Lucent Technologies
Bell Labs Innovations

LambdaUnite® MultiService Switch (MSS)

Release 4.0

Alarm Messages and Trouble Clearing Guide

365-374-095
CC109330506
Issue a
March 2003

Lucent Learning +49 911 526 2455

Notice

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

Mandatory customer information

Declaration of Conformity

The Declaration of Conformity (DoC) for this product can be found in the *LambdaUnite® MultiService Switch (MSS) Applications and Planning Guide* in the chapter "Quality and reliability", or at: *http://www.lucent.de/ecl*.

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 registered trademark of Lucent Technologies.

Metropolis is a registered trademark of Chromatis Networks, Inc.

Navis is a registered 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 365-374-095 (Issue a).

Support

Technical support

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

Information product support

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

Contents

About this information product

1 Safety

General notes on safety

Specific safety areas

Safety requirements in specific deployment phases

DCN alarms

Environmental alarms

Equipment alarms

Ethernet alarms

Linear protection switching alarms

Path-related transmission alarms

Port-related transmission alarms

Ring protection switching alarms

Synchronisation alarms

Additional alarm-related information

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* for the *LambdaUnite*® MSS Release 4.0.

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 *Alarm Messages and Trouble Clearing 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 covers tasks that are often used during trouble clearing and related information.
5	Glossary	Defines telecommunication terms and expands common telecommunication abbreviations and acronyms

Chapter	Title	Description
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 Guide (IG)
  The *LambdaUnite® MultiService Switch (MSS) Installation Guide* is a step-by-step guide to system installation and setup. It also includes information needed for pre-installation site planning and post-installation acceptance testing.
- Applications and Planning Guide (APG)
  The *LambdaUnite® MultiService Switch (MSS) Applications and Planning Guide* 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 (UOG)
  The *LambdaUnite® MultiService Switch (MSS) User Operations Guide* provides step-by-step information for use in daily system operations. The UOG demonstrates how to perform system provisioning, operations, and administrative tasks by use of the *WaveStar®* CIT.
- Alarm Messages and Trouble Clearing Guide (AMTCG)
  The *LambdaUnite® MultiService Switch (MSS) Alarm Messages and Trouble Clearing Guide* gives detailed information on each possible network element alarm message. Furthermore, the AMTCG provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.
- Operations System Engineering Guide (OSEG)
  The *LambdaUnite® MultiService Switch (MSS) Operations System Engineering Guide* serves as a reference for all TL1 commands which can be used to operate the network element. The OSEG also gives an introduction to the concept of the TL1 commands, and an instruction how to use them.
- *Navis*™ Optical EMS Provisioning Guide for *LambdaUnite®* MSS
  The *Navis™ Optical Element Management System (EMS) Provisioning Guide for LambdaUnite® MultiService Switch (MSS)* gives instructions on how to perform system provisioning, operations, and administrative tasks by use of the *Navis*™ Optical EMS.

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

Title	**Document Numbers**	
	ISO A4 format	**US Letter format**
LambdaUnite® MultiService Switch (MSS) Release 4.0 Safety Guide	109231100 (365-374-041)	–
LambdaUnite® MultiService Switch (MSS) Release 4.0 Applications and Planning Guide	109230979 (365-374-027)	109230961 (365-374-028)
LambdaUnite® MultiService Switch (MSS) Release 4.0 User Operations Guide	109230987 (365-374-029)	109230995 (365-374-030)

Title	Document Numbers	
	ISO A4 format	**US Letter format**
LambdaUnite® MultiService Switch (MSS) Release 4.0 Alarm Messages and Trouble Clearing Guide	109231027 (365-374-033)	109231035 (365-374-034)
LambdaUnite® MultiService Switch (MSS) Release 4.0 Installation Guide	109231050 (365-374-035)	109231043 (365-374-036)
LambdaUnite® MultiService Switch (MSS) Release 4.0 Operations System Engineering Guide	109231076 (365-374-037)	109231068 (365-374-038)
Navis™ Optical Element Management System (EMS) Release 8.0 Provisioning Guide for *LambdaUnite*® MultiService Switch (MSS)	109231084 (365-374-039)	109231092 (365-374-040)
CD-ROM Documentation *LambdaUnite*® MultiService Switch (MSS) Release 4.0 (all documents on one CD-ROM)	109231126 (365-374-043)	

Related training

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

Documented feature set

This manual describes *LambdaUnite*® MSS Release 4.0. 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.

Intended use

This equipment shall be used only in accordance with intended use, corresponding installation and maintenance statements as specified in this documentation. Any other use or modification is prohibited.

Optical safety

IEC Customer Laser Safety Guidelines

Lucent Technologies declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of laser products” and “Safety of optical fibre telecommunication systems”. Futhermore Lucent Technologies declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

Optical Safety Declaration (if laser modules used)

Lucent Technologies declares that this product is compliant with all essential safety requirements as stated in IEC 60825-Part 1 and 2 “Safety of Laser Products” and “Safety of Optical Fiber Telecommunication Systems”. Furthermore Lucent Technologies declares that the warning statements on labels on this equipment are in accordance with the specified laser radiation class.

Optical Fiber Communications

This equipment contains an Optical Fiber Communications semiconductor laser/LED transmitter. The following Laser Safety Guidelines are provided for this product.

General Laser Information

Optical fiber telecommunication systems, their associated test sets, and similar operating systems use semiconductor laser transmitters that emit infrared (IR) light at wavelengths between approximately 800 nanometers (nm) and 1600 nm. The emitted light is above the red end of the visible spectrum, which is normally not visible to the human eye. Although radiant en at near-IR wavelengths is officially designated invisible, some people can see the shorter wavelength energy even at power levels several orders of magnitude below any that have been shown to cause injury to the eye.

Conventional lasers can produce an intense beam of monochromatic light. The term “monochromaticity” means a single wavelength output of pure color that may be visible or invisible to the eye. A conventional laser produces a small-size beam of light, and because the beam size is small the power density (also called irradiance) is very high. Consequently, lasers and laser products are subject to federal and applicable state regulations, as well as international standards, for their safe operation.

A conventional laser beam expands very little over distance, or is said to be very well collimated. Thus, conventional laser irradiance remains relatively constant over distance. However, lasers used in lightwave systems have a large beam divergence, typically 10 to 20 degrees. Here, irradiance obeys the inverse square law (doubling the distance reduces the irradiance by a factor of 4) and rapidly decreases over distance.

Lasers and Eye Damage

The optical energy emitted by laser and high-radiance LEDs in the 400-1400 nm range may cause eye damage if absorbed by the retina. When a beam of light enters the eye, the eye magnifies and focuses the energy on the retina magnifying the irradiance. The irradiance of the energy that reaches the retina is approximately 105, or 100,000 times more than at the cornea and, if sufficiently intense, may cause a retinal burn.

The damage mechanism at the wavelengths used in an optical fiber telecommunications is thermal in origin, i.e., damage caused by heating. Therefore, a specific amount of energy is required for a definite time to heat an area of retinal tissue. Damage to the retina occurs only when one looks at the light long enough that the product of the retinal irradiance and the viewing time exceeds the damage threshold. Optical energies above 1400 nm cause corneal and skin burns, but do not affect the retina. The thresholds for injury at wavelengths greater than 1400 nm are significantly higher than for wavelengths in the retinal hazard region.

Classification of Lasers

Manufacturers of lasers and laser products in the U.S. are regulated by the Food and Drug Administration’s Center for Devices and Radiological Health (FDA/CDRH) under 21 CFR 1040. These regulations require manufacturers to certify each laser or laser product as belonging to one of four major Classes: I, II, lla, IIIa, lllb, or IV.

The International Electro-technical Commission is an international standards body that writes laser safety standards under IEC-60825. Classification schemes are similar with Classes divided into Classes 1, 1M, 2, 2M, 3R, 3B, and 4. Lasers are classified according to the accessible emission limits and their potential for causing injury. Optical fiber telecommunication systems are generally classified as Class I/1 because, under normal operating conditions, all energized laser transmitting circuit packs are terminated on optical fibers which enclose the laser energy with the fiber sheath forming a protective housing. Also, a protective housing/access panel is typically installed in front of the laser circuit pack shelves The circuit packs themselves, however, may be FDA/CDRH Class I, IIIb, or IV or IEC Class 1, 1M, 3R, 3B, or 4.

Laser Safety Precautions for Optical Fiber Telecommunication Systems

In its normal operating mode, an optical fiber telecommunication system is totally enclosed and presents no risk of eye injury. It is a Class I/1 system under the FDA and IEC classifications.

The fiber optic cables that interconnect various components of an optical fiber telecommunication system can disconnect or break, and may expose people to laser emissions. Also, certain measures and maintenance procedures may expose the technician to emission from the semiconductor laser during installation and servicing. Unlike more familiar laser devices such as solid-state and gas lasers, the emission pattern of a semiconductor laser results in a highly divergent beam. In a divergent beam, the irradiance (power density) decreases rapidly with distance. The greater the distance, the less energy will enter the eye, and the less potential risk for eye injury. Inadvertently viewing an un-terminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches normally will not cause eye injury, provided the power in the fiber is less than a few milliwatts at the near IR wavelengths and a few tens of milliwatts at the far IR wavelengths. However, damage may occur if an optical instrument such as a microscope, magnifying glass, or eye loupe is used to stare at the energized fiber end.

CAUTION

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

Laser Safety Precautions for Enclosed Systems

Under normal operating conditions, optical fiber telecommunication systems are completely enclosed; nonetheless, the following precautions shall be observed:

1. Because of the potential for eye damage, technicians should not stare into optical connectors or broken fibers
2. Under no circumstance shall laser/fiber optic operations be performed by a technician before satisfactorily completing an approved training course
3. Since viewing laser emissions directly in excess of Class I/1 limits with an optical instrument such as an eye loupe greatly increases the risk of eye damage, appropriate labels must appear in plain view, in close proximity to the optical port on the protective housing/access panel of the terminal equipment.

Laser Safety Precautions for Unenclosed Systems

During service, maintenance, or restoration, an optical fiber telecommunication system is considered unenclosed. Under these conditions, follow these practices:

1. Only authorized, trained personnel shall be permitted to do service, maintenance and restoration. Avoid exposing the eye to emissions from un-terminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters, Automatic Power Reduction (APR), and
   Automatic Power Shut Down (APSD) are engineering controls that are also used to limit emissions. However, technicians

removing or replacing laser circuit packs should not stare or look directly into the optical port with optical instruments or magnifying lenses. (Normal eye wear or indirect viewing instruments such as Find-R-Scopes are not considered magnifying lenses or optical instruments.)

2. Only authorized, trained personnel shall use optical test equipment during installation or servicing since this equipment contains semiconductor lasers (Some examples of optical test equipment are Optical Time Domain Reflectometers (OTDR's), Hand-Held Loss Test Sets.)
3. Under no circumstances shall any personnel scan a fiber with an optical test set without verifying that all laser sources on the fiber are turned off
4. All unauthorized personnel shall be excluded from the immediate area of the optical fiber telecommunication systems during installation and service.

Consult ANSI Z136.2, American National Standard for Safe Use of Lasers in the U.S.; or, outside the U.S., IEC-60825, Part 2 for guidance on the safe use of optical fiber optic communication in the workplace.

For the optical specifications please refer to the chapter "Technical specifications" in the *LambdaUnite® MultiService Switch (MSS) Applications and Planning Guide*.

Technical Documentation

The technical documentation as required by the Conformity Assessment procedure is kept at Lucent Technologies location which is responsible for this product. For more information please contact your local Lucent Technologies representative.

How to comment

To comment on this information product, go to the Online Comment Form (http://www.lucent-info.com/comments) or email your comments to the Comments Hotline (ctiphotline@lucent.com).

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

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)

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.

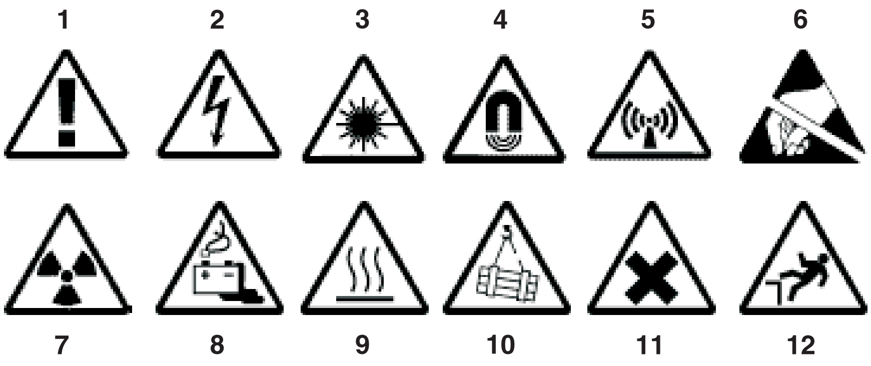
Ensure that the line circuit breaker on the Power Interface (PI) is in the "OFF" position before removing or inserting the power supply plug.

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:



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

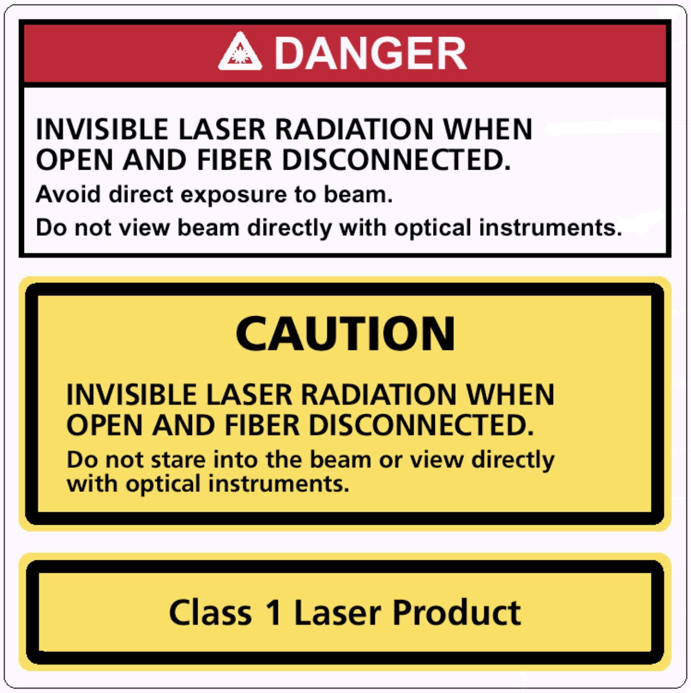
System design

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” (1-16).

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

Release 1.0, Release 2.0



DANGER

INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.

Avoid direct exposure to beam.

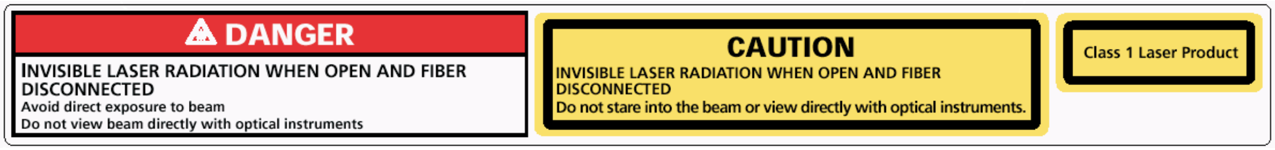
Do not view beam directly with optical instruments.

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

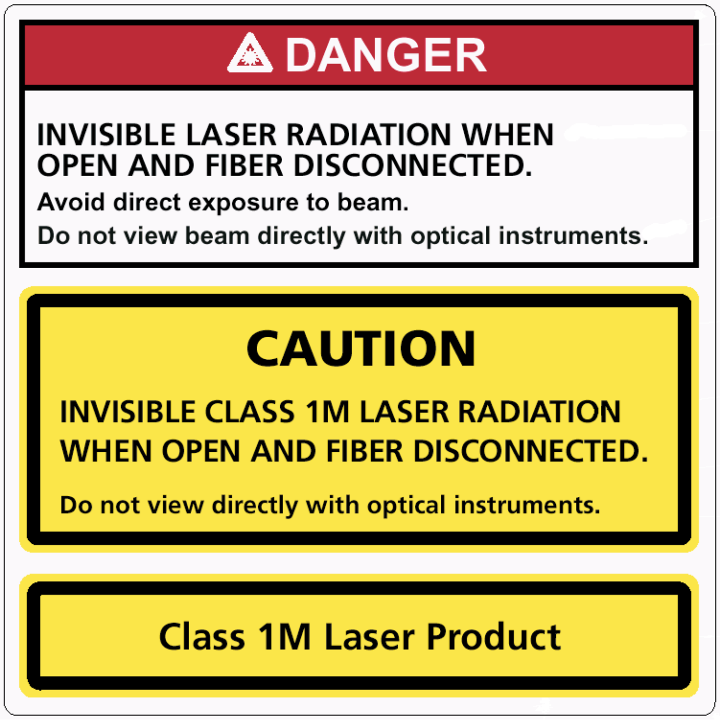
INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED
Avoid direct exposure to beam
Do not view beam directly with optical instruments

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

Release 2.1 onwards



⚠ DANGER

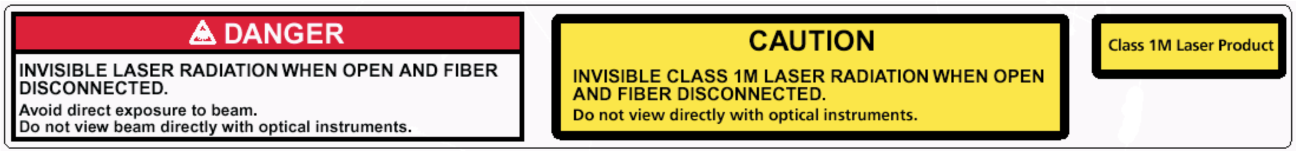
INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.
Avoid direct exposure to beam.
Do not view beam directly with optical instruments.

CAUTION

INVISIBLE CLASS 1M LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.

Do not view directly with optical instruments.

Class 1M 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 CLASS 1M LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED.
Do not view directly with optical instruments.

Class 1M 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” (1-16).

Laser safety instructions

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

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

CAUTION

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

□

Optical circuit pack specifications

Specifications The following table contains the specifications of the *LambdaUnite®* MSS optical circuit packs. Please refer to the *LambdaUnite® MSS Applications and Planning Guide* for more detailled technical specifications.

Circuit pack	**Wavelength [nm]**	**Fiber type[1] (core/cladding diameter [µm])**	**Maximum output power [mW / dBm]**	**Laser class[2] (IEC / FDA)**
155-Mbit/s optical circuit packs				
OP155M/1.3IR16 (KFA18)	1310	SM (9/125)	0.15 / -8	1 / I
622-Mbit/s optical circuit packs				
OP622/1.3IR16 (KFA17)	1310	SM (9/125)	0.15 / -8	1 / I
2.5-Gbit/s optical circuit packs				
OP2G5/1.3IOR4 (KFA12)	1310	SM (9/125)	0.5 / –3	1 / I
OP2G5/1.3LR4 (KFA203)	1310	SM (9/125)	1.6 / +2	1 / I
OP2G5/1.5LR4 (KFA204)	1550	SM (9/125)	1.6 / +2	1 / I
OP2G5-1...32PWDM (KFA20) with OM2G5/921PWDM ... 959PWDM (OM2G5A921 ... OM2G5A959)	1560.61 … 1530.33	SM (9/125)	1 / 0	1 / I
OM2G5/1.3SR1 (OM2G5A12)	1310	SM (9/125)	1 / 0	1 / I
10-Gbit/s optical circuit packs				
OP10/1.3IOR1 (KFA7)	1310	SM (9/125)	0.8 / –1	1 / I
OP10/1.5IR1 (KFA14)	1550	SM (9/125)	1.6 / +2	1 / I
OP10/1.5LR1 (KFA6)[3]	1550	SM (9/125)	20 / +13	1M / IIIb
OP10/01…80/800G (KFA9, KFA81 … 159)	1530.72 … 1562.23	SM (9/125)	0.41 / -3.8	1 / I
OP10/1…16/PWDM (KFA11, KFA61…75)	1530.33 ... 1560.61	SM (9/125)	1.6 / +2	1 / I
OP10/9285XT…8650XT (KFA210 … KFA482)	1554.537 ... 1607.466	SM (9/125)	0.63 / -2	1 / I
40-Gbit/s optical circuit packs				
OP40/1.3IOR1 (KFA202)	1311	SM (9/125)	5 / +7	1M / IIIb
OP40/1.5LR1O (KFA3)	1555.75	SM (9/125)	20 / +13	1M / IIIb
OP40/9280XT … 8650XT (KFA290 … 353)	1554.940 … 1607.466	SM (9/125)	0.5 / -3	1 / I
Gigabit-Ethernet circuit pack				

Circuit pack	Wavelength [nm]	Fiber type[1] (core/cladding diameter [µm])	Maximum output power [mW / dBm]	Laser class[2] (IEC / FDA)
GE1/SX/4 (KFA13)	850	MM (50/125)	0.4 / –4	1 / I

Notes:

1. SM: Single-mode fiber, MM: multi-mode fiber.
2. It is the class of the circuit pack, not that of the telecommunications system as a whole, that is specified.
3. The OP10/1.5LR1 circuit packs delivered with *LambdaUnite*® MSS Releases 1.0 or 2.0 are classified as Class 3A laser products in accordance with the IEC classification (cf. “Laser product classification” (1-16)).

Connector types

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

□

Laser product classification

Standards compliance

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

FDA/CDRH regulations

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

In the United States, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to "FDA/CDRH laser classification" (1-17)):

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

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

IEC requirements

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

According to the IEC classification, lasers and laser systems in the infrared wavelength range (greater than 700 nm) are assigned to one of the following classes (please refer to "IEC laser classification" (1-17)):

- Class 1,
- Class 1M,
- Class 3R,
- Class 3B or
- Class 4.

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

1. The Accessible Emission Limits (AEL) are different.
2. Class 3A applies to all wavelengths.
3. Class 3B requires strict engineering controls.
4. Classification is under single fault conditions.

FDA/CDRH laser classification

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

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

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

IEC laser classification

The following table provides an overview of laser classes for wavelengths of 1310 nm and 1550 nm in accordance with the IEC 60825-1 Ed. 1.2 (2001) standard. The precise power limits depend on the mode field diameter and the numerical aperture (NA) of the laser source.

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

Notes:

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

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

Laser class	Wavelength	Max. output power of laser radiation	
1	1310 nm	8.85 mW	+9.5 dBm
	1550 nm	10 mW	+10 dBm
3A	1310 nm	24 mW	+13.8 dBm
	1550 nm	50 mW	+17 dBm
3B	1310 nm	500 mW	+27 dBm
	1550 nm	500 mW	+27 dBm
4	1310 nm	> 500 mW	> +27 dBm
	1550 nm	> 500 mW	> +27 dBm

Notes:

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

Hazard level assignment

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

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

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

Classification of optical telecommunication equipment

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

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

□

Electrostatic discharge

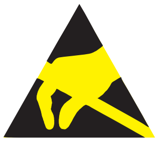
Introduction

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” (1-23)
- “Storage” (1-26)
- “Installation” (1-28)
- “Taking into operation” (1-31)
- “Operation and maintenance” (1-33)
- “Taking out of operation” (1-39)

□

Transportation

Weight

WARNING

Risk of injury due to unsecured shelf.

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

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

Packaging

CAUTION

Adverse effect on operation due to incorrect packaging.

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

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

Climatic conditions

CAUTION

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

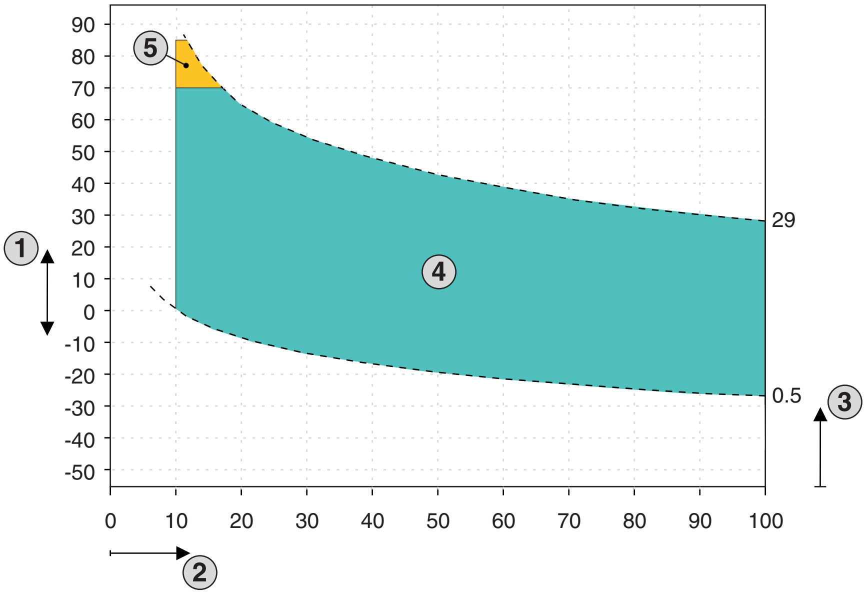
Ensure that the climatic limits for transportation and storage of LambdaUnite® MSS equipment are complied with during transportation; please refer to "Climatic limits for transportation and storage" (1-24).

Climatic limits for transportation and storage

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

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

The following climatogram visualizes these climatic limits:



Legend:

1 Air temperature in degrees Celsius [°C] or degrees Fahrenheit [°F]

2 Relative humidity [%]

3 Absolute humidity [g/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 antistatic packaging if possible. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

Packaging

⚠ **CAUTION**

Adverse effect on operation due to incorrect packaging.

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

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

Climatic conditions

⚠ **CAUTION**

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

Ensure that the climatic limits for transportation and storage of LambdaUnite® MSS equipment are complied with during storage; please refer to "Climatic limits for transportation and storage" (1-24).

□

Installation

Weight

⚠ **WARNING**

Risk of injury due to unsecured shelf.

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

At least two persons are required for lifting the shelf.

Laser warning labels

WARNING

Ineffectiveness of laser warning labels if removed or concealed.

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

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

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

Overheating

CAUTION

Risk of fire due to overheating.

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

You must therefore ensure that

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

Detector diodes

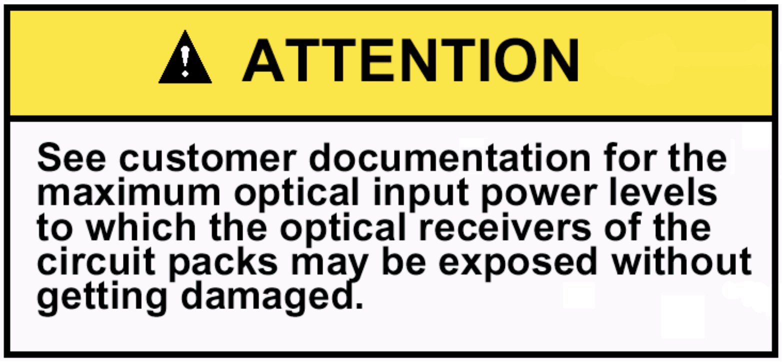
CAUTION

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

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

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

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



ATTENTION

See customer documentation for the maximum optical input power levels to which the optical receivers of the circuit packs may be exposed without getting damaged.

Receiver sensitivities

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

□

Taking into operation

Invisible laser radiation

DANGER

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

DANGER

Arcing on removing or inserting a live power supply plug.

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

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

Supply voltage

CAUTION

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

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

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

Fusing

CAUTION

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

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

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

Condensation

CAUTION

Condensation causes malfunctioning

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

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

□

Operation and maintenance

Invisible laser radiation

DANGER

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

DANGER

Arcing on removing or inserting a live power supply plug.

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

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

Laser warning labels

WARNING

Ineffectiveness of laser warning labels if removed or concealed.

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

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

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

Overheating

CAUTION

Risk of fire due to overheating.

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

You must therefore ensure that

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

Detector diodes

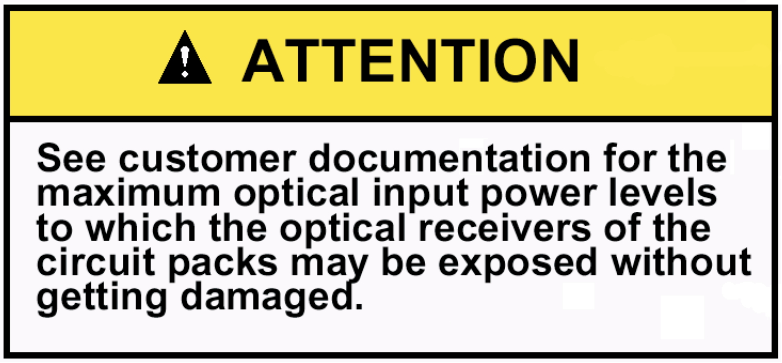
CAUTION

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

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

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

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



⚠ ATTENTION

See customer documentation for the maximum optical input power levels to which the optical receivers of the circuit packs may be exposed without getting damaged.

Receiver sensitivities

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

Short-circuit

⚠ **CAUTION**

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

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

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

Test voltage

⚠ **CAUTION**

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

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

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

Climatic conditions

⚠ **CAUTION**

Damage to system components under extreme environmental conditions.

Extreme environmental conditions can damage system components and cause malfunctioning.

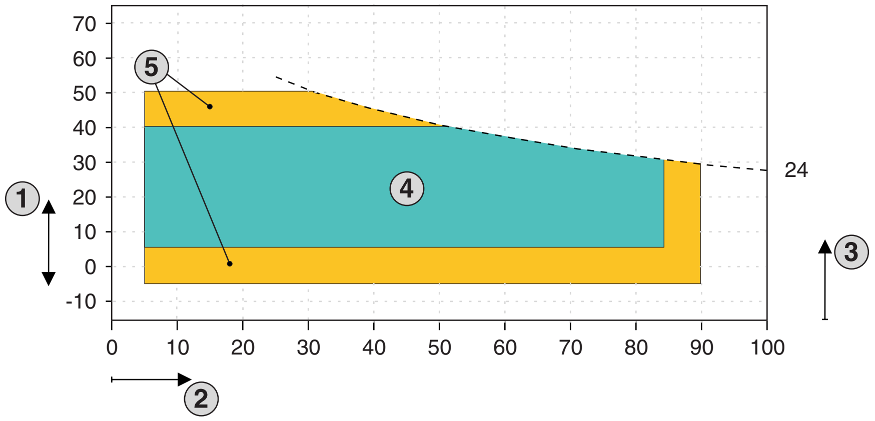
Ensure that the "Climatic limits for the operation of LambdaUnite® MSS equipment" (1-37) are complied with during operation.

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

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

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

The following climatogram visualizes these climatic limits:



Legend:

1 Air temperature in degrees Celsius [°C] or degrees Fahrenheit [°F]

2 Relative humidity [%]

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

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

5 Exceptional conditions, permissible for a short duration only.

□

Taking out of operation

Invisible laser radiation

DANGER

Injury to eyes caused by invisible laser radiation.

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

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

Arcing

DANGER

Arcing on removing or inserting a live power supply plug.

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

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

Weight

WARNING

Risk of injury due to unsecured shelf.

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

At least two persons are required for lifting the shelf.

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

Disposal

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

□

2 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" (2-9)
- "Equipment alarms" (2-21)
- "Ethernet alarms" (2-66)
- "Linear protection switching alarms" (2-80)
- "Path-related transmission alarms" (2-83)
- "Port-related transmission alarms" (2-108)
- "Ring protection switching alarms" (2-123)
- "Synchronisation alarms" (2-144)
- "Additional alarm-related information" (2-152)

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.

Defects and alarms

Please note that there is a difference between defects and alarms which is described in detail in the *LambdaUnite® MultiService Switch (MSS) User Operations Guide* in the “Alarm managment concepts” chapter.

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 *Navis™* Optical EMS **Alarm List**.

Please notice that the alarm short designations displayed when provisioning ASAPs by using the *Navis™* Optical EMS are different to those displayed in the alarm lists. For ASAP provisioning purposes the *Navis™* Optical EMS 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)
- Environment
  This alarm category is used for environmental alarms, detected by means of Miscellaneous Discrete Inputs (MDIs).
- Equipment
  This alarm category is used for hardware- and configuration-related alarms and alarms concerning the internal communication.
- Processing error
  This alarm category is used for alarms related to problems or failures of the control system software, due to overload situations for example.

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 local indications via the red “FAULT” LED on the circuit pack faceplate is ***controlled by defects***, not alarms.

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.

Related information

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.

Please note that the insertion of consequent actions, for example insertion of an Alarm Indication Signal (AIS) or a Remote Defect Indication (RDI), is ***controlled by defects***, not alarms.

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**)	ADDROV
ASAP type	Data Communications Network
Alarm category	Communication (DCN)
Alarm severity (default setting)	Major
Alarm source	DCN

Local indications

There are no specific local indications.

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 (RS/Section DCC or MS/Line DCC) provisioned for the Acknowledged Information Transfer Service (AITS).

Whether an RS/Section DCC or an MS/Line DCC is affected, can be seen from the alarm identifier (**Probable cause**).

Brief alarm overview

The following tabular overview summarizes important information concerning the `DCC MS/Line failure` alarm:

Alarm identifier (**Probable cause**)	***DCCMSF*** if an MS/Line DCC is affected, ***DCCRSF*** if an RS/Section DCC is affected.	
ASAP type	SDH/SONET ports	
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

Please refer to “Clearing DCC MS/Line failure” (3-42).

□

DCC MS/Line 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 MS/Line failure` alarm:

Alarm identifier (**Probable cause**)	DCCMSF	
ASAP type	SDH/SONET ports	
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

Please refer to “Clearing DCC MS/Line failure” (3-42).

□

DCC RS/Section 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 RS/Section failure` alarm:

Alarm identifier (**Probable cause**)	DCCRSF	
ASAP type	SDH/SONET ports	
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*.

□

DCN Provisioning Not Valid

Not supported! Although the `DCN Provisioning Not Valid` alarm is part of the "Data Communications Network" ASAP, it has no relevance for the present *LambdaUnite*® MSS release because the detection of the alarm is not supported.

□

Protocol Version Mismatch

Meaning of the alarm

The automatic exchange of link ID information between two adjacent end nodes of an enabled DCC link (RS/Section DCC or MS/Line DCC) 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.

Whether an RS/Section DCC or an MS/Line DCC is affected, can be seen from the alarm identifier (**Probable cause**).

Brief alarm overview

The following tabular overview summarizes important information concerning the `Protocol Version Mismatch` alarm:

Alarm identifier (**Probable cause**)	***LIDMSM*** if an MS/Line DCC is affected, ***LIDRSM*** if an RS/Section DCC is affected.	
ASAP type	SDH/SONET ports	
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" (2-156)).

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" (3-112).

□

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	Data Communications Network
Alarm category	Communication (DCN)
Alarm severity (default setting)	Minor
Alarm source	DCN

Local indications

There are no specific local indications.

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

□

Environmental alarms

Overview

Purpose

LambdaUnite® MSS systems feature a set of eight Miscellaneous Discrete Inputs for user-defined applications. A Miscellaneous Discrete Input can be connected to monitor a temperature probe or a fire alarm device for example. Miscellaneous Discrete Inputs can thus be used to trigger the reporting of application-specific environmental alarms.

Contents

□

Miscellaneous Discrete Input # (#=1 … 8)

Meaning of the alarm

An environmental alarm condition has been detected by an external sensor connected to the corresponding Miscellaneous Discrete Input.

Alarm message text

As the meaning of an environmental alarm depends on the specific application, the alarm message (**Environment message**) to be displayed in the *WaveStar*® CIT **NE Alarm List** is configurable. The default alarm messages are `Miscellaneous Discrete Input 1`, `Miscellaneous Discrete Input 2` … `Miscellaneous Discrete Input 8`. Please also refer to the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Miscellaneous Discrete Input` alarms:

Alarm identifier (**Probable cause**)	MISC_1, MISC_2, … , MISC_8[1]
ASAP type	Environmental (Miscellaneous Discrete)
Alarm category	Environment
Alarm severity (default setting)	Not reported (configurable individually for each of the eight environmental alarms)
Alarm source	Miscellaneous Discrete Input 1, Miscellaneous Discrete Input 2, … Miscellaneous Discrete Input 8

Notes:

1. In the *WaveStar*® CIT **NE Alarm List**, only “MISC” is displayed as the probable cause of an environmental alarm. The information, which Miscellaneous Discrete Input (MDI) has a pending alarm can be derived from the AID parameter (for example “misc_in1”).

Local indications

There are no specific local indications.

Trouble clearing

The measures to be taken to localize and clear environmental alarms depend on the specific application of the respective Miscellaneous Discrete Input.

□

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

□

Abnormal condition

Meaning of the alarm

The control system has detected manually initiated maintenance activity that could affect service or potentially mask the reporting of service affecting failures.

Abnormal conditions

These types of abnormal conditions exist:

- A forced switch is active (protection group)
- A lockout switch is active (protection group)
- The system operates in holdover mode (timing reference)
- The system operates in free-running mode (timing reference)
- A facility loopback is active (port)
- A cross-connection loopback is active (tributary)
- A test access session is active (tributary)
- The system operates in maintenance mode (system)

Brief alarm overview

The following tabular overview summarizes important information concerning the `Abnormal condition` alarm:

Alarm identifier (**Probable cause**)	ABN
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Not alarmed[1]
Alarm source	System, protection group, timing reference, port, or tributary (depending on the type of abnormal condition)

Notes:

1. Abnormal conditions are signalled by means of the event status display of the *WaveStar*® CIT.

Local indications

The yellow “ABN” LED on the user panel is lit.

Trouble clearing

The `Abnormal condition` “alarm” is to be understood as an information rather than as an alarm, and it will be cleared automatically as soon as the cause of the abnormal condition is no longer existing.

□

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 unprotected
Alarm category	Equipment
Alarm severity (default setting)	Major
Alarm source	Shelf

Local indications

There are no specific local indications.

Trouble clearing

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

□

CICTL Comm Failure

Meaning of the alarm

The `CICTL Comm Failure` alarm may have the following causes:

- The inventory EEPROM on the CI-CTL (Connection Interface of the Controller) 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 MDI/MDO status cannot be retrieved by the Controller (CTL).
  MDI/MDO status means whether an MDI or MDO port is on or off.
-

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 unprotected
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 CICTL Comm Failure” (3-6).

□

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 unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Slot

Trouble clearing

Please refer to “Clearing CICTL not Present” (3-10).

□

Circuit Pack Comm Failure

Meaning of the alarm

A protocol failure occurred in the internal data communication between a port unit, the cross-connect and timing unit (XC), 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 unprotected
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” (3-13).

□

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 a cross-connect and timing unit (XC160, XC320), 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 Protection State Dependence	
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” (3-33).

□

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, the function controller on the affected circuit pack is defective, 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 Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Slot	

Local indications

Local indications via the red "FAULT" LED of the missing circuit pack are of course not possible.

However, please be aware of the following special situations that may occur:

- In the case of a missing cross-connect and timing unit, the red "FAULT" LEDs on all circuit packs will be flashing because of a `Worker Clock Input Fail` or `Protection Clock Input Fail` ***defect*** being present. However there will be ***no*** corresponding alarm, because the `Worker Clock Input Fail` or `Protection Clock Input Fail` alarm will be suppressed due to the existence of the Circuit Pack not Present alarm of the cross-connect and timing unit. Either a Circuit Pack not Present alarm (for the cross-connect and timing unit) or no alarm at all will be reported depending on whether the missing cross-connect and timing unit remains provisioned or is deprovisioned.

- In the case of a missing port unit (OP… variants or GE1 circuit pack), the red "FAULT" LEDs on the cross-connect and timing units will be flashing due to the detected TXI Failure condition but no TXI Failure alarm will be reported because it is masked by the Circuit Pack not Present alarm (for the missing port unit).

Missing Controller

In the case of a missing Controller (CTL), no Circuit Pack not Present alarm will be reported because no autonomous alarm notification can be generated. However, the red Critical (CR) alarm LEDs on the user panel and on the rack alarm facility will be lit.

Trouble clearing

Please refer to "Clearing Circuit Pack not Present" (3-30).

□

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.

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 Protection State Dependence	
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” (3-31).

□

Comm Channel Failure

Meaning of the alarm

A protocol failure occurred in the internal data communication between one or two cross-connect and timing units and the active 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 unprotected
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” (3-34).

□

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 unprotected
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” (3-40).

□

Duplex Control not Present

Meaning of the alarm

The active Controller in a duplex control configuration cannot be protected by the standby Controller because the hardware versions of the two Controllers do not match.

A typical cause of a `Duplex Control not Present` alarm is a duplex control configuration where the active Controller is a CTL/2, and the standby Controller is a CTL/-. As the CTL/2 supports an extended functionality in comparison with the CTL/-, a CTL/2 may protect a CTL but not vice versa.

Related information

Please also refer to the equipment provisioning concepts described in the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Duplex Control not Present` alarm:

Alarm identifier (**Probable cause**)	DCTLUNAVAIL	
ASAP type	Equipment with Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
Alarm source	Slot	

Local indications

There are no specific local indications.

Trouble clearing

Please refer to “Clearing Duplex Control not Present” (3-49).

□

ECI Comm Failure

Meaning of the alarm

The ECI Comm Failure alarm may have different causes:

- The internal communication between the corresponding Electrical Connector Interface (ECI) and the Controller (CTL) is disturbed, or
- two EP155 circuit packs are present in the slots assosciated to the ECI, and the content of their EPROMs is inconsistent.

Brief alarm overview

The following tabular overview summarizes important information concerning the ECI Comm Failure alarm:

Alarm identifier (**Probable cause**)	ECICOMF
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	ECI slot

Local indications

There are no specific local indications.

Trouble clearing

Please refer to “Clearing ECI Comm Failure” (3-53).

□

ECI Mismatch Failure

Meaning of the alarm

The type of Electrical Connector Interface (ECI) used is not suitable for the current configuration.

Related information

Please also refer to the equipment provisioning concepts described in the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	ECIMISMA
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	ECI slot

Local indications

There are no specific local indications.

Trouble clearing

Please refer to “Clearing ECI Mismatch Failure” (3-57).

□

ECI not Present

Meaning of the alarm

The corresponding Electrical Connector Interface (ECI) is missing.

Brief alarm overview

The following tabular overview summarizes important information concerning the `ECI not Present` alarm:

Alarm identifier (**Probable cause**)	ECIMISS
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	ECI slot

Local indications

There are no specific local indications.

Trouble clearing

Please refer to “Clearing ECI not Present” (3-60).

□

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 unprotected
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” (3-61).

□

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 unprotected
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” (3-64).

□

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 unprotected
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” (3-68).

□

Fan Unit not Present

Meaning of the alarm

The fan unit is not installed in the shelf.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Fan Unit not Present` alarm:

Alarm identifier (**Probable cause**)	FANUNITMISS
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	Shelf

Trouble clearing

Important! A `Fan Unit not Present` **alarm should be cleared as soon as possible.**

Please refer to “Clearing Fan Unit not Present” (3-72).

□

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 unprotected
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/B Failure” (3-74).

□

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 unprotected
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/B Failure” (3-74).

□

IDE Flash Card Access Fail

Meaning of the alarm

Reading or writing from/to the system's non-volatile memory (NVM, *CompactFlash*™ card with IDE interface) is not possible.

Brief alarm overview

The following tabular overview summarizes important information concerning the `IDE Flash Card Access Fail` alarm:

Alarm identifier (**Probable cause**)	BKUPMEMP
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Major
Alarm source	Controller (CTL)

Local indications

The red "FAULT" LED on the faceplate of the Controller (CTL) is 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

□

ONI Failure on protecting CTL

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.

The actual alarm text displayed in the *WaveStar*® CIT **NE Alarm List** is: `{circuit pack name}/{circuit pack qualifier},ONI Failure on protecting CTL`. The alarm has been detected by the standby Controller (protecting CTL), and is reported for the circuit pack indicated in the alarm message ("{circuit pack name}/{circuit pack qualifier}").

Brief alarm overview

The following tabular overview summarizes important information concerning the `ONI Failure on protecting CTL` alarm:

Alarm identifier (**Probable cause**)	ONIFP	
ASAP type	Equipment unprotected	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Minor
	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

Please refer to "Clearing ONI Failure on protecting CTL" (3-99).

□

ONI Failure on working CTL

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.

The actual alarm text displayed in the *WaveStar*® CIT **NE Alarm List** is: `{circuit pack name}/{circuit pack qualifier},ONI Failure on working CTL`. The alarm has been detected by the active Controller (working CTL), and is reported for the circuit pack indicated in the alarm message.

Brief alarm overview

The following tabular overview summarizes important information concerning the `ONI Failure on working CTL` alarm:

<table>
<tr><td>Alarm identifier
(<b>Probable cause</b>)</td><td colspan="2">ONIFW</td></tr>
<tr><td>ASAP type</td><td colspan="2">Equipment unprotected</td></tr>
<tr><td>Alarm category</td><td colspan="2">Equipment</td></tr>
<tr><td rowspan="3">Alarm severity
(default setting)</td><td colspan="2">Depending on the affect-on-service attribute:</td></tr>
<tr><td>SA</td><td>Minor</td></tr>
<tr><td>NSA</td><td>Minor</td></tr>
<tr><td>Alarm source</td><td colspan="2">Circuit pack</td></tr>
</table>

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 on working CTL” (3-102).

□

Power Interface not Present

Meaning of the alarm

The Power Interface (PI) is not installed.

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 Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Power Interface (PI A, PI B)	

Trouble clearing

Please refer to “Clearing Power Interface not Present” (3-106).

□

Power Interface Read Failure

Meaning of the alarm

The inventory EEPROM on the affected Power Interface (PI A or PI B) 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.

Please note that the presence and the absence (after trouble clearing) of the `Power Interface Read Failure` alarm can only be detected if the inventory EEPROM is accessed (for example by manually retrieving the equipment parameters of a Power Interface).

Brief alarm overview

The following tabular overview summarizes important information concerning the `Power Interface Read Failure` alarm:

Alarm identifier (**Probable cause**)	PIEF	
ASAP type	Equipment with Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Power Interface (PI A, PI B)	

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

□

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 Power Interface AID (“1-1-pia” or “1-1-pib”) indicated in the **AID** column of the *WaveStar*® CIT **NE Alarm List**, or from the green “PWR ON” LED on the respective Power Interface PI A or PI 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 Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Power Interface (PI A, PI B)	

Trouble clearing

Please refer to “Clearing System Power Failure” (3-121).

□

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 unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Circuit pack

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

□

TI not Present

Meaning of the alarm

The respective Timing Interface (TI) is not installed.

Brief alarm overview

The following tabular overview summarizes important information concerning the `TI not Present` alarm:

Alarm identifier (**Probable cause**)	TIMISS
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Timing Interface (TI)

Trouble clearing

Please refer to “Clearing TI not Present” (3-129).

□

TXI Failure

Meaning of the alarm

Frame alignment has been lost for the TXI bus line “n” as indicated by the alarm identifier (**Probable cause**).

The `TXI Failure` alarm is reported by the circuit pack receiving a signal on the corresponding TXI bus line.

Please also refer to “TXI bus line numbering scheme” (2-54).

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 Protection State Dependence	
Alarm category	Equipment	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Critical
	NSA	Minor
Alarm source	Circuit pack	

Local indications

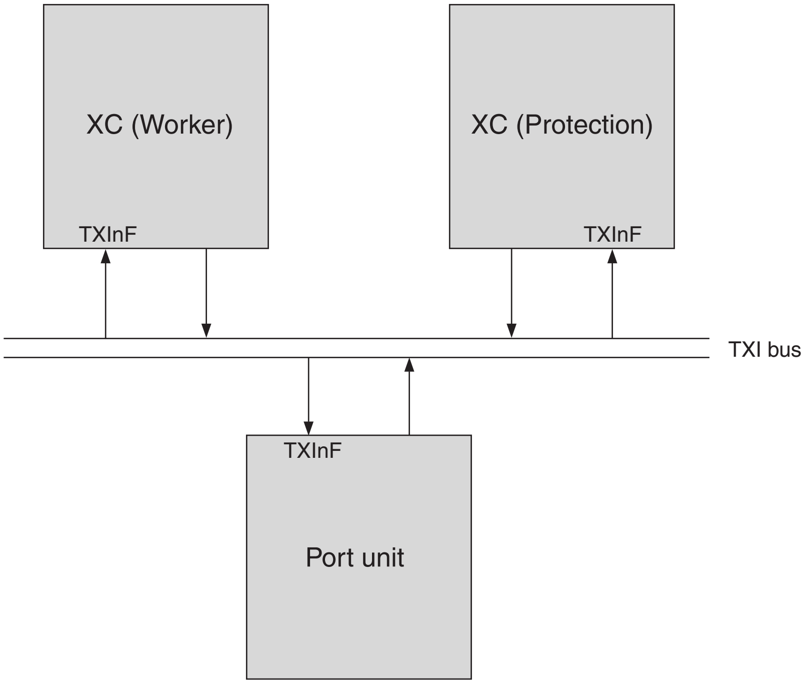
The red “FAULT” LED on the faceplate of the respective circuit pack is flashing (provided that no equipment alarm is present at the same time which would cause the red “FAULT” LED to be constantly lit).

Trouble clearing

Please refer to “Clearing TXI Failure” (3-130).

TXI bus line numbering scheme

The TXI bus interconnects port units and cross-connect and timing units (XCs) for the purpose of NE-internal distribution of transport signals. Each TXI bus line provides a transmission capacity of 2.5 Gbit/s.



A distinction has to be made between different types of circuit packs:

- Single-slot port units (port units other than OP40) with a further distinction concerning the transmission capacity per slot
- Multi-slot port units (OP40 port units, occupying 4 universal slots)
- Cross-connect and timing units (XC, in the worker and protection slot)

Single-slot port units

The TXI bus line numbering of single-slot port units with a transmission capacity of 20-Gbit/s (e.g. OP2G5D/PAR8) and the numbering of single-slot port units with a transmission capacity of 10-Gbit/s, having a 20-Gbit/s equivalent (e.g. OP2G5/1.3SR4) is different from other port units with a transmission capacity of 10-Gbit/s and no 20-Gbit/s equivalent.

In the receive direction (from the view point of a single-slot port unit), the association between the XCs and the port units in the universal slots of a *LambdaUnite*® MSS shelf is as follows (the TXI bus line numbering is independent from the slot number where the port unit is installed):

Alarm reporting circuit pack (receiver): a single-slot port unit in a universal slot **Sender: XC in the worker or protection slot as indicated below (depending on the TXI bus line and the port unit type)**		
Port unit type	**TXI bus line**	**Cross-connect and timing unit**
10-Gbit/s transmission capacity per slot, ***no*** 20-Gbit/s equivalent	1	XC in the worker slot (slot 9); identical to releases prior to release 4.0
	2	
	3	
	4	
	9	XC in the protection slot (slot 10); identical to releases prior to release 4.0
	10	
	11	
	12	
10-Gbit/s transmission capacity per slot, ***with*** 20-Gbit/s equivalent (e.g. OP2G5)	5	XC in the worker slot (slot 9)
	6	
	7	
	8	
	13	XC in the protection slot (slot 10)
	14	
	15	
	16	

Alarm reporting circuit pack (receiver): a single-slot port unit in a universal slot **Sender: XC in the worker or protection slot as indicated below (depending on the TXI bus line and the port unit type)**		
Port unit type	**TXI bus line**	**Cross-connect and timing unit**
20-Gbit/s transmission capacity (e.g. OP2G5D)	1	XC in the worker slot (slot 9)
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	XC in the protection slot (slot 10)
	10	
	11	
	12	
	13	
	14	
	15	
	16	

If, for example, a `TXI Failure` alarm (TXI9F) is reported by a single-slot port unit in a universal slot, then the TXI signal originates from the XC in the protection slot.

Multi-slot port units

In the receive direction (from the view point of an OP40), the association between the XCs and the OP40s in the universal slots of a

LambdaUnite® MSS shelf is as follows (the TXI bus line numbering is independent from the slot quadruple where the OP40 is installed):

Alarm reporting circuit pack (receiver): OP40 **Sender: XC in the worker or protection slot as indicated below (depending on the TXI bus line)**		
TXI bus line	**Cross-connect and timing unit**	**TXI bus line**
1	XC in the worker slot	17
2		18
3		19
4		20
5		21
6		22
7		23
8		24
9	XC in the protection slot	25
10		26
11		27
12		28
13		29
14		30
15		31
16		32

If, for example, a `TXI Failure` alarm (TXI19F) is reported by an OP40 port unit, then the TXI signal originates from the XC in the worker slot.

Cross-connect and timing units

In the receive direction (from the view point of an XC160 or XC320 cross-connect and timing unit), the association between the port units in the universal slots of a *LambdaUnite*® MSS shelf and the XCs is as follows (there is no difference in the TXI bus line numbering between the XC in the worker and protection slot):

Alarm reporting circuit pack (receiver): XC (in the worker or protection slot)
Sender: port unit in universal slot as indicated below (depending on the TXI bus line)

TXI bus line	Universal slot	TXI bus line	Universal slot	TXI bus line	Universal slot	TXI bus line	Universal slot
1[1, 2]	1	65[1, 2]	12	129[1, 2]	21	193[1, 2]	32
2[1, 2]		66[1, 2]		130[1, 2]		194[1, 2]	
3[1, 2]		67[1, 2]		131[1, 2]		195[1, 2]	
4[1, 2]		68[1, 2]		132[1, 2]		196[1, 2]	
5[1]		69[1]		133		197	
6[1]		70[1]		134		198	
7[1]		71[1]		135		199	
8[1]		72[1]		136		200	
9[1]	2	73[1]	13	137	22	201	33
10[1]		74[1]		138		202	
11[1]		75[1]		139		203	
12[1]		76[1]		140		204	
13[1]		77[1]		141		205	
14[1]		78[1]		142		206	
15[1]		79[1]		143		207	
16[1]		80[1]		144		208	
17[1, 2]	3	81[1, 2]	14	145[1, 2]	23	209[1, 2]	34
18[1, 2]		82[1, 2]		146[1, 2]		210[1, 2]	
19[1, 2]		83[1, 2]		147[1, 2]		211[1, 2]	
20[1, 2]		84[1, 2]		148[1, 2]		212[1, 2]	
21[1]		85[1]		149		213	
22[1]		86[1]		150		214	
23[1]		87[1]		151		215	
24[1]		88[1]		152		216	

Alarm reporting circuit pack (receiver): XC (in the worker or protection slot) **Sender: port unit in universal slot as indicated below (depending on the TXI bus line)**							
TXI bus line	**Universal slot**	**TXI bus line**	**Universal slot**	**TXI bus line**	**Universal slot**	**TXI bus line**	**Universal slot**
25[1]	4	89[1]	15	153	24	217	35
26[1]		90[1]		154		218	
27[1]		91[1]		155		219	
28[1]		92[1]		156		220	
29[1]		93[1]		157		221	
30[1]		94[1]		158		222	
31[1]		95[1]		159		223	
32[1]		96[1]		160		224	
33[1, 2]	5	97[1, 2]	16	161[1, 2]	25	225[1, 2]	36
34[1, 2]		98[1, 2]		162[1, 2]		226[1, 2]	
35[1, 2]		99[1, 2]		163[1, 2]		227[1, 2]	
36[1, 2]		100[1, 2]		164[1, 2]		228[1, 2]	
37[1]		101[1]		165		229	
38[1]		102[1]		166		230	
39[1]		103[1]		167		231	
40[1]		104[1]		168		232	
41[1]	6	105[1]	17	169	26	233	37
42[1]		106[1]		170		234	
43[1]		107[1]		171		235	
44[1]		108[1]		172		236	
45[1]		109[1]		173		237	
46[1]		110[1]		174		238	
47[1]		111[1]		175		239	
48[1]		112[1]		176		240	

Alarm reporting circuit pack (receiver): XC (in the worker or protection slot)
Sender: port unit in universal slot as indicated below (depending on the TXI bus line)

TXI bus line	Universal slot	TXI bus line	Universal slot	TXI bus line	Universal slot	TXI bus line	Universal slot
49[1, 2]	7	113[1, 2]	18	177[1, 2]	27	241[1, 2]	38
50[1, 2]		114[1, 2]		178[1, 2]		242[1, 2]	
51[1, 2]		115[1, 2]		179[1, 2]		243[1, 2]	
52[1, 2]		116[1, 2]		180[1, 2]		244[1, 2]	
53[1]		117[1]		181		245	
54[1]		118[1]		182		246	
55[1]		119[1]		183		247	
56[1]		120[1]		184		248	
57[1]	8	121[1]	19	185	28	249	39
58[1]		122[1]		186		250	
59[1]		123[1]		187		251	
60[1]		124[1]		188		252	
61[1]		125[1]		189		253	
62[1]		126[1]		190		254	
63[1]		127[1]		191		255	
64[1]		128[1]		192		256	

Notes:

1. These TXI bus lines are ***not*** applicable to the XC160 cross-connect and timing unit (as port units can only be equipped in the upper row of the DUR shelf in a configuration with XC160, i.e. in the universal slots 21 … 28 and 32 … 39). These TXI bus lines are applicable to the XC320 cross-connect and timing unit, or prepared for a future extension of the cross-connect capacity.
2. These TXI bus lines are ***not*** applicable to the XC320 cross-connect and timing unit. These TXI bus lines are prepared for a future extension of the cross-connect capacity.

If, for example, a `TXI Failure` alarm (TXI***181***F) is reported by an XC, then the TXI signal originates from the port unit installed in slot 27 (this can also be an OP40 installed in slots 25, 26, 27 and 28).

□

Unit Cooling Degraded

Meaning of the alarm

The operating temperature of the circuit pack reporting the alarm has exceeded a predefined limit.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	CPDEGR
ASAP type	Equipment unprotected
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

> **Important!** A `Unit Cooling Degraded` **alarm is the predecessor of a more severe alarm condition** (`Unit Temperature too High`)**. Therefore, it is recommended to immediately react on a** `Unit Cooling Degraded` **alarm in order to prevent a more severe situation.**

Please refer to “Clearing Unit Cooling Degraded” (3-133).

□

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 Protection State Dependence	
Alarm category	Equipment	
Alarm severity[1] (default setting)	Depending on the affect-on-service attribute:	
	SA	Major
	NSA	Minor
Alarm source	Circuit pack	

Notes:

1. For unprotected and MS-layer protected applications the `Unit Temperature too High` alarm will always be reported "non-service affecting" (NSA) and "Minor". The service state calculation will never lead to "service affecting" (SA) and "Major". In a 1+1 equipment protection application, the service state calculation is done correctly.

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" (3-135).

□

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 unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	User panel

Trouble clearing

Please refer to “Clearing User Panel Comm Failure” (3-138).

□

User Panel not Present

Meaning of the alarm

The user panel is not installed.

Brief alarm overview

The following tabular overview summarizes important information concerning the `User Panel not Present` alarm:

Alarm identifier (**Probable cause**)	UPMISS
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Minor
Alarm source	Shelf

Trouble clearing

Please refer to “Clearing User Panel not Present” (3-143).

□

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 Auto Negotiation Mismatch

Meaning of the alarm

The priority resolution mechanism precluded operation between the two end nodes of an Ethernet link because there is no common mode of operation. For example, one end node is configured to operate in full duplex mode whereas the other end node is configured to operate in half duplex mode.

Brief alarm overview

The following tabular overview summarizes important information concerning the `LAN Auto Negotiation Mismatch` alarm:

Alarm identifier (**Probable cause**)	LANANM	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Minor
	NSA	Not alarmed
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).

Auto negotiation

Auto negotiation means that both end nodes of an Ethernet link exchange information among each other concerning their possible modes of operation. If a common mode of operation exists then the mode with the highest priority acc. to the priority resolution mechanism will be selected.

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

□

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

□

max number of VLAN instances reached

Meaning of the alarm

The GARP VLAN Registration Protocol (GVRP) is enabled, and the maximum number of VLAN connections per virtual switch has been exceeded.

Maximum number of VLAN connections

Up to 64 VLAN connections can exist per virtual switch when the GARP VLAN Registration Protocol (GVRP) is enabled in the IEEE 802.1D compliant multipoint MAC bridge mode of the Gigabit Ethernet circuit pack.

Brief alarm overview

The following tabular overview summarizes important information concerning the `max number of VLAN instances reached` alarm:

Alarm identifier (**Probable cause**)	MACVLANOVFW	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Minor
	NSA	Not reported
Alarm source	Ethernet 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

□

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

□

Server Signal Fail (VCGSSF)

Meaning of the alarm

The entire payload signal transported in the affected Virtual Concatenated Group (VCG) is unusable and has been replaced by AIS (all-ones signal) due to a failure that occurred in this NE or in the upstream direction.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	VCGSSF	
ASAP type	Ethernet	
Alarm category	Communication (Transport)	
Alarm severity (default setting)	Depending on the affect-on-service attribute:	
	SA	Not reported
	NSA	Not reported
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

□

Sink End Failure of Protocol

Meaning of the alarm

A protocol failure occurred in the receive direction in the Link Capacity Adjustment Scheme (LCAS) protocol.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Sink End Failure of Protocol` alarm:

Alarm identifier (**Probable cause**)	VCGFOPR	
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

□

Source End Failure of Protocol

Meaning of the alarm

A protocol failure occurred in the transmit direction in the Link Capacity Adjustment Scheme (LCAS) protocol.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Source End Failure of Protocol` alarm:

Alarm identifier (**Probable cause**)	VCGFOPT	
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

□

primary section Mismatch

Meaning of the alarm

This alarm only applies to the optimized 1+1 MSP protocol.

The primary section indication in the received K2 byte (K2 [1-4]) does not match the expected value.

Brief alarm overview

The following tabular overview summarizes important information concerning the `primary section Mismatch` alarm:

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

Local indications

There are no specific local indications.

Trouble clearing

Please refer to .

□

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” (3-109).

□

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	Path MSA/NIM related	
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.

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	Path MSA/NIM related	
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	Path MSA/NIM related	
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 Termination	
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	Path MSA/NIM related	
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	Sub-Network Connection Protection and Unidirectional Path Switched Ring
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 indicates the number of defects in the payload.

Please notice that the detection of this alarm is supported for both SONET ***and*** SDH signals, although not requested by the standards for SDH signals.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	PDI-P	
ASAP type	Path MSA/NIM related	
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 Termination	
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	Path MSA/NIM related	
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)” (3-115).

□

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 Termination	
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	Path MSA/NIM related	
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:

<table>
<tr><td>Alarm identifier
(<b>Probable cause</b>)</td><td colspan="2">SRM-P</td></tr>
<tr><td>ASAP type</td><td colspan="2">Path MSA/NIM related</td></tr>
<tr><td>Alarm category</td><td colspan="2">Communication (Transport)</td></tr>
<tr><td rowspan="3">Alarm severity
(default setting)</td><td colspan="2">Depending on the affect-on-service attribute:</td></tr>
<tr><td>SA</td><td>Major</td></tr>
<tr><td>NSA</td><td>Minor</td></tr>
<tr><td>Alarm source</td><td colspan="2">Non-intrusively monitored path</td></tr>
</table>

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	Path MSA/NIM related	
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*.

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	Path MSA/NIM related	
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

□

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	SDH/SONET ports	
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	SDH/SONET ports	
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	SDH/SONET ports	
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	SDH/SONET ports	
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).

Possible causes

A `Loss of Frame` alarm may have the following causes:

- The receive signal does not match the port rate (due to a misconnected fiber for example). For example, an OC-12 signal is received at an OC-48/STM-16 port.
- The Section Overhead (SOH) of the SDH or SONET receive signal is not correctly structured (due to a failure of the transmit circuit pack at the far end).
- At the far end, the Optical Channel (OCh) is enabled while it is disabled at the port for which the alarm is reported.
- The receiver at the circuit pack reporting the alarm is defective.

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

Please refer to “Clearing Loss of Frame” (3-92).

□

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.

When gradually decreasing the optical input power below the receiver sensitivity limit, it might happen that first a `Loss of Frame` will be reported and at an even lower level a `Loss of Signal`.

For passive WDM and DWDM interfaces, in incidental cases when the actual receiver sensitivity is better than required, it may happen that when gradually increasing the attenuation, a `Loss of Signal` alarm is reported while no `Degraded Signal` (MSDEG) and/or `Excessive Bit Error Ratio` (MSEXC) alarm is reported first. This additionally depends on the actual threshold setting for MSDEG (10^{-9} … 10^{-5}) and MSEXC (10^{-5} … 10^{-3}).

Brief alarm overview

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

Alarm identifier (**Probable cause**)	LOS	
ASAP type	SDH/SONET ports	
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	SDH/SONET ports	
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	SDH/SONET ports	
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)” (3-114).

□

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	SDH/SONET ports	
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	SDH/SONET ports	
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.

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 bytes) have equal values.

Furthermore, the `Default K-bytes` alarm will be reported if the worker and protection port in a 4-fiber BLSR/MS-SPRing configuration are interchanged.

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	MS-SPRing and Bilateral Switched Ring 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” (3-44).

□

Duplicate Ring Node

Meaning of the alarm

The `Duplicate Ring Node` alarm is reported by all the nodes of a ring if one of the following erroneous BLSR/MS-SPRing configurations has been detected:

- There are more than 16 nodes on the ring.
- There are multiple ring nodes from the same *LambdaUnite*® MSS NE on the ring.
- There are multiple network elements with the same NE name (TID) on the ring.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	DUPL-RNG
ASAP type	MS-SPRing and Bilateral Switched Ring 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.

Related information

Please also refer to “Automatic node ID allocation” (2-160).

Trouble clearing

Please refer to “Clearing Duplicate Ring Node” (3-50).

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

□

Extra Traffic Preempted

Meaning of the alarm

Any extra traffic in the ring has been preempted (replaced by AIS) due to a ring protection switch.

The `Extra Traffic Preempted` "alarm" is to be understood as an information rather than as an alarm.

Extra traffic

When the protection channels are not being used to restore working channels, they can be used to carry additional working traffic. This additional traffic, referred to as "extra traffic", has lower priority than the traffic on the working channels. In the event of a ring protection switch, the traffic on the working channels will access the protection channels causing any extra traffic to be preempted, or removed, from the protection channels. When the failure that caused the protection switch has been cleared, the extra traffic will be restored.

Brief alarm overview

The following tabular overview summarizes important information concerning the `Extra Traffic Preempted` alarm:

Alarm identifier (**Probable cause**)	ET-PREEMPT
ASAP type	MS-SPRing and Bilateral Switched Ring 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.

□

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	MS-SPRing and Bilateral Switched Ring 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" (3-80).

□

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	MS-SPRing and Bilateral Switched Ring 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" (3-85).

□

Inconsistent Ring Protection Mode

Meaning of the alarm

The ring protection mode (**Ring Loopback**, **Shortened Path**) is not consistently provisioned for all nodes on the ring.

The `Inconsistent Ring Protection Mode` alarm is only applicable to 4-fiber MS-SPRing configurations.

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	MS-SPRing and Bilateral Switched Ring Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	4-fiber 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 an `Inconsistent Ring Protection Mode` alarm is present. 4-fiber MS-SPRing protection switching is not possible.

Trouble clearing

Please refer to “Clearing Inconsistent Ring Protection Mode” (3-90).

□

Local Squelch Map Conflict

Meaning of the alarm

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

When a bidirectional (2-way) BLSR/MS-SPRing add, drop or through cross-connection has been established with an unknown NE name (TID) for the source node (A-node) and/or destination node (Z-node), then the `Local Squelch Map Conflict` alarm is reported.

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	MS-SPRing and Bilateral Switched Ring Protection Switch
Alarm category	Communication (Transport)
Alarm severity (default setting)	Major
Alarm source	2-fiber or 4-fiber BLSR/MS-SPRing protection group

Local indications

There are no specific local indications.

Related information

Please also 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

Please refer to “Clearing Local Squelch Map Conflict” (3-91).

□

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	MS-SPRing and Bilateral Switched Ring 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	MS-SPRing and Bilateral Switched Ring 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	MS-SPRing and Bilateral Switched Ring 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” (2-156).

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” (3-116).

□

Ring Incomplete

Meaning of the alarm

A Ring Incomplete alarm is reported if no correct ring topology can be discovered, or if the ring discovery algorithm times out.

Incomplete ring discovery in fibre cut scenario

If a 2-fiber BLSR/MS-SPRing node is in a ring switching state due to a fiber cut and a ring map re-discovery is triggered, it might not complete. In this case the alarm Ring Incomplete is raised. The critical scenario is that the ring map re-discovery is triggered by a DCF (Data Communication Controller Function) or CTL (System Controller) reboot/power on. Nevertheless protection switching is not suspended in this case. The problem does not apply for a ring map re-discovery triggered by a pass-through node.

Try to avoid DCF and CTL reboots if there is a Signal Fail (SF) condition for the ring nodes of the affected NE.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	RNG-INC
ASAP type	MS-SPRing and Bilateral Switched Ring 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” (2-156).

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	MS-SPRing and Bilateral Switched Ring 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" (3-118).

□

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	MS-SPRing and Bilateral Switched Ring 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

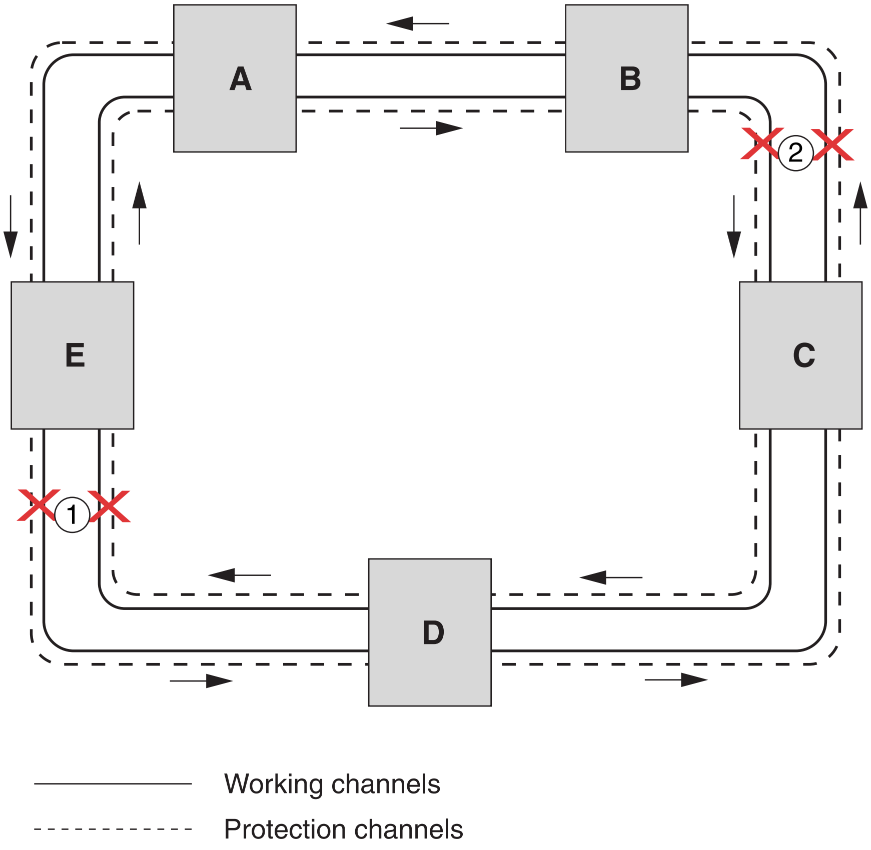
Squelching means replacing a potentially misconnected signal by an all-ones signal (Alarm Indication Signal, AIS). In the case of a *LambdaUnite*® MSS system, the traffic that cannot be protected will be squelched by replacing the payload signal with AIS (all-ones signal).

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.



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

□

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	MS-SPRing and Bilateral Switched Ring 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" (2-161).

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 network element, an `NE Clock Failure` alarm (cf. “NE Clock Failure” (2-147)) will be reported for the complete system instead of a separate `Circuit Pack Clock Failure` alarm for each circuit pack.

Note

In the case of an XC circuit pack, a `Circuit Pack Clock Failure` condition causes a `Circuit Pack Failure` alarm.

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 Protection State Dependence	
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” (3-11).

□

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” (3-96).

□

NE Clock Failure

Meaning of the alarm

A `Circuit Pack Clock Failure` condition is present for ***all*** circuit packs of the network element.

Note

In the case of an XC circuit pack, a `Circuit Pack Clock Failure` condition causes a `Circuit Pack Failure` alarm.

Brief alarm overview

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

Alarm identifier (**Probable cause**)	SYNCCLK
ASAP type	Equipment unprotected
Alarm category	Equipment
Alarm severity (default setting)	Critical
Alarm source	System

Local indications

The red “FAULT” LED on the faceplate of the cross-connect and timing unit(s) is constantly lit.

Trouble clearing

Please refer to “Clearing NE Clock Failure” (3-98).

□

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 unprotected
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) is supplied with a working and a protection timing reference from the system timing function (located on the working or protection cross-connect and timing unit, 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” (3-110).

□

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” (3-124).

□

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” (3-126).

□

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 unprotected
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 cross-connect and timing unit, 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” (3-144).

□

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. “Maximum number of ring nodes” (2-160)).

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.

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. Please refer to “Automatic node ID allocation” (2-160) for further details.

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" (2-156).

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" (2-156).

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

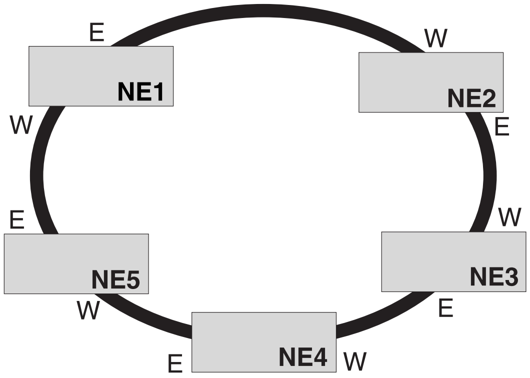
Introduction

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.

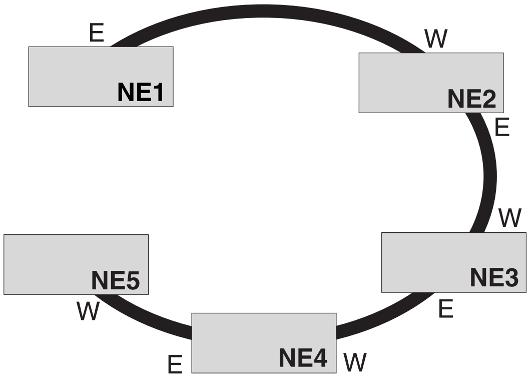
Example of a closed ring:



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" (2-160)).
- The interface port identification and the east/west (E/W) directionality information of the link to its neighbour.

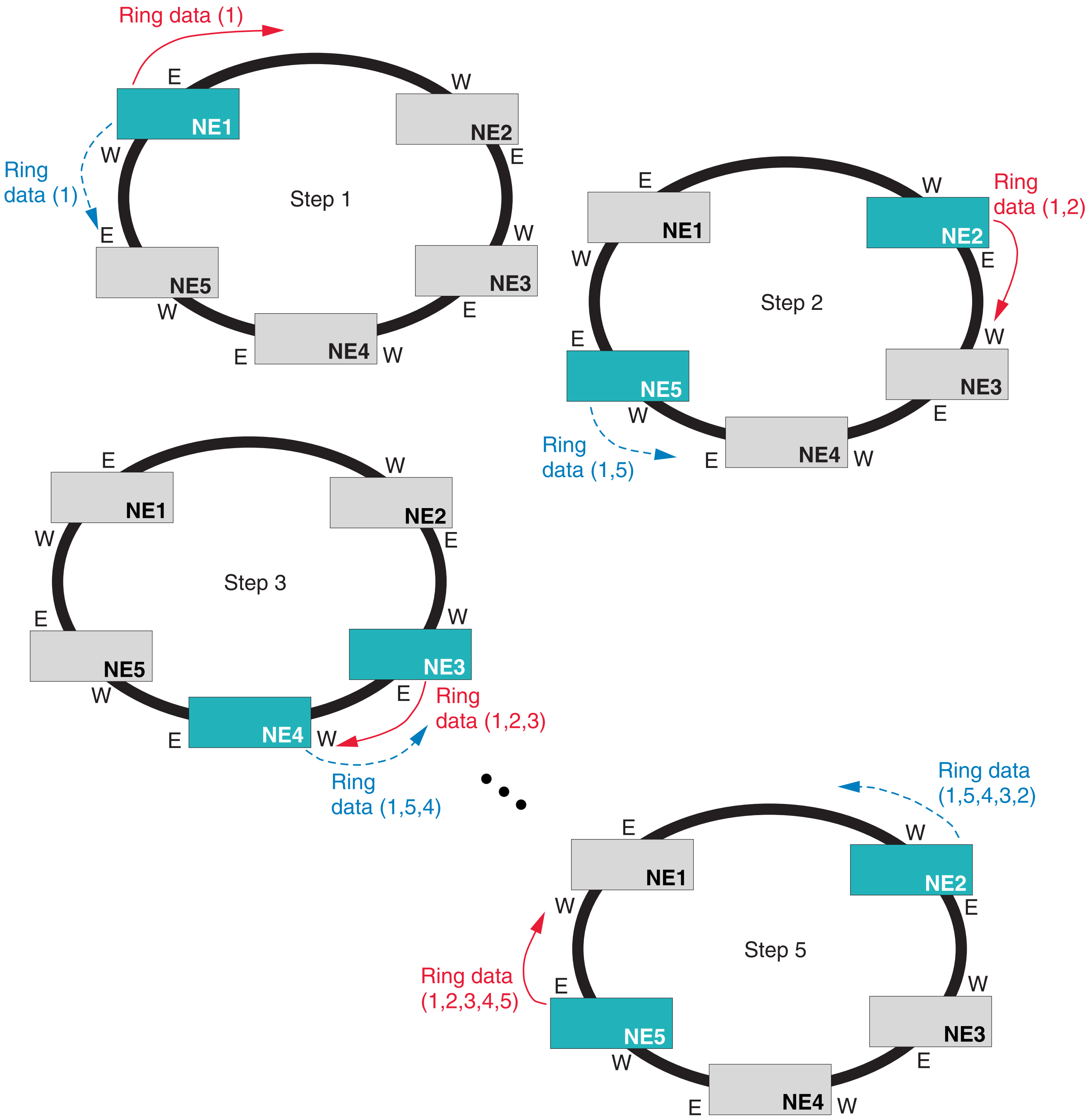
This way, at each ring node sufficient information is available to form a ring map representing the ring topology.

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" (2-156)), 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:
  - FT-2000 OC-48 Lightwave System – Add/Drop Ring Terminal,
  - *Metropolis*® DMX Access Multiplexer,
  - *WaveStar*® ADM 16/1,
  - *WaveStar*® BandWidth Manager,
  - *WaveStar*® TDM 2.5G (OC-48 2F),
  - *WaveStar*® TDM 10G (OC-192 2F),
  - *WaveStar*® TDM 10G (OC-192 4F),
  - *WaveStar*® TDM 10G (STM-64),
  - *LambdaUnite*® MultiService Switch (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), *Metropolis*® DMX Access Multiplexer 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).

□

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)" (2-109).

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.

END OF STEPS

□

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)" (2-84).

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.

END OF STEPS

□

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" (2-26).

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 Step 4.
any of the connectors (at the CI-CTL or at the fan unit) is not properly connected	proceed with the next step.

2 Complete these steps to connect the respective connector(s) properly:

1. Slightly pull out the Controller (CTL).
2. Connect the connector(s) properly.
3. Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

5 Replace the fan unit control cable, and connect the new cable properly at the CI-CTL and at the fan unit.

6 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

9 Disconnect the fan unit control cable at the CI-CTL.

10 Replace the CI-CTL.

11 Connect the fan unit control cable at the CI-CTL.

12 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

15 Replace the fan unit.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)

16 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

17 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 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" (2-27).

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)" (4-53)
the CI-CTL is not plugged	insert the CI-CTL.

END OF STEPS

□

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" (2-145).

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 cross-connect and timing 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" (4-50)

If …	**then …**
the alarm is reported by several circuit packs	replace the cross-connect and timing unit (replacing the standby circuit pack is sufficient). **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-50)

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

□

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" (2-28).

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
- Eventually, a replacement circuit pack may be required.
  This may be either a Controller (CTL/-, CTL/2), a port unit (OP…, EP155, or GE1), or one or two cross-connect and timing units (XC160, XC320).

Distinction between simplex control and duplex control mode

The appropriate trouble clearing procedure depends on the network element's control system configuration, i.e. whether CTL equipment protection is provisioned (duplex control mode) or not (simplex control mode). Depending on the control mode, please refer to:

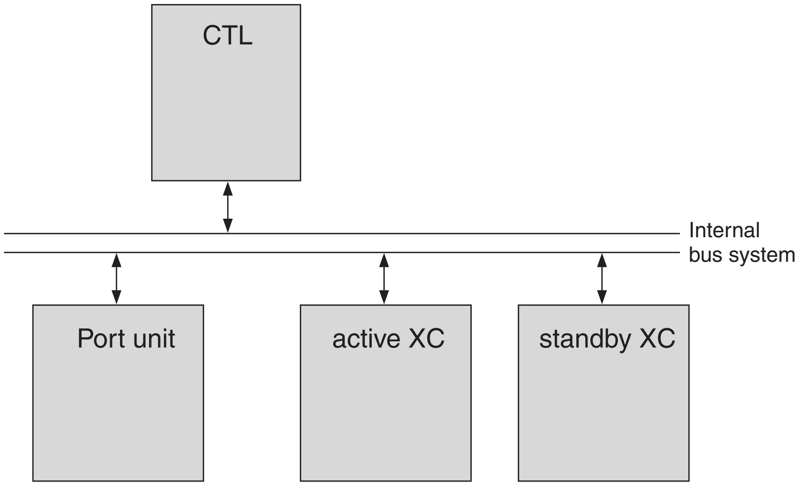
- "Trouble clearing procedure in simplex control mode" (3-14)
- "Trouble clearing procedure in duplex control mode" (3-19)

  Important! Please read the appropriate trouble clearing procedure ***completely*** before you begin.

Trouble clearing procedure in simplex control mode

Proceed as follows to clear a `Circuit Pack Comm Failure` alarm:

1 Refer to the following figure for reference:



Legend:

CTL	The Controller.
Port unit, active XC, standby XC	The circuit pack reporting the `Circuit Pack Comm Failure` alarm. This may be either a port unit (OP…, EP155, or GE1) or the active or standby cross-connect and timing unit (XC160, XC320).

2 Take a note which cross-connect and timing unit (XC) is currently the active unit, and which is standby.

3 Perform a full reset of the CTL.

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" (4-68)

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 Depending on the circuit pack reporting the alarm:

If ...	**then ...**
the alarm is reported by the active XC	proceed with the next step.
the alarm is reported by the standby XC	proceed with Step 7.
the alarm is reported by a port unit	proceed with Step 9.

6 Perform a manual protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

7 Replace the XC reporting the alarm.

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 Step 21.

9 Perform a full reset of the standby XC.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

10 Perform a manual protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

11 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

Independent from whether the alarm has cleared or not, proceed with the next step.

12 Perform a full reset of the standby XC (this is ***not*** the same XC as in Step 9!).

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

13 Perform a manual equipment protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

14 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared in Step 11, and is still cleared	Stop! You have completed this procedure.
the alarm had cleared in Step 11, and now is reported again	replace the XC which initially was the active unit (cf. Step 2). Stop! You have completed this procedure.
the alarm continued to persist in Step 11, and now has cleared	replace the XC which initially was the standby unit (cf. Step 2). Stop! You have completed this procedure.
the alarm continued to persist in Step 11, and still persists	proceed with the next step.

15 Perform a controller reset of the port unit reporting the alarm.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

16 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.

Important! A full reset of a port unit is traffic affecting!

17 Perform a full reset of the port unit reporting the alarm.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

18 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.

19 Replace the port unit reporting the alarm.

20 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.

21 Replace the Controller (CTL).

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-53)

22 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.

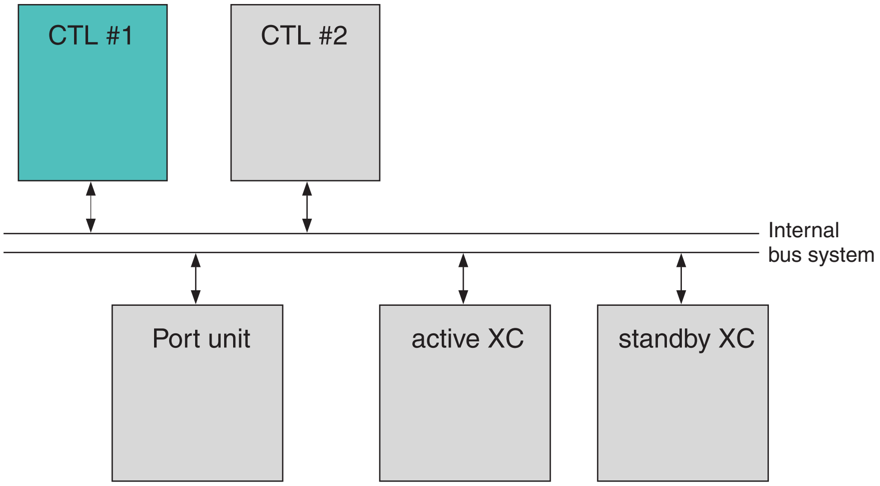
If …	then …
the alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies Service Hotline. You can reach the Lucent Technologies Service Hotline by phone, fax or e-mail: • Phone: +49 911 526 2846 • Fax: +49 911 526 3131 • E-mail: htransde@lucent.com

END OF STEPS

Trouble clearing procedure in duplex control mode

Proceed as follows to clear a `Circuit Pack Comm Failure` alarm:

1 Refer to the following figure for reference:



Legend:

CTL #1 The active Controller at the time when the alarm is being reported.

CTL #2 The standby Controller at the time when the alarm is being reported.

Port unit, active XC, standby XC — The circuit pack reporting the `Circuit Pack Comm Failure` alarm. This may be either a port unit (OP…, EP155, or GE1) or the active or standby cross-connect and timing unit (XC160, XC320).

2 Take a note which cross-connect and timing unit (XC) is currently the active unit, and which is standby.

3 Perform a manual equipment protection switch to the CTL #2 (**Manual to Protection** if CTL #1 is the Controller in the worker slot (slot 11), **Manual to Working** otherwise).

4 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	**then …**
the alarm has cleared	replace the CTL #1. Stop! You have completed this procedure. The fact that the `Circuit Pack Comm Failure` alarm is not reported by the now active CTL #2 is an indication that CTL #1 is defective. **Reference:** Please refer to: • “Replacing the Controller (CTL)” (4-53)
the alarm persists	proceed with the next step.

5 Perform a controller reset of the CTL #2.

> **Important!** It is important that the controller reset be performed as soon as possible after the manual protection switch to avoid a (now unintended) automatic CTL protection switch. No automatic protection switch will be performed as long as the synchronisation process of the CTL #2 has not yet completed.

Reference: Please refer to:

- “Initiating a circuit pack reset” (4-68)

6 Verify that CTL #2 is still the active Controller (no automatic CTL protection switch occurred).

If …	then …
CTL #2 is still the active Controller	proceed with the next step.
CTL #1 is the active Controller (an automatic CTL protection switch occurred due to the controller reset of the CTL #2)	Perform a manual equipment protection switch to the CTL #2, and then repeat Step 5 and Step 6.

7 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	then …
the alarm has cleared	replace the CTL #1. Stop! You have completed this procedure. **Reference:** Please refer to: • “Replacing the Controller (CTL)” (4-53)
the alarm persists	proceed with the next step.

8 Perform a full reset of the CTL #2.

Important! It is important that the full reset be performed as soon as possible after the manual protection switch to avoid a (now unintended) automatic CTL protection switch. No automatic protection switch will be performed as long as the synchronisation process of the CTL #2 has not yet completed.

Reference: Please refer to:

- “Initiating a circuit pack reset” (4-68)

9 Verify that CTL #2 is still the active Controller (no automatic CTL protection switch occurred).

If ...	**then ...**
CTL #2 is still the active Controller	proceed with the next step.
CTL #1 is the active Controller (an automatic CTL protection switch occurred due to the controller reset of the CTL #2)	Perform a manual equipment protection switch to the CTL #2, and then repeat Step 8 and Step 9.

10 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If ...	**then ...**
the alarm has cleared	replace the CTL #1. Stop! You have completed this procedure. **Reference:** Please refer to: • "Replacing the Controller (CTL)" (4-53)
the alarm persists	proceed with the next step.

11 Perform a manual equipment protection switch to the CTL #1 (**Manual to Protection** if CTL #2 is the Controller in the worker slot (slot 11), **Manual to Working** otherwise).

12 At the *WaveStar®* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	**then …**
the alarm has cleared	replace the CTL #2. Stop! You have completed this procedure. The fact that the `Circuit Pack Comm Failure` alarm is not reported by the now active CTL #1 is an indication that CTL #2 is defective. **Reference:** Please refer to: • “Replacing the Controller (CTL)” (4-53)
the alarm persists	proceed with the next step.

13 Perform a controller reset of the CTL #1.

> **Important!** It is important that the controller reset be performed as soon as possible after the manual protection switch to avoid a (now unintended) automatic CTL protection switch. No automatic protection switch will be performed as long as the synchronisation process of the CTL #1 has not yet completed.

Reference: Please refer to:

- “Initiating a circuit pack reset” (4-68)

14 Verify that CTL #1 is still the active Controller (no automatic CTL protection switch occurred).

If …	**then …**
CTL #1 is still the active Controller	proceed with the next step.

If …	**then …**
CTL #2 is the active Controller (an automatic CTL protection switch occurred due to the controller reset of the CTL #2)	Perform a manual equipment protection switch to the CTL #1, and then repeat Step 13 and Step 14.

15 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If …	**then …**
the alarm has cleared	replace the CTL #2. Stop! You have completed this procedure. **Reference:** Please refer to: • "Replacing the Controller (CTL)" (4-53)
the alarm persists	proceed with the next step.

16 Perform a full reset of the CTL #1.

Important! It is important that the full reset be performed as soon as possible after the manual protection switch to avoid a (now unintended) automatic CTL protection switch. No automatic protection switch will be performed as long as the synchronisation process of the CTL #1 has not yet completed.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

17 Verify that CTL #1 is still the active Controller (no automatic CTL protection switch occurred).

If …	**then …**
CTL #1 is still the active Controller	proceed with the next step.

If ...	**then ...**
CTL #2 is the active Controller (an automatic CTL protection switch occurred due to the controller reset of the CTL #1)	Perform a manual equipment protection switch to the CTL #1, and then repeat Step 16 and Step 17.

18 At the *WaveStar®* CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If ...	**then ...**
the alarm has cleared	replace the CTL #2. Stop! You have completed this procedure. **Reference:** Please refer to: • "Replacing the Controller (CTL)" (4-53)
the alarm persists	proceed with the next step.

19 Depending on the circuit pack reporting the alarm:

If ...	**then ...**
the alarm is reported by the active XC	proceed with the next step.
the alarm is reported by the standby XC	proceed with Step 21.
the alarm is reported by a port unit	proceed with Step 23.

20 Perform a manual protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

21 Replace the XC reporting the alarm.

22 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 Step 35.

23 Perform a full reset of the standby XC.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

24 Perform a manual protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

25 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

Independent from whether the alarm has cleared or not, proceed with the next step.

26 Perform a full reset of the standby XC (this is ***not*** the same XC as in Step 23!).

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

27 Perform a manual equipment protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

28 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared.

If ...	then ...
the alarm has cleared in Step 25, and is still cleared	Stop! You have completed this procedure.
the alarm had cleared in Step 25, and now is reported again	replace the XC which initially was the active unit (cf. Step 2). Stop! You have completed this procedure.
the alarm continued to persist in Step 25, and now has cleared	replace the XC which initially was the standby unit (cf. Step 2). Stop! You have completed this procedure.
the alarm continued to persist in Step 25, and still persists	proceed with the next step.

29 Perform a controller reset of the port unit reporting the alarm.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

30 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.

Important! A full reset of a port unit is traffic affecting!

31 Perform a full reset of the port unit reporting the alarm.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

32 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.

33 Replace the port unit reporting the alarm.

34 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.

35 Replace one of the two CTLs, and make the newly inserted CTL the active Controller.

Reference: Please refer to:

- “Replacing the Controller (CTL)” (4-53)

36 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 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" (2-30).

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)" (4-53)
no circuit pack is plugged	insert a circuit pack of the correct type (acc. to the actual provisioning).

END OF STEPS

□

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" (2-32).

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.

END OF STEPS

□

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" (2-29).

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" (4-50)

END OF STEPS

□

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" (2-33).

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 cross-connect and timing unit (XC160, XC320)

Trouble clearing procedure

Important! Please be aware that the terms "worker" and "protection" are used to describe the static role within a protection, whereas the terms "active" and "standby" are used to describe the current (dynamic) role in a protection. The active or standby unit always means the circuit pack which is ***currently*** the active or standby unit in an equipment protection.

Proceed as follows to clear a `Comm Channel Failure` alarm:

1 Depending on whether the alarm is reported by one or two cross-connect and timing units (XCs):

If the alarm is reported by …	then …
one XC	proceed with the next step.
two XCs at the same time	proceed with Step 4.

2

If …	**then …**
the alarm-reporting XC is currently the ***standby*** unit	perform a full reset of the XC reporting the alarm. **Reference:** Please refer to: • “Initiating a circuit pack reset” (4-68)
the alarm-reporting XC is currently the ***active*** unit	perform a manual equipment protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise). Then perform a full reset of the XC reporting the alarm (which is now the standby unit). **Reference:** Please refer to: • “Initiating a circuit pack reset” (4-68)

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	replace the XC reporting the alarm. Stop! You have completed this procedure.

4

If …	**then …**
two CTLs are installed (CTL equipment protection, duplex control)	proceed with Step 7.

If ...	then ...
only one CTL is installed (***no*** CTL equipment protection, duplex control)	proceed with the next step.

5 Perform a full reset of the CTL.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 Step 16.

7 Perform a manual equipment protection switch to the standby CTL (**Manual to Protection** if the active Controller is the CTL in the worker slot (slot 11), **Manual to Working** otherwise).

Result:

The previously standby CTL becomes the active CTL, and the previously active CTL becomes standby.

8 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	proceed with Step 16.

9 Perform a full reset of the standby CTL.

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" (4-68)

10 Perform a manual equipment protection switch to the standby CTL (**Manual to Protection** if the active Controller is the CTL in the worker slot (slot 11), **Manual to Working** otherwise).

Result:

The previously standby CTL becomes the active CTL, and the previously active CTL becomes standby.

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 Perform a manual equipment protection switch to the standby CTL (**Manual to Protection** if the active Controller is the CTL in the worker slot (slot 11), **Manual to Working** otherwise).

Result:

The previously standby CTL becomes the active CTL, and the previously active CTL becomes standby.

13 Replace the standby CTL.

14 Perform a manual equipment protection switch to the standby CTL (**Manual to Protection** if the active Controller is the CTL in the worker slot (slot 11), **Manual to Working** otherwise).

Result:

The previously standby CTL becomes the active CTL, and the previously active CTL becomes standby.

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	proceed with the next step.

16 Perform a full reset of the standby XC.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

17 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared (for the just reset XC).

If ...	then ...
the alarm has cleared	proceed with the next step.
the alarm persists	replace the standby XC, and then proceed with the next step.

18 Perform a manual protection switch to the standby XC (**Manual to Protection** if the active XC is the XC in the worker slot (slot 9), **Manual to Working** otherwise).

Result:

The previously standby XC becomes the active XC, and the previously active XC becomes standby.

19 Perform a full reset of the standby XC (make sure that this is ***not*** the same XC as in Step 16).

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

20 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the alarm has cleared (for the just reset XC).

If …	**then …**
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	replace the standby XC.

21 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 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" (2-34).

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" (4-68)

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" (4-68)

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)" (4-53)

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

END OF STEPS

Clearing DCC MS/Line failure

Purpose

Use this procedure to clear an `DCC MS/Line failure` alarm.

Related information

Please also refer to

- the corresponding alarm description → "DCC MS/Line failure" (2-12)
- the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Before you begin

You or a service technician must be on-site at the NE to clear an `DCC MS/Line 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

Trouble clearing procedure

Proceed as follows to clear an `DCC MS/Line failure` alarm:

1 Make sure that the MS-DCC (Line DCC) is enabled at both ends of the DCC link.

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 Make sure that the LAPD mode is set to **AITS** at both ends of the DCC link.

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 Make sure that the LAPD role (**USER-SIDE**, **NETWORK-SIDE**) is set to different values at both ends of the DCC link.

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

END OF STEPS

□

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" (2-124).

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 at the same time	clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.

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?

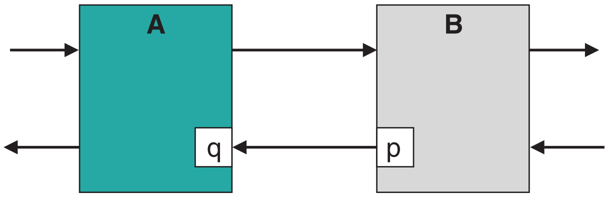
If …	**then …**
other transmission alarms are reported at the same time	clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
no other transmission alarms are reported	proceed with Step 7

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.

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" (4-50)

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" (4-50)

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.

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

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

END OF STEPS

□

Clearing Duplex Control not Present

Purpose

Use this procedure to clear a `Duplex Control not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "Duplex Control not Present" (2-35).

Before you begin

You or a service technician must be on-site at the NE to clear a `Duplex Control not Present` alarm.

Required equipment

The following equipment is required:

- A second Controller (either CTL/- or CTL/2)

Trouble clearing procedure

Proceed as follows to clear a `Duplex Control not Present` alarm:

1 Make sure that the hardware versions of the active and standby Controller match (for example 2 × CTL/-, or 2 × CTL/2).

END OF STEPS

□

Clearing Duplicate Ring Node

Purpose

Use this procedure to clear a `Duplicate Ring Node` alarm.

Related information

Please also refer to the corresponding alarm description → "Duplicate Ring Node" (2-125).

Before you begin

Prior to performing the following trouble clearing procedure, make sure that you have:

- management access via *WaveStar*® CIT or *Navis*™ Optical EMS to all ring nodes on the affected ring, and
- at least privilege codes of ***M4*** and ***P1***.

Required equipment

The following equipment is required:

- *WaveStar*® CIT or *Navis*™ Optical EMS

Trouble clearing procedure

Proceed as follows to clear a `Duplicate Ring Node` alarm:

1 Using the *WaveStar*® CIT or *Navis*™ Optical EMS, retrieve the ring map (textual or graphical representation).

2 Verify if there are more than 16 nodes on the ring.

If ...	then ...
there are more than 16 nodes on the ring	reduce the number of ring nodes, and proceed with the next step. The maximum number of nodes in a ring is restricted to 16.
the number of ring nodes is equal or less than 16	proceed with Step 4.

3 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.

4 Verify if there are duplicate NE names (target identifiers, TIDs) on the ring.

If …	**then …**
there are duplicate NE names	rename the corresponding NEs so that all NE names are unique. Then proceed with the next step.
there are ***no*** duplicate NE names	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

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.

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 ECI Comm Failure

Purpose

Use this procedure to clear an `ECI Comm Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "ECI Comm Failure" (2-36).

Before you begin

You or a service technician should be on-site at the NE to clear an `ECI Comm Failure` alarm.

Required equipment

The following equipment is required:

- *WaveStar*® CIT
- Eventually, a replacement EP155 port unit

Trouble clearing procedure

Proceed as follows to clear a `ECI Comm Failure` alarm:

1 Perform a controller reset of the standby EP155.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 standby EP155.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 manual protection switch to the standby EP155.

Result:

The two EP155 port units in the universal slot pair that corresponds to the ECI reporting the alarm, change their role in the STM-1E equipment protection.

6 Perform a controller reset of the standby EP155.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 Perform a full reset of the standby EP155.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 Perform a controller reset of the CTL.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 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" (4-68)

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 ECI reporting the alarm by an ECI of the same type.

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

END OF STEPS

□

Clearing ECI Mismatch Failure

Purpose

Use this procedure to clear a `ECI Mismatch Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "ECI Mismatch Failure" (2-37).

Before you begin

You or a service technician must be on-site at the NE to clear a `ECI Mismatch Failure` alarm.

Required equipment

The following equipment may be eventually required:

- Either an ECI/155MP8 or ECI/155ME8 Electrical Connector Interface (ECI).
  The type of ECI needed (ECI/155MP8 or ECI/155ME8) depends on the desired configuration (protected or unprotected STM-1E transmission functionality).
  Please also refer to the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.
- *WaveStar®* CIT

Trouble clearing procedure

Proceed as follows to clear a `ECI Mismatch Failure` alarm:

1 Depending on the type of ECI installed in the ECI slot, for which the alarm is being reported:

If …	then …
an ECI/155ME8 is installed	proceed with the next step.
an ECI/155MP8 is installed	proceed with Step 3.

2

If ...	then ...
an STM-1E equipment protection group exists involving the ECI and two EP155 port units in the corresponding universal slot pair	replace the ECI/155ME8 by an ECI/155MP8. The ECI/155ME8 is not suitable for STM-1E equipment protection.
an STM-1E equipment protection group exists (ECI/155MP8 with 2 × EP155), and you have installed the ECI/155ME8 in order to convert a protected configuration into an unprotected configuration with two EP155s (ECI/155ME8 with 2 × EP155)	delete the STM-1E equipment protection group.

3

If ...	then ...
you just have installed two EP155 port units and the ECI/155MP8 in order to configure an STM-1E equipment protection	create the corresponding STM-1E equipment protection group.
you just have deleted the STM-1E equipment protection group involving the ECI/155MP8	replace the ECI/155MP8 by an ECI/155ME8, or deprovision one of the associated EP155 port units. The ECI/155MP8 is not suitable for an unprotected configuration with two EP155 port units.

END OF STEPS

Additional information

The type of ECI needed (ECI/155MP8 or ECI/155ME8) depends on the desired configuration (protected or unprotected STM-1E transmission functionality).

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

□

Clearing ECI not Present

Purpose

Use this procedure to clear a `ECI not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "ECI not Present" (2-38).

Before you begin

You or a service technician must be on-site at the NE to clear a `ECI not Present` alarm.

Required equipment

The following equipment is required:

- Either an ECI/155MP8 or ECI/155ME8 Electrical Connector Interface (ECI).
  The type of ECI needed (ECI/155MP8 or ECI/155ME8) depends on the desired configuration (protected or unprotected STM-1E transmission functionality).
  Please also refer to the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Trouble clearing procedure

Proceed as follows to clear a `ECI not Present` alarm:

1 Install a suitable Electrical Connector Interface (ECI).

END OF STEPS

□

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" (2-39).

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:

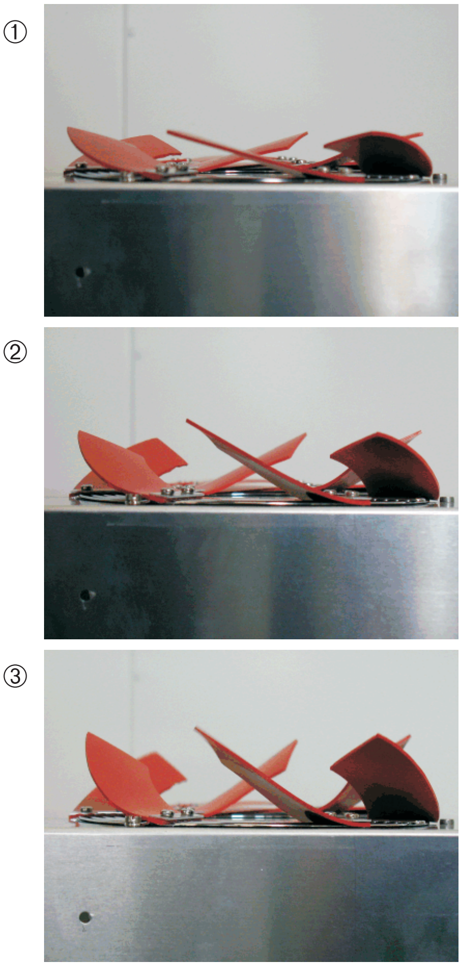
- A fully functional fan unit

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)

END OF STEPS

□

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 → "Fan Unit Comm Failure" (2-40).

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 Step 4.
any of the connectors (at the CI-CTL or at the fan unit) is not properly connected	proceed with the next step.

2 Complete these steps to connect the respective connector(s) properly:

1. Slightly pull out the Controller (CTL).
2. Connect the connector(s) properly.
3. Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

5 Replace the fan unit control cable, and connect the new cable properly at the CI-CTL and at the fan unit.

6 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

9 Disconnect the fan unit control cable at the CI-CTL.

10 Replace the CI-CTL.

11 Connect the fan unit control cable at the CI-CTL.

12 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

15 Replace the fan unit.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)

16 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

17 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 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" (2-41).

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.

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" (3-71) .

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

END OF STEPS

`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)” (4-53) 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 Unit not Present

Purpose

Use this procedure to clear a `Fan Unit not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "Fan Unit not Present" (2-42).

Before you begin

You or a service technician must be on-site at the NE to clear a `Fan Unit not Present` 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

The following equipment is required:

- *WaveStar*® CIT
- A fully functional fan unit

Trouble clearing procedure

⚠ **CAUTION**

A network element may fail without proper cooling.

A network element which is operated without a fan unit for more than two minutes may fail due to overheating.

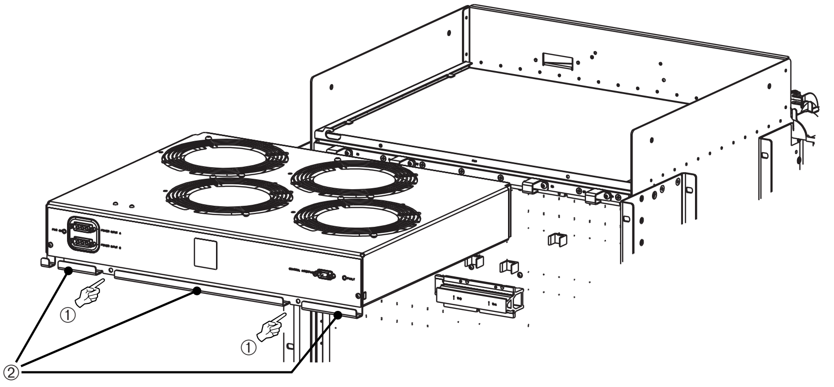
Therefore, do not operate a network element without a fan unit.

Proceed as follows to clear a `Fan Unit not Present` alarm:

1 Install the fan unit. Proceed as described in the following steps.

2 If required, loosen the screws (1) of the fan unit drawer (with your fingers).

Refer to the following figure for clarification and further reference.



3 Slide the fan unit drawer from its position by using the handles (2).

4 Place the fan unit into the fan unit drawer, and slide the fan unit drawer back into the shelf.

5 Connect the power and alarm connectors of the fan unit.

6 With your fingers, fasten the screws of the fan unit drawer.

END OF STEPS

□

Clearing Fan Voltage Feed A/B Failure

Purpose

Use this procedure to clear a `Fan Voltage Feed A Failure` or `Fan Voltage Feed B Failure` alarm.

Related information

Please also refer to the corresponding alarm description:

- → "Fan Voltage Feed A Failure" (2-43)
- → "Fan Voltage Feed B Failure" (2-44)

Before you begin

You or a service technician must be on-site at the NE to clear a `Fan Voltage Feed A 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.

The following trouble clearing procedure is based on the assumption that the "FAN output" of the Power Interfaces (PI A, PI B) and the fan unit power inputs ("Power Input A", "Power Input B") are interconnected as follows:

- "FAN output" of the PI A → Fan unit "Power Input A"
- "FAN output" of the PI B → Fan unit "Power Input B"

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

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` or `Fan Voltage Feed B Failure` alarm:

1 The measures to be taken depend on the type of Power Interface used:

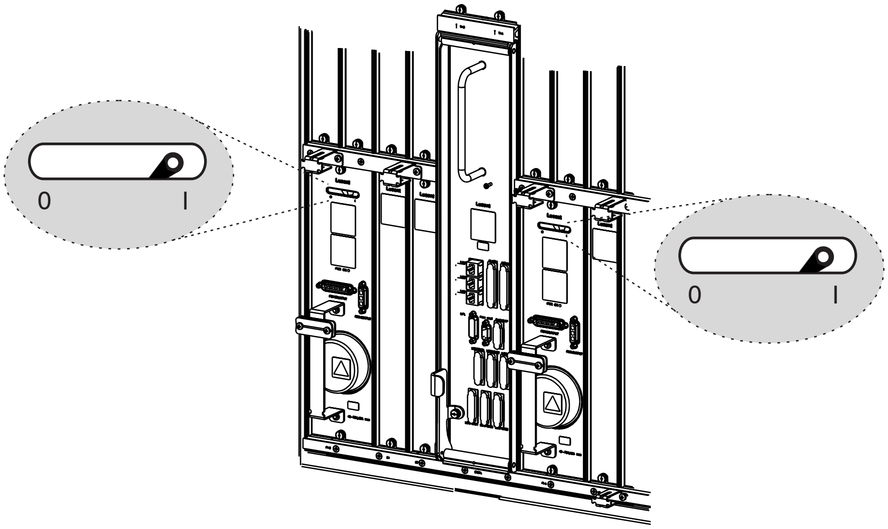
If …	**then …**
the PI/- variant is used	proceed with the next step.
the PI/100 variant is used	proceed with Step 4.

2 At the *WaveStar*® CIT, check the **NE Alarm List**.

If …	**then …**
a `System Power Failure` alarm is reported at the same time	proceed with Step 5.
no `System Power Failure` alarm is reported	proceed with the next step

3 Make sure that the circuit breaker on the affected Power Interface is in the ON position (“I”), and then proceed with Step 6.

Circuit breaker on the Power Interfaces:



4 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" (3-121)), and then proceed with Step 6.
no `System Power Failure` alarm is reported	proceed with Step 7.

5 Measure the actual supply voltage at the affected system power feeder of the exchange battery.

If …	**then …**
the voltage is within the normal range (≥ 38.0 V DC, negative polarity)	replace the Power Interface reporting the `System Power Failure` alarm.

If …	**then …**
the voltage is out of range	repair the exchange battery.

6 At the *WaveStar*® CIT, check the **NE Alarm List**, and check if the alarm (`Fan Voltage Feed A Failure` or `Fan Voltage Feed B Failure`) has cleared.

If …	**then …**
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

7 Is a fan unit power cable installed between the corresponding fan unit power input (“Power Input A”, “Power Input B”) and the “FAN output” of the associated Power Interface (PI A, PI B)?

If …	**then …**
yes	proceed with Step 9.
no	install a fan unit power cable between the fan unit power input and the “FAN output” of the associated Power Interface, and then proceed with the next step.

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 Are the connectors of the power cable connected properly at both the fan unit power input and the “FAN output” of the associated Power Interface?

If …	**then …**
yes	proceed with Step 11.
no	connect the connectors properly, and then proceed with the next step.

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 power cable between the corresponding fan unit power input (“Power Input A”, “Power Input B”) and the “FAN output” of the associated Power Interface (PI A, PI B).

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 associated Power Interface (PI A, PI B).

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

END OF STEPS

□

Clearing Improper APS Codes

Purpose

Use this procedure to clear an `Improper APS Codes` alarm.

Related information

Please also refer to the corresponding alarm description → "Improper APS Codes" (2-128).

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.

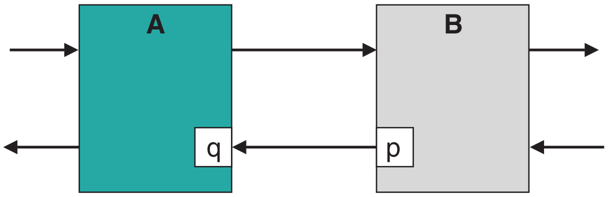
If ...	then ...
the alarm has cleared	Stop! You have completed this procedure.
the alarm persists	proceed with the next step.

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” (4-50)

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" (4-50)

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

END OF STEPS

□

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" (2-128).

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?

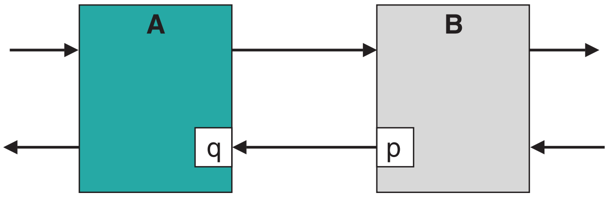
If ...	**then ...**
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and then proceed with the next step.
No	proceed with Step 7

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.

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" (4-50)

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" (4-50)

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.

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

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

END OF STEPS

□

Clearing Inconsistent Ring Protection Mode

Purpose

Use this procedure to clear an `Inconsistent Ring Protection Mode` alarm.

Related information

Please also refer to the corresponding alarm description → "Inconsistent Ring Protection Mode" (2-130).

Before you begin

Prior to performing the following trouble clearing procedure, make sure that you have:

- management access via *WaveStar*® CIT or *Navis*™ Optical EMS to all ring nodes pertaining to the affected 4-fiber MS-SPRing protection group, and
- at least privilege codes of ***M4*** and ***P1***.

Required equipment

The following equipment is required:

- *WaveStar*® CIT or *Navis*™ Optical EMS

Trouble clearing procedure

Proceed as follows to clear an `Inconsistent Ring Protection Mode` alarm:

1 Define the ring protection mode consistently to either **Ring Loopback** or **Shortened Path** for all nodes on the ring.

END OF STEPS

□

Clearing Local Squelch Map Conflict

Purpose Use this procedure to clear a `Local Squelch Map Conflict` alarm.

Related information

Please also refer to the corresponding alarm description → “Local Squelch Map Conflict” (2-131).

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 `Local Squelch Map Conflict` alarm:

1 Correct the A-node/Z-node configuration (source/destination node information) for the affected BLSR/MS-SPRing protection group by using the *WaveStar*® CIT.

> **Important!** When you are modifying a 2-way cross-connection, then only one leg (direction) of the cross-connection can be modified at a time. Therefore, successively correct the A-node/Z-node configuration for ***both*** legs of the 2-way cross-connection.

Example:

If, for example, the source and/or destination node names contain quotes, then delete these quotes.

Reference: Please also refer to the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*:

- Modifying a cross-connection

END OF STEPS

□

Clearing Loss of Frame

Purpose

Use this procedure to clear a `Loss of Frame` alarm.

Related information

Please also refer to the corresponding alarm description → "Loss of Frame" (2-114).

Before you begin

You or a service technician should be on-site at the near-end NE and at the far-end NE to clear a `Loss of Frame` 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 or *Navis*™ Optical EMS for monitoring both the near-end (alarm-reporting) NE as well as the far-end NE.
- A network analyzer, if available.

Instructions

1 Is the Optical Channel enabled at the far end?

If ...	then ...
Yes	disable the Optical Channel at the far-end NE.
No	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 Is a network analyzer available for checking the receive signal?

If ...	then ...
Yes	proceed with the next step.
No	proceed with Step 7.

4 Using the network analyzer, check if the signal rate of the received signal matches the signal rate of the port reporting the alarm.

5 Does the signal rate of the received signal match the signal rate of the port reporting the alarm?

If ...	then ...
Yes	proceed with the next step.
No	assign the signal structure correctly at the far-end NE.

6 Is the Section Overhead (SOH) of the received signal structured correctly?

If ...	then ...
Yes	replace the receiver circuit pack reporting the alarm. Stop! You have completed this procedure.
No	replace the associated transmitter circuit pack at the far-end NE. Stop! You have completed this procedure. The SOH is not correctly formed at the far-end NE.

7 At the alarm-reporting port, loop the optical output to the optical input.

Reference:

"Performing optical fiber loopbacks manually" (4-32)

8 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	replace the receiver circuit pack reporting the alarm. Stop! You have completed this procedure.

9 Does the port rate of the transmit port (at the far-end NE) match the port rate of the alarm-reporting receive port?

If ...	**then ...**
Yes	replace the associated transmitter circuit pack at the far-end NE. The SOH is not correctly formed at the far-end NE.
No	assign a suitable transmitter circuit pack at the far-end NE.

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.

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 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" (2-146).

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" (3-127) to check the quality of an external timing reference.
> - "Checking line timing references" (3-128) to check the quality of a line timing reference.

END OF STEPS

□

Clearing max number of VLAN instances reached

Purpose

Use this procedure to clear a `max number of VLAN instances reached` alarm.

Related information

Please also refer to:

- the corresponding alarm description → "max number of VLAN instances reached" (2-73)
- the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Before you begin

You or a service technician should be on-site at the NE to clear a `max number of VLAN instances reached` 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
- Possibly, an additional Gigabit Ethernet circuit pack is required.

Trouble clearing procedure

Proceed as follows to clear a `max number of VLAN instances reached` alarm:

1 If possible, reduce the number of VLAN connections by deleting dispensible VLAN tags from the static VLAN lists of ***all*** nodes participating in the Virtual LAN.

Otherwise (if there are no dispensible VLAN tags), consider installing an additional Gigabit Ethernet circuit pack in the network element reporting the alarm.

END OF STEPS

□

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" (2-147).

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 cross-connect and timing unit (XC160, XC320)

Trouble clearing procedure

Proceed as follows to clear a `NE Clock Failure` alarm:

1 Replace the cross-connect and timing unit (replacing the standby circuit pack is sufficient).

> **Important!** To clear the alarm, it is sufficient to replace the standby circuit pack. However, ***both*** cross-connect and timing units are defective.

> **Reference:** Please refer to:
>
> - "Replacing a circuit pack by a circuit pack of the same type" (4-50)

END OF STEPS

□

Clearing ONI Failure on protecting CTL

Purpose

Use this procedure to clear an `ONI Failure on protecting CTL` alarm.

Related information

Please also refer to the corresponding alarm description → "ONI Failure on protecting CTL" (2-46).

Before you begin

You or a service technician should be on-site at the NE to clear an `ONI Failure on protecting CTL` 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 on protecting CTL` alarm:

1 Verify that the latches of the circuit pack for which the alarm is reported are closed.

If …	then …
the latches are properly closed	proceed with Step 3.
the latches are ***not*** properly closed	close the latches (the circuit pack performs a full reset), wait for the circuit pack to re-initialize, 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 Perform a controller reset of the standby Controller.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 standby Controller.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

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 circuit pack for which the alarm is reported.

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 standby Controller.

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-53)

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 ONI Failure on working CTL

Purpose

Use this procedure to clear an `ONI Failure on working CTL` alarm.

Related information

Please also refer to the corresponding alarm description → "ONI Failure on working CTL" (2-47).

Before you begin

You or a service technician should be on-site at the NE to clear an `ONI Failure on working CTL` 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 on working CTL` alarm:

1 Verify that the latches of the circuit pack for which the alarm is reported are closed.

If …	**then …**
the latches are properly closed	proceed with Step 3.
the latches are ***not*** properly closed	close the latches (the circuit pack performs a full reset), wait for the circuit pack to re-initialize, 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 Perform a controller reset of the standby Controller.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

4 Perform a manual protection switch to the just reset Controller.

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 standby Controller.

Reference: Please refer to:

- "Initiating a circuit pack reset" (4-68)

7 Perform a manual protection switch to the just reset Controller.

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 for which the alarm is reported.

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 standby Controller.

Reference: Please refer to:

- "Replacing the Controller (CTL)" (4-53)

12 Perform a manual protection switch to the newly inserted Controller.

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.

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 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 → "Power Interface not Present" (2-48)
- "Configuration rules" (4-60)

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).

END OF STEPS

□

Clearing Power Interface Read Failure

Purpose

Use this procedure to clear a `Power Interface Read Failure` alarm.

Related information

Please also refer to

- the corresponding alarm description → " Power Interface Read Failure" (2-49)
- "Configuration rules" (4-60)

Before you begin

You or a service technician must be on-site at the NE to clear a `Power Interface Read Failure` alarm.

Perform the following trouble clearing procedure from the ***rear side*** of the shelf.

Required equipment

The following equipment is required to complete this procedure:

- *WaveStar*® CIT or *Navis*™ Optical EMS

Trouble clearing procedure

Proceed as follows to clear a `Power Interface Read Failure` alarm:

1 Replace the Power Interface (PI).

2 Retrieve the equipment parameters of that Power Interface (by using the RTRV-EQPT TL1 command, or by retrieving the equipment details using the *WaveStar*® CIT or *Navis*™ Optical EMS graphical user interfaces) to make sure that the `Power Interface Read Failure` alarm has cleared.

END OF STEPS

□

Clearing primary section Mismatch

Purpose

Use this procedure to clear a `primary section Mismatch` alarm.

Related information

Please also refer to:

- the corresponding alarm description → "max number of VLAN instances reached" (2-73)
- the *LambdaUnite® MultiService Switch (MSS) User Operations Guide*.

Before you begin

You or a service technician should be on-site at the NE to clear a `primary section 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
- Possibly, an additional Gigabit Ethernet circuit pack is required.

Trouble clearing procedure

Proceed as follows to clear a `primary section Mismatch` alarm:

1 END OF STEPS

□

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" (2-82).

Instructions Proceed as follows to clear a `Prot. Arch. Mismatch` alarm:

1 Define the protection architecture consistently at both ends of the protection line.

END OF STEPS

□

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" (2-148).

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 cross-connect and timing unit (XC160, XC320)

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" (4-50)

If …	**then …**
the alarm is reported by several circuit packs	replace the cross-connect and timing unit in the protection slot (slot 10, cf. "Configuration rules" (4-60)). **Reference:** Please refer to: • "Replacing a circuit pack by a circuit pack of the same type" (4-50)

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

□

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

END OF STEPS

□

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 → "Remote Defect Indication (RFI-L)" (2-119).

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.

END OF STEPS

□

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)" (2-98).

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.

END OF STEPS

□

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" (2-135).

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" (4-68)

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" (4-68)

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

END OF STEPS

□

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" (2-138).

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" (4-68)

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" (4-68)

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

END OF STEPS

□

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" (2-51).

Before you begin

You or a service technician must be on-site at the NE to clear a `System Power 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.

The following trouble clearing procedure is based on the assumption that the "FAN output" of the Power Interfaces (PI A, PI B) and the fan unit power inputs ("Power Input A", "Power Input B") are interconnected as follows:

- "FAN output" of the PI A → Fan unit "Power Input A"
- "FAN output" of the PI B → Fan unit "Power Input B"

Required equipment

Make sure that the following equipment is available:

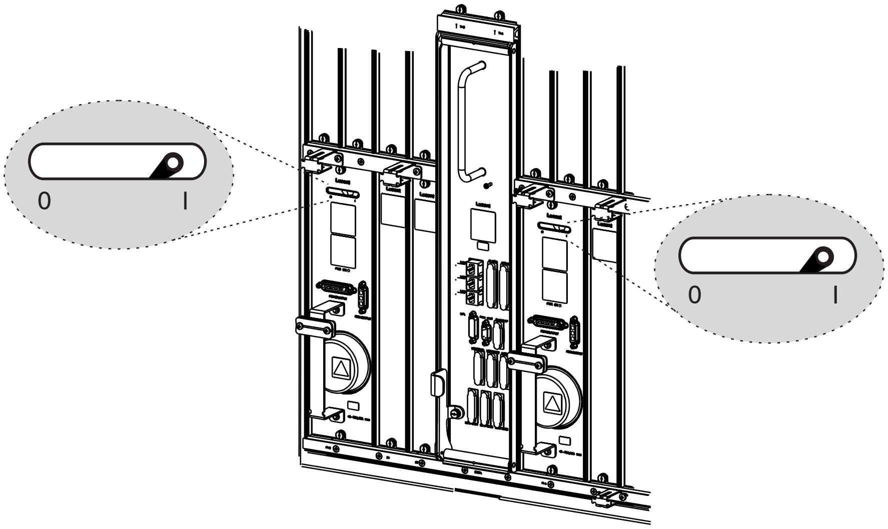
- *WaveStar*® CIT
- A volt meter
- A replacement Power Interface (PI)

Trouble clearing procedure

Proceed as follows to clear a `System Power Failure` alarm:

1 Make sure that the circuit breaker on the affected Power Interface is in position "I".

Circuit breaker on the Power Interfaces:



2 At the *WaveStar*® CIT, refresh the **NE Alarm List**, and check if the `System Power Failure` alarm has cleared.

If ...	then ...
the alarm has cleared	Stop! You have completed this procedure.
the `System Power Failure` alarm persists	proceed with Step 3.

3 Measure the actual supply voltage at the affected system power feeder of the exchange battery.

If ...	then ...
the voltage is within the nominal range (≥ 38.0 V DC, negative polarity)	replace the Power Interface reporting the `System Power Failure` alarm.

If …	then …
the voltage is out of range	repair the exchange battery.

END OF STEPS

□

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" (2-149).

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**).

END OF STEPS

□

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 → "Timing Reference Failure" (2-150).

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" (3-127)
to check the quality of an external timing reference.
- "Checking line timing references" (3-128)
to check the quality of a line timing reference.

END OF STEPS

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" (3-126).

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.

END OF STEPS

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 Analyzer.

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" (4-50)
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.

END OF STEPS

□

Clearing TI not Present

Purpose

Use this procedure to clear a `TI not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "TI not Present" (2-53).

Before you begin

You or a service technician must be on-site at the NE to clear a `TI not Present` alarm.

Required equipment

Make sure that you have a Timing Interface (TI) available.

Trouble clearing procedure

Proceed as follows to clear a `TI not Present` alarm:

1 Install the Timing Interface.

END OF STEPS

□

Clearing TXI Failure

Purpose

Use this procedure to clear a `TXI Failure` alarm.

Related information

Please also refer to the corresponding alarm description → "TXI Failure" (2-54).

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 Identify the affected TXI bus line.

The affected TXI bus line can be seen from the alarm identifier (**Probable cause**). When the **Probable cause** is TXI2F for example, then the TXI bus line number 2 is affected.

2 From the alarm message displayed in the *WaveStar*® CIT **NE Alarm List**, identify the circuit pack reporting the alarm.

3 Use the TXI bus line numbering scheme (see "TXI bus line numbering scheme" (2-54)) to identify the sender of the TXI signal on the affected TXI bus line.

Result:

You have identified a port unit and a cross-connect and timing unit, one of them being the sender of the TXI signal on the affected TXI bus line, and the other being the alarm-reporting circuit pack.

4 Replace the port unit identified in the previous 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

If the XC identified in Step 3 ...	**then ...**
is currently the ***active*** unit in the 1+1 XC equipment protection	perform a manual equipment protection switch to the second XC, and then proceed with the next step.
is currently the ***standby*** unit in the 1+1 XC equipment protection	proceed with the next step.

7 Replace the XC identified in Step 3.

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.

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 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" (2-62).

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 " (3-61) • "Clearing Fan Unit Failure" (3-68) • "Clearing Unit Temperature too High" (3-135)
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.

END OF STEPS

□

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 → "Unit Cooling Degraded" (2-62).

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: • "Clearing Fan Failure " (3-61) • "Clearing Fan Unit Failure" (3-68)
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.

END OF STEPS

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)" (4-53) 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" (2-64).

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 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 Step 4.
any of the connectors (at the CI-CTL or at the fan unit) is not properly connected	proceed with the next step.

2 Complete these steps to connect the respective connector(s) properly:

1. Slightly pull out the Controller (CTL).
2. Connect the connector(s) properly.
3. Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 Slightly pull out the Controller (CTL).

5 Replace the fan unit control cable, and connect the new cable properly at the CI-CTL and at the fan unit.

6 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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 user panel.

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 Slightly pull out the Controller (CTL).

11 Disconnect the fan unit control cable at the CI-CTL.

12 Replace the CI-CTL.

13 Connect the fan unit control cable at the CI-CTL.

14 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

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	proceed with the next step.

16 Slightly pull out the Controller (CTL).

17 Replace the fan unit.

Reference: Please refer to:

- "Replacing the fan unit" (4-15)

18 Re-insert the CTL, and wait for the system to re-initialize.

Important! Pulling-out and re-inserting 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

19 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 User Panel not Present

Purpose

Use this procedure to clear a `User Panel not Present` alarm.

Related information

Please also refer to the corresponding alarm description → "User Panel not Present" (2-65).

Before you begin

You or a service technician must be on-site at the NE to clear a `User Panel not Present` alarm.

Required equipment

Make sure that you have a user panel available.

Trouble clearing procedure

Proceed as follows to clear a `User Panel not Present` alarm:

1 Install the user panel.

END OF STEPS

□

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" (2-151).

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 cross-connect and timing 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" (4-50)

If …	**then …**
the alarm is reported by several circuit packs	replace the cross-connect and timing unit in the worker slot (slot 9, cf. “Configuration rules” (4-60)). **Reference:** Please refer to: • “Replacing a circuit pack by a circuit pack of the same type” (4-50)

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

This chapter covers tasks that are often used during trouble clearing and additional related information. Instead of describing a trouble clearing task to its fullest extent, the repetitive part is included here in this chapter.

Contents

□

Retrieving the *WaveStar*® CIT NE Alarm List

Purpose

Use this procedure to retrieve detailled 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.

END OF STEPS

□

The *WaveStar®* CIT NE Alarm List

The “NE Alarm List” window

The *WaveStar®* CIT provides a list of current alarms, the **NE Alarm List**, to retrieve 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. Please refer to the *LambdaUnite® MSS User Operations Guide* for information on how to set the date and time of the system.
Time	
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**CommonAlarms 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
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 detailled 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.

END OF STEPS

Identifying SDH tributaries in alarm messages

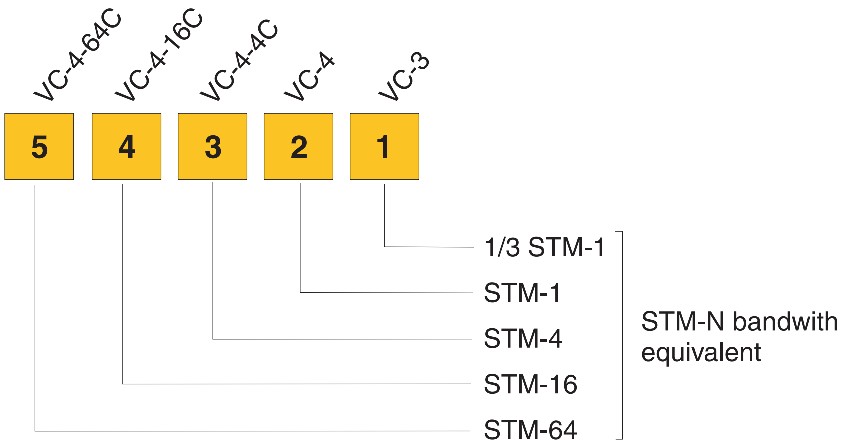
Purpose

Use this procedure to uniquely identify SDH tributaries in case of tributary alarms reported in the *WaveStar*® CIT **NE Alarm List** or **NE Alarm Log**.

Representation of SDH tributaries in alarm messages

When tributary alarms are reported, the alarm messages in the *WaveStar*® CIT **NE Alarm List** or **NE Alarm Log** contain the signal level affected, but not the port type. Therefore, a five-digit representation is used for SDH tributary AIDs to facilitate the correct identification of SDH tributaries. Please also refer to “SONET and SDH tributary numbering format” (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

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).

END OF STEPS

□

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

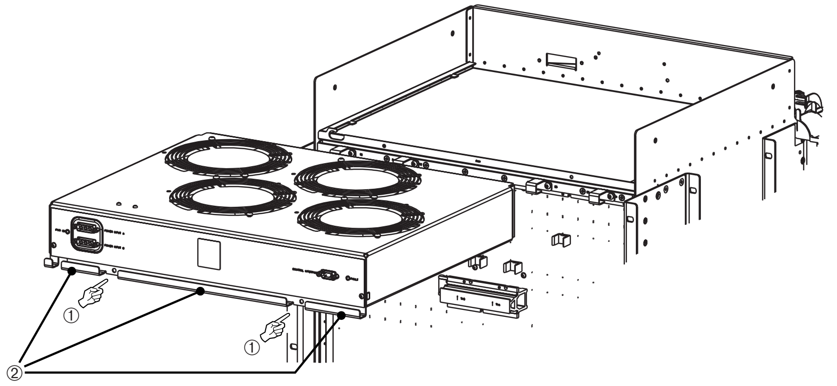
A network element may fail without proper cooling.

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 supply cables and the fan unit control cable.

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 supply cables and the fan unit control cable.

8 With your fingers, fasten the screws of the fan unit drawer.

END OF STEPS

□

Replacing the air filter

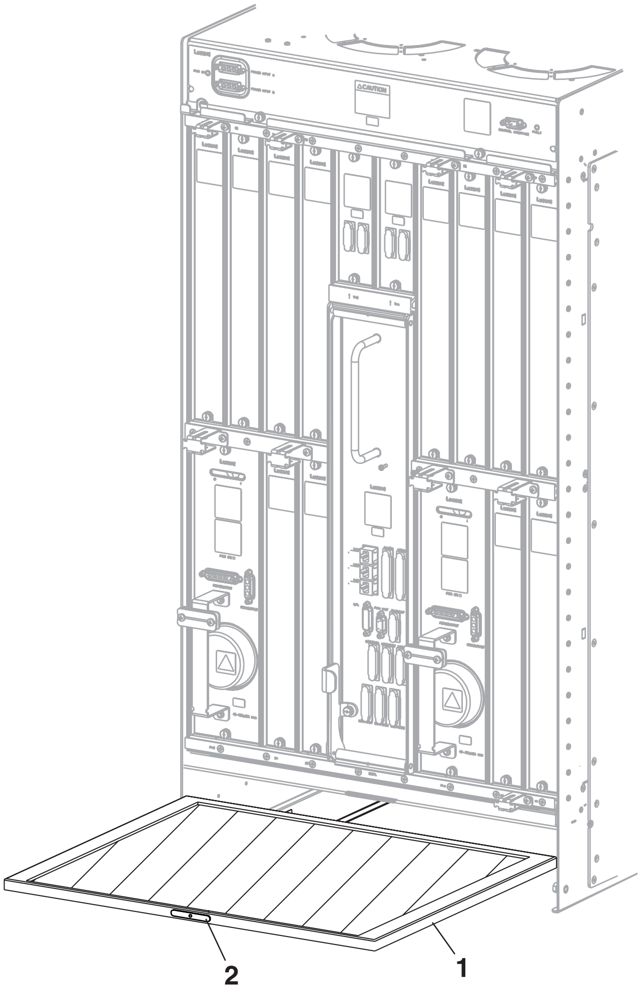
When to use

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.

END OF STEPS

□

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.

END OF STEPS

□

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.

END OF STEPS

□

Performing cross-connection loopbacks

Purpose

Use this procedure to operate cross-connection loopbacks.

Related information

Please also refer to “Cross-connection loopbacks” (4-73).

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.

Observe the rules for performing a cross-connection loopback (see “Cross-connection loopbacks” (4-73)).

Required privilege

You must have at least privilege codes of ***S1 and P2 and M3*** to perform or release cross-connection loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to operate a cross-connection loopback:

1 Select **Fault** → **Analysis** → **Cross-Connect Loopback...** from the *WaveStar*® CIT **System View** main menu.

Result:

The **Crossconnect Loopback** equipment selection window opens.

2 Select the desired tributary from the **Crossconnect Loopback** equipment selection window, and click **Select**.

Result:

The **crossConnect Loopback** window opens. The AID of the selected tributary and the type of the respective port are displayed in the **Tributary AID** and **Port Type/Rate** fields.

3 By means of the display-only fields in the upper region of the window (**Tributary AID**, **Port Type/Rate**), verify that you selected the desired tributary.

4 Select the signal rate of the cross-connection loopback to be operated by means of the **Loopback Rate** drop-down list box.

Additional information

Depending on the selected tributary, the selection choices for the loopback rate will automatically be restricted to suitable rates.

5 Whether you are going to perform a "normal" or a forced cross-connection loopback depends on the **Cross Connect Status** (display only filed below the **Loopback Rate** drop-down list box):

If ...	**then ...**
the **Cross Connect Status** is **No**	there is currently no cross-connection for the selected tributary. You are going to perform a "normal" cross-connection loopback.
the **Cross Connect Status** is **Yes**	there is currently a cross-connection for the selected tributary. You are going to perform a ***forced*** cross-connection loopback.

6 Verify that the **Cross Connect Loopback Status** is **No Loopback** (there is currently no cross-connection loopback active for the selected tributary).

7 Click **Operate** to perform the cross-connection loopback ("normal" or forced cross-connection loopback; cf. Step 5).

Important! Operating a cross-connection loopback, especially a forced cross-connection loopback, may be service affecting!

8 If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window that opens.

END OF STEPS

Releasing a cross-connection loopback

Purpose

Use this procedure to dismantle (release) a cross-connection loopback.

Related information

Please also refer to "Cross-connection loopbacks" (4-73).

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 P2 and M3*** to perform or release cross-connection loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to release a cross-connection loopback:

1 Select **Fault** → **Analysis** → **Cross-Connect Loopback…** from the *WaveStar*® CIT **System View** main menu.

Result:

The **Crossconnect Loopback** equipment selection window opens.

2 Select the desired tributary from the **Crossconnect Loopback** equipment selection window, and click **Select**.

Result:

The **crossConnect Loopback** window opens. The AID of the selected tributary and the type of the respective port are displayed in the **Tributary AID** and **Port Type/Rate** fields.

3 By means of the display-only fields in the upper region of the window (**Tributary AID**, **Port Type/Rate**), verify that you selected the desired tributary.

4 Select the signal rate of the cross-connection loopback to be released by means of the **Loopback Rate** drop-down list box.

Additional information

Depending on the selected tributary, the selection choices for the loopback rate will automatically be restricted to suitable rates.

5 Verify that you selected the correct tributary, and that the **Cross Connect Loopback Status** is **Loopback Running**.

6 Click **Release**, if you want to dismantle the cross-connection loopback on the respective tributary, and confirm your selection by clicking **Yes** in the confirmation window that opens.

END OF STEPS

□

Performing facility loopbacks

Purpose

Use this procedure to operate near-side or far-side facility loopbacks.

Related information

Please also refer to “Facility loopbacks” (4-76).

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

> **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
  1. Select **Configuration** → **Provision…** from the **System View** main menu,
  2. choose the port on which you want to operate a facility loopback from the equipment selection window, and
  3. click **Provision**.
  4. In the **Provision Parameters for Protection Group or Equipment** window, set the **Service Condition** to **Out Of Service**.
- Option 2
  1. In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.
  2. In the pop-up menu that opens, select the **Provision Port #** menu item (“#” represents the port number).
  3. 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
  1. Select **Fault** → **Analysis** → **Facility Loopback…** from the **System View** main menu,
  2. choose the port on which you want to operate a facility loopback from the equipment selection window that will be opened, and
  3. click **Select**.
- Option 2
  1. In the **System View**, right-click on the alarm LED of the port on which you want to operate a facility loopback.
  2. In the pop-up menu that opens, select the **Facility Loopback** menu item.

4 By means of the read-only fields in the upper region of the window (**Port AID**, **Port Type/Rate**, **Facility Loopback Status**), verify that you selected the desired port, and that no loopback is currently active.

5 Select the type of facility loopback to be operated by means of the **Facility Loopback Type** checkboxes:

- **Nearside Facility** or
- **Farside Facility**.

6 Click the button in the lower left-hand-side corner of the window which may be labelled either **Operate** or **Force**.

The button will be labelled **Operate** if the corresponding port is an optical port, is protected and ***not*** active, and if the switch request state is “Lockout of protection”. Otherwise it will be labelled **Force**.

Important! Operating a facility loopback may be service affecting!

7 If you want to proceed, confirm your selection by clicking **Yes** in the confirmation window that will be opened.

END OF STEPS

□

Releasing a facility loopback

Purpose Use this procedure to dismantle (release) a near-side or far-side 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.

END OF STEPS

□

Performing optical fiber loopbacks manually

Purpose

Front access to the optical connectors on the optical circuit pack faceplates allows manual optical loopbacks. These loopbacks are performed by connecting an optical output port to the corresponding optical input port.

Manual loopbacks are similar in function to far-side facility loopbacks. The advantage of a manual loopback is that the entire signal path is tested including the physical interface.

Before you begin

> **Important!** If a fiber loop is made between an input and an output on the same Gigabit Ethernet port or between Gigabit Ethernet ports on the same circuit pack there is a chance that all Gigabit Ethernet transmission over the loop is blocked. The chance of occurrence depends on the length of the fiber. It is recommended to use a fiber of approximately 3 meters or 6-7 meters.

Make sure that the required equipment listed below is available before you begin.

Required equipment

The following equipment is required to perform this task:

- Clean protection caps to cover the fiber endfaces of the optical interfaces,
- Suitable optical fiber (“loopback cable”), see *LambdaUnite® MSS Installation Guide*,
- Suitable optical attenuator (see “Optical circuit pack parameters” (4-35)).

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.

Important! The normal traffic will be interrupted during a manual loopback.

Proceed as follows to manually perform a loopback on an optical port unit:

1 Determine the required optical attenuation depending on the selected optical circuit pack type (please refer to “Optical circuit pack parameters” (4-35)).

2 At the circuit pack faceplate, remove the optical connections from both the optical input and output and cover the fiber endfaces with protection caps.

Make a record of these disconnections so they can be re-established after the loopback.

3 Mount the optical attenuator at the optical input and cover it with a protection cap.

4 Equip the loopback cable with optical connectors.

5 Clean all optical fiber endfaces, connectors and couplings (please refer to “Cleaning optical fiber connectors” (4-19) and “Cleaning optical fiber couplings” (4-21)).

6 Connect one end of the loopback cable to the port unit input.

7 Connect the other end of the loopback cable to the port unit output.

END OF STEPS

□

Optical circuit pack parameters

Optical parameters and recommended attenuation

The following tables provide an overview of the transmitter output power ranges and the permitted receiver input power ranges (receiver sensitivity) for the different optical circuit packs as well as a recommendation for the optical attenuation that should be used when performing manual loopbacks.

40-Gbit/s circuit packs

These are the relevant optical parameters of the 40-Gbit/s circuit packs:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA3	OP40/1.5LR1O	+10 … +13	−14 … +2	15 dB
KFA202	OP40/1.3IOR1	+5 … +7	−2 … +4	5 dB
KFA290 … KFA354	OP40/9280XT ... 8650XT	–5 … –3	−10.5 … −0.5	3 dB

10-Gbit/s circuit packs

These are the relevant optical parameters of the 10-Gbit/s circuit packs:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA7	OP10/1.3IOR1	−6 … −1	−11 … −1	3 dB
KFA14	OP10/1.5IR1	−1 … +2	−14 … −1	5 dB
KFA6	OP10/1.5LR1	+10 … +13	−14 … −1	17 dB
KFA9, KFA81 … KFA159	OP10/01…80/800G	–6.2 … –3.8	−20 … −13	12 dB
KFA11, KFA61 … KFA75	OP10/1…16/PWDM	−1 … +2	−21 … −8	15 dB
KFA210 … KFA482	OP10/9285XT…8650XT	approx. –2	−13 … −3	7 dB

2.5-Gbit/s circuit packs

These are the relevant optical parameters of the 2.5-Gbit/s circuit packs:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA12	OP2G5/1.3IOR4	−10 … −3	−18 … −3	3 dB
KFA203	OP2G5/1.3LR4	−2 … +2	−27 … −8	15 dB
KFA204	OP2G5/1.5LR4	−2 … +2	−28 … −8	15 dB
KFA20 with OM2G5A921 ... OM2G5A959	OP2G5-1...32PWDM with OM2G5/921PWDM ... OM2G5/959PWDM	−3 … 0	−28 … −8	10 - 15 dB

622-Mbit/s circuit pack

These are the relevant optical parameters of the 622-Mbit/s circuit pack:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA17	OP622/1.3IR16	−15 … −8	−28 … −8	7 dB

155-Mbit/s circuit pack

These are the relevant optical parameters of the optical 155-Mbit/s circuit pack:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA18	OP155M/1.3IR16	−15 … −8	−28 … −8	7 dB

Gigabit Ethernet circuit pack

These are the relevant optical parameters of the Gigabit Ethernet circuit pack:

App. Code	Functional name	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
KFA13 (4 ports)	GE1/SX/4	–9.5 … −4	–17 … −12.5	7 - 8 dB

Related information

For related information, please refer to:

- *LambdaUnite® MSS Installation Guide* (Ordering codes and specifications, fiber-optic cables, attenuators),
- *LambdaUnite® MSS Applications and Planning Guide* (Technical specifications).

□

Retrieving a list of currently active loopbacks

Purpose

Use this procedure to retrieve an overview of currently active loopbacks in the system.

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 M1*** to release a cross-connection loopback.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to retrieve an overview of currently active loopbacks:

1 Select **View** → **Loopback...** from the *WaveStar*® CIT **System View** main menu.

Result:

The **View Loopback List** equipment selection window opens.

2 You can retrieve an overview of all active loopbacks (of any type) in the complete shelf, or on a certain circuit pack or port, or an overview of active cross-connection loopbacks of a particular rate in the complete shelf, or on a certain circuit pack, port or tributary:

If ...	**then ...**
you want a list of all active loopbacks (of any type) in the complete shelf	select **Shelf 1 (DUR)** from the equipment selection window, and continue with Step 3.

If …	**then …**
you want a list of all active loopbacks (of any type) on a certain circuit pack	select the desired circuit pack from the equipment selection window, and continue with Step 3.
you want a list of all active loopbacks (of any type) on a certain port	select the desired port from the equipment selection window, and continue with Step 3.
you want a list of all active cross-connection loopbacks of a particular rate in the complete shelf	select **Shelf 1 (DUR)** from the equipment selection window, and continue with Step 4.
you want a list of all active cross-connection loopbacks of a particular rate on a certain circuit pack	select the desired circuit pack from the equipment selection window, and continue with Step 4.
you want a list of all active cross-connection loopbacks of a particular rate on a certain port	select the desired port the equipment selection window, and continue with Step 4.
you want to see whether a cross-connection loopback is currently active on a certain tributary	select the desired tributary from the equipment selection window, and continue with Step 4.

3 Select **ALL** from the **Port Type/Rate Selection** drop-down list box in the **Port Type/Rate Selection** window that opens. Continue with Step 5.

4 Select the desired tributary rate from the **Port Type/Rate Selection** drop-down list box in the **Port Type/Rate Selection** window that opens. Continue with the next step.

5 Click **OK** in the **Port Type/Rate Selection** window.

Result:

The **View Loopback** window opens (the AID of the selected system component is also indicated in the window title). The currently active loopbacks (**Nearside Facility**, **Farside Facility**, **Cross Connect**) on the selected system component are displayed in a tabular form.

Additional information

Several **View Loopback** windows may be open at the same time.

6 As an option, you can store or print the currently displayed list of active loopbacks:

If …	**then …**
you want to store the 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 list	click the **Print** button and specify a printer.

7 Click **Close** to dismiss the window.

END OF STEPS

□

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
- For connecting the *WaveStar*® CIT (or *Navis*™ Optical EMS) to the system via LAN connections using a hub, the following hubs are recommeded:
  - ***Hewlett Packard:***
    J3128A / Advanced Stack Hub-8E
  - ***Allied Telesyn:***
    MR820TR
    3024SL
    MR815T
    MR415T

Safety precautions

To assure both personal safety and the proper functioning of the *LambdaUnite*® MSS system, it is imperative to review and understand these warnings and precautions prior to performing this task.

CAUTION

Possible material damage due to electrostatic discharge

Handling circuit packs or working on a LambdaUnite® MSS system can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a LambdaUnite® MSS system.

Important! If provisioning changes were made after the last backup files were created, use the appropriate *WaveStar®* CIT commands to manually apply the recent provisioning changes to the just-restored database.

Instructions Complete the following steps to manually restore a database to a network element:

1 From the **System View** main menu, enter the maintenance condition via **Fault** → **Enter/Exit Maintenance Condition...** → **Enter Maintenance Condition...**

2 Confirm the resulting system message by clicking **OK**.

3 Select **Configuration** → **Software** → **Remote Restore...** from the **System View** main menu.

Result:

The **Restore Database** window will be opened.

4 Proceed as follows:

IF	**THEN**
you want to restore the database directly from the PC where the *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.

6 Select the **FTTD** tab and specify the **TID**, presentation selector (**Psel**), session selector (**Ssel**), transport selector (**Tsel**) and the **NSAP Address** for the FTTD information.

7 Select the **FTP** tab and specify the **Server** (IP address or server name), port information (optional), User name (optional) and password (optional) for the FTP information.

Proceed with Step 8.

Important! Be careful to select the correct backup files to restore to the NE.

8 Specify the path to the folder where the backup files reside.

9 Verify your settings and correct if necessary. Then click **Restore**.

10 Confirm the resulting system message by clicking **YES**.

Result:

The **NE Data Restore in Progress** window appears. When the database restore is complete, the system will perform a reset. As a consequence, the management association between the *WaveStar*® CIT and the NE will be lost. After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar*® CIT to the NE.

11 Connect to the NE again.

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

13 Confirm the resulting system message by clicking **OK**.

The *LambdaUnite*® MSS NE will now perform a system reset. As a consequence, the management association between the *WaveStar*® CIT and the NE will be lost. After the system reset has finished, you can re-establish the management association by again connecting the *WaveStar*® CIT to the NE.

END OF STEPS

□

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.

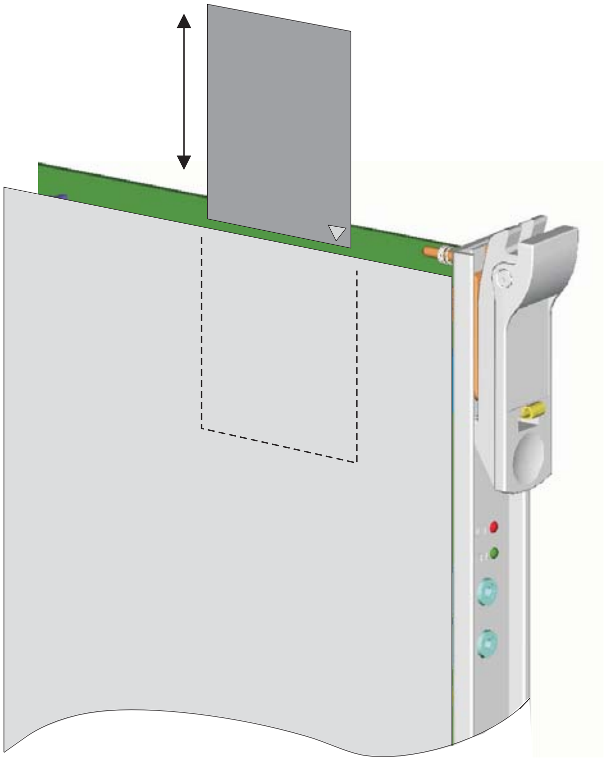
Regular database backups

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, vendor-formatted*** *CompactFlash*™ card into the drive of the PC where the database backups are stored.

2 By using the *Windows*® Explorer, copy the most recent database backup to the new *CompactFlash*™ card.

3 Unmount the *CompactFlash*™ card (“slot power off”).

4 Eject the *CompactFlash*™ card from the PC drive.

5 If not yet done, remove the Controller (CTL) where the (presumedly defective) *CompactFlash*™ card resides from its slot.

6 Eject the “old” *CompactFlash*™ card from the CTL *CompactFlash*™ drive.

7 Insert the new *CompactFlash*™ card into the CTL *CompactFlash*™ drive.

8 Re-insert the CTL.

Result:

The CTL performs a recovery which should successfully complete.

END OF STEPS

□

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" (1-20)).

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" (4-49).

2 Remove the circuit pack from its slot.

3 Cover the now unequipped slot(s) with a blank faceplate (cf. "Configuration rules" (4-60)).

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.

END OF STEPS

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)” (4-53).

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” (1-20)).

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” (4-60)), insert the replacement circuit pack.

END OF STEPS

□

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” (1-20)).

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” (4-49).

2 Remove the circuit pack from its slot.

3 Cover the now unequipped slot(s) temporarily with a blank faceplate (cf. “Configuration rules” (4-60)).

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” (4-60)).

7 Insert the new circuit pack.

If you did not pre-provision the circuit pack, then it will now be auto-provisioned.

END OF STEPS

□

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 green "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).

END OF STEPS

□

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

Purpose

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

Before you begin

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

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

Required equipment

The following equipment is required to perform this procedure:

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

Related Information

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

NE with one XC320 circuit pack to exchange

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions as described in the "Alarm Messages and Trouble Clearing Guide, Chapter 1".

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

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

2 Perform a forced switch to the worker XC320 circuit pack.

> **Important!** Make sure to perform the forced switch not on the empty slot.

3 Remove the blank faceplate of the protection slot.

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

4 Insert the spare XC320 circuit pack into this preprovisioned protection slot and wait until it finished the boot-up and comes up properly.

> **Important!** Make sure that you have inserted a XC320 circuit pack, not a XC320/A circuit pack.

5 Release the forced switch to the worker XC320 circuit pack and perform a forced switch to this new XC320 circuit pack in the protection slot.

Check that the traffic is ok.

6 Remove the other XC320 circuit pack of the worker slot and deprovision the slot by *WaveStar*® CIT.

7 Insert the new XC320/A circuit pack into this slot and wait until it finished the boot-up and comes up properly.

8 Release the forced switch to the active XC320 and perform a forced switch to this new XC320/A circuit pack in the worker slot.

Check that the traffic is ok.

9 Remove the XC320 circuit pack of the protection slot and deprovision this slot by *WaveStar*® CIT.

10 Cover the protecion slot with a blank faceplate.

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

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

END OF STEPS

NE with two XC320 circuit packs to exchange

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Hold circuit packs only at the edges or on the insertion and removal facilities. Always observe the ESD instructions as described in the "Alarm Messages and trouble clearing Guide, Chapter 1".

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

1 Using the *WaveStar*® CIT, perform a forced switch to the worker XC320 circuit pack.

2 Remove the XC320 circuit pack of the protection slot and deprovision this slot by *WaveStar*® CIT.

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

3 Insert the XC320/A circuit pack into this preprovisioned protection slot and wait until it finished the boot-up and comes up properly.

4 Release the forced switch to the worker XC320 circuit pack and perform a forced switch to this new XC320/A circuit pack in the protection slot, check, that the traffic is ok.

5 Remove the other XC320 circuit pack of the (now) protection slot and deprovision the slot by *WaveStar*® CIT.

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

6 Insert the new XC320/A circuit pack into this slot and wait until it finished the boot-up and comes up properly.

7 Release the forced switch to the worker XC320.

END OF STEPS

□

Replacing a defective optical fiber

Purpose

Use this procedure to replace a defective optical fiber.

Before you begin

You or a service technician need to be on-site at the NE to replace a defective optical fiber.

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 fiber.
- An edge cutter.

Instructions

1 Disconnect the defective optical fiber from the circuit pack port.

2 Cut off the optical fiber connector.

CAUTION

Cutting the wrong fiber will be traffic affecting!

Make sure to cut the defective fiber only.

3 Cut the defective optical fiber at the subrack entrance.

4 Remove the fiber.

5 Route the new fiber on top of the existing fiber bundles.

6 Connect the new fiber to the circuit pack port.

END OF STEPS

□

Configuration rules

Supported LXC configurations

These LXC configurations are supported:

- LXC configuration with XC160 cross-connect and timing unit(s)
- LXC configuration with XC320 cross-connect and timing unit(s)
- LXC configuration supporting ONNS applications

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

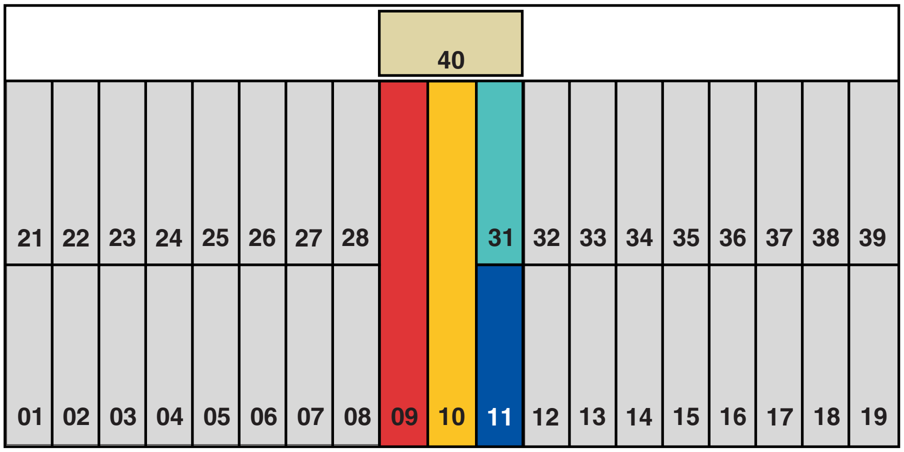
DUR shelf

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

As a general rule, a DUR shelf is designed such that optical interfaces can be accessed from the front while electrical interfaces can be accessed from the rear side.

Available slots on the front side

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



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

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

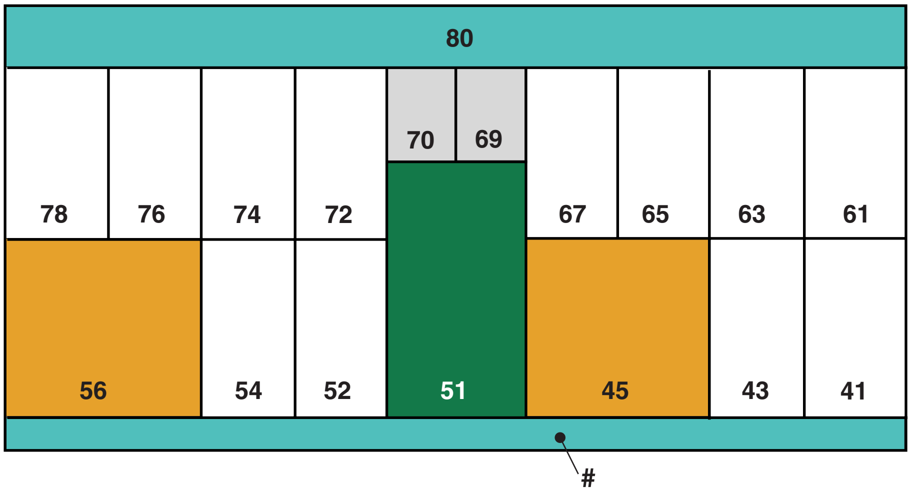
Slots		**Slot equipage**
1-8 12-19 21-28 32-39	Universal slots[1]	Universal slots can be used for any mix of port units:[2] • Electrical 155-Mbit/s port units (EP155…)[3]For the electrical 155-Mbit/s port units, there are dedicated slots for the electrical connection interfaces (ECI) on the rear side of the shelf. • Optical 155-Mbit/s port units (OP155…) • 622-Mbit/s port units (OP622…) • 2.5-Gbit/s port units (OP2G5…) • 10-Gbit/s port units (OP10…) • 40-Gbit/s port units (OP40…)An OP40 port unit occupies four universal slots. • 1-Gigabit Ethernet interface (GE1) • 10-Gigabit Ethernet WANPHY interface (realised on an OP10 port unit)
09	XC (W) slot	Cross-connect and timing unit (XC) – worker (W).[4] This XC is paired with the XC in the protection slot in a 1+1 non-revertive protection mode configuration. Furthermore, the XC contains the timing generator function for the NE.
10	XC (P) slot	Cross-connect and timing unit (XC) – protection (P).[4] This XC is paired with the XC in the worker slot in a 1+1 non-revertive protection mode configuration. Furthermore, the XC contains the timing generator function for the NE.
11	CTL (W) slot	Controller (CTL) – worker (W).[4] Controller including the non-volatile memory (NVM, *CompactFlash*™ card). After initial system startup (power on), this Controller takes on the active role.
31	CTL (P) slot	Controller (CTL) – protection (P).[4] Optionally, a second Controller can be equipped for CTL equipment protection (duplex control). After initial system startup (power on), this Controller takes on the standby role.
40		User panel
The slots 20, 29, and 30 do ***not*** exist.		

Notes:

1. Slots for port units are called “universal slots”. The maximal transmission capacity of a port unit in a universal slot can be 20 Gbit/s.
2. Each port unit occupies one universal slot, if not stated otherwise.
3. EP155 circuit packs can only be used in a DUR shelf of type DUR/2.
4. The terms “worker” and “protection” are used to describe the static role within a protection, whereas the terms “active” and “standby” are used to describe the current (dynamic) role.

Available slots on the rear side

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



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

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

Slots	Slot equipage
41	– (reserved for future applications)
43	– (reserved for future applications)

Slots	Slot equipage
45	Power interface (PI A) The PI/100 variant of the power interface requires a wider slot than the PI/- variant (as indicated by the dashed lines).
51	Connection interface of the Controller (CI-CTL)
52	– (reserved for future applications)
54	– (reserved for future applications)
56	Power interface (PI B) The PI/100 variant of the power interface requires a wider slot than the PI/- variant (as indicated by the dashed lines).
61, 63, 65, 67	Electrical connection interfaces (ECI)
69	Timing interface (TI A)
70	Timing interface (TI B)
72, 74, 76, 78	Electrical connection interfaces (ECI)
80	Fan unit

General configuration rules and guidelines

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

1. Use the configurator tool to verify if a certain subrack equipage is permitted.
   For example: Do not install a GE1 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. 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.
4. ***Do not*** insert circuit packs simultaneously. When several circuit packs have to be inserted, they should be inserted one after the other, with intervals of at least one second.

5. Cover unequipped slots and OM sockets with blank faceplates to guarantee proper cooling, airflow and EMC behavior. Do not leave unequipped slots uncovered for more than ***ten*** (10) minutes to avoid overheating of the system. Disregarding this warning could cause the system to fail and voids warranty.
   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.
6. 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.

Specific configuration rules and guidelines

Specific configuration rules and guidelines apply to the different *LambdaUnite*® MSS system configurations that can be realized.

These specific configuration rules and guidelines depend on the type of cross-connect and timing unit used. Therefore, please refer to:

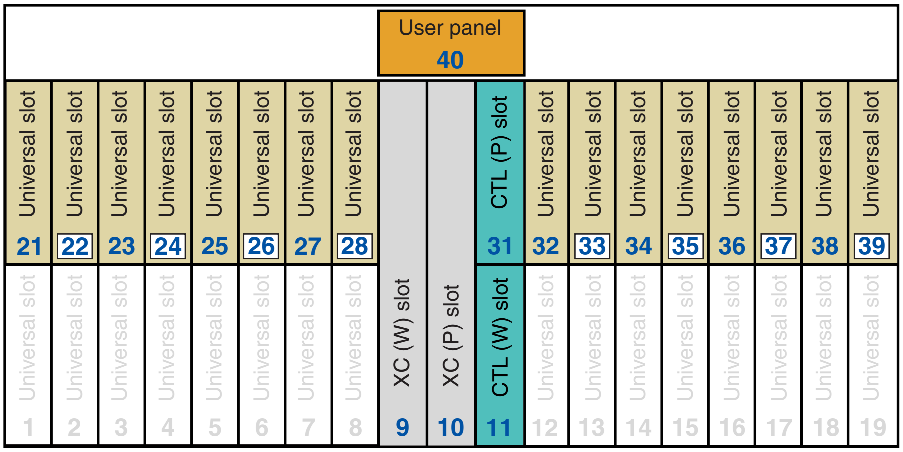
- "LXC configuration with XC160" (4-64)
- "LXC configuration with XC320" (4-65)
- "LXC configuration supporting ONNS applications" (4-66)

LXC configuration with XC160

XC160 cross-connect and timing units have a switching capacity of 160 Gbit/s.

Observe these rules and guidelines with regard to an LXC configuration with XC160 cross-connect and timing unit(s):

1. It is recommended to use ***two*** XC160 cross-connect and timing units. Thus, both the cross-connnect function as well as the timing function are automatically 1+1 equipment protected. However, an LXC configuration with a single XC160 cross-connect and timing unit is also supported.
2. Port units can only be equipped in the upper row of the DUR shelf, i.e. in the universal slots 21 … 28 and 32 … 39.
   For port units with a transmission capacity of 20 Gbit/s (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules), only the universal slots 22, 24, 26, 28, 33, 35, 37, and 39 can be used. The slot left to a slot where such a port unit is installed has to remain unequipped.
   Cover all unequipped slots with blank faceplates (see “General configuration rules and guidelines” (4-63)).
3. XC160 cross-connect and timing units support ONNS applications (cf. “LXC configuration supporting ONNS applications” (4-66)).



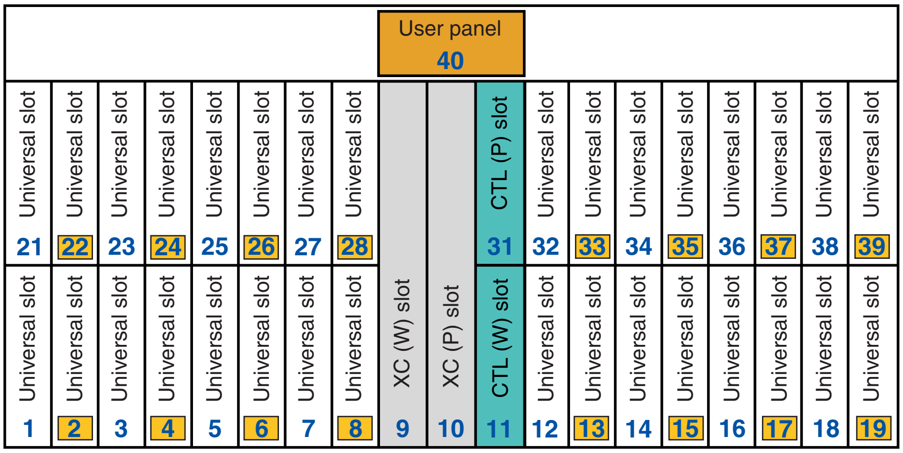
front view

LXC configuration with XC320

XC320 cross-connect and timing units have a switching capacity of 320 Gbit/s.

Observe these rules and guidelines with regard to an LXC configuration with XC320 cross-connect and timing unit(s):

1. It is recommended to use ***two*** XC320 cross-connect and timing units. Thus, both the cross-connnect function as well as the timing function are automatically 1+1 equipment protected. However, an LXC configuration with a single XC320 cross-connect and timing unit is also supported.
2. For port units with a transmission capacity of 20 Gbit/s (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules), only the universal slots 2, 4, 6, 8, 13, 15, 17, 19, 22, 24, 26, 28, 33, 35, 37, and 39 can be used. The slot left to a slot where such a port unit is installed has to remain unequipped. Cover all unequipped slots with blank faceplates (see "General configuration rules and guidelines" (4-63)).
3. Only the XC320/B variants of the XC320 cross-connect and timing units support ONNS applications (cf. "LXC configuration supporting ONNS applications" (4-66)).



front view

LXC configuration supporting ONNS applications

A special shelf equipage is required for ONNS applications.

Observe these rules and guidelines with regard to an LXC configuration supporting ONNS applications:

1. Only Controllers of type ***CTL/2*** and cross-connect and timing units of type ***XC320/B or XC160*** can be used for ONNS applications.
   It is recommended to use ***two*** Controllers of type CTL/2 (duplex control) and ***two*** XC320/B or two XC160 cross-connect and timing units. Thus, both the Controllers as well as the cross-connect and timing units are automatically 1+1 equipment protected.
2. All available port units can be used for ONNS applications.
   The permissible shelf equipage depends on the type of XC cross-connect and timing unit used:
   - XC160
     Port units can only be equipped in the upper row of the DUR shelf, i.e. in the universal slots 21 … 28 and 32 … 39.
     For port units with a transmission capacity of 20 Gbit/s (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules), only the universal slots 22, 24, 26, 28, 33, 35, 37, and 39 can be used. The slot left to a slot where such a port unit is installed has to remain unequipped.
   - XC320/B
     For port units with a transmission capacity of 20 Gbit/s (for example an OP2G5D/PAR8 parent board, equipped with 8 optical modules), only the universal slots 2, 4, 6, 8, 13, 15, 17, 19, 22, 24, 26, 28, 33, 35, 37, and 39 can be used. The slot left to a slot where such a port unit is installed has to remain unequipped.

   Cover all unequipped slots with blank faceplates (see "General configuration rules and guidelines" (4-63)).

□

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.

END OF STEPS

□

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.

END OF STEPS

□

Cross-connection loopbacks

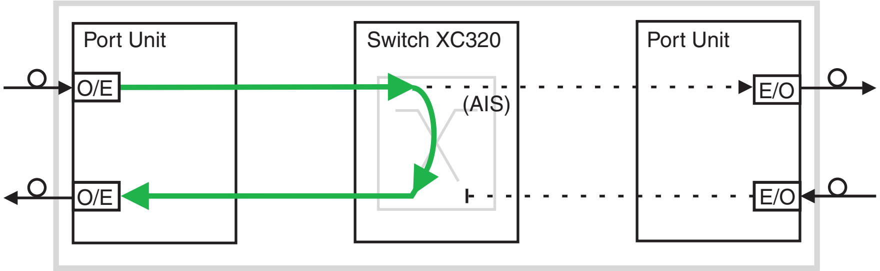
Overview

Cross-connection loopbacks can be used to analyze tributary signals.

Functional principle

A cross-connection loopback can be regarded as a unidirectional cross-connection from an input to its related output. There are no bidirectional cross-connection loopbacks.

The following schematical diagram depicts the functional principle of cross-connection loopbacks.



The selected input tributary is looped back (cross-connected) in the XC320 switch unit to the output of the same tributary.

> **Important!** For cross connection loopbacks it is possible to specify a tributary rate of a different standard than the port interface standard, for example an SDH rate on a SONET port. In the resulting notifications or responses the rate is determined by the interface standard of the port, and then differs from the rate specified for the cross-connection loopback. Therefore, it is recommended ***not*** to use an SDH tributary rate on a SONET port, and vice versa.

Dependence on the tributary operation mode

Cross-connection loopbacks can be switched on tributaries on ports configured for fixed-rate tributary operation, and on tributaries on ports configured for adaptive-rate tributary operation:

- For tributaries on ports configured for ***fixed-rate*** tributary operation, cross-connection loopbacks are only possible if the rate of the cross-connection loopback is compatible to the rates defined for the corresponding input and output tributaries. Compatible means, that, for example, a VC-4 cross-connection loopback can be switched on a VC-4 tributary or on an STS-3c tributary and vive versa.
- For tributaries on ports configured for ***adaptive-rate*** tributary operation, cross-connection loopbacks are only possible if the rate of the cross-connection loopback is supported by the corresponding port, and if the tributary boundary is compatible with the requested loopback rate. Compatible means, that, for example, for a VC-4 or STS-3c cross-connection loopback, the corresponding tributary must start at a position where also a VC-4 or STS-3c tributary would start (tributary positions 1, 4, 7, 10 … for STS-3c tributaries, or the corresponding timeslots for VC-4 tributaries, cf. “SDH/SONET tributary numbering” (4-79)).

This implies, that the rates of the corresponding input and output tributaries must be configured to the same value.

Normal cross-connection loopbacks

A normal cross-connection loopback on a port configured for ***fixed-rate*** tributary operation is only possible, if there are no existing cross-connections for the corresponding tributary.

A normal cross-connection loopback on a port configured for ***adaptive-rate*** tributary operation is only possible, if there are no existing cross-connections for the corresponding tributary, and if the tributary, for which the loopback is requested, does not overlap with any existing cross-connection.

Forced cross-connection loopbacks

By means of a forced cross-connection loopback on a port configured for ***fixed-rate*** tributary operation, it is possible to perform a cross-connection loopback even if there is an existing cross-connection for the corresponding tributary. Existing cross-connections are preempted when a forced cross-connection loopback is performed. Preempted means that AIS is inserted in the downstream direction, and the signal in the upstream direction (in the case of a bidirectional cross-connection) is terminated.

Preempting existing cross-connections by means of a forced cross-connection loopback on a port configured for ***adaptive-rate*** tributary operation is only possible, if the rate of the existing cross-connection and the rate of the requested cross-connection loopback are equal. This implies in particular, that forced cross-connection loopbacks are not possible for tributary rates smaller than the rate of the existing adaptive-rate cross-connection itself.

When the cross-connection loopback is released, any previously existing cross-connections are automatically restored.

> **Important!** It is ***not*** possible to switch a cross-connection on a tributary while a cross-connection loopback is active on this tributary.

Cross-connection loopbacks on path-protected cross-connections

Performing a forced cross-connection loopback on the working or protection leg of a path-protected cross-connection leads to a Signal Fail (SF) condition on the corresponding leg of the path-protected cross-connection. An SF condition on the working leg causes a protection switch. An SF condition on the protection leg prevents a protection switch from the working to the protection leg.

“ABN” LED

The yellow “ABN” LED on the *LambdaUnite*® MSS user panel is lit as long as a cross-connection loopback is active.

□

Facility loopbacks

Overview

Facility loopbacks are loopbacks switched on whole ports. They make it possible to verify the correct system operation and may facilitate troubleshooting of problems.

There are two types of facility loopbacks:

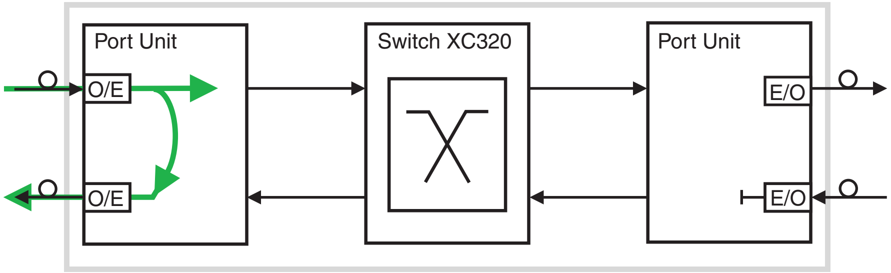
- Near-side facility loopbacks
  The signal on the input port is looped to the corresponding output port with transpassing as few NE components as possible.
  Near-side facility loopbacks can be switched on all out-of-service optical interface ports.
- Far-side facility loopbacks
  The transmission signal to the output port in the NE is looped back to the corresponding input port with passing through as many equipment components as possible.
  Far-side facility loopbacks can be switched on all out-of-service optical interface ports as well as on 1-Gbit/s Ethernet ports.

Near-side facility loopbacks

Near-side facility loopbacks can be used to test the correct cabling between two network elements including the involved interface ports.

Functional principle

The following schematical diagram depicts the functional principle of near-side facility loopbacks.



The incoming signal at the input port is, after optical-to-electrical conversion, entirely looped back to the output port.

Near-side facility loopbacks are characterized as follows:

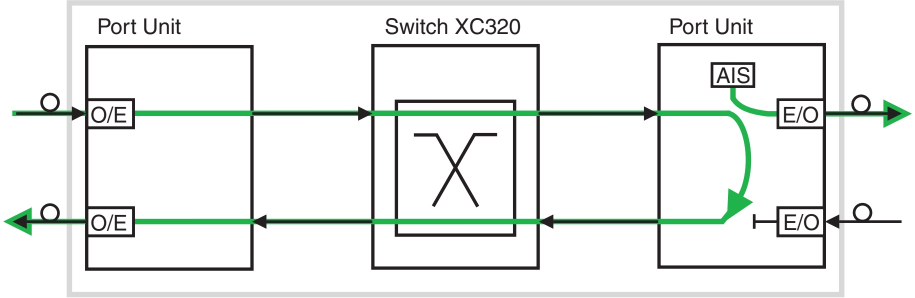
- Near-side facility loopbacks are transparent, the signal transmitted in the downstream direction is not changed.
- The signal transmitted in the original (downstream) direction is different from the signal looped back. Particular Section/RS and Line/MS Overhead bytes, such as those used for frame alignment (A1, A2) or bit error monitoring (B1, B2) for example, are not looped back but processed. The Path Overhead (POH) and the payload signal, however, are looped back unchanged.
- The incoming signal in the upstream direction is terminated during the loopback.

Far-side facility loopbacks

Far-side facility loopbacks can be used to test signal paths through a network element.

Functional principle

The following schematical diagram depicts the functional principle of far-side facility loopbacks.



Far-side facility loopbacks are characterized as follows:

- Far-side facility loopbacks are non-transparent, the signal transmitted in the original (downstream) direction is different from the signal looped back. Line AIS (SONET) or MS-AIS (SDH) respectively is inserted into the outgoing signal in the downstream direction during the loopback.
- The signal is not changed before it is looped back.
- The incoming signal in the upstream direction is terminated during the loopback.

Configuration Rules

Consider the following configuration rules to perform facility loopbacks:

- Before a (near-side or far-side) facility loopback can be performed, the corresponding port must be set out-of-service.
- When a (near-side or far-side) facility loopback is active, no line timing references can be assigned.
- When a line timing reference is assigned, no facility loopbacks can be performed.
- After an upgrade of the NE software (Release 2.1 → Release 3.0) perform a full reset of all installed OP155 circuit packs. Otherwise, it may happen that near-side facility loopbacks are only possible on ports 1 and 9 of the OP155 circuit packs.

Related information

Please refer to:

- "Performing facility loopbacks" (4-27)
- "Releasing a facility loopback" (4-30)

□

SDH/SONET tributary numbering

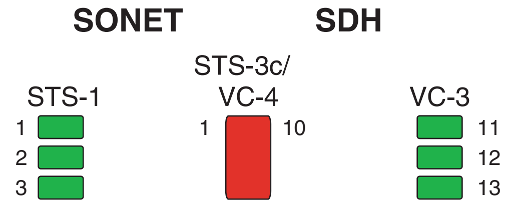
Overview

In this section, the SDH and SONET tributary numbering scheme will be described in detail.

A special numbering format is used for SDH tributaries whereas the SONET tributary numbering format is relatively straight-forward. Moreover, the tributary numbering depends on the port rate, and therefore the subsequent description is structured in accordance with the *LambdaUnite*® MSS SDH/SONET port rates.

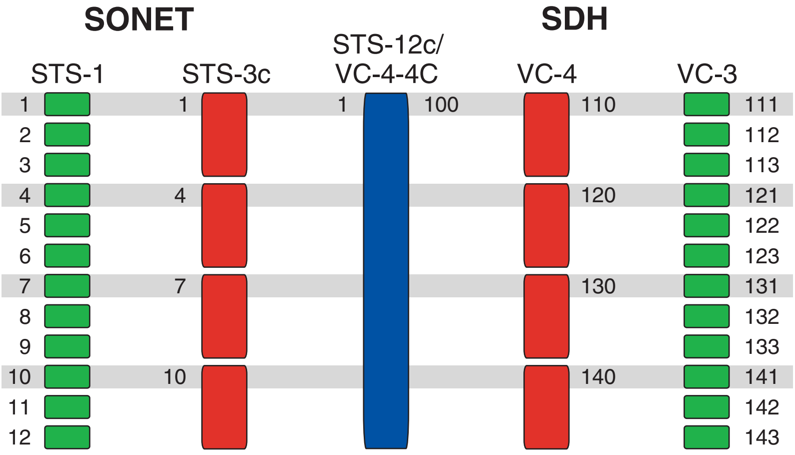
OC-3/STM-1 port

The following figure shows the possible substructuring of an OC-3/STM-1 signal and the associated SDH and SONET tributary numbering schemes.

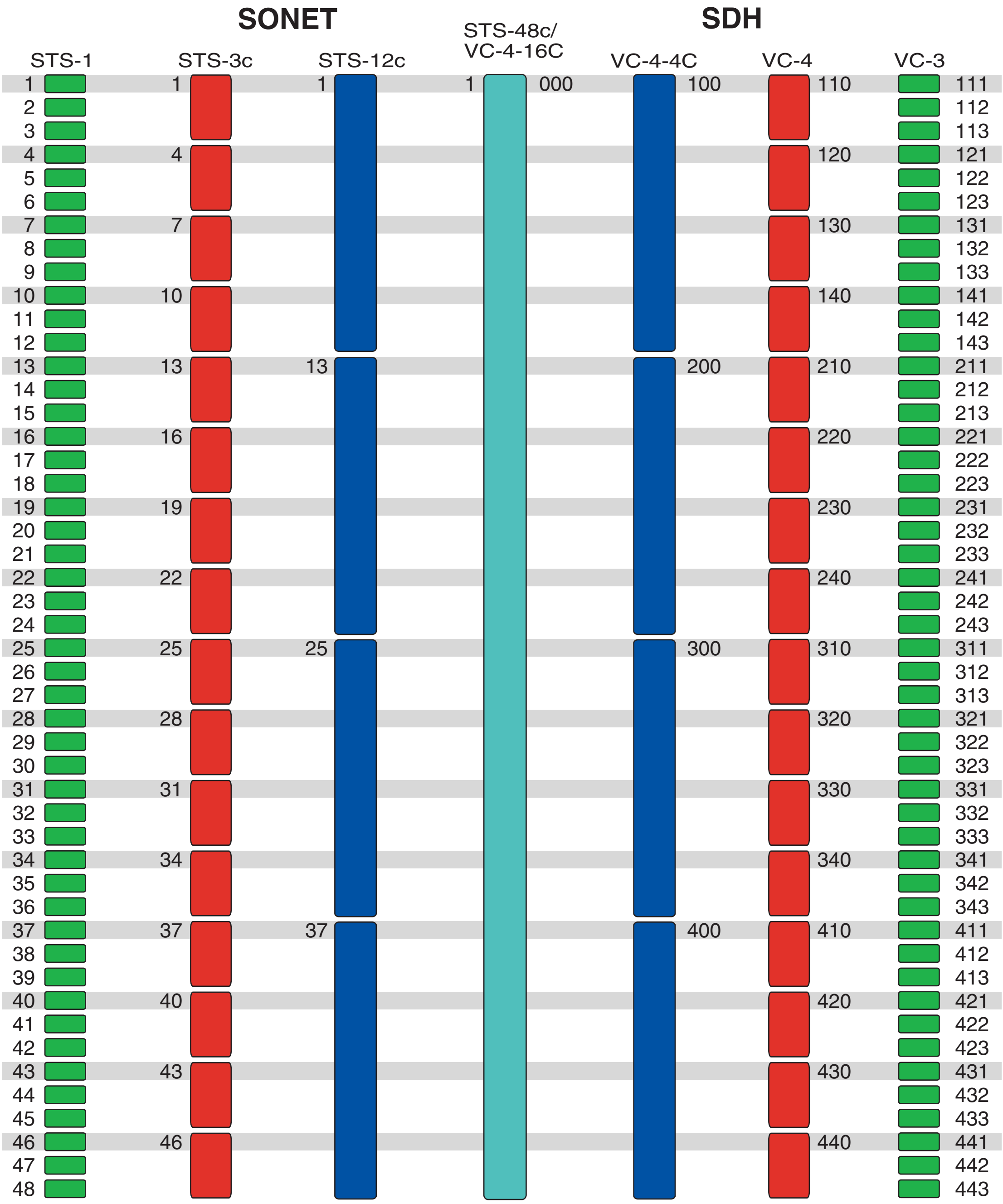


OC-12/STM-4 port

The following figure shows the possible substructuring of an OC-12/STM-4 signal and the associated SDH and SONET tributary numbering schemes.

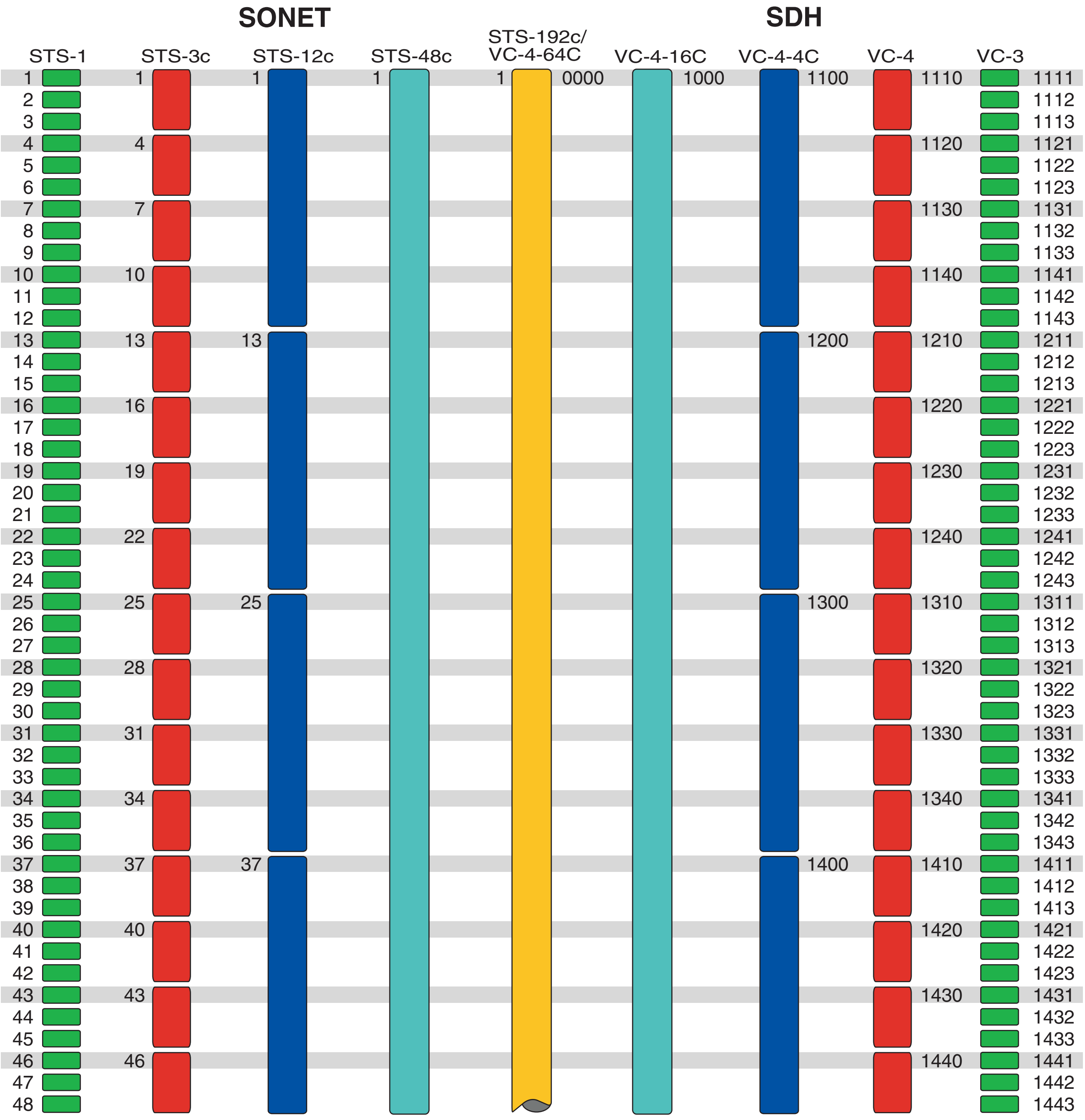


OC-48/STM-16 port The following figure shows the possible substructuring of an OC-48/STM-16 signal and the associated SDH and SONET tributary numbering schemes.



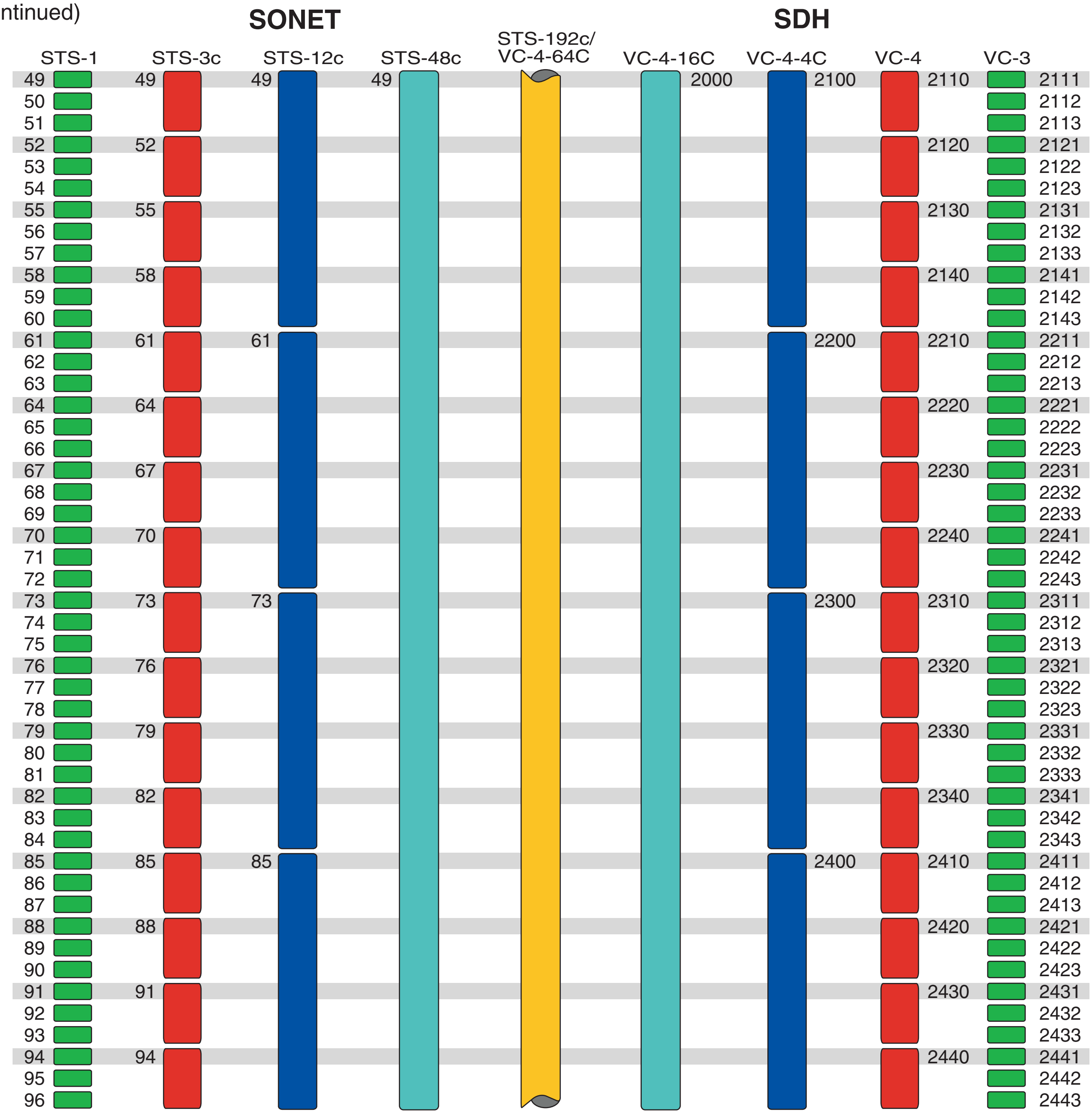
OC-192/STM-64 port

The following figure shows the possible substructuring of an OC-192/STM-64 signal and the associated SDH and SONET tributary numbering schemes.



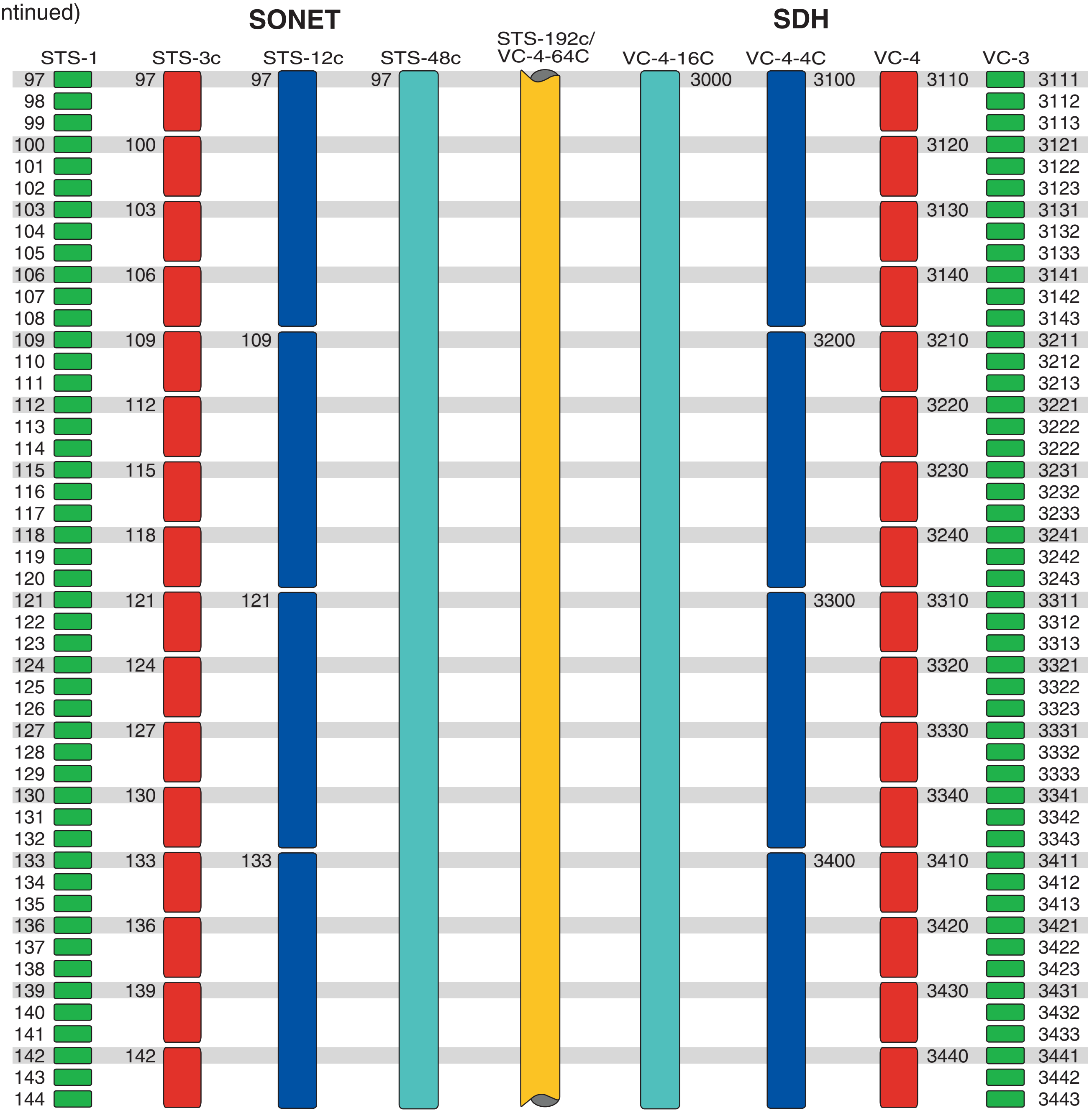
		SONET					SDH	
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
1	1	1	1	1 0000	1000	1100	1110	1111
2								1112
3								1113
4	4						1120	1121
5								1122
6								1123
7	7						1130	1131
8								1132
9								1133
10	10						1140	1141
11								1142
12								1143
13	13	13				1200	1210	1211
14								1212
15								1213
16	16						1220	1221
17								1222
18								1223
19	19						1230	1231
20								1232
21								1233
22	22						1240	1241
23								1242
24								1243
25	25	25				1300	1310	1311
26								1312
27								1313
28	28						1320	1321
29								1322
30								1323
31	31						1330	1331
32								1332
33								1333
34	34						1340	1341
35								1342
36								1343
37	37	37				1400	1410	1411
38								1412
39								1413
40	40						1420	1421
41								1422
42								1423
43	43						1430	1431
44								1432
45								1433
46	46						1440	1441
47								1442
48								1443

(continued)



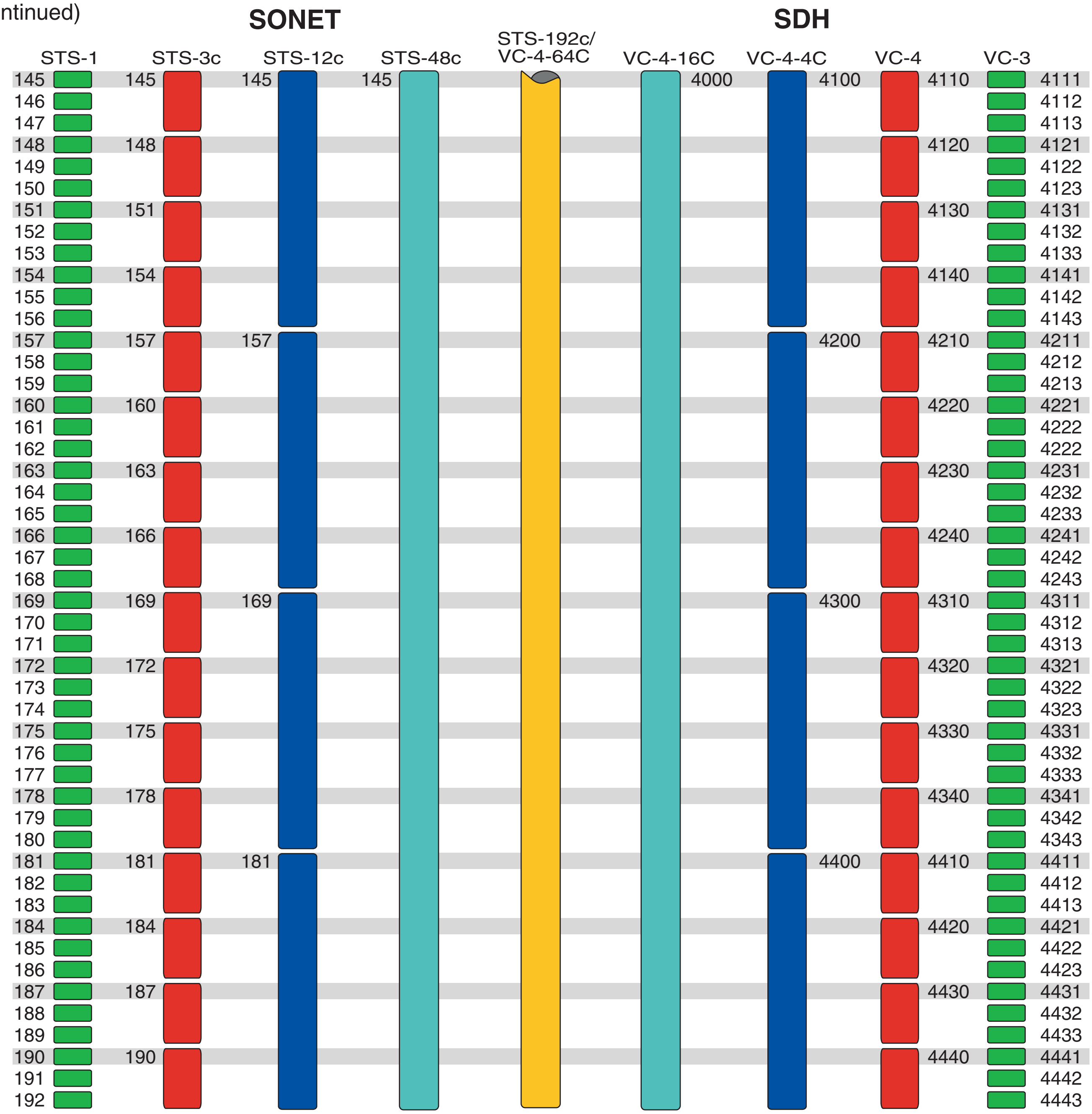
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
49	49	49	49		2000	2100	2110	2111
50								2112
51								2113
52	52						2120	2121
53								2122
54								2123
55	55						2130	2131
56								2132
57								2133
58	58						2140	2141
59								2142
60								2143
61	61	61				2200	2210	2211
62								2212
63								2213
64	64						2220	2221
65								2222
66								2223
67	67						2230	2231
68								2232
69								2233
70	70						2240	2241
71								2242
72								2243
73	73	73				2300	2310	2311
74								2312
75								2313
76	76						2320	2321
77								2322
78								2323
79	79						2330	2331
80								2332
81								2333
82	82						2340	2341
83								2342
84								2343
85	85	85				2400	2410	2411
86								2412
87								2413
88	88						2420	2421
89								2422
90								2423
91	91						2430	2431
92								2432
93								2433
94	94						2440	2441
95								2442
96								2443

(continued)



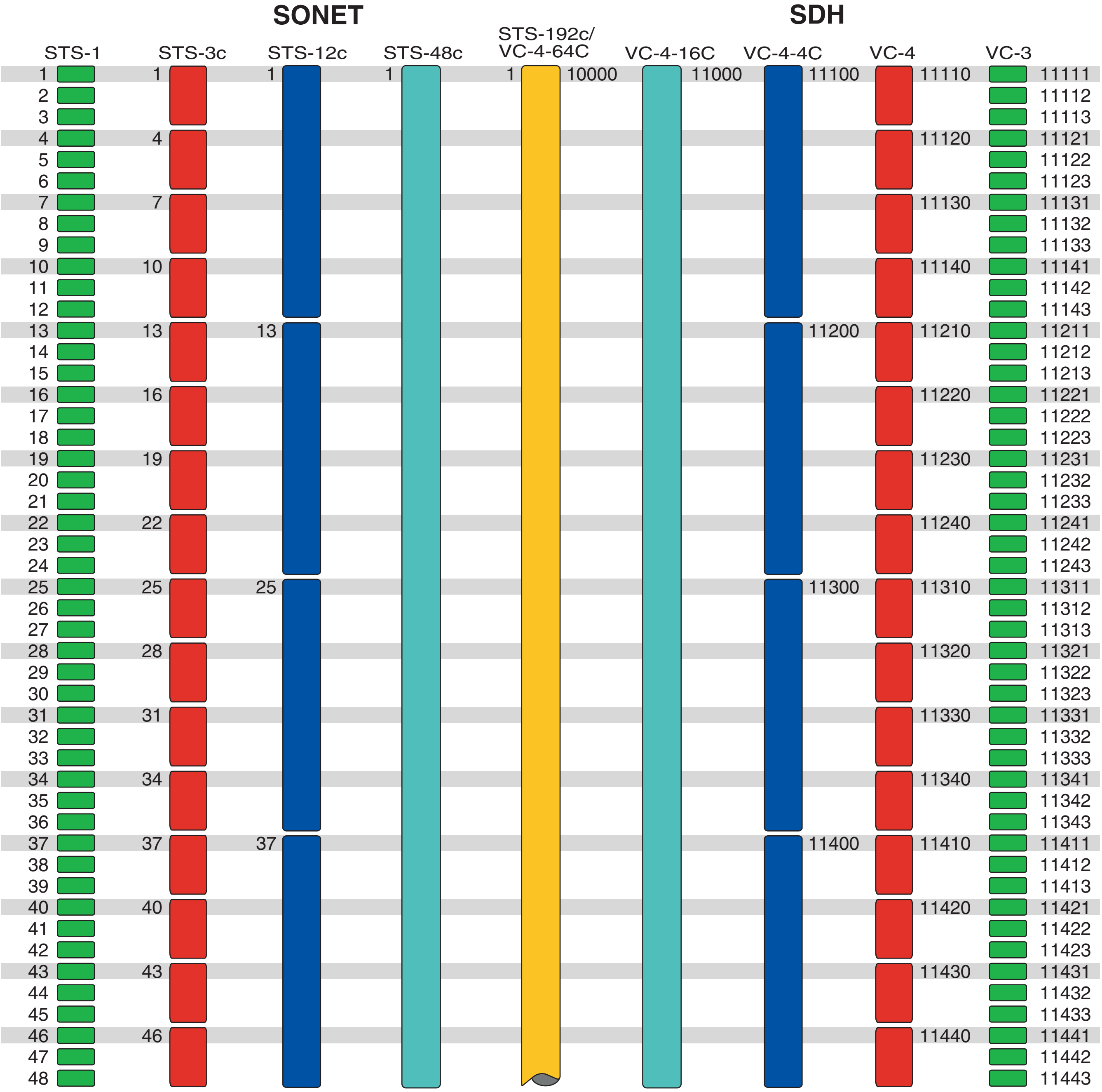
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
97	97	97	97		3000	3100	3110	3111
98								3112
99								3113
100	100						3120	3121
101								3122
102								3123
103	103						3130	3131
104								3132
105								3133
106	106						3140	3141
107								3142
108								3143
109	109	109				3200	3210	3211
110								3212
111								3213
112	112						3220	3221
113								3222
114								3222
115	115						3230	3231
116								3232
117								3233
118	118						3240	3241
119								3242
120								3243
121	121	121				3300	3310	3311
122								3312
123								3313
124	124						3320	3321
125								3322
126								3323
127	127						3330	3331
128								3332
129								3333
130	130						3340	3341
131								3342
132								3343
133	133	133				3400	3410	3411
134								3412
135								3413
136	136						3420	3421
137								3422
138								3423
139	139						3430	3431
140								3432
141								3433
142	142						3440	3441
143								3442
144								3443

(continued)



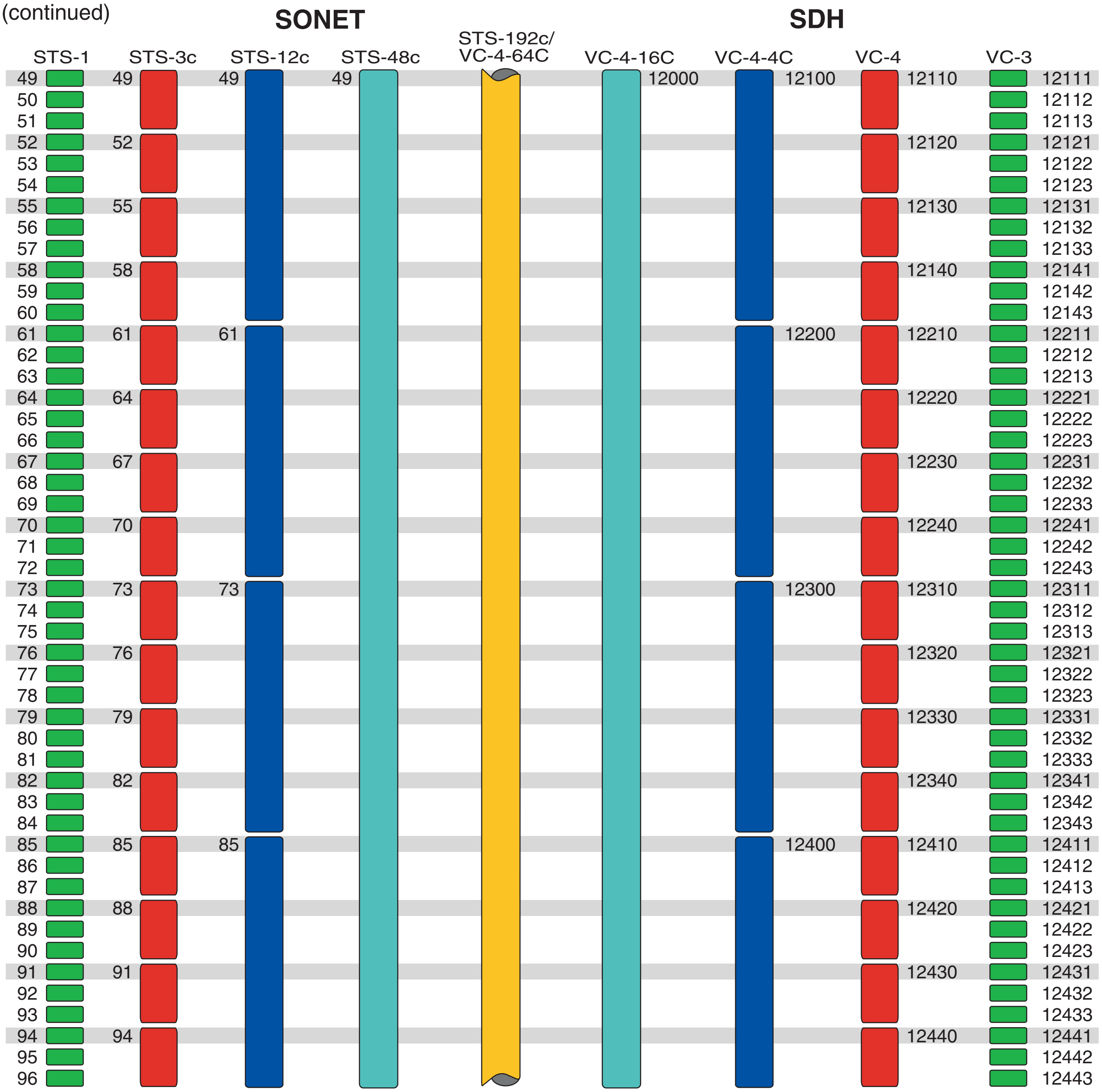
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
145	145	145	145		4000	4100	4110	4111
146								4112
147								4113
148	148						4120	4121
149								4122
150								4123
151	151						4130	4131
152								4132
153								4133
154	154						4140	4141
155								4142
156								4143
157	157	157				4200	4210	4211
158								4212
159								4213
160	160						4220	4221
161								4222
162								4222
163	163						4230	4231
164								4232
165								4233
166	166						4240	4241
167								4242
168								4243
169	169	169				4300	4310	4311
170								4312
171								4313
172	172						4320	4321
173								4322
174								4323
175	175						4330	4331
176								4332
177								4333
178	178						4340	4341
179								4342
180								4343
181	181	181				4400	4410	4411
182								4412
183								4413
184	184						4420	4421
185								4422
186								4423
187	187						4430	4431
188								4432
189								4433
190	190						4440	4441
191								4442
192								4443

OC-768/STM-256 port The following figure shows the possible substructuring of an OC-768/STM-256 signal and the associated SDH and SONET tributary numbering schemes.



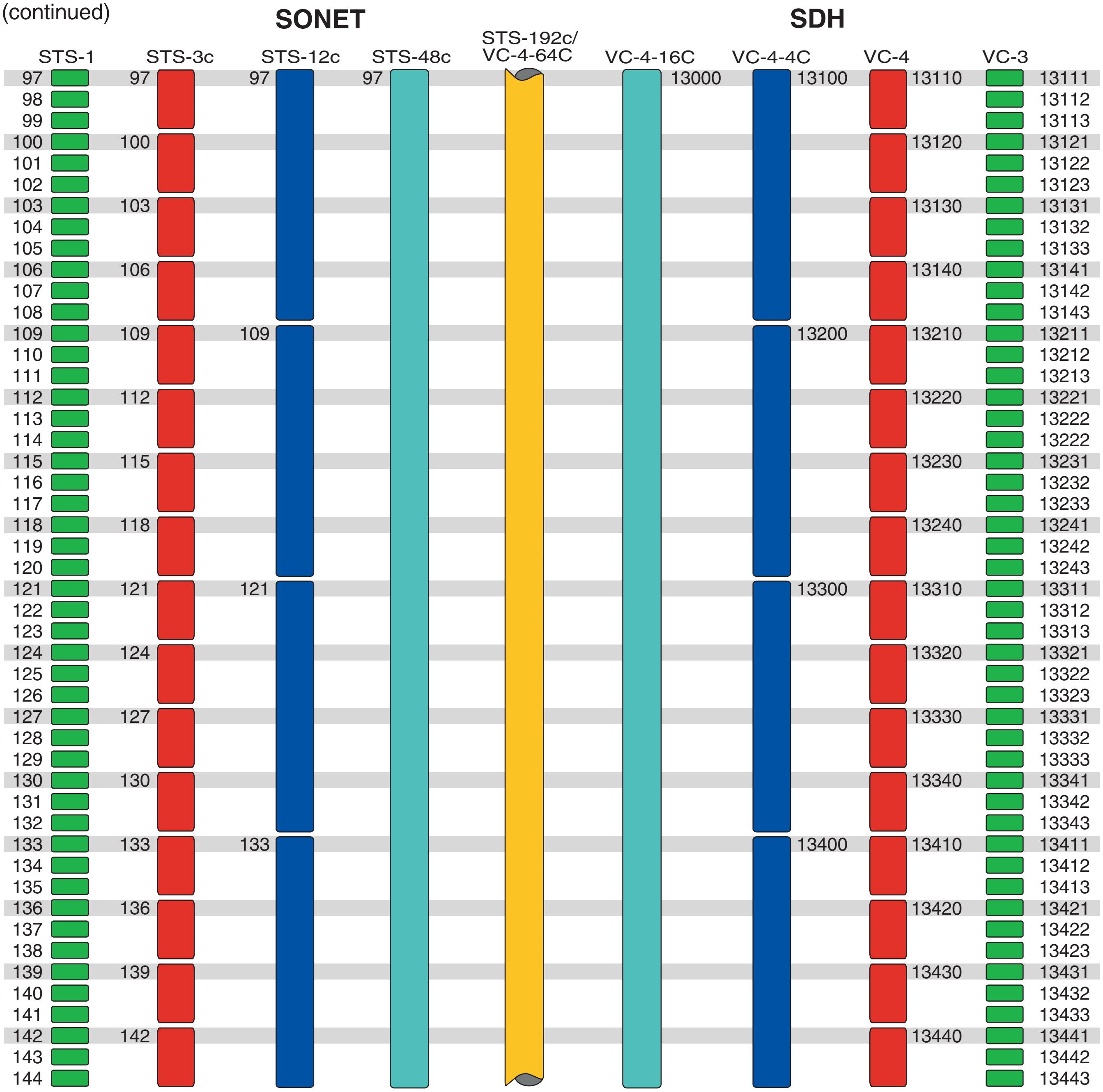
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
1	1	1	1	1 10000	11000	11100	11110	11111
2								11112
3								11113
4	4						11120	11121
5								11122
6								11123
7	7						11130	11131
8								11132
9								11133
10	10						11140	11141
11								11142
12								11143
13	13	13				11200	11210	11211
14								11212
15								11213
16	16						11220	11221
17								11222
18								11223
19	19						11230	11231
20								11232
21								11233
22	22						11240	11241
23								11242
24								11243
25	25	25				11300	11310	11311
26								11312
27								11313
28	28						11320	11321
29								11322
30								11323
31	31						11330	11331
32								11332
33								11333
34	34						11340	11341
35								11342
36								11343
37	37	37				11400	11410	11411
38								11412
39								11413
40	40						11420	11421
41								11422
42								11423
43	43						11430	11431
44								11432
45								11433
46	46						11440	11441
47								11442
48								11443

(continued)



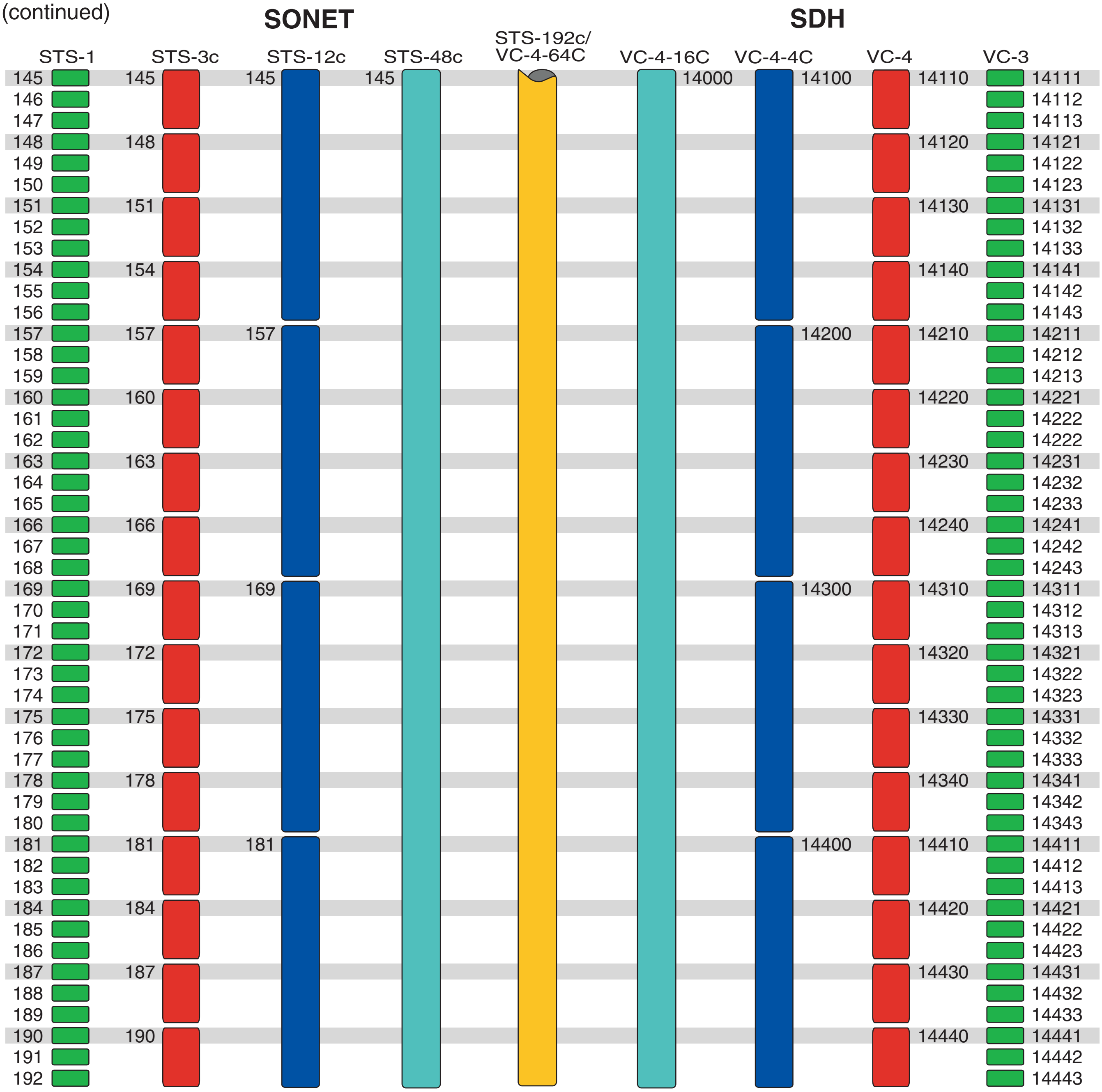
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
49	49	49	49		12000	12100	12110	12111
50								12112
51								12113
52	52						12120	12121
53								12122
54								12123
55	55						12130	12131
56								12132
57								12133
58	58						12140	12141
59								12142
60								12143
61	61	61				12200	12210	12211
62								12212
63								12213
64	64						12220	12221
65								12222
66								12223
67	67						12230	12231
68								12232
69								12233
70	70						12240	12241
71								12242
72								12243
73	73	73				12300	12310	12311
74								12312
75								12313
76	76						12320	12321
77								12322
78								12323
79	79						12330	12331
80								12332
81								12333
82	82						12340	12341
83								12342
84								12343
85	85	85				12400	12410	12411
86								12412
87								12413
88	88						12420	12421
89								12422
90								12423
91	91						12430	12431
92								12432
93								12433
94	94						12440	12441
95								12442
96								12443

(continued)



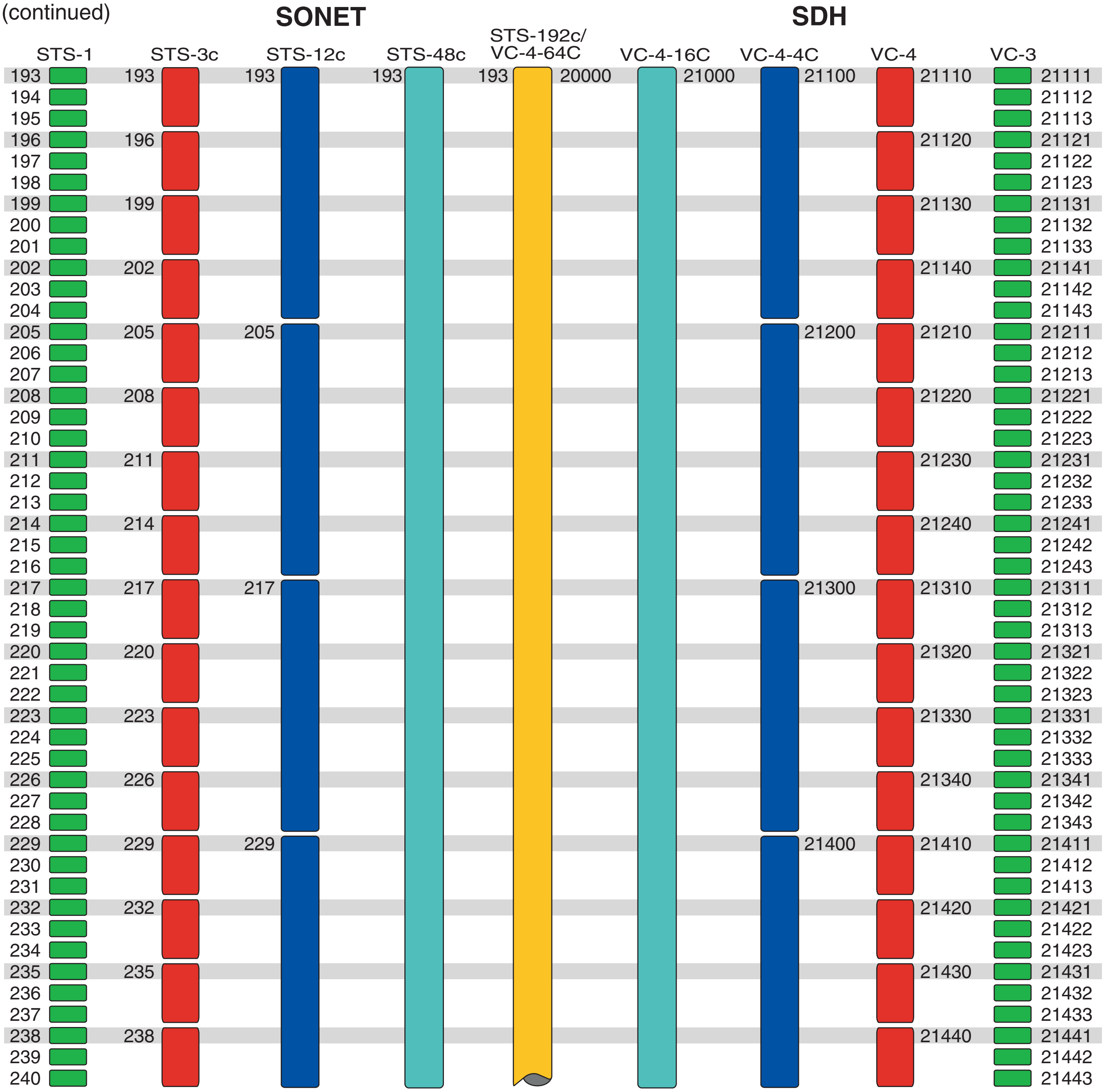
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
97	97	97	97		13000	13100	13110	13111
98								13112
99								13113
100	100						13120	13121
101								13122
102								13123
103	103						13130	13131
104								13132
105								13133
106	106						13140	13141
107								13142
108								13143
109	109	109				13200	13210	13211
110								13212
111								13213
112	112						13220	13221
113								13222
114								13222
115	115						13230	13231
116								13232
117								13233
118	118						13240	13241
119								13242
120								13243
121	121	121				13300	13310	13311
122								13312
123								13313
124	124						13320	13321
125								13322
126								13323
127	127						13330	13331
128								13332
129								13333
130	130						13340	13341
131								13342
132								13343
133	133	133				13400	13410	13411
134								13412
135								13413
136	136						13420	13421
137								13422
138								13423
139	139						13430	13431
140								13432
141								13433
142	142						13440	13441
143								13442
144								13443

(continued)



SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
145	145	145	145		14000	14100	14110	14111
146								14112
147								14113
148	148						14120	14121
149								14122
150								14123
151	151						14130	14131
152								14132
153								14133
154	154						14140	14141
155								14142
156								14143
157	157	157				14200	14210	14211
158								14212
159								14213
160	160						14220	14221
161								14222
162								14222
163	163						14230	14231
164								14232
165								14233
166	166						14240	14241
167								14242
168								14243
169	169	169				14300	14310	14311
170								14312
171								14313
172	172						14320	14321
173								14322
174								14323
175	175						14330	14331
176								14332
177								14333
178	178						14340	14341
179								14342
180								14343
181	181	181				14400	14410	14411
182								14412
183								14413
184	184						14420	14421
185								14422
186								14423
187	187						14430	14431
188								14432
189								14433
190	190						14440	14441
191								14442
192								14443

(continued)



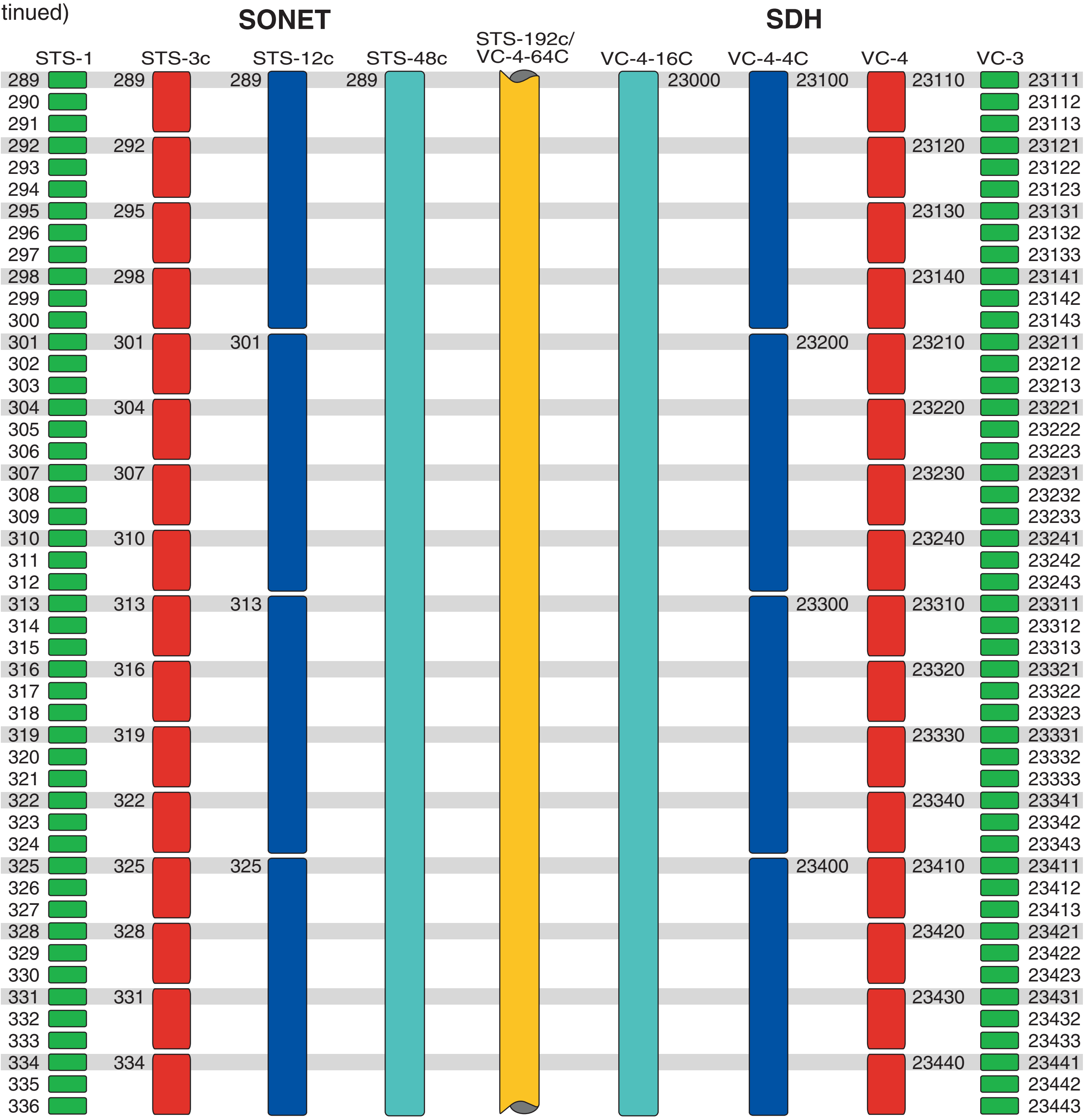
		SONET					SDH		
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/	VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
193	193	193	193	193	20000	21000	21100	21110	21111
194									21112
195									21113
196	196							21120	21121
197									21122
198									21123
199	199							21130	21131
200									21132
201									21133
202	202							21140	21141
203									21142
204									21143
205	205	205					21200	21210	21211
206									21212
207									21213
208	208							21220	21221
209									21222
210									21223
211	211							21230	21231
212									21232
213									21233
214	214							21240	21241
215									21242
216									21243
217	217	217					21300	21310	21311
218									21312
219									21313
220	220							21320	21321
221									21322
222									21323
223	223							21330	21331
224									21332
225									21333
226	226							21340	21341
227									21342
228									21343
229	229	229					21400	21410	21411
230									21412
231									21413
232	232							21420	21421
233									21422
234									21423
235	235							21430	21431
236									21432
237									21433
238	238							21440	21441
239									21442
240									21443

(continued)

STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
241	241	241	241		22000	22100	22110	22111
242								22112
243								22113
244	244						22120	22121
245								22122
246								22123
247	247						22130	22131
248								22132
249								22133
250	250						22140	22141
251								22142
252								22143
253	253	253				22200	22210	22211
254								22212
255								22213
256	256						22220	22221
257								22222
258								22223
259	259						22230	22231
260								22232
261								22233
262	262						22240	22241
263								22242
264								22243
265	265	265				22300	22310	22311
266								22312
267								22313
268	268						22320	22321
269								22322
270								22323
271	271						22330	22331
272								22332
273								22333
274	274						22340	22341
275								22342
276								22343
277	277	277				22400	22410	22411
278								22412
279								22413
280	280						22420	22421
281								22422
282								22423
283	283						22430	22431
284								22432
285								22433
286	286						22440	22441
287								22442
288								22443

SONET SDH

(continued)

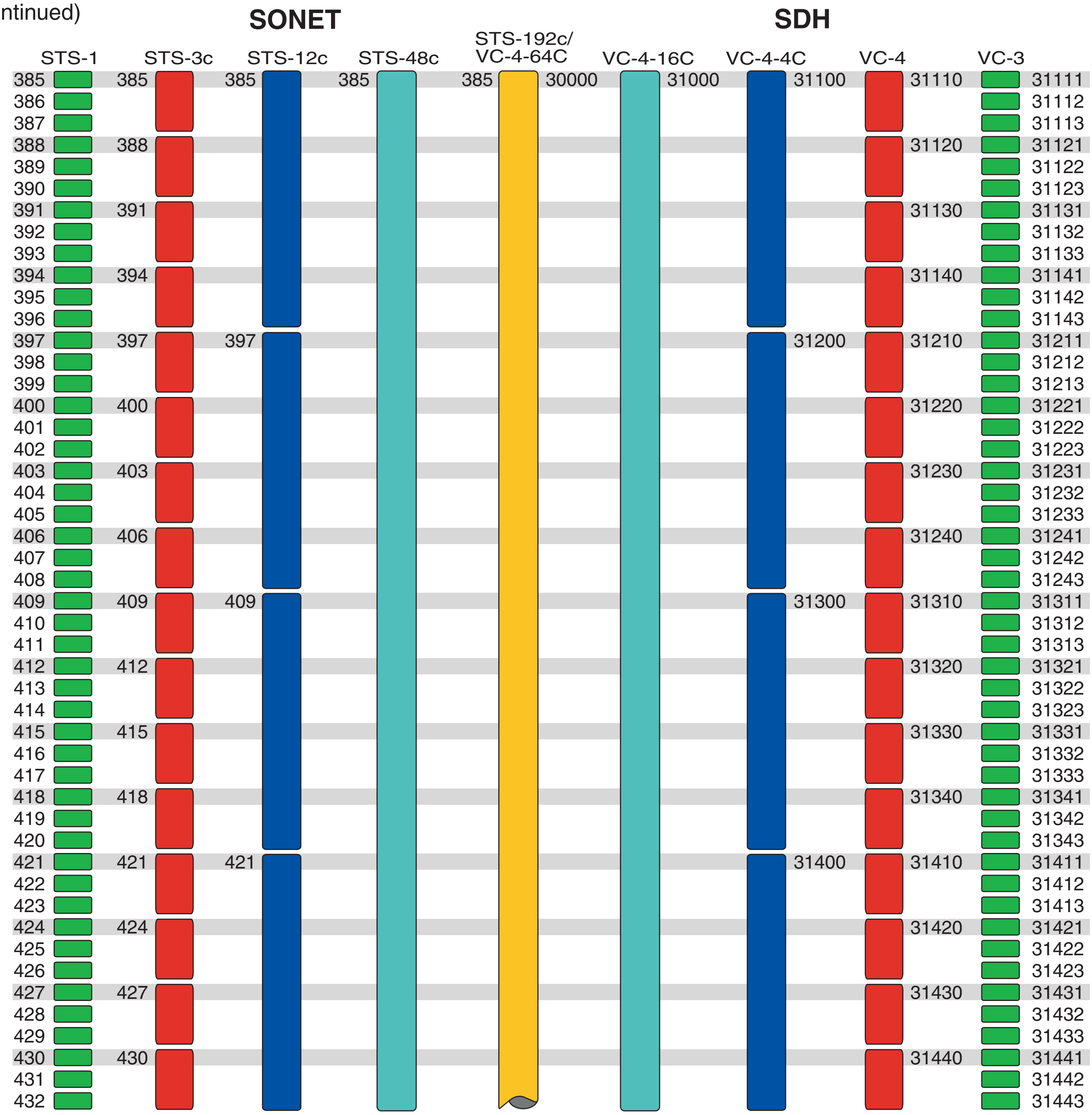


SONET						SDH		
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
289	289	289	289		23000	23100	23110	23111
290								23112
291								23113
292	292						23120	23121
293								23122
294								23123
295	295						23130	23131
296								23132
297								23133
298	298						23140	23141
299								23142
300								23143
301	301	301				23200	23210	23211
302								23212
303								23213
304	304						23220	23221
305								23222
306								23223
307	307						23230	23231
308								23232
309								23233
310	310						23240	23241
311								23242
312								23243
313	313	313				23300	23310	23311
314								23312
315								23313
316	316						23320	23321
317								23322
318								23323
319	319						23330	23331
320								23332
321								23333
322	322						23340	23341
323								23342
324								23343
325	325	325				23400	23410	23411
326								23412
327								23413
328	328						23420	23421
329								23422
330								23423
331	331						23430	23431
332								23432
333								23433
334	334						23440	23441
335								23442
336								23443

(continued)

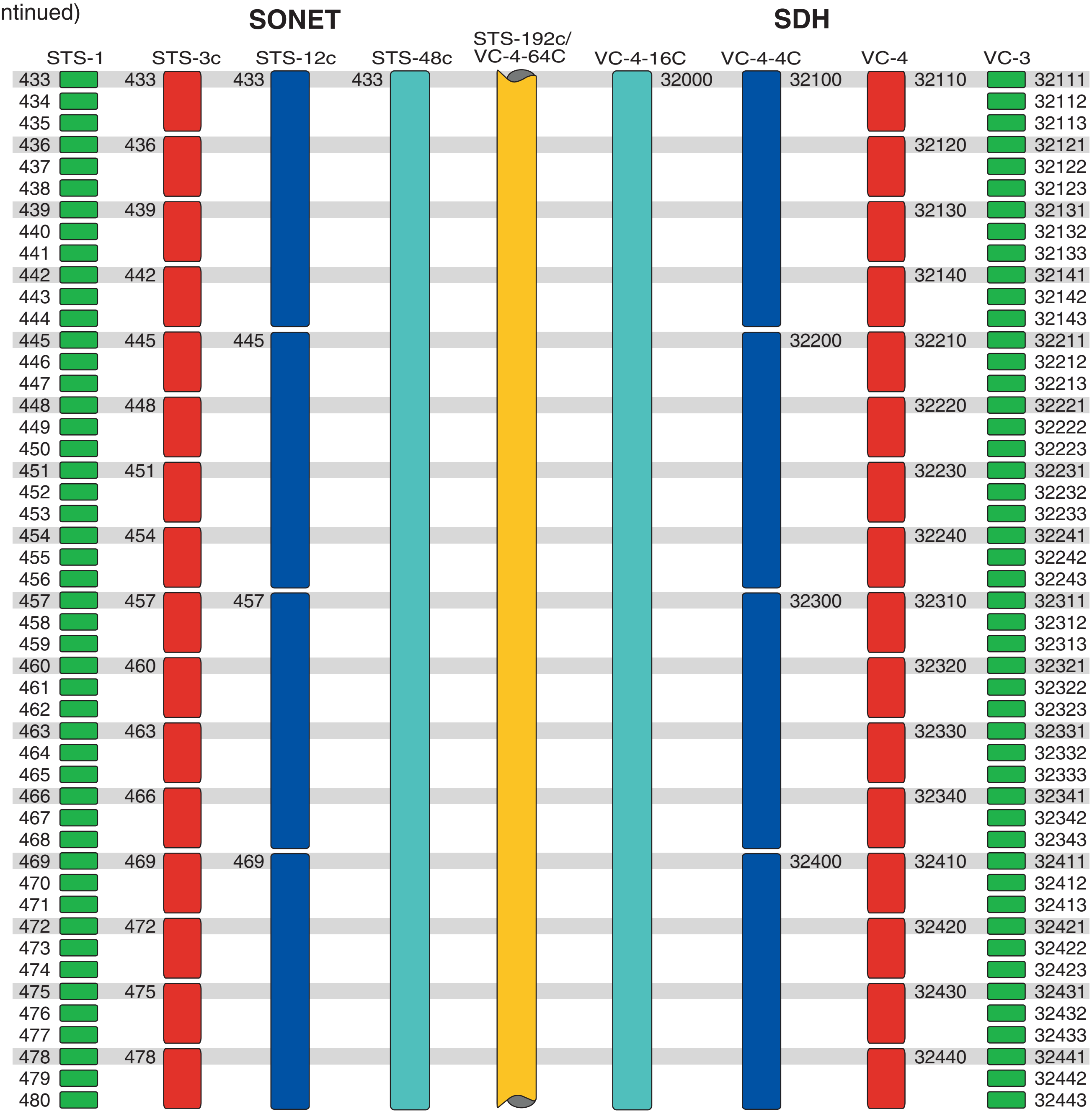
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
337	337	337	337		24000	24100	24110	24111
338								24112
339								24113
340	340						24120	24121
341								24122
342								24123
343	343						24130	24131
344								24132
345								24133
346	346						24140	24141
347								24142
348								24143
349	349	349				24200	24210	24211
350								24212
351								24213
352	352						24220	24221
353								24222
354								24222
355	355						24230	24231
356								24232
357								24233
358	358						24240	24241
359								24242
360								24243
361	361	361				24300	24310	24311
362								24312
363								24313
364	364						24320	24321
365								24322
366								24323
367	367						24330	24331
368								24332
369								24333
370	370						24340	24341
371								24342
372								24343
373	373	373				24400	24410	24411
374								24412
375								24413
376	376						24420	24421
377								24422
378								24423
379	379						24430	24431
380								24432
381								24433
382	382						24440	24441
383								24442
384								24443

(continued)



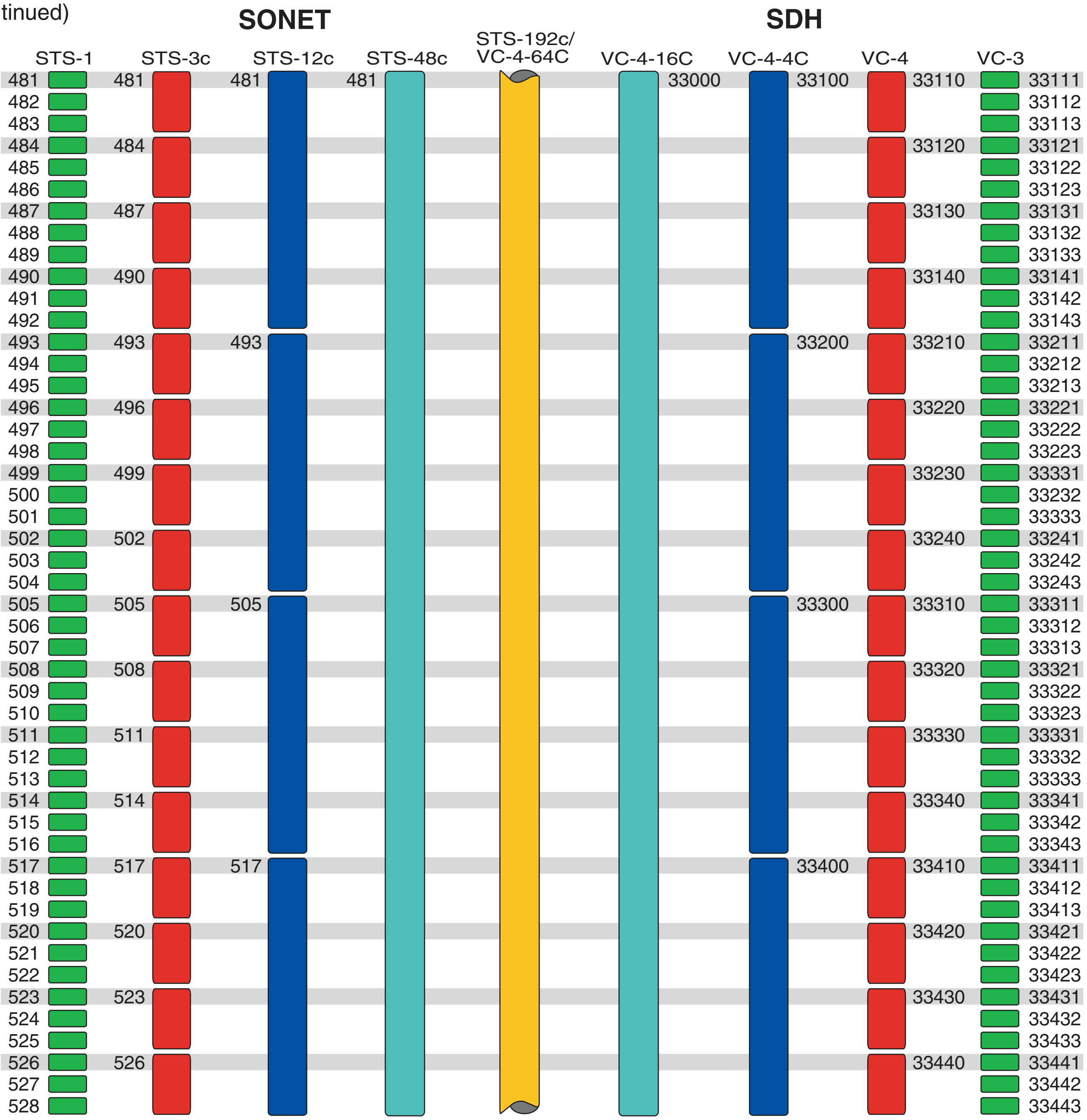
SONET STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	SDH VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
385	385	385	385	385	30000	31000	31100	31110	31111
386									31112
387									31113
388	388							31120	31121
389									31122
390									31123
391	391							31130	31131
392									31132
393									31133
394	394							31140	31141
395									31142
396									31143
397	397	397					31200	31210	31211
398									31212
399									31213
400	400							31220	31221
401									31222
402									31223
403	403							31230	31231
404									31232
405									31233
406	406							31240	31241
407									31242
408									31243
409	409	409					31300	31310	31311
410									31312
411									31313
412	412							31320	31321
413									31322
414									31323
415	415							31330	31331
416									31332
417									31333
418	418							31340	31341
419									31342
420									31343
421	421	421					31400	31410	31411
422									31412
423									31413
424	424							31420	31421
425									31422
426									31423
427	427							31430	31431
428									31432
429									31433
430	430							31440	31441
431									31442
432									31443

(continued)

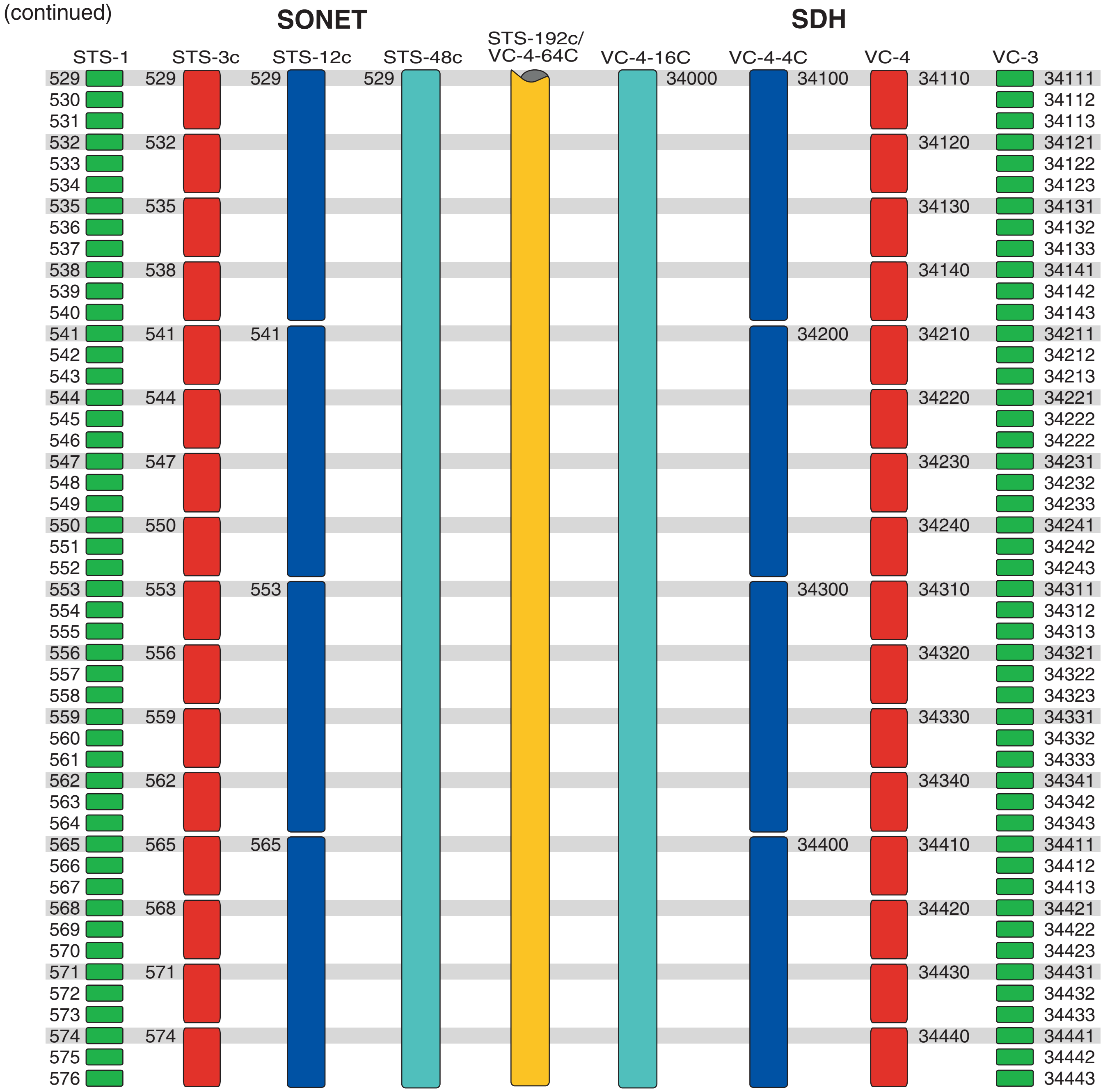


STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
433	433	433	433		32000	32100	32110	32111
434								32112
435								32113
436	436						32120	32121
437								32122
438								32123
439	439						32130	32131
440								32132
441								32133
442	442						32140	32141
443								32142
444								32143
445	445	445				32200	32210	32211
446								32212
447								32213
448	448						32220	32221
449								32222
450								32223
451	451						32230	32231
452								32232
453								32233
454	454						32240	32241
455								32242
456								32243
457	457	457				32300	32310	32311
458								32312
459								32313
460	460						32320	32321
461								32322
462								32323
463	463						32330	32331
464								32332
465								32333
466	466						32340	32341
467								32342
468								32343
469	469	469				32400	32410	32411
470								32412
471								32413
472	472						32420	32421
473								32422
474								32423
475	475						32430	32431
476								32432
477								32433
478	478						32440	32441
479								32442
480								32443

(continued)



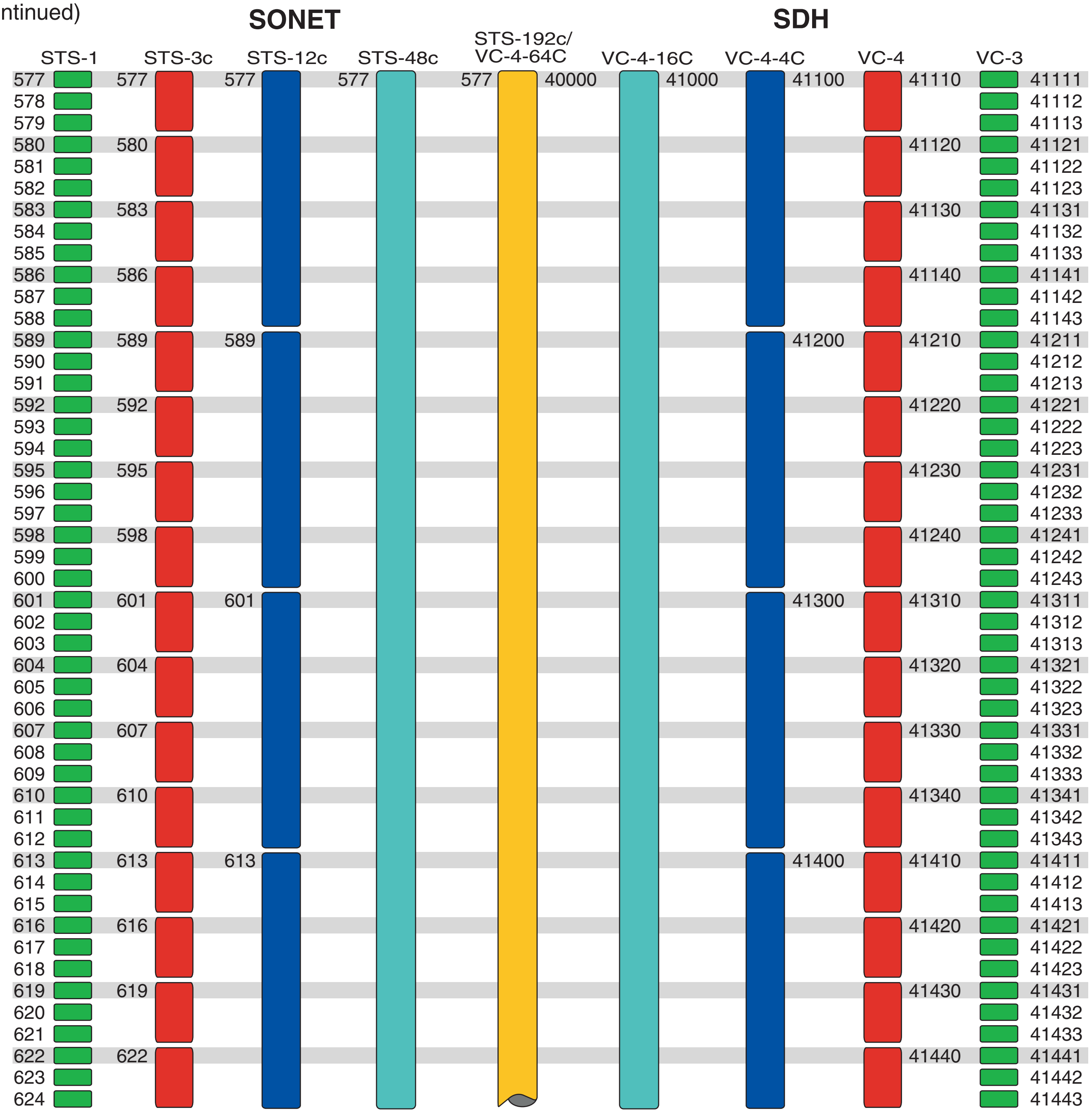
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
481	481	481	481		33000	33100	33110	33111
482								33112
483								33113
484	484						33120	33121
485								33122
486								33123
487	487						33130	33131
488								33132
489								33133
490	490						33140	33141
491								33142
492								33143
493	493	493				33200	33210	33211
494								33212
495								33213
496	496						33220	33221
497								33222
498								33223
499	499						33230	33331
500								33232
501								33333
502	502						33240	33241
503								33242
504								33243
505	505	505				33300	33310	33311
506								33312
507								33313
508	508						33320	33321
509								33322
510								33323
511	511						33330	33331
512								33332
513								33333
514	514						33340	33341
515								33342
516								33343
517	517	517				33400	33410	33411
518								33412
519								33413
520	520						33420	33421
521								33422
522								33423
523	523						33430	33431
524								33432
525								33433
526	526						33440	33441
527								33442
528								33443



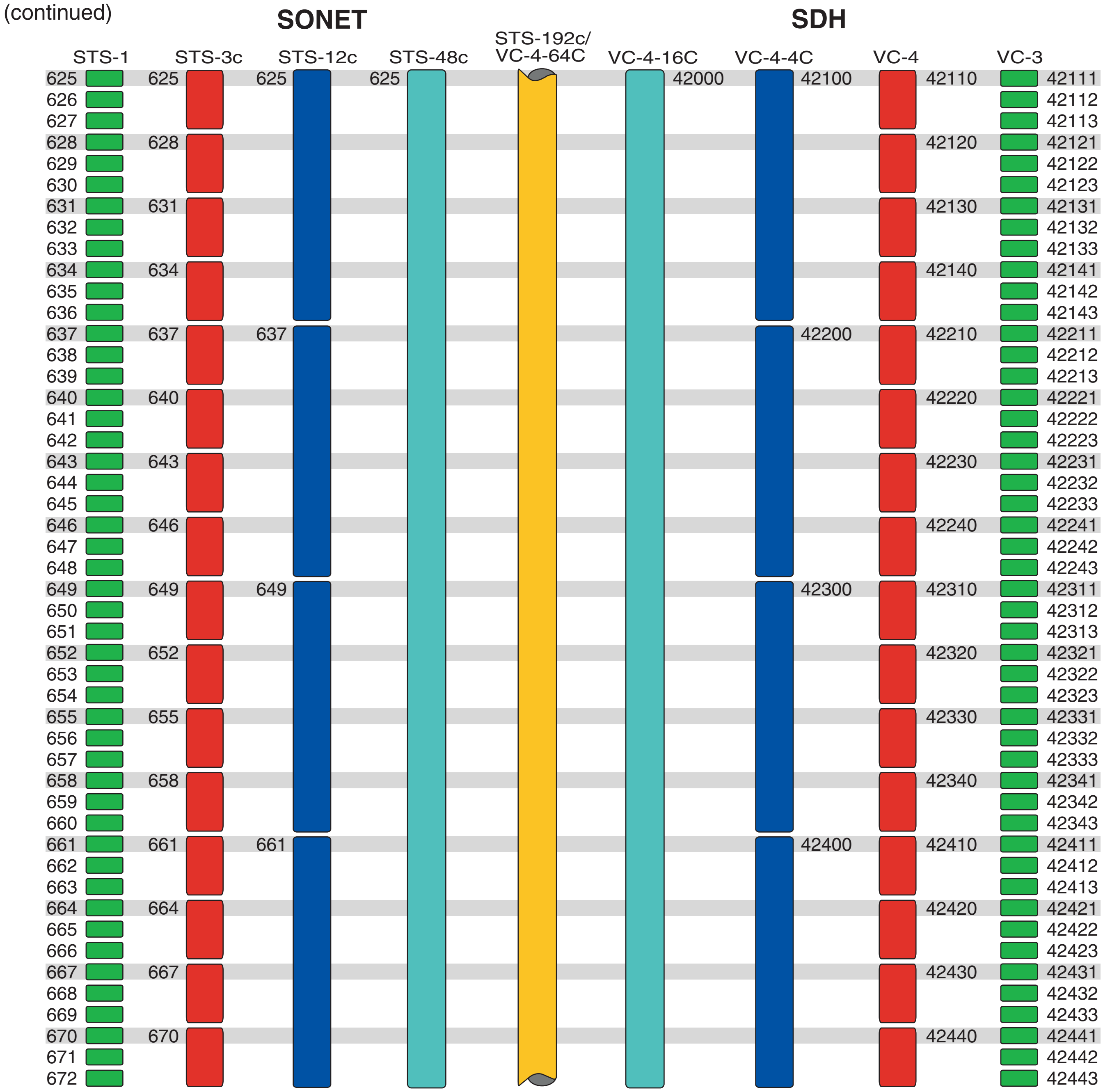
(continued)

SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
529	529	529	529		34000	34100	34110	34111
530								34112
531								34113
532	532						34120	34121
533								34122
534								34123
535	535						34130	34131
536								34132
537								34133
538	538						34140	34141
539								34142
540								34143
541	541	541				34200	34210	34211
542								34212
543								34213
544	544						34220	34221
545								34222
546								34222
547	547						34230	34231
548								34232
549								34233
550	550						34240	34241
551								34242
552								34243
553	553	553				34300	34310	34311
554								34312
555								34313
556	556						34320	34321
557								34322
558								34323
559	559						34330	34331
560								34332
561								34333
562	562						34340	34341
563								34342
564								34343
565	565	565				34400	34410	34411
566								34412
567								34413
568	568						34420	34421
569								34422
570								34423
571	571						34430	34431
572								34432
573								34433
574	574						34440	34441
575								34442
576								34443

(continued)



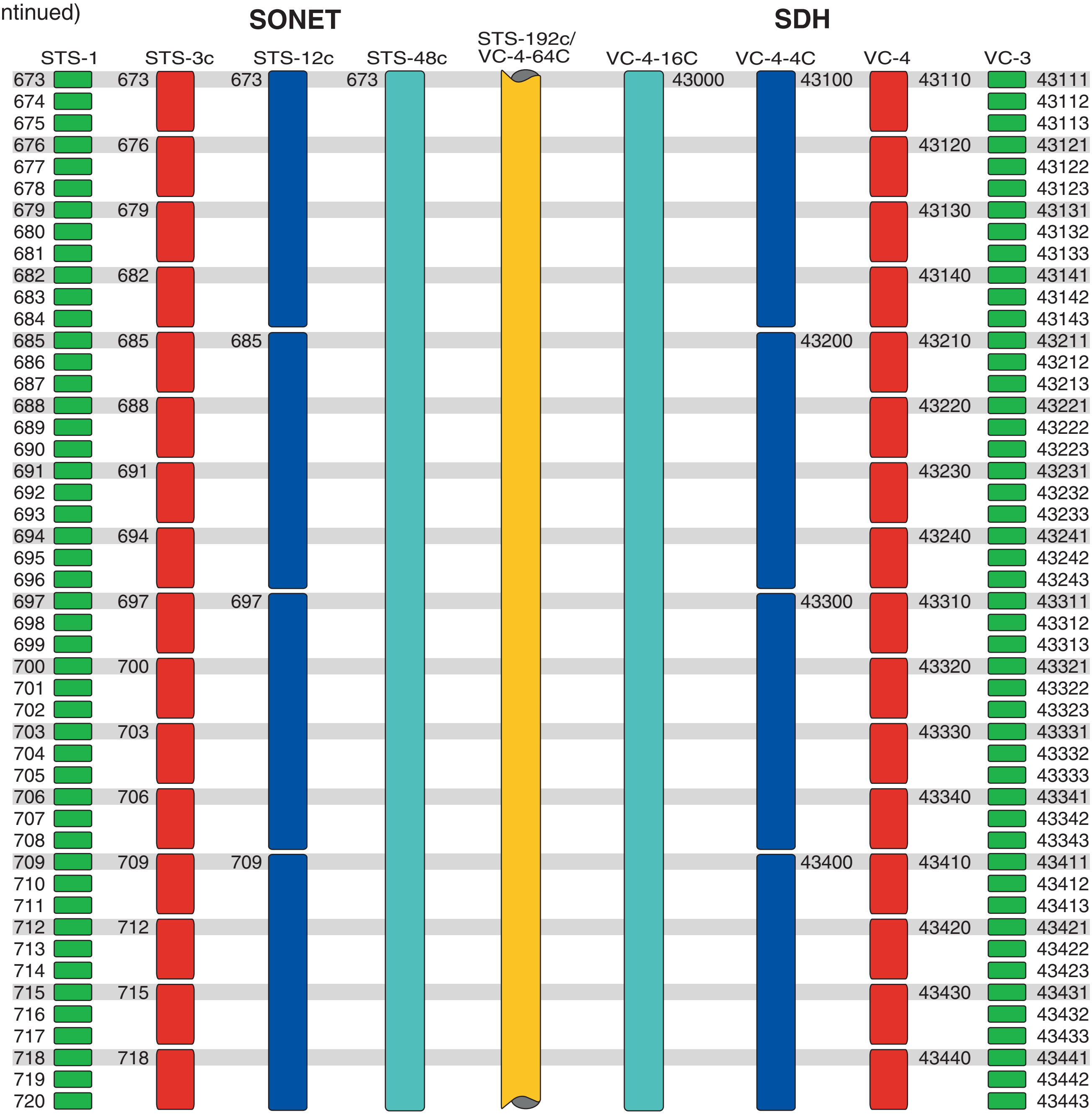
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C		VC-4-16C	VC-4-4C	VC-4	VC-3
577	577	577	577	577	40000	41000	41100	41110	41111
578									41112
579									41113
580	580							41120	41121
581									41122
582									41123
583	583							41130	41131
584									41132
585									41133
586	586							41140	41141
587									41142
588									41143
589	589	589					41200	41210	41211
590									41212
591									41213
592	592							41220	41221
593									41222
594									41223
595	595							41230	41231
596									41232
597									41233
598	598							41240	41241
599									41242
600									41243
601	601	601					41300	41310	41311
602									41312
603									41313
604	604							41320	41321
605									41322
606									41323
607	607							41330	41331
608									41332
609									41333
610	610							41340	41341
611									41342
612									41343
613	613	613					41400	41410	41411
614									41412
615									41413
616	616							41420	41421
617									41422
618									41423
619	619							41430	41431
620									41432
621									41433
622	622							41440	41441
623									41442
624									41443



(continued)

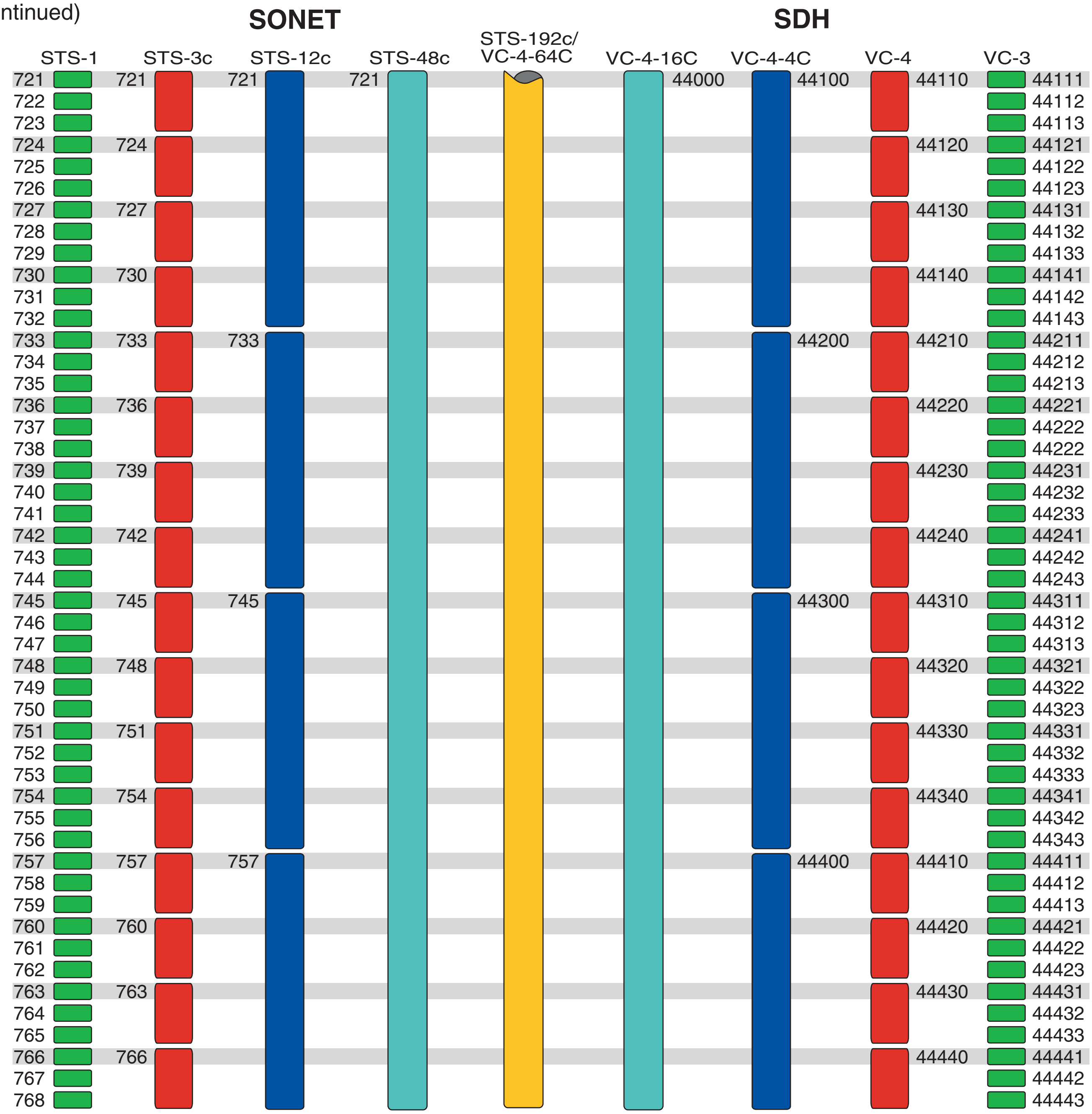
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
625	625	625	625		42000	42100	42110	42111
626								42112
627								42113
628	628						42120	42121
629								42122
630								42123
631	631						42130	42131
632								42132
633								42133
634	634						42140	42141
635								42142
636								42143
637	637	637				42200	42210	42211
638								42212
639								42213
640	640						42220	42221
641								42222
642								42223
643	643						42230	42231
644								42232
645								42233
646	646						42240	42241
647								42242
648								42243
649	649	649				42300	42310	42311
650								42312
651								42313
652	652						42320	42321
653								42322
654								42323
655	655						42330	42331
656								42332
657								42333
658	658						42340	42341
659								42342
660								42343
661	661	661				42400	42410	42411
662								42412
663								42413
664	664						42420	42421
665								42422
666								42423
667	667						42430	42431
668								42432
669								42433
670	670						42440	42441
671								42442
672								42443

(continued)



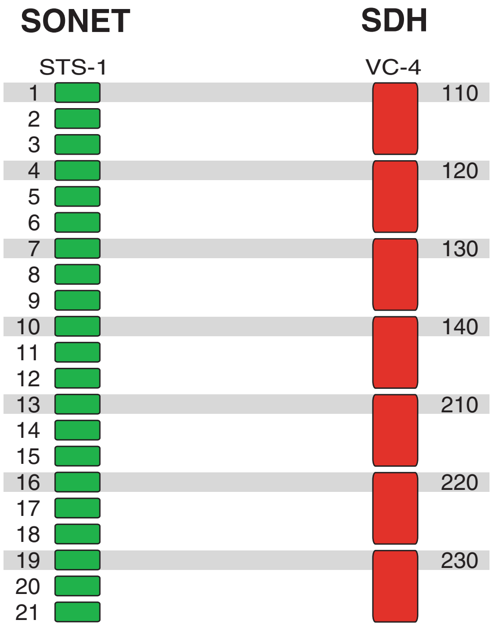
SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/ VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
673	673	673	673		43000	43100	43110	43111
674								43112
675								43113
676	676						43120	43121
677								43122
678								43123
679	679						43130	43131
680								43132
681								43133
682	682						43140	43141
683								43142
684								43143
685	685	685				43200	43210	43211
686								43212
687								43213
688	688						43220	43221
689								43222
690								43223
691	691						43230	43231
692								43232
693								43233
694	694						43240	43241
695								43242
696								43243
697	697	697				43300	43310	43311
698								43312
699								43313
700	700						43320	43321
701								43322
702								43323
703	703						43330	43331
704								43332
705								43333
706	706						43340	43341
707								43342
708								43343
709	709	709				43400	43410	43411
710								43412
711								43413
712	712						43420	43421
713								43422
714								43423
715	715						43430	43431
716								43432
717								43433
718	718						43440	43441
719								43442
720								43443

(continued)



SONET					SDH			
STS-1	STS-3c	STS-12c	STS-48c	STS-192c/VC-4-64C	VC-4-16C	VC-4-4C	VC-4	VC-3
721	721	721	721		44000	44100	44110	44111
722								44112
723								44113
724	724						44120	44121
725								44122
726								44123
727	727						44130	44131
728								44132
729								44133
730	730						44140	44141
731								44142
732								44143
733	733	733				44200	44210	44211
734								44212
735								44213
736	736						44220	44221
737								44222
738								44222
739	739						44230	44231
740								44232
741								44233
742	742						44240	44241
743								44242
744								44243
745	745	745				44300	44310	44311
746								44312
747								44313
748	748						44320	44321
749								44322
750								44323
751	751						44330	44331
752								44332
753								44333
754	754						44340	44341
755								44342
756								44343
757	757	757				44400	44410	44411
758								44412
759								44413
760	760						44420	44421
761								44422
762								44423
763	763						44430	44431
764								44432
765								44433
766	766						44440	44441
767								44442
768								44443

VCG port The following figure shows the possible substructuring of a VCG port signal and the associated SDH and SONET tributary numbering schemes.



□

5 Exceptional situations not reflected by alarm messages

Overview

Purpose This chapter contains information about exceptional situations that may occur during the operation of a *LambdaUnite*® MSS network element, and which are not reflected by alarm messages.

Contents

□

Solving (and avoiding) Controller recovery problems

Purpose

Use these procedures to solve Controller (CTL) recovery problems, and to proactively avoid such problems. CTL recovery problems means that a CTL fails to recover (reboot).

Possible reasons

CTL recovery problems may be caused by a corrupted and thus unreadable *CompactFlash*™ card. A *CompactFlash*™ card may be damaged when its power supply is interrupted while it is accessed for a read or write operation.

These situations can be distinguished in which CTL recovery problems may occur:

1. When a CTL is re-inserted which was not adequately removed from its slot (without following the → “Recommended procedure for removing a CTL from its slot” (5-6)).
2. When the power supply is restored after a `System Power Failure`. The *CompactFlash*™ card may have been damaged when the system power was lost.
3. When a network element is taken into operation again which was previously taken out of operation without following the → “Recommended deinstallation procedure” (5-7).

Solving CTL recovery problems

1

If …	then …
the problem has occurred after a `System Power Failure`	carry out Step 2 to Step 7.

If …	then …
the problem has occurred during a re-installation	proceed with Step 8. Assumptions The following assumptions are made in that case: - No circuit packs are equipped, i.e. the shelf is empty, when the power is switched on. - Subsequently a CTL is installed in the worker slot (CTL-W, with an existing NE configuration database stored on its *CompactFlash*™ card). - The CTL-W does not recover. This installation sequence complies to the procedure for the first installation as described in the *LambdaUnite*® *MSS Installation Guide*.

2

If …	then …
there is only one CTL equipped (simplex control)	replace the currently used *CompactFlash*™ card. **Reference:** “Replacing a defective *CompactFlash*™ card” (4-45)
there are two CTLs equipped (duplex control), and one of them failed to recover	1. remove the CTL that failed to recover from its slot, 2. insert a ***new, vendor-formatted*** *CompactFlash*™ card into the *CompactFlash*™ drive, and 3. re-insert the CTL.
there are two CTLs equipped (duplex control), and both failed to recover	proceed with the next step.

3 Replace the currently used *CompactFlash*™ card for one of the two CTLs by following the procedure for replacing a defective *CompactFlash*™ card.

Reference:

"Replacing a defective *CompactFlash*™ card" (4-45)

4 Wait for the just inserted CTL to recover.

5 Remove the second CTL from its slot.

6 Insert a ***new, vendor-formatted*** *CompactFlash*™ card into the *CompactFlash*™ drive of the second CTL.

7 Re-insert the second CTL.

Result:

The NE configuration database will be synchronized between the two CTLs.

8 Remove the CTL-W from its slot.

9

If …	then …
a protection CTL (duplex CTL, CTL-P) is available (depends on the previous NE configuration)	insert the CTL-P into the protection slot, and proceed with the next step.
no protection CTL (duplex CTL, CTL-P) is available	replace the currently used *CompactFlash*™ card for the CTL-W by following the procedure for replacing a defective *CompactFlash*™ card. **Reference:** "Replacing a defective *CompactFlash*™ card" (4-45)

10

If …	then …
the just inserted CTL-P recovers successfully	1. install all the remaining circuit packs, 2. insert a ***new, vendor-formatted*** *CompactFlash*™ card into the *CompactFlash*™ drive of the CTL-W, and 3. re-insert the CTL-W. Stop! You have completed this procedure.
the just inserted CTL-P does not recover	replace the currently used *CompactFlash*™ card for the CTL-W by following the procedure for replacing a defective *CompactFlash*™ card. **Reference:** “Replacing a defective *CompactFlash*™ card” (4-45)

11 Wait for the CTL-W to recover.

12 Install all the remaining circuit packs.

13 Install the CTL-P.

14

If …	then …
the CTL-P recovers successfully	Stop! You have completed this procedure.
the CTL-P does not recover	1. insert a ***new, vendor-formatted*** *CompactFlash*™ card into the *CompactFlash*™ drive of the CTL-P, and 2. re-insert the CTL-P.

15 Wait for the CTL-W to recover.

Stop! You have completed this procedure.

END OF STEPS

Recommended procedure for removing a CTL from its slot

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Circuit packs must therefore always be kept in antistatic covers. Use the original antistatic packaging if possible. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

In order to avoid damaging the *CompactFlash*™ card, proceed as follows to remove a CTL from its slot:

1 Open the latches of the CTL to be removed.

Important! ***Do not remove the CTL from its slot at that time!***

Result:

The green "ACTIVE" LED on the faceplate of the CTL starts flashing.

2 Wait until the green "ACTIVE" LED has stopped flashing (about five seconds).

3 Remove the CTL from its slot.

Important! Use the original antistatic packaging for storage and transport, if possible.

END OF STEPS

Recommended deinstallation procedure

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Circuit packs must therefore always be kept in antistatic covers. Use the original antistatic packaging if possible. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-20)).

Proceed as follows to take a network element (NE) out of operation:

1 If two CTLs are equipped (duplex control), then open the latches of the standby CTL. Otherwise, proceed with Step 4.

Important! ***Do not remove the standby CTL from its slot at that time!***

Result:

The green "ACTIVE" LED on the faceplate of the standby CTL starts flashing.

2 Wait until the green "ACTIVE" LED has stopped flashing (about five seconds).

3

If ...	then ...
you want to temporarily switch off the NE (while maintaining the configuration)	slightly pull out the standby CTL (approx. 2 cm), so that there is no connection to the backplane.

If ...	then ...
you want to completely deinstall the NE (for example, to move it to another location, and re-install it)	remove the standby CTL from its slot. Use the original antistatic packaging for storage and transport, if possible.

4 Open the latches of the active CTL.

Important! ***Do not remove the active CTL from its slot at that time!***

Result:

The green "ACTIVE" LED on the faceplate of the active CTL starts flashing.

5 Wait until the green "ACTIVE" LED has stopped flashing (about five seconds).

6

If ...	then ...
you want to temporarily switch off the NE (while maintaining the configuration)	slightly pull out the active CTL (approx. 2 cm), so that there is no connection to the backplane.
you want to completely deinstall the NE (for example, to move it to another location, and re-install it)	remove the active CTL from its slot. Use the original antistatic packaging for storage and transport, if possible.

7 Switch off the NE power supply by means of the circuit breakers on both Power Interfaces (position 0 = OFF).

8 Remove all other circuit packs from the shelf. Use the original antistatic packaging for storage and transport, if possible.

END OF STEPS

□

System autonomously entered the maintenance condition

Maintenance condition

The maintenance condition (or "maintenance mode") is an exceptional mode of operation characterized as follows:

- The system behaves as if the Controller was not present (transmission services are ***not*** affected).
- The internal communication between the Controller and the function controllers on circuit packs is disabled.
- A software download from the Controller to the function controllers on circuit packs is not possible.
- Only those autonomous state change events (i.e. also notifications) that do not change the active configuration database (NVM) are allowed.
- Only a limited set of operations is allowed:
  - Changing the NE name (***only*** possible in maintenance mode).
  - Setting the NE's date and time.
  - Changing the default value for the NE's synchronization mode (***only*** possible in maintenance mode).
  - Changing the default value for the optical interface standard.
  - Changing the default value for the tributary operation mode.
  - Setting an IP address, both for IP access on LAN, and for the SCN (***only*** possible in maintenance mode).
  - Setting the IP default router address and LAN port (***only*** possible in maintenance mode).
  - Setting the T-TD raw mode and length value port.
  - Setting the LAN status (general, OSI, IP), designated router, osinode, and TLSS of LANs.
  - Performing a database download.
  - Retrieving data from the active configuration database (NVM).
  - Leaving (terminating) the maintenance mode (***only*** possible in maintenance mode).
- Write access to the active configuration database (NVM) is restricted to those data related to the limited set of operations that are allowed in maintenance mode.

The maintenance mode can either be entered manually to perform operations that are only possible in maintenance mode, such as changing the NE name (TID) for example, or autonomously by the system when an exceptional situation occurred.

Reasons for autonomously entering the maintenance mode

The following description lists the possible reasons why a *LambdaUnite*® MSS system autonomously enters the maintenance mode, and gives recommendations how to resolve the “problem”:

1. An empty database is detected during startup
   Perform a database restore using the most recent database backup.
2. A new database is detected during startup
   Perform a database restore using the most recent database backup, or leave the maintenance mode (see “Leaving the maintenance mode” (5-11)) if you are absolutely sure that the current system configuration and the configuration database on the NVM are compatible.
3. A Controller of type CTL/- is present, and during startup it is detected that the **Cross-Connect Application** is set to **ONNS**.
   The CTL/- Controller variant does not support ONNS applications. For ONNS applications the CTL/2 Controller variant is mandatory.
   Either adapt the system equipage to meet the requirements for using ONNS, or provision the system according to the current equipage.

Empty database

An empty database is detected during startup

Perform a database restore using the most recent database backup.

New database

A new database is detected during startup

Perform a database restore using the most recent database backup, or leave the maintenance mode (see “Leaving the maintenance mode” (5-11)) if you are absolutely sure that the current system configuration and the configuration database on the NVM are compatible.

Unsuitable Controller variant

A Controller of type CTL/- is present, and during startup it is detected that the **Cross-Connect Application** is set to **ONNS**.

The CTL/- Controller variant does ***not*** support ONNS applications. For ONNS applications the CTL/2 Controller variant is mandatory.

Either adapt the system equipage to meet the requirements for using ONNS, or provision the system according to the current equipage.

Unsuitable optical interface module

An optical interface module has been detected which is not qualified for the use within a *LambdaUnite*® MSS system.

Make sure that all optical interface modules used are qualified for the use within *LambdaUnite*® MSS systems. Only the recommended versions of optical interface modules are guaranteed to meet the *LambdaUnite*® MSS system requirements (with regard to the EMC/ESD performance or transmission characteristics for example).

Please refer to the *LambdaUnite® MSS Applications and Planning Guide* and the *LambdaUnite® MSS User Operations Guide* for information on the recommended versions of optical interface modules.

Leaving the maintenance mode

You can terminate (leave) the maintenance mode by selecting **Fault** → **Enter/Exit Maintenance Condition...** → **Exit Maintenance Condition....** from the *WaveStar*® CIT **System View** main menu.

> **Important!** Do not leave the maintenance mode unless you are absolutely sure that the current system configuration and the configuration database on the NVM are compatible.

□

Appendix A: A comparison of *LambdaUnite*® MSS and WaveStar® TDM 10G (STM-64) alarms

Overview

Purpose This appendix contains an overview table for comparing similar *LambdaUnite*® MSS and WaveStar® TDM 10G (STM-64) alarm messages.

Contents

□

Tabular overview of *LambdaUnite*® MSS and WaveStar® TDM 10G (STM-64) alarms

Overview table

The following table gives an overview of *LambdaUnite*® MSS and WaveStar® TDM 10G (STM-64) alarm messages. It provides a means to compare similar alarm messages which may have differnt probable causes and/or alarm descriptions.

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
PORT	“{aidtype}” is one of OC3, OC12, OC48, OC192, OC768, STM1E, STM1, STM4, STM16, STM64, STM256			“{rr}” is one of STM1, STM1E, STM4, STM16, STM64		
	sa_ochlof, nsa_ochlof	OCHLOF	Communication-Transport, {aidtype} port, OCh Loss of Frame	–	–	–
	sa_ochpfdi, nsa_ochpfdi	OCHPFDI	Communication-Transport, {aidtype} port, Forward Defect Indication	–	–	–
	sa_ochptim, nsa_ochptim	OCHPTIM	Communication-Transport, {aidtype} port, Trace Identifier Mismatch	–	–	–
	sa_ochpplm, nsa_ochpplm	OCHPPLM	Communication-Transport, {aidtype} port, Payload Mismatch	–	–	–
	sa_predcmlos, nsa_predcmlos	PREDCMLOS	Communication-Transport, {aidtype} port, Pre DCM Signal Loss	–	–	–
	sa_postdcmlos, nsa_postdcmlos	POSTDCMLOS	Communication-Transport, {aidtype} port, Post DCM Signal Loss	–	–	–
	sa_los, nsa_los	LOS	Communication-Transport, {aidtype} port, Loss of Signal	sa_stmf_los, nsa_stmf_los	STMLOS	Communications, {rr} port, STM Loss of Signal
	sa_lof, nsa_lof	LOF	Communication-Transport, {aidtype} port, Loss of Frame	sa_rdf_lof, nsa_rsf_lof	STMLOF	Communications, {rr} port, STM Loss of Frame
	sa_rstim, nsa_rstim	RSTIM	Communication-Transport, {aidtype} port, Trace Identifier Mismatch	sa_rsf_tim, nsa_rsf_tim	RSTIM	Communications, {rr} port, RSect Trace Identifier Mismatch
	sa_msexc, nsa_msexc	MSEXC	Communication-Transport, {aidtype} port, Excessive Bit Error Ratio	sa_msf_exc, nsa_msf_exc	MSEXC	Communications, {rr} port, MSect Excessive Error

Tabular overview of *LambdaUnite*® MSS and WaveStar® TDM 10G (STM-64) alarms

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	sa_msdeg, nsa_msdeg	MSDEG	Communication-Transport, {aidtype} port, Degraded Signal	sa_msf_deg, nsa_msf_deg	MSDEG	Communications, {rr} port, MSect Signal Degrade
	sa_aisl, nsa_aisl	AIS-L	Communication-Transport, {aidtype} port, Alarm Indication Signal	sa_msf_ais, nsa_msf_ais	MSAIS	Communications, {rr} port, MSect Alarm Indication Signal
	sa_msssf, nsa_msssf	MSSSF	Communication-Transport, {aidtype} port, Server Signal Fail	sa_msf_ssf, nsa_msf_ssf	MSSSF	Communications, {rr} port, MSect Server Signal Failure
	sa_mspssf, nsa_mspssf	MSPSSF	Communication-Transport, {aidtype} port, Prot. Server Signal Fail	–	–	–
	sa_rfil, nsa_rfil	RFI-L	Communication-Transport, {aidtype} port, Remote Defect Indication	sa_msf_rdi, nsa_msf_rdi	MSRDI	Communications, {rr} port, MSect Remote Failure Indication
	nsa_dccrsf	DCCRSF	Communication-Transport, {aidtype} port, DCC failure	sa_dccrs, nsa_dccrs	DCCRSF	Communications, {rr} port, DCC RSect Failure
	nsa_lidrsm	LIDRSM	Communication-Transport, {aidtype} port, Protocol Version Mismatch	sa_lidrsmm, nsa_lidrsmm	LIDRSM	Communications, {rr} port, LinkID RSect Mismatch
	nsa_dccmsf	DCCMSF	Communication-Transport, {aidtype} port, DCC failure	sa_dccms, nsa_dccms	DCCMSF	Communications, {rr} port, DCC MSect Failure
	nsa_lidmsm	LIDMSM	Communication-Transport, {aidtype} port, Protocol Version Mismatch	sa_lidmsmm, nsa_lidmsmm	LIDMSM	Communications, {rr} port, LinkID MSect Mismatch
PATH	{aidtype} is one of STS1, STS3C, STS12C, STS48C, STS192C, VC3, VC4, VC44C, VC416C, VC464C			{rr} is one of VC3, VC4, VC44C, VC416C		
	sa_ais, nsa_ais	AIS-P	Communication-Transport, {aidtype} path, Alarm Indication Signal	sa_auf_ais, nsa_auf_ais	AUAIS	Communications, {rr} CS, AU Alarm Indication Signal

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	sa_lop, nsa_lop	LOP-P	Communication-Transport, {aidtype} path, Loss of Pointer	sa_auf_lop, nsa_auf_lop	AULOP	Communications {rr} CS, AU Loss of Pointer
	sa_srm, nsa_srm	SRM-P	Communication-Transport, {aidtype} path, Signal Rate Mismatch	sa_auf_srm, nsa_auf_srm	AUSRM	Communications, {rr} CS, AU Signal Rate Mismatch
	sa_uneq, nsa_uneq	UNEQ-P	Communication-Transport, {aidtype} path, Unequipped	sa_hpf_uneq, nsa_hpf_uneq	HPUNEQ	Communications, {rr} CS, HP Unequip
	sa_tim, nsa_tim	TIM-P	Communication-Transport, {aidtype} path, Trace Identifier Mismatch	sa_hpf_tim, nsa_hpf_tim	HPTIM	Communications, {rr} CS, HP Trace Identifier Mismatch
	sa_exc, nsa_exc	EXC-P	Communication-Transport, {aidtype} path, Excessive Bit Error Ratio	sa_hpf_exc, nsa_hpf_exc	HPEXC	Communications, {rr} CS, HP Excessive Error
	sa_deg, nsa_deg	DEG-P	Communication-Transport, {aidtype} path, Degraded Signal	sa_hpf_deg, nsa_hpf_deg	HPDEG	Communications, {rr} CS, HP Signal Degrade
	sa_ssf, nsa_ssf	SSF-P	Communication-Transport, {aidtype} path, Server Signal Fail			
	sa_rfi, nsa_rfi	RFI-P	Communication-Transport, {aidtype} path, Remote Defect Indication	sa_hpf_rdi, nsa_hpf_rdi	HPRDI	Communications, {rr} CS, HP Remote Defect Indication
	sa_pdi, nsa_pdi	PDI-P	Communication-Transport, {aidtype} path, Payload Defect Indication	–	–	–
PATHTERM (Path termination)	{aidtype} is one of STS1, VC4			{rr} is one of VC3, VC4		
	sa_thpssf, nsa_thpssf	THPSSF	Communication-Transport, {aidtype} CS, Server Signal Fail	hpf_ssf	HPSSF	Communications, {rr} CS, HP Server Signal Failure

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	sa_thplop, nsa_thplop	THPLOP	Communication-Transport, {aidtype} CS, Loss of Pointer	hpf_lop	HPLOP	Communications, {rr} CS, HP Loss of Pointer
	sa_thpuneq, nsa_thpuneq	THPUNEQ	Communication-Transport, {aidtype} CS, Unequipped	hpf_uneq	HPUNEQ	Communications, {rr} CS, HP Unequip
	sa_thptim, nsa_thptim	THPTIM	Communication-Transport, {aidtype} CS, Trace Identifier Mismatch	hpf_tim	HPTIM	Communications, {rr} CS, HP Trace Identifier Mismatch
	sa_thpexc, nsa_thpexc	THPEXC	Communication-Transport, {aidtype} CS, Excessive Bit Error Ratio	–	–	–
	sa_thpdeg, nsa_thpdeg	THPDEG	Communication-Transport, {aidtype} CS, Degraded Signal	hpf_deg	HPDEG	Communications, {rr} CS, HP Signal Degrade
	sa_thprdi, nsa_thprdi	THPRDI	Communication-Transport, {aidtype} CS, Remote Defect Indication	hpf_rdi	HPRDI	Communications, {rr} CS, HP Remote Defect Indication
	sa_thpplm, nsa_thpplm	THPPLM	Communication-Transport, {aidtype} CS, Payload Mismatch	hpf_plm	HPPLM	Communications, {rr} CS, HP Payload Label Mismatch
	sa_vclom, nsa_vclom	VCLOM	Communication-Transport, {aidtype} CS, Loss of Multiframe	hpf_lom	LOM	Communications, {rr} CS, Loss of Multiframe
	sa_vcsqm, nsa_vcsqm	VCSQM	Communication-Transport, {aidtype} CS, Sequence Number Mismatch	hpf_sqm	SQM	Communications, {rr} CS, Sequence Number Mismatch
ENET (Ethernet)						
	sa_vcg_loa, nsa_vcg_loa	VCGLOA	Communication-Transport, VCG, Loss of Alignment	sa_loa, nsa_loa	LOA	Communications, VCG, Loss of Alignment
	sa_vcg_lopc, nsa_vcg_lopc	VCGLOPC	Communication-Transport, VCG, Partial Transport Capacity Loss	sa_lopc, nsa_lopc	CLOPC	Communications, VCG, Loss of Partial Capacity

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	sa_vcg_lotc, nsa_vcg_lotc	VCGLOTC	Communication-Transport, VCG, Total Transport Capacity Loss	sa_lotc, nsa_lotc	CLOTC	Communications, VCG, Loss of Total Capacity
	sa_vcg_fopt, nsa_vcg_fopt	VCGFOPT	Communication-Transport, VCG, Source End Failure of Protocol	sa_fopt, nsa_fopt	CFOPT	Communications, VCG, Failure of Protocol Tx
	sa_vcg_fopr, nsa_vcg_fopr	VCGFOPR	Communication-Transport, VCG, Sink End Failure of Protocol	sa_fopr, nsa_fopr	CFOPR	Communications, VCG, Failure of Protocol Rx
	sa_vcg_ssf, nsa_vcg_ssf	VCGSSF	Communication-Transport, VCG, Server Signal Fail	sa_vcgsf, nsa_vcgsf	VCGSF	Communications, VCG, VCG Signal Fail
	sa_gfp_lof, nsa_gfp_lof	GFPLOF	Communication-Transport, VCG, GFP Loss of Frame	sa_gfplof, nsa_gfplof	GFPLOF	Communications, VCG, Loss of Frame Delineation
	sa_lan_los, nsa_lan_los	LANLOS	Communication-Transport, 1GE, LAN Loss of Signal	sa_lanlos, nsa_lanlos	LOS	Communications, Enet port, Loss of Signal
	sa_lan_anm, nsa_lan_anm	LANANM	Communication-Transport, 1GE, LAN Auto Negotiation Mismatch	sa_lananm, nsa_lananm	ANM	Communications, Enet port, Auto Negotiation Mismatch
	sa_vlan_maxno, nsa_vlan_ maxno	MACvLANOVFW	max number of VLAN instances reached	–	–	–
SNCP_UPSR						
	psinh	PSI	Communication-Transport, Path prot group, Path Switch Inhibit	psinh	PSI	Communications, Path prot grp, Path Switch Inhibited
	psfail	FAILTOSW	Communication-Transport, Path prot group, Path Switch Denial	psfail	FAILTOSW	Communications, Path prot grp, Path Switch Failure
MSSPRING-BLSR						

ASAP Type	*LambdaUnite*® MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	inaps	APSC	Communication-Transport, MSSPRING-BLSR prot group, Inconsistent APS Codes	blsrinaps	APSC	Communications, BLSR/MS-SPRing prot grp, Inconsistent APS Codes
	imaps	IMAPS	Communication-Transport, MSSPRING-BLSR prot group, Improper APS Codes	blsrimaps	APSPROV	Communications, BLSR/MS-SPRing prot grp, Improper APS Codes
	nid_confl	NID-CONFL	Communication-Transport, MSSPRING-BLSR prot group, Node ID Mismatch	nidm	NID-CONFL	Communications, BLSR/MS-SPRing prot grp, Node ID Mismatch
	dkb	DKB	Communication-Transport, MSSPRING-BLSR prot group, Default K-bytes	blsrdkb	BLSR-DKB	Communications, BLSR/MS-SPRing prot grp, Default K-bytes
	rng_pss	RNG-PSS	Communication-Transport, MSSPRING-BLSR prot group, Ring Protection Switch Suspended	rpss	OVRDSW	Communications, BLSR/MS-SPRing prot grp, Ring Prot Switching Suspended
	ts	TS	Communication-Transport, MSSPRING-BLSR prot group, Traffic Squelched	blsrts	RNG-SQUELCH	Communications, {rr} port, Traffic Squelched
	dupl_rng	DUPL-RNG	Communication-Transport, MSSPRING-BLSR prot group, Duplicate Ring Node	dprn	DUPL-RNG	Communications, BLSR/MS-SPRing prot grp, Duplicate Ring Node
	ropn	RNG-OPEN	Communication-Transport, MSSPRING-BLSR prot group, Open Ring	ropn	RNG-OPEN	Communications, BLSR/MS-SPRing prot grp, Ring Open
	sqmap_confl	SQMAP-CONFL	Communication-Transport, MSSPRING-BLSR prot group, Local Squelch Map Conflict	rsmc	SQMAP-CONFL	Communications, BLSR/MS-SPRing prot grp, Local Squelch Map Conflict
	rng_inc	RNG-INC	Communication-Transport, MSSPRING-BLSR prot group, Ring Incomplete	rinc	RNG-INC	Communications, BLSR/MS-SPRing prot grp, Ring Incomplete

ASAP Type	*LambdaUnite®* MSS			WaveStar® TDM 10G (STM-64)		
	ASAP Parameter	Condition Type (probable cause)	Alarm Description	ASAP Parameter	Condition Type (probable cause)	Alarm Description
	rng_urt	RNG-URT	Communication-Transport, MSSPRING-BLSR prot group, Unknown Ring Type	urt	RNG-URT	Communications, BLSR/MS-SPRing prot grp, Unknown Ring Type
	rng_irpm	RNG-IRPM	Communication-Transport, MSSPRING-BLSR prot group, Inconsistent Ring Protection Mode	irpm	RNG-IRPM	Communications, BLSR/MS-SPRing prot grp, Inconsistent Ring Prot Mode
	rng_dscvy	RNG-DSCVY	Communication-Transport, MSSPRING-BLSR prot group, Ring Discovery in Progress	rdip	RNG-DSCVY	Communications, BLSR/MS-SPRing prot grp, Ring Discovery in Progress
	et_preempt	ET-PREEMPT	Communication-Transport, MSSPRING-BLSR prot group, Extra Traffic Preempted	etp	RNG-PREEMPT	Communications, BLSR/MS-SPRing prot grp, Extra Traffic Preempted

□

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*** explicitely 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.

EMP (Equipment Management Protocol)
The Equipment Management Protocol (EMP) is used for basic equipment management purposes, such as equipage supervision, reset and recovery control and software download.

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

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*** explicitely 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.

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.

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