the *CompactFlash*

....

card. If the serial numbers match, the CTL circuit pack will perform a reset (full reset).

E N D   O F   S T E P S

....

□

Configuration rules

Shelf equipage (front view)   The following figure provides an overview of the front-side slots in a *LambdaUnite*™ MSS DUR shelf and their equipage.

									40										
										31	32	33	34	35	36	37	38	39
21	22	23	24	25	26	27	28												
01	02	03	04	05	06	07	08	**09**	**10**	**11**	12	13	14	15	16	17	18	19	
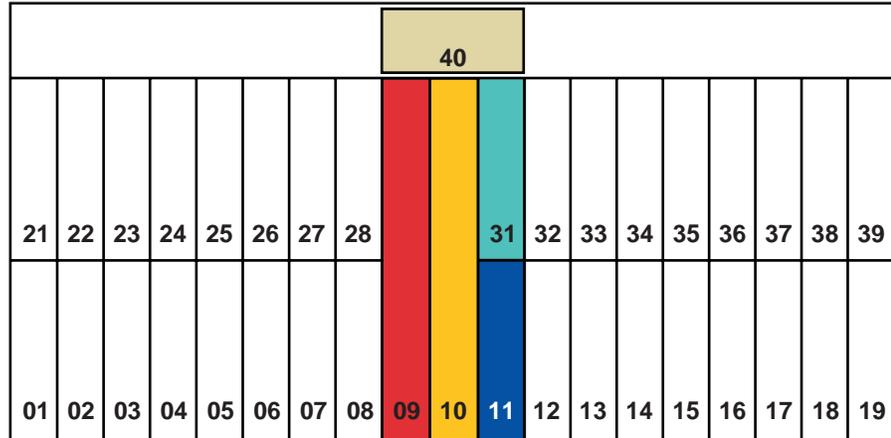
Legend:

01 … 08, 12 … 19, 21 … 28, 32 … 39	Port units (OP… variants, GE1): • OP2G5 port units occupy one slot. • OP10 port units occupy a group of two neighbouring slots. • GE1 port units occupy one slot.
09	XC320 (Worker)
10	XC320 (Protection)
11	CTL (Worker)
31	CTL (Protection)
40	User panel

Shelf equipage (rear view)   The following figure provides an overview of the rear-side slots in a *LambdaUnite* MSS DUR shelf and their equipage.
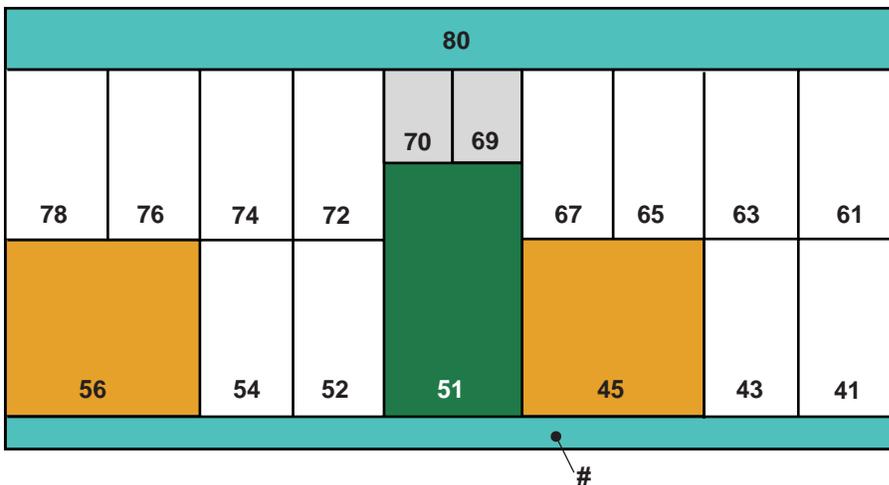
Legend:

45	Power Interface (PI) A
51	Connection Interface for the Controller (CI-CTL)
56	Power Interface (PI) B
69	Timing Interface (TI) A
70	Timing Interface (TI) B
80	Fan unit
#	Air filter
41, 43, 52, 54, 61, 63, 65, 67, 72, 74, 76, 78	Reserved for future applications

Rules and guidelines   Observe the following 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 circuit pack in the lower row of the subrack below an OP10 circuit pack in the upper row. This applies to all supported OP10 versions except the OP10/1.3IOR1.

2. 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.

3. Cover unequipped slots with blank faceplates. Do not leave unequipped slots uncovered for more than ***ten*** (10) minutes to avoid overheating of the system.
    The cooling of the *LambdaUnite* MSS system relies on sufficient airflow. Uncovered slots prevent an adequate cooling because *LambdaUnite* MSS systems make use of the stack effect.

4. In order 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 remove the CTL from its slot at that time.***
        The green "ACTIVE" LED on the faceplate of the CTL starts flashing.

    b. Wait until the "ACTIVE" LED has stopped flashing (about five seconds).

    c. Remove the CTL from its slot.

5. 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.

6. Do not insert a standby Controller (CTL) into slot 31. Leave this slot unequipped instead, and cover it with a blank faceplate.

                                                                                    ☐

Initiating a circuit pack reset

....

Purpose   Use this procedure to reset a circuit pack.

A circuit pack reset is only possible for circuit packs with an integrated controller (function controller). Circuit packs with function controller are also called "subsystems".

Types of reset   These types of reset can be distinguished:

- Controller reset
  A controller reset is a partial shutdown of a subsystem, which does not affect the basic transmission service provided by the subsystem as a whole. Only the subsystem's controller part, hardware and software, is shut down.

- Full reset
  A full reset is a shutdown of a whole subsystem with basic transmission service affected. A full reset affects both the subsystem controller and the controlled hardware.
  Please note, that a full reset of the Controller (CTL), in contrast to a controller reset of the CTL, affects

  - MS/Line performance monitoring, and

  - Automatic Protection Switching (APS) on MS/Line level (SDH: Multiplex Section Protection (MSP) and MS-SPRing; SONET: Line Protection and BLSR)

LED indications

When performing a reset, the indications via the circuit pack faceplate LEDs will be as follows, depending on the type of reset:

Type of reset	"ACTIVE" LED	"FAULT" LED
Full reset	–	●
Controller reset	●	●
– LED is off; ● LED is on		

Before you begin   Please read the instructions first.

If you want to initiate a controller reset for a particular circuit pack, or if you are not on site at the network element, make sure that you

....

have the required privileges, and that the required equipment is available.

Required privilege

You must have at least privilege codes of **S4** *and* **M4**.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

1 Depending on the type of reset, proceed as follows:

If you want to initiate a …	then …
Full reset	proceed with Step 2.
Controller reset	proceed with Step 4.

2 There are two possible ways to initiate a full reset of a circuit pack, depending on whether you are on site at the network element or not:

If you are …	then …
on site at the NE	proceed with Step 3.
not on site at the NE	proceed with Step 4.

Important! A full reset of a circuit pack may be service affecting!

3 If you want to proceed, follow these instructions depending on the type of circuit pack to be reset:

If you want to reset …	then …
the CTL	proceed as follows in order to avoid damage to the NE database stored on the *CompactFlash*™ card: 1. Open at least one of the latches of the CTL to be reset. The green "ACTIVE" LED on the faceplate of the CTL starts flashing. 2. Wait until the "ACTIVE" LED has stopped flashing (about five seconds). 3. Close the latches of the CTL.
a circuit pack other than the CTL	open and close the latches of the corresponding circuit pack.

Result:

The corresponding circuit pack will perform a full reset.

....

4   By means of the *WaveStar* CIT, establish a management association to the respective NE.

....

5   From the *WaveStar* CIT **System View** main menu, select **Fault → Reset → Slot…**

Result:

The **Reset Slot** window is opened.

....

6   Specify the slot where the corresponding circuit pack resides by selecting the slot from the equipment selection tree on the left-hand side of the **Reset Slot** window. Alternatively, you may also enter the slot AID directly into the **Enter AID** field.

....

7   Click **Select**.

....

8   Specify the type of reset by means of the **Reset Type** checkboxes on the right-hand side of the **Reset Slot** window.

....

9   Click **Apply**.

Important! A full reset of a circuit pack may be service affecting!

10   If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window.

E N D   O F   S T E P S

Initiating a system reset

Purpose   You may initiate a system reset to bring the entire system in a defined state if you suspect it to be in a faulty state. As a result the entire system will be re-initialized.

Before you begin   Make sure that you have the required privileges, and that the required equipment is available.

Required privilege

You must have at least privilege codes of **S4** *and* **M4**.

Required equipment

The following equipment is required to perform this task:

* *WaveStar*® CIT

Instructions

1   By means of the *WaveStar* CIT, establish a management association to the respective NE.

2   From the *WaveStar* CIT **System View** main menu, select **Fault** → **Reset** → **System…**

Important! A system reset may be service affecting!

3   If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window.

The *LambdaUnite*™ MSS NE will now perform a system reset. As a consequence, the management association between the *WaveStar* CIT and the NE will be lost. After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar* CIT to the NE.

E ND   OF   S TEPS

□

Glossary

μ
Microns

NUMERICS

0x1 Line Operation

0x1 means unprotected operation. The connection between network elements has one bidirectional line (no protection line).

1+1 Line Protection

A protection architecture in which the transmitting equipment transmits a valid signal on both the working and protection lines. The receiving equipment monitors both lines. Based on performance criteria and OS control, the receiving equipment chooses one line as the active line and designates the other as the standby line.

1xN Equipment Protection

1xN protection pertains to N number of circuit pack/port units protected by one circuit pack or port unit. When a protection switch occurs, the working signals are routed from the failed pack to the protection pack. When the fault clears, the signals revert to the working port unit.

12NC (12-digit Numerical Code)

Used to uniquely identify an item or product. The first ten digits uniquely identify an item. The eleventh digit is used to specify the particular variant of an item. The twelfth digit is used for the revision issue. Items with the first eleven digits the same, are functionally equal and may be exchanged.

A   ABN

Abnormal (condition)

ABS (Absent)

Used to indicate that a given circuit pack is not installed.

AC

Alternating Current

Accessible Emission Limits (AEL)

The maximum accessible emission level permitted within a particular laser class (directly at the aperture).

Acknowledged Information Transfer Service (AITS)

The confirmed mode of operation of the LAPD protocol.

ACO (Alarm Cut-Off)

A button on the user panel used to silence audible alarms.

ACT (Active)

Used to indicate that a circuit pack or module is in-service and currently providing service functions.

Adaptive-rate tributary operation of a port (Pipe mode)

Mode of operation of a port in which tributaries are *not* explicitly provisioned for the expected signal rates. The signal rates are automatically identified.

ADM (Add/Drop Multiplexer)

The term for a synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

AEL

→ "Accessible Emission Limits" (GL-2)

Agent

Performs operations on managed objects and issues events on behalf of these managed objects. All SDH managed objects will support at least an agent. Control of distant agents is possible via local "Managers".

AGNE

Alarm Gateway Network Element

AID (Access Identifier)

A technical specification for explicitly naming entities (both physical and logical) of an NE using a grammar comprised of ASCII text, keywords, and grammar rules.

AIS (Alarm Indication Signal)

A code transmitted downstream in a digital network that indicates that an upstream failure has been detected and alarmed if the upstream alarm has not been suppressed.

AITS

→ "Acknowledged Information Transfer Service" (GL-2)

Alarm

Visible or audible signal indicating that an equipment failure or significant event/condition has occurred.

Alarm Correlation

The search for a directly-reported alarm that can account for a given symptomatic condition.

Alarm Severity

An attribute defining the priority of the alarm message. The way alarms are processed depends on the severity.

Alarm Suppression

Selective removal of alarm messages from being forwarded to the GUI or to network management layer OSs.

Alarm Throttling

A feature that automatically or manually suppresses autonomous messages that are not priority alarms.

Aligning

Indicating the head of a virtual container by means of a pointer, for example, creating an Administrative Unit (AU) or a Tributary Unit (TU).

AMI (Alternate Mark Inversion)

A line code that employs a ternary signal to convert binary digits, in which successive binary ones are represented by signal elements that are normally of alternative positive and negative polarity but equal in amplitude and in which binary zeros are represented by signal elements that have zero amplitude.

Anomaly

A difference between the actual and desired operation of a function.

ANSI

American National Standards Institute

APD

Avalanche Photo Diode

APS

Automatic Protection Switching

ASCII (American Standard Code for Information Interchange)

A standard 7-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

ASN.1
Abstract Syntax Notation 1

Assembly
Gathering together of payload data with overhead and pointer information (an indication of the direction of the signal).

Association
A logical connection between manager and agent through which management information can be exchanged.

Asynchronous
The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

ATM (Asynchronous Transfer Mode)
A high-speed transmission technology characterized by high bandwidth and low delay. It utilizes a packet switching and multiplexing technique which allocates bandwidth on demand.

Attribute
Alarm indication level: critical, major, minor, or no alarm.

AU (Administrative Unit)
Carrier for TUs.

AU PTR (Administrative Unit Pointer)
Indicates the phase alignment of the VC-N with respect to the STM-N frame. The pointer position is fixed with respect to the STM-N frame.

AUG
Administrative Unit Group

AUTO (Automatic)
One possible state of a port or slot. When a port is in the AUTO state and a good signal is detected, the port automatically enters the IS (in-service) state. When a slot is in the AUTO state and a circuit pack is detected, the slot automatically enters the EQ (equipped) state.

Autolock
Action taken by the system in the event of circuit pack failure/trouble. System switches to protection and prevents a return to the working circuit pack even if the trouble clears. Multiple protection switches on a circuit pack during a short period of time cause the system to autolock the pack.

Autonomous Message
A message transmitted from the controlled Network Element to a management system which was not a response to a command originating from the management system.

....

AVAIL
Available

B **Bandwidth**
The difference in Hz between the highest and lowest frequencies in a transmission channel. The data rate that can be carried by a given communications circuit.

Baud Rate
Transmission rate of data (bits per second) on a network link.

BCSR
Bidirectional Circuit-Switched Ring

BCSR_restPA
BCSR enhanced with restoration of non-affected protection access (extra traffic).

BER (Bit Error Rate)
The ratio of error bits received to the total number of bits transmitted.

Bidirectional Line
A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bidirectional Ring
A ring in which both directions of traffic between any two nodes travel through the same network elements (although in opposite directions).

Bidirectional Switch
Protection switching performed in both the transmit and receive directions.

BIP-N (Bit Interleaved Parity-N)
A method of error monitoring over a specified number of bits (BIP-3 or BIP-8).

Bit
The smallest unit of information in a computer, with a value of either 0 or 1.

Bit Error Rate Threshold
The point at which an alarm is issued for bit errors.

BLD OUT LG
Build-Out Lightguide

BLSR
Bidirectional Line-Switched Ring

Bridge Cross-Connection

The setting up of a cross-connection leg with the same input tributary as that of an existing cross-connection leg. Thus, forming a 1:2 bridge from an input tributary to two output tributaries.

Broadband Communications

Voice, data, and/or video communications at greater than 2 Mb/s rates.

Broadband Service Transport

STM-1 concatenation transport over the *LambdaUnite*™ MSS for ATM applications.

Byte

Refers to a group of eight consecutive binary digits.

C   C

Container

CC (Clear Channel)

A digital circuit where no framing or control bits are required, thus making the full bandwidth available for communications.

CC (Cross-Connection)

Path-level connections between input and output tributaries or specific ports within a single NE. Cross-connections are made in a consistent way even though there are various types of ports and various types of port protection. Cross-Connections are reconfigurable interconnections between tributaries of transmission interfaces.

Cell Relay

Fixed length cells. For example, ATM with 53 octets.

CEPT

Conférence Européenne des Administrations des Postes et des Télécommunications

CFR

Code of Federal Regulations

Channel

A sub-unit of transmission capacity within a defined higher level of transmission capacity.

Circuit

A set of transmission channels through one or more network elements that provides transmission of signals between two points, to support a single communications path.

CIT or *WaveStar*® CIT (Craft Interface Terminal)

The user interface terminal used by craft personnel to communicate with a network element.

CL
Clear

CLEI
Common Language Equipment Identifier

Client
Computer in a computer network that generally offers a user interface to a server.

CLLI
Common Language Location Identifier

Closed Ring Network
A network formed of a ring-shaped configuration of network elements. Each network element connects to two others, one on each side.

CM (Configuration Management)
Subsystem that configures the network and processes messages from the network.

CMI
Coded Mark Inversion

CMIP
Common Management Information Protocol. OSI standard protocol for OAM&P information exchange.

CMISE
Common Management Information Service Element

CO (Central Office)
A building where common carriers terminate customer circuits.

Co-Resident
A hardware configuration where two applications can be active at the same time independently on the same hardware and software platform without interfering with each others functioning.

Collocated
System elements that are located in the same location.

Command Group
An administrator-defined group that defines commands to which a user has access.

Concatenation

A procedure whereby multiple virtual containers are associated one with each other resulting in a combined capacity that can be used as a single container across which bit sequence integrity is maintained.

Core diameter (Mode field diameter)

The diameter of the fiber core which is the center of the optical fiber. The transmitted light is propagated through the core.

Correlation

A process where related hard failure alarms are identified.

CP

Circuit Pack

CPE

Customer Premises Equipment

CR (Critical (alarm))

Alarm that indicates a severe, service-affecting condition.

CRC

Cyclical Redundancy Check

Cross-Connect Map

Connection map for an SDH Network Element; contains information about how signals are connected between high speed time slots and low speed tributaries.

Crosstalk

An unwanted signal introduced into one transmission line from another.

CSD

Clock and synchronisation distribution function

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

CTIP

Customer Training and Information Products

CTL

Controller

CTS

Customer Technical Support within Lucent Technologies

D   DACS/DCS

Digital Access Cross-Connect System

Data

A collection of system parameters and their associated values.

Database Administrator

A user who administers the database of the application.

dB

Decibels

DC

Direct Current

DCC (Data Communications Channel)

The embedded overhead communications channel in the synchronous line, used for end-to-end communications and maintenance. The DCC carries alarm, control, and status information between network elements in a synchronous network.

DCE (Data Communications Equipment)

The equipment that provides signal conversion and coding between the data terminating equipment (DTE) and the line. The DCE may be separate equipment or an integral part of the DTE or of intermediate equipment. A DCE may perform other functions usually performed at the network end of the line.

DCF

Data Communications Function

DCN

Data Communications Network

Default

An operation or value that the system or application assumes, unless a user makes an explicit choice.

Default Provisioning

The parameter values that are preprogrammed as shipped from the factory.

Defect

A limited interruption of the ability of an item to perform a required function. It may or may not lead to maintenance action depending on the results of additional analysis.

Demultiplexing

A process applied to a multiplexed signal for recovering signals combined within it and for restoring the distinct individual channels of these signals.

DEMUX (Demultiplexer)

A device that splits a combined signal into individual signals at the receiver end of transmission.

Deprovisioning

The inverse order of provisioning. To manually remove/delete a parameter that has (or parameters that have) previously been provisioned.

Digital Link

A transmission span such as a point-to-point 2 Mb/s, 34 Mb/s, 140 Mb/s, VC12, VC3 or VC4 link between controlled network elements. The channels within a digital link are insignificant.

Digital Multiplexer

Equipment that combines by time-division multiplexing several digital signals into a single composite digital signal.

Digital Section

A transmission span such as an STM-N signal. A digital section may contain multiple digital channels.

Disassembly

Splitting up a signal into its constituents as payload data and overhead (an indication of the direction of a signal).

Dispersion

Time-broadening of a transmitted light pulse.

Dispersion Shifted Optical Fiber

1330/1550 nm minimum dispersion wavelength.

Divergence

When there is unequal amplification of incoming wavelengths, the result is a power divergence between wavelengths.

DNI (Dual Node Ring Interworking)

A topology in which two rings are interconnected at two nodes on each ring and operate so that inter-ring traffic is not lost in the event of a node or link failure at an interconnecting point.

Doping

The addition of impurities to a substance in order to attain desired properties.

Downstream

At or towards the destination of the considered transmission stream, for example, looking in the same direction of transmission.

DPLL

Digital Phase Locked Loop

DRAM

Dynamic Random Access Memory

Drop and Continue

A circuit configuration that provides redundant signal appearances at the outputs of two network elements in a ring. Can be used for Dual Node Ring Interworking (DNI) and for video distribution applications.

Drop-Down Menu

A menu that is displayed from a menu bar.

DSNE (Directory Service Network Element)

A designated Network Element that is responsible for administering a database that maps Network Elements names (node names) to addresses (node Id). There can be one DSNE per (sub)network.

DTE (Data Terminating Equipment)

The equipment that originates data for transmission and accepts transmitted data.

DTMF

Dual Tone Multifrequency

DUS

Do not Use for Synchronization

DWDM (Dense Wavelength Division Multiplexing)

Transmitting two or more signals of different wavelengths simultaneously over a single fiber.

E   EBER (Excessive Bit Error Ratio)

The calculated average bit error ratio over a data stream.

ECC

Embedded Control Channel

EEPROM

Electrically Erasable Programmable Read-Only Memory

EIA (Electronic Industries Association)

A trade association of the electronic industry that establishes electrical and functional standards.

EM

Event Management

EMC (Electromagnetic Compatibility)

A measure of equipment tolerance to external electromagnetic fields.

EMI (Electromagnetic Interference)

High-energy, electrically induced magnetic fields that cause data corruption in cables passing through the fields.

EMS

Element Management System

Entity

A specific piece of hardware (usually a circuit pack, slot, or module) that has been assigned a name recognized by the system.

Entity Identifier

The name used by the system to refer to a circuit pack, memory device, or communications link.

EoS (Ethernet over SDH)

Generic name for the mapping of MAC frames (Ethernet frames) into SDH standard or virtually concatenated VC-n. It involves encapsulation, framing, scrambling, mapping and management of VC-n-Xv.

EPROM

Erasable Programmable Read-Only Memory

EQ (Equipped)

Status of a circuit pack or interface module that is in the system database and physically in the frame, but not yet provisioned.

ES (Errored Seconds)

A performance monitoring parameter. ES "type A" is a second with exactly one error; ES "type B" is a second with more than one and less than the number of errors in a severely errored second for the given signal. ES by itself means the sum of the type A and type B ESs.

ESD

Electrostatic Discharge

ESP

Electrostatic Protection

....

GLOSSARY
GL - 1 2

Lucent Technologies

365-374-057
Issue a, January 2002

Establish

A user initiated command, at the *WaveStar* CIT, to create an entity and its associated attributes in the absence of certain hardware.

ETSI

European Telecommunications Standards Institute

Event

A significant change. Events in controlled Network Elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs in a controlled Network Element, the controlled Network Element will generate an alarm or status message and send it to the management system.

Event Driven

A required characteristic of network element software system: NEs are reactive systems, primarily viewed as systems that wait for and then handle events. Events are provided by the external interface packages, the hardware resource packages, and also by the software itself.

Externally Timed

An operating condition of a clock in which it is locked to an external reference and is using time constants that are altered to quickly bring the local oscillator's frequency into approximate agreement with the synchronization reference frequency.

Extra traffic

Unprotected traffic that is carried over protection channels when their capacity is not used for the protection of working traffic.

F   Fault

Term used when a circuit pack has a hard (not temporary) fault and cannot perform its normal function.

Fault Management

Collecting, processing, and forwarding of autonomous messages from network elements.

FCC

Federal Communications Commission

FDA/CDRH

The Food and Drug Administration's Center for Devices and Radiological Health.

FDDI (Fiber Distributed Data Interface)

Fiber interface that connects computers and distributes data among them.

FE (Far End)

Any other network element in a maintenance subnetwork other than the one the user is at or working on. Also called remote.

FEBE (Far-End Block Error)
An indication returned to the transmitting node that an errored block has been detected at the receiving node. A block is a specified grouping of bits.

FEPROM (Flash EPROM)
A technology that combines the nonvolatility of EPROM with the in-circuit reprogrammability of EEPROM (electrically-erasable PROM).

FERF (Far-End Receive Failure)
An indication returned to a transmitting Network Element that the receiving Network Element has detected an incoming section failure. Also known as RDI.

FIT (Failures in Time)
Circuit pack failure rates per 10^9 hours as calculated using the method described in Reliability Prediction Procedure for Electronic Equipment, BellCore Method I, Issue 5, September 1995.

Fixed-rate tributary operation of a port
Mode of operation of a port in which tributaries are provisioned for the expected signal rates. This provisioning information is used for crossconnection rate validation and for alarm handling (for example "Loss of Pointer").

Folded Rings
Folded (collapsed) rings are rings without fiber diversity. The terminology derives from the image of folding a ring into a linear segment.

Forced
Term used when a circuit pack (either working or protection) has been locked into a service-providing state by user command.

FR (Frame Relay)
A form of packet switching that relies on high-quality phone lines to minimize errors. It is very good at handling high-speed, bursty data over wide area networks. The frames are variable lengths and error checking is done at the end points.

Frame
The smallest block of digital data being transmitted.

Framework
An assembly of equipment units capable of housing shelves, such as a bay framework.

Free Running
An operating condition of a clock in which its local oscillator is not locked to an internal synchronization reference and is using no storage techniques to sustain its accuracy.

G **GB**
Gigabytes

Gbit/s
Gigabits per second

GHz
Gigahertz

Global Wait to Restore Time
Corresponds to the time to wait before switching back to the timing reference. It occurs after a timing link failure has cleared. This time applies for all timing sources in a system hence the name global. This can be between 0 and 60 minutes, in increments of one minute.

GNE (Gateway Network Element)
A network element that passes information between other network elements and management systems through a data communication network.

H **Hard Failure**
An unrecoverable nonsymptomatic (primary) failure that causes signal impairment or interferes with critical network functions, such as DCC operation.

HDB3 (High Density Bipolar 3 Code)
Line code for 2 Mb/s transmission systems.

HDLC (High Level Data Link Control)
OSI reference model datalink layer protocol.

HMI
Human Machine Interface

HML (Human Machine Language)
A standard language developed by the ITU for describing the interaction between humans and dumb terminals.

HO
High Order

Holdover
An operating condition of a clock in which its local oscillator is not locked to an external reference but is using storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronization reference.

Hot Standby

A circuit pack ready for fast, automatic placement into operation to replace an active circuit pack. It has the same signal as the service going through it, so that choice is all that is required.

HPA (Higher Order Path Adaptation)

Function that adapts a lower order Virtual Container to a higher order Virtual Container by processing the Tributary Unit pointer which indicates the phase of the lower order Virtual Container Path Overhead relative to the higher order Virtual Container Path Overhead and assembling/disassembling the complete higher order Virtual Container.

HPC (Higher Order Path Connection)

Function that provides for flexible assignment of higher order Virtual Containers within an STM-N signal.

HPT (Higher Order Path Termination)

Function that terminates a higher order path by generating and adding the appropriate Virtual Container Path Overhead to the relevant container at the path source and removing the Virtual Container Path Overhead and reading it at the path sink.

HS

High Speed

HW

Hardware

Hz

Hertz

I   **I/O**

Input/Output

IAO LAN

Intraoffice Local Area Network

ID

Identifier

IDE

→ "Integrated Device (or Drive) Electronics" (GL-17)

IEC

International Electro-Technical Commission

IEEE

Institute of Electrical and Electronics Engineers

IMF

Infant Mortality Factor

Insert

To physically insert a circuit pack into a slot, thus causing a system initiated restoral of an entity into service and/or creation of an entity and associated attributes.

Integrated Device (or Drive) Electronics (IDE)

A hard-drive interface which has all of its controller electronics integrated into the drive itself.

Interface Capacity

The total number of STM-1 equivalents (bidirectional) tributaries in all transmission interfaces with which a given transmission interface shelf can be equipped at one time. The interface capacity varies with equipage.

Intermediate System (IS)

A system which routes/relays management information. An SDH Network Element may be a combined intermediate and end system.

IPC

Inter Processor Communications

IS (In-Service)

A memory administrative state for ports. IS refers to a port that is fully monitored and alarmed.

IS-IS Routing

The Network Elements in a management network, route packets (data) between each other using an IS-IS level protocol. The size of a network running IS-IS Level 1 is limited, and therefore certain mechanisms are employed to facilitate the management of larger networks.
For STATIC ROUTING, the capability exists for disabling the protocol over the LAN connections, effectively causing the management network to be partitioned into separate IS-IS Level 1 areas. In order for the network management system to communicate with a specific Network Element in one of these areas, the network management system must identify through which so-called Gateway Network Element this specific Network Element is connected to the LAN. All packets to this specific Network Element are routed directly to the Gateway Network Element by the network management system, before being re-routed (if necessary) within the Level 1 area.
For DYNAMIC ROUTING an IS-IS Level 2 routing protocol is used allowing a number of Level 1 areas to interwork. The Network Elements which connect an IS-IS area to another area are set to run the IS-IS Level 2 protocol within the Network Element and on the connection between other Network Elements. Packets can now be routed between IS-IS areas and the network management system does not have to identify the Gateway Network Elements.

ISDN

Integrated Services Digital Network

ITM

Integrated Transport Management

ITM-NM

Integrated Transport Management Network Module

ITU

International Telecommunications Union

ITU-T

International Telecommunications Union — Telecommunication standardization sector. Formerly known as CCITT: Comité Consultatif International Télégrafique & Téléphonique; International Telegraph and Telephone Consultative Committee.

J   Jitter

Short term variations of amplitude and frequency components of a digital signal from their ideal position in time.

K   Kbit/s

Kilobits per second

L   LAN (Local Area Network)

A communications network that covers a limited geographic area, is privately owned and user administered, is mostly used for internal transfer of information within a business, is normally contained within a single building or adjacent group of buildings, and transmits data at a very rapid speed.

LBC

Laser Bias Current

LBFC

Laser Backface Currents

LBO (Lightguide Build-Out)

An attenuating (signal-reducing) element used to keep an optical output signal strength within desired limits.

LCAS (Link Capacity Adjustment Scheme)

The Link Capacity Adjustment Scheme is a protocol that allows to dynamically change the

number of payload carrying VC-n's in a Virtual Concatenation Group (VCG). Under management control a VC-n can in-service be added to or deleted from a VCG. Furthermore, VC-n's for which a Trail Signal Fail (TSF) condition is present can be removed autonomously from the VCG and added to the group again as soon as the TSF condition is no longer present.

LCN
Local Communications Network

LED
Light-Emitting Diode

LH
Long Haul

Line
A transmission medium, together with the associated equipment, required to provide the means of transporting information between two consecutive network elements. One network element originates the line signal; the other terminates it.

Line Protection
The optical interfaces can be protected by line protection. Line protection switching protects against failures of line facilities, including the interfaces at both ends of a line, the optical fibers, and any equipment between the two ends. Line protection includes protection of equipment failures.

Line Timing
Refers to a network element that derives its timing from an incoming STM-N signal.

Link
The mapping between in-ports and out-ports. It specifies how components are connected to one another.

Lockout of Protection
The *WaveStar* CIT command that prevents the system from switching traffic to the protection line from a working line. If the protection line is active when a "Lockout of Protection" is entered – this command causes the working line to be selected. The protection line is then locked from any Automatic, Manual, or Forced protection switches.

Lockout State
The Lockout State shall be defined for each working or protection circuit pack. The two permitted states are: None – meaning no lockout is set for the circuit pack, set meaning the circuit pack has been locked out. The values (None & Set) shall be taken independently for each working or protection circuit pack.

LOF
Loss of Frame

LOH
Line Overhead

LOM
Loss of Multiframe

Loop Timing
A special case of line timing. It applies to network elements that have only one OC-N/STM-N interface. For example, terminating nodes in a linear network are loop timed.

Loopback
Type of diagnostic test used to compare an original transmitted signal with the resulting received signal. A loopback is established when the received optical or electrical external transmission signal is sent from a port or tributary input directly back toward the output.

LOP
Loss of Pointer

LOS
Loss of Signal

Loss Budget
Loss (in dB) of optical power due to the span transmission medium (includes fiber loss and splice losses).

LPA (Lower order Path Adaptation)
Function that adapts a PDH signal to a synchronous network by mapping the signal into or de-mapping the signal out of a synchronous container.

LPC (Lower Order Path Connection)
Function that provides for flexible assignment of lower order VCs in a higher order VC.

LPT (Lower Order Path Termination)
Function that terminates a lower order path by generating and adding the appropriate VC POH to the relevant container at the path source and removing the VC POH and reading it at the path sink.

LS
Low Speed

LTE
Line Terminating Equipment

M **µm**

Micrometer

MAC

Media Access Control

MAF

Management Application Function

Maintenance Condition

An equipment state in which some normal service functions are suspended, either because of a problem or to perform special functions (copy memory) that can not be performed while normal service is being provided.

Management Connection

Identifies the type of routing used (STATIC or DYNAMIC), and if STATIC is selected allows the gateway network element to be identified.

Manager

Capable of issuing network management operations and receiving events. The manager communicates with the agent in the controlled network element.

Manual Switch State

A protection group shall enter the Manual Switch State upon the initiation and successful completion of the Manual Switch command. The protection group leaves the Manual Switch state by means of the Clear or Forced Switch commands. While in the Manual Switch state the system may switch the active unit automatically if required for protection switching.

Mapping

The logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices or addresses on another network.

MB

Megabytes

Mbit/s

Megabits per second

MCF (Message Communications Function)

Function that provides facilities for the transport and routing of Telecommunications Management Network messages to and from the Network Manager.

MD (Mediation Device)

Allows for exchange of management information between Operations System and Network

Elements.

MDI
Miscellaneous Discrete Input

MDO
Miscellaneous Discrete Output

MEC (Manufacturer Executable Code)
Network Element system software in binary format that after being downloaded to one of the stores can be executed by the system controller of the network element.

MEM
Memory

Mid-Span Meet
The capability to interface between two lightwave network elements of different vendors. This applies to high-speed optical interfaces.

MIPS
Millions of Instructions Per Second

Miscellaneous Discrete Interface
Allows an operations system to control and monitor equipment collocated within a set of input and output contact closures.

MJ (Major (alarm))
Indicates a service-affecting failure, main or unit controller failure, or power supply failure.

MMI
Man-Machine Interface

MML
Human-Machine Language

MN (Minor (alarm))
Indicates a non-service-affecting failure of equipment or facility.

MO
Managed Object

Mode field diameter (Core diameter)

MS
Multiplexer Section

ms

Millisecond

MS-SPRING (Multiplex Section Shared Protection Ring)

A protection method used in Add-Drop Multiplexer Network Elements.

MSOH

Multiplex Section Overhead

MSP (Multiplex Section Protection)

Provides capability for switching a signal from a working to a protection section.

MST (Multiplex Section Termination)

Function that generates the Multiplexer Section OverHead in the transmit direction and terminates the part of the Multiplexer Section overhead that is acceptable in the receive direction.

MTBF (Mean Time Between Failures)

The expected time between failures, usually expressed in hours.

MTBMA

Mean Time Between Maintenance Activities

MTIE

Maximum Time Interval Error

MTPI

Multiplexer Timing Physical Interface

MTS (Multiplexer Timing Source)

Function that provides timing reference to the relevant component parts of the multiplex equipment and represents the SDH Network Element clock.

MTTR

Mean Time To Repair

Multiplexer

A device (circuit pack) that combines two or more transmission signals into a combined signal on a shared medium.

Multiplexing

A procedure by which multiple lower order path layer signals are adapted into a higher order path, or the multiple higher order path layer signals are adapted into a multiplex section.

N   NA

Not Applicable

NE (Network Element)

A node in a telecommunication network that supports network transport services and is directly manageable by a management system.

NEBS

Network Equipment-Building System

nm

Nanometer (10^{-9} meters)

NMON (Not Monitored)

A provisioning state for equipment that is not monitored or alarmed.

NMS

Network Management System

No Request State

This is the routine-operation quiet state in which no external command activities are occurring.

Node

A network element in a ring or, more generally, in any type of network. In a network element supporting interfaces to more than one ring, node refers to an interface that is in a particular ring. Node is also defined as all equipment that is controlled by one system controller. A node is not always directly manageable by a management system.

Non-Revertive Switching

In non-revertive switching, an active and stand-by line exist on the network. When a protection switch occurs, the standby line is selected to support traffic, thereby becoming the active line. The original active line then becomes the stand-by line. This status remains in effect even when the fault clears. That is, there is no automatic switch back to the original status.

Non-Synchronous

The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

NPI

Null Pointer Indication

NPPA (Non-Preemptible Protection Access)

Non-preemptible protection access increases the available span capacity for traffic which does not require protection by a ring, but which cannot be preempted.

NRZ
Nonreturn to Zero

NSA
Non-Service Affecting

NSAP Address (Network Service Access Point Address)
Network Service Access Point Address (used in the OSI network layer 3). An automatically assigned number that uniquely identifies a Network Element for the purposes of routing DCC messages.

NVM (Non-Volatile Memory)
Memory that retains its stored data after power has been removed. An example of NVM would be a hard disk.

O   O&M
Operation and Maintenance

OA
Optical Amplifier

OAM&P
Operations, Administration, Maintenance, and Provisioning

OC, OC-n
Optical Carrier

OC-12
Optical Carrier, Level 12 Signal (622.08 Mbit/s)

OC-192
Optical Carrier, Level 192 (9953.28 Mb/s) (10 Gbit/s)

OC-3
Optical Carrier, Level 3 Signal (155 Mbit/s)

OC-48
Optical Carrier, Level 48 (2488.32 Mb/s) (2.5 Gbit/s)

OI (Operations Interworking)
The capability to access, operate, provision, and administer remote systems through craft interface access from any site in a SDH network or from a centralized operations system.

OLS

Optical Line System

ONI (Operations Network Interface)

The Operations Network Interface is used to transport management information between circuit packs.

OOF

Out-of-Frame

OOS (Out-of-Service)

The circuit pack is not providing its normal service function (removed from either the working or protection state) either because of a system problem or because the pack has been removed from service.

Open Ring Network

A network formed of a linear chain-shaped configuration of network elements. Each network element connects to two others, one on each side, except for two network elements at the ends which are connected on only one side. A closed ring can be formed by adding a connection between the two end nodes.

Operations Interface

Any interface providing you with information on the system behaviour or control. These include the equipment LEDs, user panel, *WaveStar* CIT, office alarms, and all telemetry interfaces.

Operator

A user of the system with operator-level user privileges.

Optical Line Signal

A multiplexed optical signal containing multiple wavelengths or channels.

Original Value Provisioning

Preprogramming of a system's original values at the factory. These values can be overridden using local or remote provisioning.

OS (Operations System)

A central computer-based system used to provide operations, administration, and maintenance functions.

OSF

Open Software Foundation Operations System Function

OSI (Open Systems Interconnection)

Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Outage

A disruption of service that lasts for more than 1 second.

OW (Orderwire)

A dedicated voice-grade line for communications between maintenance and repair personnel.

....

P   Parameter

A variable that is given a value for a specified application. A constant, variable, or expression that is used to pass values between components.

Parity Check

Tests whether the number of ones (or zeros) in an array of binary bits is odd or even; used to determine that the received signal is the same as the transmitted signal.

Pass-Through

Paths that are cross-connected directly across an intermediate node in a network.

Path

A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Terminating Equipment

Network elements in which the path overhead is terminated.

PCB

Printed Circuit Board

PCM

Pulse Code Modulation

PCMCIA

Personal Computer Memory Card International Association

PDH

Plesiochronous Digital Hierarchy

PI

Physical Interface

Pipe mode (Adaptive-rate tributary operation of a port)

Mode of operation of a port in which tributaries are *not* explicitly provisioned for the expected signal rates. The signal rates are automatically identified.

....

Platform

A family of equipment and software configurations designed to support a particular application.

Plesiochronous Network

A network that contains multiple subnetworks, each internally synchronous and all operating at the same nominal frequency, but whose timing may be slightly different at any particular instant.

PM (Performance Monitoring)

Measures the quality of service and identifies degrading or marginally operating systems (before an alarm would be generated).

PMD (Polarization Mode Dispersion)

Output pulse broadening due to random coupling of the two polarization modes in an optical fiber.

POH (Path Overhead)

Informational bytes assigned to, and transported with the payload until the payload is demultiplexed. It provides for integrity of communication between the point of assembly of a virtual container and its point of disassembly.

Pointer

An indicator whose value defines the frame offset of a virtual container with respect to the frame reference of the transport entity on which it is supported.

POP

Point of Presence

Port (also called Line)

The physical interface, consisting of both an input and output, where an electrical or optical transmission interface is connected to the system and may be used to carry traffic between network elements. The words "port" and "line" may often be used synonymously. "Port" emphasizes the physical interface, and "line" emphasizes the interconnection. Either may be used to identify the signal being carried.

Port State Provisioning

A feature that allows a user to suppress alarm reporting and performance monitoring during provisioning by supporting multiple states (automatic, in-service, and not monitored) for low-speed ports.

POTS

Plain Old Telephone Service

PP
Pointer Processing

PRC (Primary Reference Clock)
The main timing clock reference in SDH equipment.

Preprovisioning
The process by which the user specifies parameter values for an entity in advance of some of the equipment being present. These parameters are maintained only in NVM. These modifications are initiated locally or remotely by either a CIT or an OS. Preprovisioning provides for the decoupling of manual intervention tasks (for example, install circuit packs) from those tasks associated with configuring the node to provide services (for example, specifying the entities to be cross-connected).

PRI
Primary

Proactive Maintenance
Refers to the process of detecting degrading conditions not severe enough to initiate protection switching or alarming, but indicative of an impending signal fail or signal degrade defect.

Protection Access
To provision traffic to be carried by protection tributaries when the port tributaries are not being used to carry the protected working traffic.

Protection Group Configuration
The members of a group and their roles, for example, working protection, line number, etc.

Protection Path
One of two signals entering a path selector used for path protection switching or dual ring interworking. The other is the working path. The designations working and protection are provisioned by the user, whereas the terms active path and standby path indicate the current protection state.

Protection State
When the working unit is currently considered active by the system and that it is carrying traffic. The "active unit state" specifically refers to the receive direction of operation — since protection switching is unidirectional.

PROTN (Protection)
Extra capacity (channels, circuit packs) in transmission equipment that is not intended to be used for service, but rather to serve as backup against equipment failures.

PROV (Provisioned)
Indicating that a circuit pack is ready to perform its intended function. A provisioned circuit pack can be active (ACT), in-service (IS), standby (STBY), provisioned out-of-service (POS), or

out-of-service (OOS).

PRS (Primary Reference Source)
According to the Telcordia GR-1244-CORE and ANSI T1.101 standards, a Primary Reference Source provides the basic reference signal for the timing or synchronization of other clocks within a network. The long term accuracy of the timing signal is maintained at 1×10^{-11} or better with verification to coordinated universal time (UTC). For *LambdaUnite* MSS systems, PRS is synonymous with Stratum-1 (ST-1).

PSDN ()
Public Switched Data Network

PSTN
Public Switched Telephone Network

PTE
Path Terminating Equipment

PWR
Power

PWR ON
Power On

Q   Q-LAN
Thin Ethernet LAN which connects the manager to Gateway Network Elements so that management information between Network Elements and management systems can be exchanged.

QL (Quality Level)
The quality of the timing signal(s) provided to clock a Network Element. The level is provided by the Synchronization Status Marker which can accompany the timing signal. If the System and Output Timing Quality Level mode is "Enabled", and if the signal selected for the Station Clock Output has a quality level below the Acceptance Quality Level, the Network Element "squelches" the Station Clock Output Signal, which means that no signal is forwarded at all.

Possible levels are:

- PRC (Primary Reference Clock)
- SSU_T (Synchronization Supply Unit - Transit)
- SSU_L (Synchronization Supply Unit - Local)
- SEC (SDH Equipment Clock)
- DUS (Do not Use for Synchronization)

QOS

Quality of Service

....

R   RAM

Random Access Memory

RDI (Remote Defect Indication)

An indication returned to a transmitting terminal that the receiving terminal has detected an incoming section failure. [Previously called far-end-receive failure (FERF).]

Reactive Maintenance

Refers to detecting defects/failures and clearing them.

Receive-Direction

The direction towards the Network Element.

Regeneration

The process of reconstructing a digital signal to eliminate the effects of noise and distortion.

Regenerator Loop

Loop in a Network Element between the Station Clock Output(s) and one or both Station Clock Inputs, which can be used to dejitterize the selected timing reference in network applications.

Regenerator Section Termination (RST)

Function that generates the Regenerator Section Overhead (RSOH) in the transmit direction and terminates the RSOH in the receive direction.

Reliability

The ability of a software system performing its required functions under stated conditions for a stated period of time. The probability for an equipment to fulfill its function. Some of the ways in which reliability is measured are: MTBF (Mean Time Between Failures) expressed in hours; Availability = (MTBF)/(MTBF+MTTR)(%) [where MTTR = mean time to restore]; outage in minutes per year; failures per hour; percentage of failures per 1,000 hours.

Remote Network Element

Any Network Element that is connected to the referenced Network Element through either an electrical or optical link. It may be the adjacent node on a ring, or N nodes away from the reference. It also may be at the same physical location but is usually at another (remote) site.

Restore Timer

Counts down the time (in minutes) during which the switch waits to let the worker line recover before switching back to it. This option can be set to prevent the protection switch continually switching if a line has a continual transient fault. This field is grayed out if the mode is non-revertive.

....

Revertive

A protection switching mode in which, after a protection switch occurs, the equipment returns to the nominal configuration (that is, the working equipment is active, and the protection equipment is standby) after any failure conditions that caused a protection switch to occur, clear, or after any external switch commands are reset. (See "Non-Revertive".)

Revertive Switching

In revertive switching, there is a working and protection high-speed line, circuit pack, etc. When a protection switch occurs, the protection line, circuit pack, etc. is selected. When the fault clears, service "reverts" to the working line.

Ring

A configuration of nodes comprised of network elements connected in a circular fashion. Under normal conditions, each node is interconnected with its neighbor and includes capacity for transmission in either direction between adjacent nodes. Path switched rings use a head-end bridge and tail-end switch. Line switched rings actively reroute traffic over the protection capacity.

Route

A series of contiguous digital sections.

Router

An interface between two networks. While routers are like bridges, they work differently. Routers provide more functionality than bridges. For example, they can find the best route between any two networks, even if there are several different networks in between. Routers also provide network management capabilities such as load balancing, partitioning of the network, and trouble-shooting.

RSOH

Regenerator Section OverHead; part of SOH

RST

Regenerator Section Termination

RT

Remote Terminal

RTRV

Retrieve

RZ (Return to Zero)

A code form having two information states (termed zero and one) and having a third state or an at-rest condition to which the signal returns during each period.

....

GLOSSARY
GL - 3 2

S   SA
Service Affecting

SA
Section Adaptation

SD
Signal Degrade

SDH (Synchronous Digital Hierarchy)
A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

SDS
Standard Directory Service based on ANSI recommendation T1.245

SEC
Secondary

SEC
SDH Equipment Clock

Section
The portion of a transmission facility, including terminating points, between a terminal network element and a line-terminating network element, or two line-terminating network elements.

Section Adaptation
Function that processes the AU-pointer to indicate the phase of the VC-3/4 POH relative to the STM-N SOH and assembles/disassembles the complete STM-N frame.

Self-Healing
A network's ability to automatically recover from the failure of one or more of its components.

SEMF (Synchronous Equipment Management Function)
Function that converts performance data and implementation specific hardware alarms into object-oriented messages for transmission over the DCC and/or Q-interface. It also converts object-oriented messages related to other management functions for passing across the S reference points.

Server
Computer in a computer network that performs dedicated main tasks which generally require sufficient performance.

Service

The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

SES (Severely Errored Seconds)

This performance monitoring parameter is a second in which a signal failure occurs, or more than a preset amount of coding violations (dependent on the type of signal) occurs.

SH

Short Haul

Single-Ended Operations

Provides operations support from a single location to remote Network Elements in the same SDH subnetwork. With this capability you can perform operations, administration, maintenance, and provisioning on a centralized basis. The remote Network Elements can be those that are specified for the current release.

Site Address

The unique address for a Network Element.

Slot

A physical position in a shelf designed for holding a circuit pack and connecting it to the backplane. This term is also used loosely to refer to the collection of ports or tributaries connected to a physical circuit pack placed in a slot.

SM (Single-Mode Fiber)

A low-loss, long-span optical fiber typically operating at either 1310 nm, 1550 nm, or both.

SMN

SDH Management Network

SNC/I

SubNetwork Connection (protection) / Inherent monitoring

SNC/N

SubNetwork Connection (protection) / Non-Intrusive Monitoring

SNR (Signal-to-Noise Ratio)

The relative strength of signal compared to noise.

Software Backup

The process of saving an image of the current network element's databases, which are contained in its NVM, to a remote location. The remote location could be the *WaveStar* CIT or an OS.

Software Download

The process of transferring a generic (full or partial) or provisioned database from a remote entity to the target network element's memory. The remote entity may be the *WaveStar* CIT or an OS. The download procedure uses bulk transfer to move an uninterpreted binary file into the network element.

Software ID

Number that provides the software version information for the system.

SOH (Section Overhead)

Capacity added to either an AU-4 or assembly of AU-3s to create an STM-1. Contains always STM-1 framing and optionally maintenance and operational functions. SOH can be subdivided in MSOH (multiplex section overhead) and RSOH (regenerator section overhead).

SONET (Synchronous Optical Network)

The North American standard for the rates and formats that defines optical signals and their constituents.

Span

An uninterrupted bidirectional fiber section between two network elements.

Span Growth

A type of growth in which one wavelength is added to all lines before the next wavelength is added.

SPE

Synchronous Payload Envelope

SPI

SDH Physical Interface

Squelch Map

This map contains information for each cross-connection in a ring and indicates the source and destination nodes for the low-speed circuit that is part of the cross-connection. This information is used to prevent traffic misconnection in rings with isolated nodes or segments.

SSM

Synchronization Status Message

SSU_L

Synchronization Supply Unit — Local Node

SSU_T

Synchronization Supply Unit — Transit Node

Standby Path

One of two signals entering a constituent path selector, the standby path is the path not currently being selected.

State

The state of a circuit pack indicates whether it is defective or normal (ready for normal use).

Station Clock Input

An external clock may be connected to a Station Clock Input.

Status

The indication of a short-term change in the system.

STBY (Standby)

The circuit pack is in service but is not providing service functions. It is ready to be used to replace a similar circuit pack either by protection or by duplex switching.

STM

Synchronous Transport Module (SDH)

STM-N (Synchronous Transport Module, Level N)

A building block information structure that supports SDH section layer connections, where N represents a multiple of 155.52 Mb/s. Normally N=1, 4, 16, or 64.

STS

Synchronous Transport Signal (SONET)

Subnetwork

A group of interconnected/interrelated Network Elements. The most common connotation is a synchronous network in which the Network Elements have data communications channel (DCC) connectivity.

Supervisor

A user of the application with supervisor user privileges.

Suppression

A process where service-affecting alarms that have been identified as an "effect" are not displayed to a user.

SYNC

Synchronizer

Synchronization Messaging

Synchronization messaging is used to communicate the quality of network timing, internal timing status, and timing states throughout a subnetwork.

....

GLOSSARY
GL-36

Lucent Technologies

365-374-057
Issue a, January 2002

Synchronous

The essential characteristic of time scales or signals such that their corresponding significant instances occur at precisely the same average rate, generally traceable to a single Stratum-1 source.

Synchronous Network

The synchronization of transmission systems with synchronous payloads to a master (network) clock that can be traced to a reference clock.

Synchronous Payload

Payloads that can be derived from a network transmission signal by removing integral numbers of bits from every frame. Therefore, no variable bit-stuffing rate adjustments are required to fit the payload in the transmission signal.

SYSCTL

System Controller circuit pack

System Administrator

A user of the computer system on which the system's OS software application can be installed.

T   TARP

TID Address Resolution Protocol

TCA (Threshold-Crossing Alert)

A message sent from a network element indicating that a certain performance monitoring parameter has exceeded a specified threshold.

TDM (Time Division Multiplexing)

A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a portion of each signal one after another.

Through (or Continue) Cross-Connection

A cross-connection within a ring, where the input and output tributaries have the same tributary number but are in lines opposite each other.

Through Timing

Refers to a network element that derives its transmit timing in the east direction from a received line signal in the east direction and its transmit timing in the west direction from a received line signal in the west direction.

THz
Terrahertz (10^{12} Hz)

TID (Target Identifier)
A provisionable parameter that is used to identify a particular Network Element within a network. It is a character string of up 20 characters where the characters are letters, digits, or hyphens (-).

TL1 (Transaction Language One)
A machine-to-machine communications language that is a subset of ITU's human-machine language.

TMN
Telecommunications Management Network

TR
Technical Requirement

Transmit-Direction
The direction outwards from the Network Element.

Tributary
A signal of a specific rate (2 Mb/s, 34 Mb/s, 140 Mb/s, VC12, VC3, VC4, STM-1 or STM-4) that may be added to or dropped from a line signal.

Tributary
A path-level unit of bandwidth within a port, or the constituent signal(s) being carried in this unit of bandwidth, for example, an STM-1 tributary within an STM-N port.

Tributary Unit Pointer
Indicates the phase alignment of the VC with respect to the TU in which it resides. The pointer position is fixed with respect to the TU frame.

True Wave™ Optical Fiber
Lucent Technologies' fiber generally called non-zero dispersion-shift fiber, with a controlled amount of chromatic dispersion designed for amplified systems in the 1550/1310 nm range.

TSA (Time Slot Assignment)
A capability that allows any tributary in a ring to be cross-connected to any tributary in any lower-rate, non-ring interface or to the same-numbered tributary in the opposite side of the ring.

TSI (Time Slot Interchange)
The ability of the user to assign cross-connections between any tributaries of any lines within a Network Element. Three types of TSI can be defined: Hairpin TSI, Interring TSI (between rings), and Intraring TSI (within rings).

TSO
Technical Support Organization

TTP
Trail Termination Point

TU (Tributary Unit)
An information structure which provides adaptation between the lower order path layer and the higher path layer. Consists of a VC-n plus a tributary unit pointer TU PTR.

TUG
Tributary Unit Group

Two-Way Point-to-Point Cross-Connection
A two-legged interconnection, that supports two-way transmission, between two and only two tributaries.

Two-Way Roll
The operation which moves a two-way cross-connection between tributary i and tributary j to a two-way cross-connection between the same tributary i and a new tributary k with a single user command.

U   UAS (Unavailable Seconds)
In performance monitoring, the count of seconds in which a signal is declared failed or in which 10 consecutively severely errored seconds (SES) occurred, until the time when 10 consecutive non-SES occur.

UITS
Unacknowledged Information Transfer Service. Unconfirmed mode of LAPD operation.

UNEQ
Path Unequipped

Upstream
At or towards the source of the considered transmission stream, for example, looking in the opposite direction of transmission.

User Privilege
Permissions a user must perform on the computer system on which the system software runs.

UTC (Universal Coordinated Time)
A time-zone independent indication of an event. The local time can be calculated from the Universal Coordinated Time.

V   V

Volts

VAC

Volts Alternating Current

Value

A number, text string, or other menu selection associated with a parameter.

Variable

An item of data named by an identifier. Each variable has a type, such as int or Object, and a scope.

VC-n (Virtual Container of n-th order)

Container of n-th order with path overhead.

VC-n-Xv (A group of X virtually concatenated VC-n's)

A group of X individual Virtual Containers of n-th order that form a Virtual Concatenated Group (VCG). The X in VC-n-Xv always denotes the actual number of VC-n's that are transported in the VCG which may vary when the Link Capacity Adjustment Scheme (LCAS) is active.

VCG (Virtual Concatenated Group)

A group of Virtual Containers that are virtually concatenated to offer larger payload bandwidth.

VDC

Volts Direct Current

VF

Voice frequency

Virtual

Refers to artificial objects created by a computer to help the system control shared resources.

Virtual Circuit

A logical connection through a data communication (for example, X.25) network.

Voice Frequency (VF) Circuit

A 64 kilobit per second digitized signal.

Volatile Memory

Type of memory that is lost if electrical power is interrupted.

W   WAD
Wavelength Add/Drop

WAN (Wide Area Network)
A communication network that uses common-carrier provided lines and covers an extended geographical area.

Wander
Long term variations of amplitude frequency components (below 10 Hz) of a digital signal from their ideal position in time possibly resulting in buffer problems at a receiver.

Wavelength Interchange
The ability to change the wavelength associated with an STM-N signal into another wavelength.

***WaveStar* OLS 40G/80G/400G**
WaveStar Optical Line System 40G/80G/400G

WDCS
Wideband Digital Cross-Connect System

WDM (Wavelength Division Multiplexing)
A means of increasing the information-carrying capacity of an optical fiber by simultaneously transmitting signals at different wavelengths.

Wideband Communications
Voice, data, and/or video communication at digital rates from 64 kb/s to 2 Mb/s.

Working
Label attached to a physical entity. In case of revertive switching the working line or unit is the entity that is carrying service under normal operation. In case of nonrevertive switching the label has no particular meaning.

Working State
The working unit is currently considered active by the system and that it is carrying traffic.

WRT (Wait to Restore Time)
Corresponds to the time to wait before switching back after a failure has cleared, in a revertive protection scheme. This can be between 0 and 15 minutes, in increments of one minute.

WS
Work Station

WTR (Wait to Restore)
Applies to revertive switching operation. The protection group enters the WTR state when all

Equipment Fail (EF) conditions are cleared, but the system has not yet reverted back to its working line. The protection group remains in the WTR state until the Wait-to-Restore timer completes the WTR time interval.

X   X.25

An ITU standard defining the connection between a terminal and a public packet-switched network

X.25 Interface/Protocol

The ITU packet-switched interface standard for terminal access that specifies three protocol layers: physical, link, and packet for connection to a packet-switched data network.

Z   Zero Code Suppression

A technique used to reduce the number of consecutive zeros in a line-coded signal (B3ZS, B8ZS).

Index