Lucent Technologies
Bell Labs Innovations

WaveStar® TDM 10G (STM-64)

Alarm Messages and Trouble Clearing Guide

365-371-523
CC109149799
Issue b
October 2001

Notice

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

Mandatory customer information

Safety

Strictly observe the warnings and safety instructions described in Chapter 1 ("Safety") before carrying out work of any kind on the equipments and systems described!

Trademarks

The following Trademarks are used in this manual:

WaveStar is a registered trademark of Lucent Technologies.

Windows NT is a registered trademark of Microsoft Corporation.

Ordering information

The order number of this document is CC109149799 (365-371-523) (Issue b).

Support

Information product support

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

Technical support

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

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar® TDM 10G (STM-64)
Alarm Messages and Trouble Clearing Guide

365-371-523 Issue b October 2001

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

1. Was the information product:

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

Please provide any additional comments:

____

____

2. Please rate the effectiveness of this information product:

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

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

____

____

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

____

____

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

____

____

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

Name: ____________________ Date: ____________

Company/organization: ____________ Telephone number: ____________

Address: ________________________________

Email address: ____________ Job function: ____________

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

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar® TDM 10G (STM-64)
Alarm Messages and Trouble Clearing Guide

365-371-523 Issue b October 2001

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

1. Was the information product:

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

Please provide any additional comments:

____

____

2. Please rate the effectiveness of this information product:

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

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

____

____

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

____

____

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

____

____

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

Name: ______________________ Date: ______________

Company/organization: ______________ Telephone number: ______________

Address: ______________________________

Email address: ______________ Job function: ______________

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

Contents

2 Alarm messages

About this information product

Purpose

The *WaveStar*® TDM 10G (STM-64) *Alarm Messages and Trouble Clearing Guide* (AMTCG) provides information on the alarm messages that can be generated by the *WaveStar* TDM 10G (STM-64) network elements. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.

Reason for reissue

This is the second issue of the *WaveStar TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide* for *WaveStar* TDM 10G (STM-64) Release 4.0.

Safety labels

Please refer to chapter 1 (“Safety”).

Intended audience

The intended audience of this *WaveStar TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide*primarily consists of people who are responsible for the maintenance of network elements and for the supervision of transmission operation.

Training of personnel

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

How to use this information product

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

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

Chapter	Title	Description
Preface	About this information product	The preface • describes the guide's purpose, intended audience, and organization, • lists related documentation, • explains how to comment on this document.
1	Safety	contains a series of very important safety instructions concerning the handling of *WaveStar* TDM 10G (STM-64) network elements.
2	Alarm messages	contains descriptions of the alarms which can be generated by the *WaveStar* TDM 10G (STM-64) network elements.
3	Trouble clearing	describes the measures to be taken for localising and clearing faults on the *WaveStar* TDM 10G (STM-64) network elements. It is based on the network element alarms that can be generated.
4	Supporting procedures	describes tasks and procedures that are often referred to during trouble clearing or maintenance activities.
5	Glossary	defines telecommunication terms and expands common telecommunication abbreviations and acronyms.
6	Index	lists specific subjects and their corresponding page numbers.

Conventions used

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

Numbering

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

Cross references

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

Keyword blocks

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

Typographical conventions

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

- Elements of the graphical user interface (GUI)
  These are examples of text that appears on a graphical user interface (GUI), such as menu options, window titles or pushbuttons:
  - **Provision…**, **Delete**, **Apply**, **Close**, **OK** (pushbuttons)
  - **Provision Timing/Sync** (window title)
  - **View Equipment Details…** (menu option)
  - **Administration** → **Security** → **User Provisioning…** (path for invoking a window)
- Filenames and system path information
  These are examples of filenames and system path information:
  - *setup.exe*
  - *C:\Program Files\Lucent Technologies*
- Keyboard entries
  These are examples of keyboard entries:
  - **F1**, **Esc X**, **Alt-F**, **Ctrl-D**, **Ctrl-Alt-Del** (simple keyboard entries)
    A hyphen between two keys means that both keys have to be pressed simultaneously. Otherwise, a single key has to be pressed, or several keys have to be pressed in sequence.
  - `copy abc xyz` (command)
    A complete command has to be entered.
- Alarms and error messages

These are examples of alarms and error messages:

- `STM Loss of Signal`
- `Circuit Pack Failure`
- `HP-UNEQ`, `MS-AIS`, `STMLOS`, `STMLOF`
- `Not enough disk space available`

Abbreviations

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

Related documentation

This section briefly describes the documents that are included in the *WaveStar* TDM 10G (STM-64) documentation set.

- Installation Manual
  The *WaveStar TDM 10G (STM-64) Installation Manual* is a step-by-step guide to system installation and setup. It also includes information needed for pre-installation site planning and post-installation acceptance testing.
- Applications, Planning, and Ordering Guide
  The *WaveStar TDM 10G (STM-64) Application, Planning and Ordering Guide (APOG)* is for use by network planners, analysts and managers. It is also for use by the Lucent Account Team. It presents a detailed overview of the system, describes its applications, gives planning requirements, engineering rules, ordering information, and technical specifications.
- User Operations Guide
  The *WaveStar TDM 10G (STM-64) User Operations Guide (UOG)*provides step-by-step information for use in daily system operations. The User Operations Guide (UOG) manual demonstrates how to perform system provisioning, operations, and administrative tasks by use of *WaveStar* CIT.
- Alarm Messages and Trouble Clearing Guide
  The *WaveStar TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide (AMTCG)* gives detailed information on each possible alarm message. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.
- TL1 Reference Manual

The *WaveStar TDM 10G (STM-64) TL1 Reference Manual* serves as a reference for all TL1 commands which can be used to operate the network element. The manual also gives an introduction to the concept of the TL1 commands and instructs how to use them.

- *WaveStar* SNMS Provisioning Guide (Application *WaveStar* TDM 10G (STM-64))
  The *WaveStar TDM 10G (STM-64) SNMS Provisioning Guide (Application WaveStar TDM 10G (STM-64))* gives instructions on how to perform system provisioning, operations, and administrative tasks by use of *WaveStar* SNMS.

The following table lists the documents included in the *WaveStar* TDM 10G documentation set.

Document Number	Title
CC109149773 (365-371-521)	*WaveStar* TDM 10G (STM-64) Applications, Planning, and Ordering Guide
CC109149781 (365-371-522)	*WaveStar* TDM 10G (STM-64) User Operations Guide
CC109149823 (365-371-525)	*WaveStar* TDM 10G (STM-64) Installation Manual
CC109149831 (365-371-526)	*WaveStar* TDM 10G (STM-64) TL1 Reference Manual
CC109149799 (365-371-523)	*WaveStar* TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide
CC109149807 (365-371-524)	*WaveStar* SNMS Provisioning Guide (Application *WaveStar* TDM 10G (STM-64))
CC109149856	CD-ROM Documentation *WaveStar* TDM 10G (STM-64) (all manuals on one CD-ROM)

How to comment

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

Customer comment form

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

How to order

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

Lucent Technologies Network Systems GmbH

Customer Training and Information Products (CTIP-SDH)

Thurn- und-Taxis-Str. 10

90327 Nürnberg, Germany

Fax: +49 911 526 3545

1 Safety

Overview

Purpose This chapter provides important safety instructions.

Contents

General notes on safety

Overview

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.

Not only must the general instructions in this chapter on safety be observed, but also the specific safety instructions in the individual chapters.

All safety instructions have a uniform appearance. Please refer to “Structure of safety instructions” (1-2).

The *WaveStar*® TDM 10G (STM-64) 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.

Potential sources of danger

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:

- live parts,
- laser light,
- hot surfaces,
- sharp edges, or
- components sensitive to electrostatic discharge.

Structure of safety instructions

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 serious burns to the hands and damage to the eyes.

Ensure that the line circuit-breaker on the Rack Connection Panel (RCP) 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.

Special safety instructions

The aspects of "laser safety" and "handling of components sensitive to electrostatic discharge (ESD)" are of vital importance for the *WaveStar* TDM 10G (STM-64) equipment. Therefore, the key safety instructions for these subjects are summarised in the sections "Laser safety" (1-5) and "Electrostatic discharge" (1-12).

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 unit/system must be under the ***permissible conditions only***.
  See accompanying documentation and information on the unit/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 unit/system, the personnel requires ***special training***.
- The unit/system must be operated by ***expert and authorised users only***.

The user must operate the unit/system only after having ***read and understood*** the 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 unit/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 unit/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 unit/system.
- Only use ***tested and virus-free*** floppy disks and streamer tapes.

Laser safety

System design

The Lucent Technologies *WaveStar*® TDM 10G (STM-64) system complies with 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 Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH) regulations and the international standards IEC-60825 or DIN/EN 60825 are met. Please also refer to "Laser product classification" (1-10).

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 or DIN/EN 60825 define the maximum output power of laser radiation for each laser class in accordance with the wavelength.

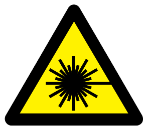
Laser class	Wavelength	Max. output power of laser radiation
1	1310 nm	8.85 mW
	1550 nm	10 mW
3A	1310 nm	24 mW
	1550 nm	50 mW
3B	1310 nm	0.5 W
	1550 nm	0.5 W

Laser warning labels

The laser warning labels indicate either only the laser class or both the laser class and the maximum output power of laser radiation.

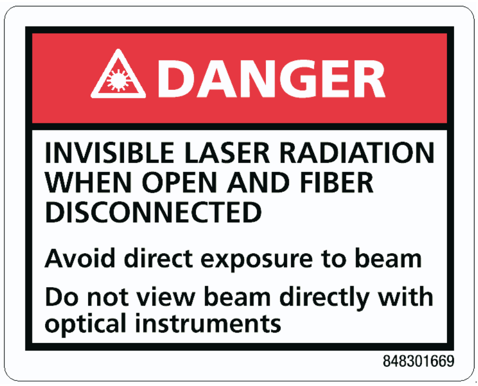
The following figure shows different types of laser warning labels and their characteristics.

❶



❷

❸



Legend

Legend to the different types of laser warning labels:

1. Laser warning symbol.
2. This laser warning label is mounted on the front cover outside. It always refers to normal operation.
3. This laser warning label is affixed inside the subrack.

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 can result in exposure to dangerous radiation.
- 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.

Optical circuit pack specifications

Specifications The following table contains the specifications of the optical circuit packs.

Circuit pack	Wavelength [nm]	Fiber type (core/cladding diameter) [µm]	Max. average output (normal operation)	Laser class (IEC / FDA)
OC3/STM1 Port Units				
1.3SR4, 4 ports (LEY16)	1310	SM (9.0/125)	−8.0 dBm	1 / I
1.3IR-SR8, 8 ports (LEY23)	1310	SM (9.0/125)	−8.0 dBm	1 / I
1.3LR4, 4 ports (LEY15)	1310	SM (9.0/125)	0.0 dBm	1 / I
OC12/STM4 Port Units				
1.3SR2 (LEY14)	1310	SM (9.0/125)	−8.0 dBm	1 / I
1.3LR2 (LEY13)	1310	SM (9.0/125)	+2.0 dBm	1 / IIIb
1.5LR1 (LEY190)	1550	SM (9.0/125)	+2.0 dBm	1 / I
OC48/STM16 Port Units				
1.3SR1 (LEY182)	1310	SM (9.0/125)	–1.0 dBm	1 / I
1.3LR1 (LEY7)	1310	SM (9.0/125)	+2.5 dBm	1 / IIIb
1.5LR1 (LEY8)	1550	SM (9.0/125)	+4.0 dBm	1 / I
OLS400G DWDM compatible (LEY101...180)	1530...1565	SM (9.0/125)	–4.8 dBm	1 / I
OLS80G DWDM compatible (LEY50...65)	1530...1565	SM (9.0/125)	–4.8 dBm	1 / I
OC192/STM64 Port Units				
1.5SR1 (LEY67)	1550	SM (9.0/125)	+2.0 dBm	1 / I
1.5IR1 (LEY69)	1550	SM (9.0/125)	+2.0 dBm	1 / I
1.5IRS1 (LEY97)	1550	SM (9.0/125)	+2.0 dBm	1 / I
DWDM compatible (LEY201...240)	1530...1565	SM (9.0/125)	–4.8 dBm	1 / I
Passive Optics (LEY284...299)	1530...1565	SM (9.0/125)	+2.0 dBm	1 / I
Optical Amplifiers				
OBA10G/1.5LR1 (SEN3)	1530 to 1565	SM (9.0/125)	+13 dBm	3A / IIIb
OBPA10G/1.5VR1 (SEN4)	1530 to 1565	SM (9.0/125)	+13 dBm	3A / IIIb
Ditech optical amplifiers	Please refer to the Ditech documentation.			

Important! It is the class of the circuit pack, not that of the telecommunications system as a whole, that is specified.

Connector types

With the exception of the 8-port OC3/STM1/S-1.1/1.3 µm port unit (LEY23), the DWDM-compatible OC192/STM64 port units (LEY201...240) and the optical booster amplifiers (SEN3, SEN4) and depending on the configuration, each of the optical circuit packs can be equipped with either of the following connector types:

- ST
- SC
- FC/PC

OC3/STM1/1.3IR-SR8 port unit

The 8-port OC3/STM1/1.3IR-SR8 (LEY23) circuit packs are equipped with LC-type connectors.

DWDM-compatible OC192/STM64 port units

The DWDM-compatible OC192/STM64 port units (LEY201...240) are equipped with LC-type connectors.

Optical booster amplifiers

The optical booster amplifiers (SEN3, SEN4) can be equipped with either of the following connector types:

- SC
- FC/PC

Laser product classification

Standards compliance

The *WaveStar*® TDM 10G (STM-64) product complies with both 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 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:

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

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

IEC requirements

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

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

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

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

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.

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:

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

Classification of optical telecommunication equipment

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

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

Electrostatic discharge

Overview

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

All semiconductor components are basically sensitive to electrostatic discharge. The electrostatic discharge can also affect the components indirectly via contacts or conductor tracks.

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 discharge.
- 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.

Important safety instructions for *WaveStar*® TDM 10G (STM-64) systems

Instructions

Especially observe the following safety instructions, they are of particular importance for *WaveStar* TDM 10G (STM-64) systems:

Invisible laser radiation

DANGER

Injury to eyes caused by invisible laser radiation.

WaveStar TDM 10G (STM-64) 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" (1-5)).

Power supply plug

DANGER

Arcing on removing or inserting a live power supply plug.

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

Ensure that the line circuit-breaker on the Rack Connection Panel (RCP) is in the "OFF" position before removing or inserting the power supply plug.

Shielded 10BaseT LAN cables

DANGER

Risk of electrical shock and/or serious injury

There is a risk of electrical shock and/or serious injury if shielded 10BaseT LAN cables are used, and the applicable national safety requirements have not been met.

*The usage of **shielded** 10BaseT LAN cables is only allowed if the applicable national safety requirements have been met by the user. Otherwise, there is a risk of electrical shock and/or serious injury.*

Electrostatic discharge (ESD)

CAUTION

Destruction of components by electrostatic discharge.

Electronic components can be destroyed by electrostatic discharge.

Plug-in units must therefore always be kept in antistatic covers. Use the original packaging if possible. Always observe the ESD instructions (cf. "Electrostatic discharge" (1-12)).

Overheating

CAUTION

Risk of fire due to overheating.

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

Therefore, ensure that the fans of a fan unit are not obstructed and strictly observe the six-month periodic fan filter replacement interval to avoid clogging of the filter and to always ensure a sufficient air flow!

2 Alarm messages

Overview

Purpose

The present chapter contains information about the alarm messages that can be reported by *WaveStar*® TDM 10G (STM-64) network elements.

Introduction

This chapter on network element (NE) alarm messages is organized as follows:

- The alarm descriptions are aphabetically ordered according to the alarm text displayed in the **Description** column of the *WaveStar* CIT **NE Alarm List**.
- For each NE alarm the following information is provided:
  - Meaning of the alarm
  - General alarm information
    includes the alarm's short designation, its alarm category, the type of Alarm Severity Assignment Profile (ASAP) the alarm belongs to, its default severity etc. Furthermore, a reference to the corresponding trouble clearing procedure is provided.
  - Additional alarm-related background information, if appropriate.

General alarm information

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

- Probable cause (alarm identifier),
- Alarm category,
- ASAP type,

- Default alarm severity,
- Alarm source,
- Local indications,
- Consequent actions,
- Effect on protection switching.

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

Probable cause (alarm identifier)

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

Please notice that the alarm short designation shown in both the *WaveStar* CIT **NE Alarm List** as well as in the *WaveStar* SNMS **Alarm List** is identical for the individual alarms. Nevertheless a distinction is made between *WaveStar* CIT and *WaveStar* SNMS in the general alarm information table. The reason is that the alarm short designations displayed when provisioning ASAPs by using the *WaveStar* SNMS are different to those displayed in the alarm lists. For ASAP provisioning purposes the *WaveStar* SNMS alarm short designations are preceeded by “SA_” or “NSA_” (`SA_STMF-LOS` and `NSA_STMF-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 general alarm information table.

Please refer to the 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” indicates the alarm category the corresponding alarm belongs to.

The following alarm categories are defined:

- The “Communication” alarm category is used for SDH transmission alarms, system timing and timing reference alarms and for alarms related to transmission protection switching.
- The “Equipment” alarm category is used for transmission, timing and control equipment circuit pack alarms, power supply system alarms, fan unit alarms and for alarms which are due to configuration problems.

- The “Processing” alarm category is used for control system software faults, autonomous reset events, storage problems and software version mismatches.
- The “Quality of service” alarm category is used for performance monitoring (PM) alarms.

ASAP type

The “ASAP type” indicates the Alarm Severity Assignment Profile (ASAP) the corresponding alarm belongs to.

Please refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for information about the available ASAP types.

Default alarm severity

The “Default alarm severity” indicates the factory settings of the corresponding alarm’s severity.

Alarm severities can be modified by means of Alarm Severity Assignment Profiles (ASAPs).

Alarm source

The “Alarm source” 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.

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

Each alarm that can be signalled via the user panel LEDs can be assigned one of the following alarm severities:

- Prompt, Critical (indicated via the red LED labelled “CR”),
- Prompt, Major (indicated via the red LED labelled “MJ”), or
- Deferred (indicated via the yellow LED labelled “MN”).

An alarm LED is lit, if at least one alarm of the corresponding severity is present.

Please refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for further information.

Consequent actions

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

Effect on protection switching

The “Effect on protection switching” entry briefly describes, where applicable, how protection switching is influenced by the corresponding alarm.

Service hotline

For the present *WaveStar* TDM 10G (STM-64) release, alarm descriptions and related maintenance and trouble clearing measures cannot be provided to the full extend. If you need technical support please contact the Lucent Technologies service hotline:

Telephone:	+49 911 526 2846
Facsimile:	+49 911 526 3131
E-mail:	htransde@lucent.com

Contents

Alarm Test

Meaning of the alarm

An alarm test is currently in progress.

The alarm indicators activated by an alarm test are the visual and audible office alarm outputs and the CR, MJ and MN LEDs on the user panel.

The `Alarm Test` alarm is a temporary indication, it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `Alarm Test` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `ALMTST` *WaveStar* CIT: `TSA`
Alarm category	Equipment
ASAP type	System Events
Default alarm severity	Not Reported
Alarm source	System
Local indications	An alarm test is performed. Please refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for a description of the sequence of indications during an alarm test.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `Alarm Test` alarm, the alarm will be cleared as soon as the alarm test has finished.

APS Channel Mismatch

Failure of APS protocol

This alarm is not supported for *WaveStar*® TDM 10G (STM-64) systems.

Since the alarm indicates a K1/K2 byte failure and thus constitutes a failure of the MSP automatic protection switching (APS) protocol it contributes to the `APS Failure of Protocol` alarm.

APS Failure of Protocol

Meaning of the alarm

Inconsistent or invalid K1/K2 bytes have been detected in a bidirectional 1+1 MSP configuration.

APS protocol

The K1 and K2 Multiplex Section Overhead (MSOH) bytes are used to transport the MSP automatic protection switching (APS) protocol in compliance with ITU-T Rec. G.841 and ETS 300 746.

General alarm information

The following brief overview provides important information concerning the `APS Failure of Protocol` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `FOP` *WaveStar* CIT: `APSFOP`
Alarm category	Communication
ASAP type	Automatic Protection Switch
Default alarm severity	Prompt, Major
Alarm source	1+1 optical protection group (Multiplex Section Protection, MSP)
Local indications	
Consequent actions	
Effect on protection switching	

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

APS Far-End Prot Line Failure

Failure of APS protocol

This alarm is not supported for *WaveStar*® TDM 10G (STM-64) systems.

Since the alarm indicates a K1/K2 byte failure and thus constitutes a failure of the MSP automatic protection switching (APS) protocol it contributes to the `APS Failure of Protocol` alarm.

APS Mode Mismatch

Failure of APS protocol

This alarm is not supported for *WaveStar*® TDM 10G (STM-64) systems.

Since the alarm indicates a K1/K2 byte failure and thus constitutes a failure of the MSP automatic protection switching (APS) protocol it contributes to the `APS Failure of Protocol` alarm.

APS Prot Switch Byte Failure

Failure of APS protocol

This alarm is not supported for *WaveStar*® TDM 10G (STM-64) systems.

Since the alarm indicates a K1/K2 byte failure and thus constitutes a failure of the MSP automatic protection switching (APS) protocol it contributes to the `APS Failure of Protocol` alarm.

AU Alarm Indication Signal

Meaning of the alarm

The incoming signal contains AU-AIS.

AU-AIS has been inserted by an upstream system as an indication to downstream equipment that the upstream system has detected a fault in the incoming signal or an equipment failure that has impacted the associated signal.

General alarm information

The following brief overview provides important information concerning the `AU Alarm Indication Signal` alarm:

Probable cause (alarm identifier)	*WaveStar®* SNMS: `AUF_AIS` *WaveStar* CIT: `AUAIS`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	
Effect on protection switching	

Trouble clearing

Please refer to “Clearing AU Alarm Indication Signal” (3-3).

AU Loss of Pointer

Meaning of the alarm

The expected signal structure cannot be found in the receive signal. The AU-N pointer has an invalid value, or too many consecutive New Data Flags (NDF) have been detected.

General alarm information

The following brief overview provides important information concerning the `AU Loss of Pointer` alarm:

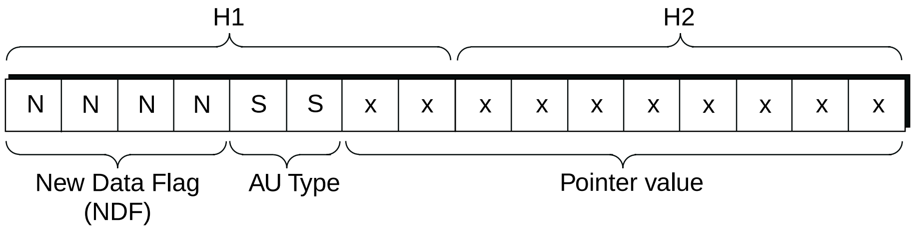
Probable cause (alarm identifier)	*WaveStar*® SNMS: `AUF_LOP` *WaveStar* CIT: `AULOP`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	
Effect on protection switching	

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Composition of the AU-N pointer

The AU-N pointer points to the start of the VC-n, i.e. the J1 byte in the VC-n Path Overhead (POH). The pointer value indicates the spacing in bytes between the pointer and the J1 byte and is contained in bits 7 to 16 of the H1 and H2 bytes; these are treated as a single 16-bit word.



Valid pointer value

AU-3 and AU-4 pointer values between 0 and 782 are regarded as valid.

New Data Flag

“NDF enabled” (“1001” in the first four bits of the H1 byte) is inserted if the AU-N pointer value changes for reasons not attributable to a stuffing operation.

If at least three of the four N bits contain the appropriate binary value, “NDF enabled” is considered as detected, i.e. if the N bits have the following values: “0001”, “1000”, “1001”, “1011” or “1101”.

AU Type

The “SS” bits indicate the AU-N type, their value is “10” for both AU-3 and AU-4.

Concatenation indication

For VC-4-4C and VC-4-16C signals a concatenation indication is used in the AU-N pointer to indicate a concatenated payload. The first AU-4 has a normal AU-4 pointer, all subsequent AU-4s contain the concatenation indication (H1/H2=“1001101111111111”) in the AU-4 pointer.

AU Signal Rate Mismatch

Meaning of the alarm

A mismatch has been detected in the input signal between the expected and the actual AU type.

General alarm information

The following brief overview provides important information concerning the `AU Signal Rate Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `AUF_SRM` *WaveStar* CIT: `AUSRM`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	–
Effect on protection switching	An AU Signal Rate Mismatch causes a path protection switch.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Auto Database Backup Failure

Not relevant! Although the `Auto Database Backup Failure` alarm is part of the "System Events" ASAP, it has no relevance for *WaveStar*® TDM 10G (STM-64) systems because an automatic database backup is not supported.

Automatic Laser Shutdown

Meaning of the alarm

The detection of an `STM Loss of Signal` condition led to an Automatic Laser Shutdown (ALS) on the optical circuit pack reporting the alarm.

The ALS functionality is implemented to avoid uncontrolled emission of laser radiation at unterminated fiber ends.

General alarm information

The following brief overview provides important information concerning the `Automatic Laser Shutdown` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `ALS` *WaveStar* CIT: `ALS`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

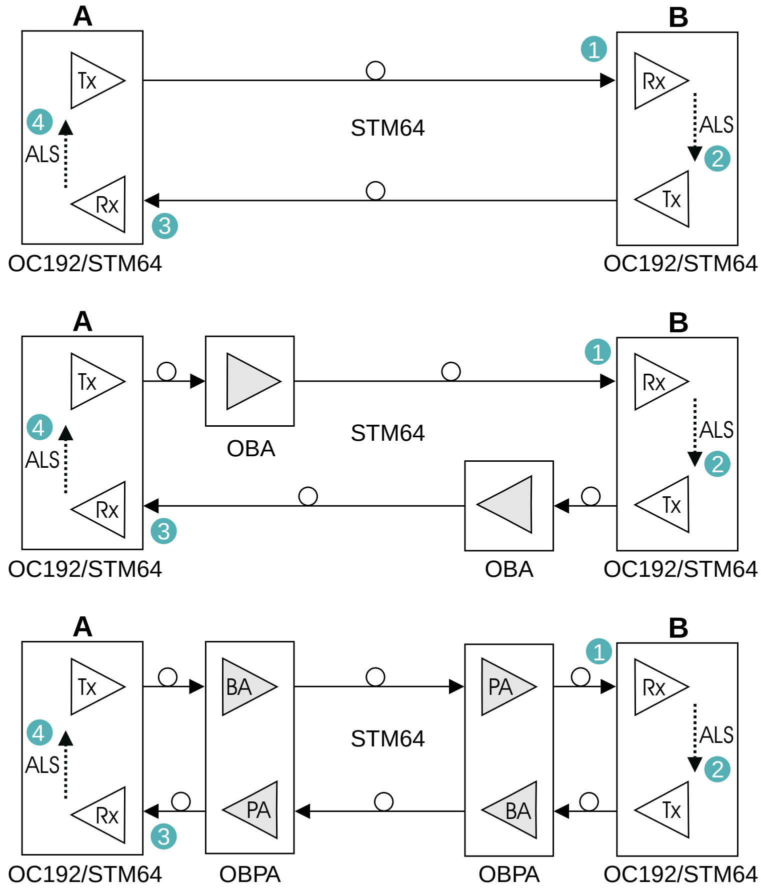
Circuit packs supporting the ALS functionality

The following circuit packs, where applicable in connection with optical amplifiers (OBA10G, OBPA10G), support the ALS functionality:

- OC192/STM64/1.5IR1 (LEY69),
- OC192/STM64/1.5IRS1 (LEY97),
- OC192/STM64/DWDM28 (LEY228).

Important! In conjunction with *WaveStar* OLS400G, ALS on the OC192/STM64/DWDM28 (LEY228) circuit pack should be disabled by means of the *WaveStar* CIT or *WaveStar* SNMS.

ALS scenarios The following figure shows three possible configurations where an ALS may occur.



In principle the behaviour with respect to the ALS functionality is the same for all three configurations (see the numbering in the figure):

1. The OC192/STM64 port unit in NE “B” detects an STM Loss of Signal condition and the corresponding alarm is reported.
2. As a consequence of the loss of signal, the laser in NE “B” is switched off by an ALS and the corresponding alarm is reported.
3. The OC192/STM64 port unit in NE “A” now also detects an STM Loss of Signal condition because the laser in NE “B” has been switched off, and the corresponding alarm is reported.
4. As a consequence, the laser in NE “A” is also switched off by an ALS and the corresponding alarm is reported.

Related information Please also refer to the *WaveStar TDM 10G (STM-64) User Operations Guide*.

Autonomous Reset

Meaning of the alarm

An `Autonomous Reset` alarm is reported immediately before a circuit pack is reset due to a fatal software error.

The `Autonomous Reset` alarm is a temporary indication; it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `Autonomous Reset` alarm:

Probable cause (alarm identifier)	*WaveStar®* SNMS: `ARST` *WaveStar* CIT: `AUTORESET`
Alarm category	Processing
ASAP type	System Events
Default alarm severity	Info
Alarm source	Circuit pack
Local indications	The red “FAULT” LED on the circuit pack is lit, it will be switched off during the restart.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `Autonomous Reset` alarm, the alarm will be cleared during the restart of the circuit pack.

BLSR Default K-bytes

Meaning of the alarm

The source node ID and the destination node ID in the received APS bytes (K1 and K2 bytes in the Multiplex Section Overhead (MSOH)) have equal values.

Default K-bytes

The K1 and K2 bytes are used to transport the MS-SPRing automatic protection switching (APS) protocol. Default K1 and K2 bytes with identical source node and destination node IDs are inserted when a ring node is not in a position to properly signal the MS-SPRing protection switching protocol, and therefore cannot properly execute MS-SPRing protection switching.

General alarm information

The following brief overview provides important information concerning the `BLSR Default K-bytes` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `BLSRDKB` *WaveStar* CIT: `BLSR-DKB`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is not possible.

Trouble clearing

Please refer to “Clearing BLSR Default K-bytes” (3-5).

BLSR Improper APS Codes

Meaning of the alarm

A `BLSR Improper APS Codes` alarm is reported

- if an expected request code in the K1 byte (bits 1 to 4) is not received within a predefined time limit of two seconds, or
- when invalid APS bytes (K1 and K2 bytes in the Multiplex Section Overhead (MSOH)) 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).

General alarm information

The following brief overview provides important information concerning the `BLSR Improper APS Codes` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `BLSRIMAPS` *WaveStar* CIT: `APSPROV`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPRing protection group
Local indications	–
Consequent actions	–
Effect on protection switching	An existing ring protection switch will be released when the BLSR Improper APS Codes condition is received on the long path. In a typical 2-fiber 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 BLSR Improper APS Codes” (3-10).

Background information

Please also refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for a general description of 2-fiber MS-SPRing protection switching.

BLSR Inconsistent APS Codes

Meaning of the alarm

The values of the APS bytes (K1 and K2 bytes in the Multiplex Section Overhead (MSOH)) 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.

General alarm information

The following brief overview provides important information concerning the `BLSR Inconsistent APS Codes` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `BLSRINAPS` *WaveStar* CIT: `APSC`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPRing protection group
Local indications	–
Consequent actions	–
Effect on protection switching	An existing ring protection switch will be released when the BLSR Inconsistent APS Codes condition is received on the long path. In a typical 2-fiber 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 BLSR Inconsistent APS Codes” (3-15).

BLSR Traffic Squelched

Meaning of the alarm

The `BLSR Traffic Squelched` alarm is reported by a ring node for each STM-N channel on which the traffic has been squelched.

General alarm information

The following brief overview provides important information concerning the `BLSR Traffic Squelched` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `BLSRTS` *WaveStar* CIT: `RNG-SQUELCH`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPRing protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Background information

Please refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for a general description of 2-fiber 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

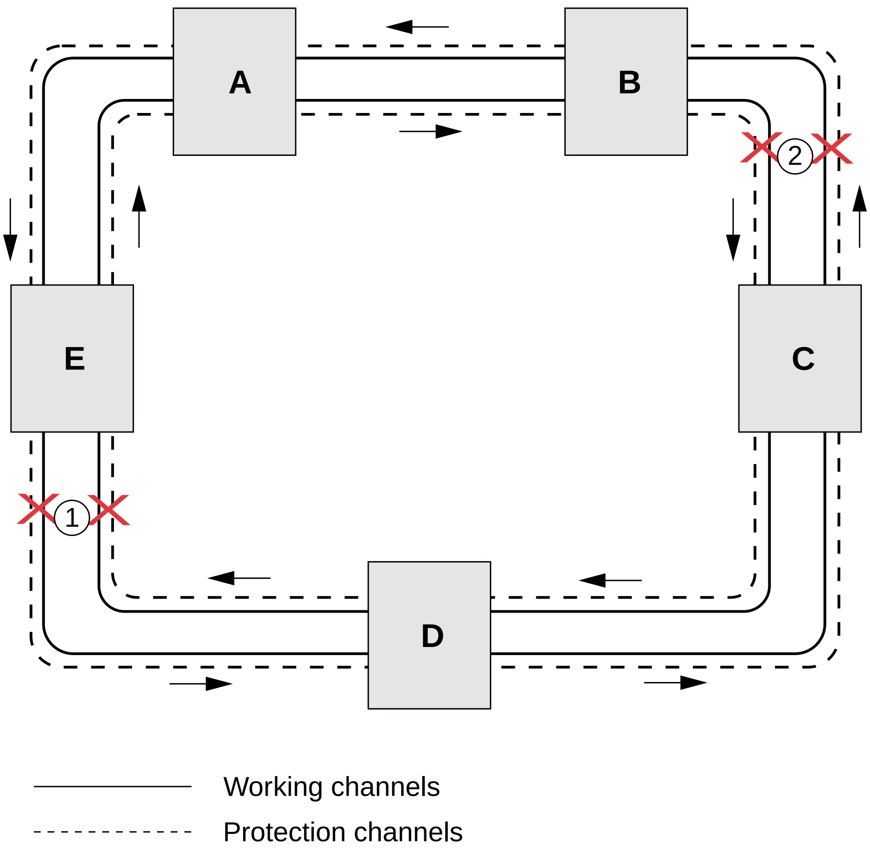
Squelching means replacing a potentially misconnected signal by an all-ones signal (Alarm Indication Signal, AIS). In the case of a *WaveStar* TDM 10G (STM-64) system, the traffic that cannot be protected will be squelched by replacing the payload signal with AU-AIS.

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.

Circuit Pack Failure

Meaning of the alarm

The alarm-reporting circuit pack is defective.

General alarm information

The following brief overview provides important information concerning the `Circuit Pack Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `CPFAIL` *WaveStar* CIT: `EQPT`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	
Consequent actions	–
Effect on protection switching	

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Circuit Pack Invalid

Meaning of the alarm

An invalid slot equipage status has been detected.

Depending on the slot equipage status, the following variants of the `Circuit Pack Invalid` alarm can be distinguished:

- `Circuit Pack Invalid, Illegal`
- `Circuit Pack Invalid, Unexpected`
- `Circuit Pack Invalid, Unknown`

General alarm information

The following brief overview provides important information concerning the `Circuit Pack Invalid` alarm:

Probable cause (alarm identifier)	*WaveStar®* SNMS: `CPINV` *WaveStar* CIT: `PRCDRERR` (procedure error)
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	Slot
Local indications	
Consequent actions	
Effect on protection switching	

Trouble clearing

Please refer to “Clearing Circuit Pack Invalid” (3-19).

Slot equipage status

The slot equipage status describes the state of the association between a slot and a circuit pack assigned to that slot.

Possible values of the slot equipage status are:

Empty	There is no circuit pack in the slot.
Unknown	A circuit pack is present in the slot but the latches (insertion and removal facilities) are not closed.

Unexpected	A circuit pack is present in the slot, is permitted for that slot, and the latches are closed. However, another type of circuit pack has previously been provisioned or preprovisoned for the slot.
Illegal	A circuit pack is present in the slot, and the latches are closed. However, the circuit pack is not permitted for that slot.
Valid	A circuit pack is present in the slot, is permitted and provisioned for that slot, and the latches are closed.

Configurable circuit packs per slot

The following tables list the configurable circuit packs per slot for the *WaveStar* TDM 10G (STM-64) main shelf and extension shelf.

Please observe the following notes:

- The STM1EE4 circuit pack (LEY40) can only be used for unprotected configurations.
- OC48/STM16 port units as well as the GE1/SX2 circuit pack always occupy two paired slots (01/02, 03/04, … , 13/14, 15/16).

Main shelf

In the main shelf, the circuit packs listed in the following table are permitted (provisionable) for the indicated slots.

Shelf	Slot AID	Provisionable circuit pack		
		Type	Variant	App. Code
1-1	switch0	SWITCH	STS576	LEY4
1-1	ctlmem0	CTL	SYS50DM	LEY10B
1-1	dccei	ADJCTL	DCC32EI	LEY1
1-1	ctlmem1	reserved		
1-1	tmg0	TMG	STRAT3	LLY2B
1-1	tmg1	TMG	STRAT3	LLY2B
1-1	switch1	SWITCH	STS576	LEY4
1-2	oaw, oae	OBA10G	1.5LR1	SEN3
		OBPA10G	1.5VR1	SEN4
1-2	pprocw	PPROC	STS192	LEY3
1-2	switch0	SWITCH	STS576	LEY4
1-2	ppls0	PPROC	STS192	LEY3

Shelf	Slot AID	Provisionable circuit pack		
		Type	**Variant**	**App. Code**
1-2	dccei	ADJCTL	DCC32EI	LEY1
1-2	ctlmem0	CTL	SYS50DM	LEY10B
1-2	ctlmem1	reserved		
1-2	tmg0	TMG	STRAT3	LLY2B
1-2	tmg1	TMG	STRAT3	LLY2B
1-2	ppls1	PPROC	STS192	LEY3
1-2	switch1	SWITCH	STS576	LEY4
1-2	pproce	PPROC	STS192	LEY3
1-1	01 … 08	STM1EE4	4	LEY40
		STM1E	4	LEY44
		OC3/STM1	1.3SR4	LEY16 (4 ports)
			1.3IR-SR8	LEY23 (8 ports)
			1.3LR4	LEY15 (4 ports)
		OC12/STM4	1.3LR2	LEY13
			1.3SR2	LEY14
			1.5LR2	LEY190
1-1	01/02, 03/04, 05/06, 07/08	OC48/STM16	1.3LR1	LEY7
			1.5LR1	LEY8
			DWDM… (OLS80G)	LEY50 – 65
			DWDM… (OLS400G)	LEY101 – 180
			1.3SR1	LEY182
		GE1	SX2	LEY309
1-1	eprn	STM1E	4	LEY44
1-1	eprotsw	EPS	64	LEY42

Shelf	Slot AID	Provisionable circuit pack		
		Type	**Variant**	**App. Code**
1-1	09 … 16	STM1EE4	4	LEY40
		STM1E	4	LEY44
		OC3/STM1	1.3SR4	LEY16 (4 ports)
			1.3IR-SR8	LEY23 (8 ports)
			1.3LR4	LEY15 (4 ports)
		OC12/STM4	1.3LR2	LEY13
			1.3SR2	LEY14
			1.5LR2	LEY190
1-1	09/10, 11/12, 13/14, 15/16	OC48/STM16	1.3LR1	LEY7
			1.5LR1	LEY8
			DWDM… (OLS80G)	LEY50 – 65
			DWDM… (OLS400G)	LEY101 – 180
			1.3SR1	LEY182
		GE1	SX2	LEY309
1-2	trw, tre	OC192/STM64	1.5SR1	LEY67
			1.5IR1	LEY69
			1.5IRS1	LEY97
			DWDM…	LEY201 – 240
			POU…	LEY284 – 299

Extension shelf

In the extension shelf, the circuit packs listed in the following table are permitted (provisionable) for the indicated slots.

Slot AID	Provisionable circuit pack		
	Type	**Variant**	**App. Code**
	STM1EE4	4	LEY40
	STM1E	4	LEY44
	OC3/STM1	1.3SR4	LEY16 (4 ports)
		1.3IR-SR8	LEY23 (8 ports)
		1.3LR4	LEY15 (4 ports)
	OC12/STM4	1.3LR2	LEY13
		1.3SR2	LEY14
		1.5LR2	LEY190
01/02, 03/04, 05/06, 07/08	OC48/STM16	1.3LR1	LEY7
		1.5LR1	LEY8
		DWDM… (OLS80G)	LEY50 – 65
		DWDM… (OLS400G)	LEY101 – 180
		1.3SR1	LEY182
	GE1	SX2	LEY309
switch0	SWITCH	STS576	LEY4
ctlmem0	CTL	SYS50DM	LEY10B
dccei	ADJCTL	DCC32EI	LEY1
ctlmem1	reserved		
tmg0	TMG	STRAT3	LLY2B
tmg1	TMG	STRAT3	LLY2B
switch1	SWITCH	STS576	LEY4
09 … 16	STM1EE4	4	LEY40
	STM1E	4	LEY44
	OC3/STM1	1.3SR4	LEY16 (4 ports)
		1.3IR-SR8	LEY23 (8 ports)
		1.3LR4	LEY15 (4 ports)
	OC12/STM4	1.3LR2	LEY13
		1.3SR2	LEY14
		1.5LR2	LEY190

Slot AID	Provisionable circuit pack		
	Type	**Variant**	**App. Code**
09/10, 11/12, 13/14, 15/16	OC48/STM16	1.3LR1	LEY7
		1.5LR1	LEY8
		DWDM… (OLS80G)	LEY50 – 65
		DWDM… (OLS400G)	LEY101 – 180
		1.3SR1	LEY182
	GE1	SX2	LEY309

Circuit Pack Unequipped/Missing

Meaning of the alarm

Although the circuit pack indicated in the alarm message is provisioned for the corresponding slot there is no circuit pack plugged-in.

General alarm information

The following brief overview provides important information concerning the `Circuit Pack Unequipped/Missing` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `CPUNEQ` *WaveStar* CIT: `REPLUNITMISS`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	–
Consequent actions	–
Effect on protection switching	The service is switched to the protection circuit pack if an equipment protection exists.

Trouble clearing

Please refer to “Clearing Circuit Pack Unequipped/Missing” (3-22).

Circuit Provisioning Error

Not relevant! Although the `Circuit Provisioning Error` alarm is part of the "BLSR/MS SPRing Protection Switch" ASAP, it has no relevance for the present *WaveStar*® TDM 10G (STM-64) release.

ClkOut Quality Failure

Meaning of the alarm

The clock signal at the external timing output port is squelched or replaced by AIS because the timing reference signal has failed. This means that either no timing reference signal is available, or the quality of the timing reference signal is insufficient.

General alarm information

The following brief overview provides important information concerning the `ClkOut Quality Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `CLKOUTQF` *WaveStar* CIT: `CLKOUTQF`
Alarm category	Communication
ASAP type	System Timing
Default alarm severity	Deferred
Alarm source	System timing, external timing output port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing ClkOut Quality Failure” (3-24).

DCC MSect Failure

Meaning of the alarm

The DCC-M link via the optical interface port indicated in the alarm message is unavailable.

A failure of a DCC-M link is usually associated with “higher level alarms” at the same optical interface port, such as

- `STM Loss of Signal`,
- `STM Loss of Frame`,
- `MSect Alarm Indication Signal`,
- `MSect Excessive Error`, or
- a hardware failure of the circuit packs involved in the DCC-M transmission.

General alarm information

The following brief overview provides important information concerning the `DCC MSect Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `DCCMS` *WaveStar* CIT: `DCCMSF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

DCC RSect Failure

Meaning of the alarm

The DCC-R link via the optical interface port indicated in the alarm message is unavailable.

A failure of a DCC-R link is usually associated with "higher level alarms" at the same optical interface port, such as

- `STM Loss of Signal`,
- `STM Loss of Frame`, or
- a hardware failure of the circuit packs involved in the DCC-R transmission.

General alarm information

The following brief overview provides important information concerning the `DCC RSect Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `DCCRS` *WaveStar* CIT: `DCCRSF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

DCC Tunnel Overflow

Meaning of the alarm

An automatically calculated IP route could not be stored in the routing table, because the maximum capacity of the routing table is exceeded.

General alarm information

The following brief overview provides important information concerning the `DCC Tunnel Overflow` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `DCCTO` *WaveStar* CIT: `DCCTO`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing DCC Tunnel Overflow” (3-26).

Capacity of the routing table

For each network element, up to 90 IP routes can be manually configured and stored in the routing table. Furthermore, up to 150 automatically calculated IP routes can be stored. Thus, a maximum of 240 IP routes can be stored in the routing table.

Related information

Please also refer to the *WaveStar TDM 10G (STM-64) User Operations Guide*.

Duplicate Ring Node

Meaning of the alarm

The `Duplicate Ring Node` alarm is reported by all the nodes in a ring if an erroneous MS-SPRing configuration has been detected.

General alarm information

The following brief overview provides important information concerning the `Duplicate Ring Node` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `DPRN` *WaveStar* CIT: `DUPL-RNG`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is suspended, no further MS-SPRing protection switching requests will be processed.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Erroneous MS-SPRing configurations

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

- Multiple ring nodes from the same *WaveStar* TDM 10G (STM-64) NE on the same ring.
- More than 16 nodes in a ring.

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

1. Duplicate TIDs (NE names)
   In the same ring there are multiple ring nodes from the same NE or multiple NEs with the same TID.
2. Duplicate NSAP addresses
   In the same ring there are multiple ring nodes from the same NE or multiple NEs with the same system identifier.
3. Duplicate node IDs
   There are more than 16 nodes in the ring.

Automatic node ID allocation

Each node within a ring is automatically allocated a node identifier (node ID). The node ID is a 4-bit address used in the 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
- a DCC controller (ADJCTL/DCCEI circuit pack) is re-initialized.

Maximum number of ring nodes

As the node ID is a 4-bit address, its value range is from 0 to 15, thus allowing a maximum of 16 nodes in a ring.

Environmental alarms on miscellaneous discrete inputs

Meaning

WaveStar® TDM 10G (STM-64) systems feauture a set of eight miscellaneous discrete inputs (MDIs) for user-defined applications. An MDI can be connected to monitor a temperature probe or a fire alarm device for example. MDIs can thus be used to trigger the reporting of application-specific environmental alarms.

General alarm information

The following brief overview provides important information concerning environmental alarms:

Probable cause (alarm identifier)	*WaveStar* SNMS: `ENVRON` *WaveStar* CIT: `MISC`
Alarm category	Environmental
ASAP type	Environmental
Default alarm severity	Not Reported
Alarm source	Miscellaneous Discrete Input (MDI)
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing environmental alarms” (3-28).

Related information

Please refer to the *WaveStar TDM 10G (STM-64) Installation Manual* for information about the electrical specifications and the pin assignment of the miscellaneous discrete inputs (MDIs) and miscellaneous discrete outputs (MDOs).

E/W Cable Error

Meaning of the alarm

Especially in rings where *WaveStar*® ADM-16/1 network elements are involved, it is necessary that the interface ports are strictly cabled east to west. A violation of this rule leads to an `E/W Cable Error` alarm.

The directionality of the interface port cabling is of no relevance as long as no *WaveStar* ADM-16/1 network elements are involved.

General alarm information

The following brief overview provides important information concerning the `E/W Cable Error` alarm:

Probable cause (alarm identifier)	*WaveStar* SNMS: `CABLE` *WaveStar* CIT: `RNG-CERR`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is suspended, no further MS-SPRing protection switching requests will be processed.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Extra Traffic Preempted

Meaning of the alarm

Any extra traffic in the ring has been preempted due to a ring protection switch.

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.

General alarm information

The following brief overview provides important information concerning the `Extra Traffic Preempted` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `ETP` *WaveStar* CIT: `RNG-PREEMPT`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Info
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Fan Failure

Meaning of the alarm

A `Fan Failure` alarm indicates that a fan unit problem has occurred. The possible causes of a `Fan Failure` alarm will be described following the general alarm information.

In the case of a Fan Failure, the running fans of the relevant fan unit operate at maximum speed to optimize the air flow.

General alarm information

The following brief overview provides important information concerning the `Fan Failure` alarm:

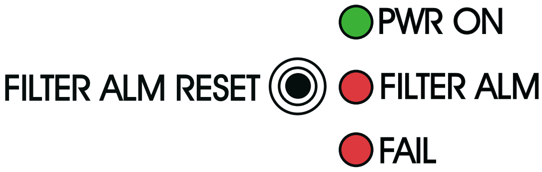
Probable cause (alarm identifier)	*WaveStar*® SNMS: `FAN` *WaveStar* CIT: `INT`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	Shelf
Local indications	via LEDs on the fan unit faceplate; please refer to the description following this overview.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

LEDs on the fan unit faceplate

Three LEDs are accomodated on the fan unit faceplate, “PWR ON”, “FILTER ALM” and “FAIL”. Beside the “FILTER ALM” LED a reset switch labelled “FILTER ALM RESET” is located.



PWR ON (green)	The PWR ON LED is lit as long as the fan unit is powered by one of the redundant power supplies.
FILTER ALM (red)	The FILTER ALM LED has no function in the present *WaveStar* TDM 10G (STM-64) release.
FAIL (red)	The FAIL LED is lit whenever a Fan Failure alarm is present while one of the redundant power supplies is available.
FILTER ALM RESET	The filter alarm reset switch has no function in the present *WaveStar* TDM 10G (STM-64) release.

Overheating

CAUTION

Risk of fire due to overheating.

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

Therefore, ensure that the fans of a fan unit are not obstructed and strictly observe the six-month periodic fan filter replacement interval to avoid clogging of the filter and to always ensure a sufficient air flow!

Possible causes of the alarm

These are the possible causes of a Fan Failure alarm:

1. Both power supplies have failed.
2. One of the two redundant power supplies has failed.
3. Two or more fans have failed.

4. A single fan has failed.
5. Filter alarm.

Alarm severity and visual indications

The alarm severity of a `Fan Failure` alarm depends on the affect on service (SA/NSA assignment) and on the actual value of the alarm severity assigned in the corresponding Alarm Severity Assignment Profile (ASAP).

The following tabular overview illustrates the SA/NSA assignment as well as the indications of the fan unit LEDs depending on the alarm cause (see possible causes):

	1	**2**	**3**	**4**	**5**
SA/NSA assignment	SA	SA	SA	NSA	NSA
PWR ON	off	on	on	on	on
FILTER ALM[1]	–	–	–	–	–
FAIL	off	on	on	on	on

Notes:

1. The FILTER ALM LED has no function in the present *WaveStar* TDM 10G (STM-64) release.

File Error

Meaning of the alarm

An error occurred during an autonomous file access (initiated by software) to the PCMCIA card. This is a non-hardware-related error such as non-recoverable data corruption or incompatibility errors.

General alarm information

The following brief overview provides important information concerning the `File Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `FERR` *WaveStar* CIT: `FERR`
Alarm category	Processing
ASAP type	System Events
Default alarm severity	Info
Alarm source	System controller
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

A `File Error` is an event, no user action is required.

HP Excessive Error

Meaning of the alarm

The bit error ratio (BER) in the higher order path, calculated using the B3 byte of the VC 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}.

General alarm information

The following brief overview provides important information concerning the `HP Excessive Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_EXC` *WaveStar* CIT: `HPEXC`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

HP Payload Label Mismatch

Meaning of the alarm

A mismatch has been detected between the expected and the actual payload structure of the path signal.

The signal label in the received path signal is not the same as the expected signal label which is either "equipped, non-specific" or "asynchronous mapping" (cf. C2 signal label).

General alarm information

The following brief overview provides important information concerning the `HP Payload Label Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_PLM` *WaveStar* CIT: `HPPLM`
Alarm category	Communication
ASAP type	Path Termination SDH
Default alarm severity	Prompt, Critical
Alarm source	VC-3, VC-4
Local indications	–
Consequent actions	AU-AIS (all-ones signal in the entire AU including the AU pointer) is inserted in the downstream direction. HP-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

C2 signal label

The signal label describes the payload structure contained in a path. The signal label for higher order paths is transmitted in the C2 byte of the VC-3 or VC-4 Path Overhead (POH).

These are, in hexadecimal representation, the predefined values of the C2 signal label (C2SL):

C2SL	Meaning
0x00	Unequipped
0x01	Equipped, non-specific

C2SL	Meaning
0x02	TUG structure
0x03	Locked TU
0x04	Asynchronous mapping of 34368 or 44736 kbit/s into the container C-3
0x05 … 0x11	reserved
0x12	Asynchronous mapping of 139264 kbit/s into the container C-4
0x13	ATM (Asynchronous Transfer Mode)
0x14	MAN (Metropolitan Area Network)
	DQDB (Distributed Queue Dual Bus)
0x15	FDDI (Fibre Distributed Data Interface)
0x16 … 0xFF	reserved

HP Remote Defect Indication

Meaning of the alarm

The signal in the higher order path contains HP-RDI.

The network element at the far end of the higher order path (in the downstream direction) has detected an error in the incoming signal and, as a consequent action, has inserted HP-RDI into the outgoing signal in the upstream direction.

HP-RDI is inserted as a result of `STM Loss of Signal`, `STM Loss of Frame`, `MSect Alarm Indication Signal`, `MSect Excessive Error`, `AU Alarm Indication Signal` and `AU Loss of Pointer`.

General alarm information

The following brief overview provides important information concerning the `HP Remote Defect Indication` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_RDI` *WaveStar* CIT: `HPRDI`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to "Clearing HP Remote Defect Indication" (3-30).

HP Signal Degrade

Meaning of the alarm

The bit error ratio (BER) in the higher order path, calculated using the B3 byte of the VC Path Overhead (POH), has exceeded the provisioned **HP DEG Threshold**.

The **HP DEG Threshold** can be set in terms of integer powers of ten between 10^{-5} and 10^{-9}. The default setting is 10^{-6}.

Please observe the required measurement times that have to elapse before a particular BER can be detected; cf. “Required measurement times” (2-55).

General alarm information

The following brief overview provides important information concerning the `HP Signal Degrade` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_DEG` *WaveStar* CIT: `HPDEG`
Alarm category	Communication
ASAP type	VC-N(c) Tributary
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	VC-n
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Required measurement times

Especially if the **HP DEG Threshold** is set to 10^{-7}, 10^{-8} or 10^{-9}, relatively long measurement times have to be taken into account to determine the bit error ratio.

BER	Required measurement time acc. to ITU-T Rec. G.783
10^{-3}	10 ms
10^{-4}	100 ms

BER	Required measurement time acc. to ITU-T Rec. G.783
10^{-5}	1 s
10^{-6}	10 s
10^{-7}	100 s
10^{-8}	1000 s (16 min, 40 s)
10^{-9}	10000 s (2 h, 46 min, 40 s)

HP Trace Identifier Mismatch

Meaning of the alarm

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

General alarm information

The following brief overview provides important information concerning the `HP Trace Identifier Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_TIM` *WaveStar* CIT: `HPTIM`
Alarm category	Communication
ASAP type	Path Termination SDH
Default alarm severity	Prompt, Critical
Alarm source	VC-3, VC-4
Local indications	–
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction. HP-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

HP Unequip

Meaning of the alarm

The VC-n (n=3 or 4) 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).

General alarm information

The following brief overview provides important information concerning the `HP Unequip` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HPF_UNEQ` *WaveStar* CIT: `HPUNEQ`
Alarm category	Communication
ASAP type	"VC-N(c) Tributary" or "Path Termination SDH", depending on whether • a through-connected path is to be monitored non-intrusively (→ VC-N(c) Tributary), or • a path termination is to be monitored (→ Path Termination SDH).
Default alarm severity	Depending on the ASAP type: • ASAP type "VC-N(c) Tributary": - Service Affecting (SA): Prompt, Critical - Non-Service Affecting (NSA): Not Reported • ASAP type "Path Termination SDH": Prompt, Critical
Alarm source	VC-3, VC-4
Local indications	–
Consequent actions	If `HP Unequip` has been detected at the path termination: • AIS (all-ones signal) is inserted in the downstream direction. • HP-RDI is inserted in the upstream (opposite) direction. The detection of `HP Unequip` at a non-intrusive monitoring (NIM) point does ***not*** result in consequent actions.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

C2 Signal Label

The Signal Label (SL) describes the payload structure of a path. The Signal Label for higher order paths is transmitted in the C2 byte of the VC-3 or VC-4 Path Overhead (POH).

These are, in hexadecimal representation, the predefined values of the C2 Signal Label:

C2 Signal Label	Meaning
0x00	Unequipped
0x01	Equipped, non-specific
0x02	TUG structure
0x03	Locked TU
0x04	Asynchronous mapping of 34368 or 44736 kbit/s into the container C-3
0x05 … 0x11	reserved
0x12	Asynchronous mapping of 139264 kbit/s into the container C-4
0x13	ATM (Asynchronous Transfer Mode)
0x14	MAN (Metropolitan Area Network) DQDB (Distributed Queue Dual Bus)
0x15	FDDI (Fibre Distributed Data Interface)
0x16 … 0xFF	reserved

Inconsistent Ring Prot Mode

Meaning of the alarm

Not all nodes in a ring are provisioned to use the same protection mode.

General alarm information

The following brief overview provides important information concerning the `Inconsistent Ring Prot Mode` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `BLSRDKB` *WaveStar* CIT: `BLSR-DKB`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is suspended, no further MS-SPRing protection switching requests will be processed.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Intruder Alert

Meaning of the alarm

Too many invalid user authentication attempts have been encountered for the user ID indicated in the alarm message. With the same user ID, it is not possible to login to the respective NE for a configurable time interval, the **User Id Lockout Period**.

Using the *WaveStar*® CIT, the maximum permissible number of invalid user authentication attempts can be defined by means of the **User Id Lockout Threshold**; please also refer to “Security administration” in the *WaveStar TDM 10G (STM-64) User Operations Guide*.

The alarm will be stored in the **NE Alarm Log**.

General alarm information

The following brief overview provides important information concerning the `Intruder Alert` alarm:

Probable cause (alarm identifier)	*WaveStar* SNMS: `IA` *WaveStar* CIT: `IA`
Alarm category	Security
ASAP type	The alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

The `Intruder Alert` alarm cannot be cleared.

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, e.g. one node is configured to operate in full duplex mode while the other node is configured to operate in half duplex mode.

General alarm information

The following brief overview provides important information concerning the `LAN Auto Negotiation Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LANANM` *WaveStar* CIT: `ANM`
Alarm category	Communication
ASAP type	Ethernet
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Not Reported
Alarm source	Ethernet port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Auto negotiation

WaveStar TDM 10G (STM-64) systems have an auto negotiation functionality implemented in acc. with IEEE 802.3 (§ 37 – “Auto-Negotiation function, type 1000BASE-X”). 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.

Configurable modes of operation

These modes of operation can be configured for *WaveStar* TDM 10G (STM-64) systems:

- Full duplex,
- Auto negotiate.

LAN Loss of Signal

Meaning of the alarm

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

General alarm information

The following brief overview provides important information concerning the `LAN Loss of Signal` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LANLOS` *WaveStar* CIT: `LOS`
Alarm category	Communication
ASAP type	Ethernet
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Not Reported
Alarm source	Ethernet port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Line Sync Reference Failure

Meaning of the alarm

The clock reference signal derived from an incoming STM-16 or STM-64 signal that is assigned as timing reference has failed or cannot be used for synchronisation.

Possible causes of the alarm

A `Line Sync Reference Failure` alarm is reported as a consequence of the following transmission alarms:

- `STM Loss of Signal`,
- `STM Loss of Frame`,
- `MSect Alarm Indication Signal`,
- `MSect Excessive Error`.

Furthermore, a hardware error on the corresponding port unit also leads to a `Line Sync Reference Failure` alarm.

General alarm information

The following brief overview provides important information concerning the `Line Sync Reference Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LINESYNC` *WaveStar* CIT: `SYNC`
Alarm category	Communication
ASAP type	System Timing
Default alarm severity	Prompt, Major
Alarm source	Assigned timing reference
Local indications	–
Consequent actions	–
Effect on protection switching	A `Line Sync Reference Failure` alarm causes a protection switch to another timing reference signal.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

LinkID MSect Mismatch

Meaning of the alarm

The link identification message received from the remote end node of the DCC-M (Line DCC) concerned contains a protocol version number that is not supported by the local node's NE software.

General alarm information

The following brief overview provides important information concerning the `LinkID MSect Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LIDMSMM` *WaveStar* CIT: `LIDMSM`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Link identification information

WaveStar TDM 10G (STM-64) network elements autonomously exchange link identification messages between the end nodes of enabled DCC links. Link identification information is used to automatically and unambiguously discover the ring or network topology.

The exchanged link identification messages contain the following information for both end nodes of an enabled DCC link:

- Link identification protocol version number
  The version number specifies which version of the link identification protocol is running at the end node.
- 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.

LinkID RSect Mismatch

Meaning of the alarm

The link identification message received from the remote end node of the DCC-R (Section DCC) concerned contains a protocol version number that is not supported by the local node's NE software.

Please also refer to "LinkID MSect Mismatch" (2-66).

General alarm information

The following brief overview provides important information concerning the `LinkID RSect Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LIDRSMM` *WaveStar* CIT: `LIDRSM`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Local NUT Not Operational

Meaning of the alarm

The operational NUT configuration is inconsistent with the local NUT configuration.

This situation may be caused by a DCC protocol failure for example.

Related information

Please also refer to the description of the NUT functionality (cf. “Non-preemptible unprotected traffic” (2-91)).

General alarm information

The following brief overview provides important information concerning the `Local Squelch Map Conflict` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NUTNOPR` *WaveStar* CIT: `NUTNOPR`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Not Reported
Alarm source	Tributary (VC-3, VC-4, VC-4-4C, VC-4-16C)
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Local Squelch Map Conflict

Meaning of the alarm

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

Please also refer to Background information.

General alarm information

The following brief overview provides important information concerning the `Local Squelch Map Conflict` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RSMC` *WaveStar* CIT: `SQMAP-CONFL`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Deferred
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Background information

Please refer to the *WaveStar TDM 10G (STM-64) User Operations Guide* for a general description of 2-fiber MS-SPRing protection switching.

Ring circuits

A ring circuit is a provisioned path within a ring at VC-3, VC-4, VC-4-4C or VC-4-16C tributary level, 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.

Local Squelch Map Inconsistent

Not relevant! Although the `Local Squelch Map Inconsistent` alarm is part of the "BLSR/MS SPRing Protection Switch" ASAP, it has no relevance for the present *WaveStar*® TDM 10G (STM-64) release.

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-n's (n=3 or 4) in the Virtual Concatenated Group (VCG) exceeds the range that can be compensated by buffering.

General alarm information

The following brief overview provides important information concerning the `Loss of Alignment` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LOA` *WaveStar* CIT: `LOA`
Alarm category	Communication
ASAP type	Ethernet
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Not Reported
Alarm source	Virtual Concatenated Group (VCG)
Local indications	–
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

VC-n-Xv payload realignment

The different VC-n's (n=3 or 4) of a VC-n-Xv 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-n's until the "slowest" VC-n 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-n is larger than the correction range, realignment is no longer possible and a `Loss of Alignment` alarm will be reported.

Loss of Frame Delineation

Meaning of the alarm

The beginning of an Ethernet over SDH (EoS) frame could not be recovered by the EoS frame delineation procedure.

General alarm information

The following brief overview provides important information concerning the `Loss of Frame Delineation` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `GFPLOF` *WaveStar* CIT: `GFPLOF`
Alarm category	Communication
ASAP type	Ethernet
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Not Reported
Alarm source	Virtual Concatenated Group (VCG)
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Ethernet over SDH frame delineation

The Ethernet over SDH (EoS) frame delineation procedure uses the received EoS frame’s core header to find the beginning of each EoS frame.

Loss of Multiframe

Meaning of the alarm

The receiver of the Gigabit Ethernet circuit pack 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).

Please note that Loss of Multiframe is not supported for VC-3, but only for VC-4.

General alarm information

The following brief overview provides important information concerning the `Loss of Multiframe` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `LOM` *WaveStar* CIT: `LOM`
Alarm category	Communication
ASAP type	Path Termination SDH
Default alarm severity	Prompt, Critical
Alarm source	VC-4 of a Virtual Concatenated Group (VCG)
Local indications	–
Consequent actions	AIS (all-ones signal in the affected VC-4 signals) is inserted in the downstream direction.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Virtual concatenation multiframe indicators

The consecutive frames of the VC-4 signals 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. The different 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 a 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 a 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-4 signals (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-4 signals, and, at the receiver, to compensate possible delay differences between the VC-4 signals of the Virtual Concatenated Group.

Mate Circuit Pack Unequipped

Meaning of the alarm

The `Mate Circuit Pack Unequipped` alarm applies only to circuit packs which depend on a partner (mate) circuit pack to provide a certain functionality. For *WaveStar*® TDM 10G (STM-64) systems, the STM-64 port unit functionality is realised by means of an OC192/STM64 circuit pack in combination with an associated pointer processing (PPROC/STS192) circuit pack.

The `Mate Circuit Pack Unequipped` alarm is reported for a circuit pack as shown in the following table when any one of the two partnering circuit packs is already provisioned while its mate circuit pack is:

- either preprovisioned and not yet plugged into its slot, or
- neither preprovisioned nor provisioned.

Mate circuit pack association

The following table shows the association between the circuit packs that might report a `Mate Circuit Pack Unequipped` alarm and their mate circuit packs.

Alarm-reporting circuit pack		Associated mate circuit pack	
OC192/STM64	in slot “tre”	PPROC/STS192	in slot “pproce”
	in slot “trw”		in slot “pprocw”
PPROC/STS192	in slot “pproce”	OC192/STM64	in slot “tre”
	in slot “pprocw”		in slot “trw”

Notice that once the two partnering circuit packs have both been provisioned, any subsequent circuit pack removal will ***not*** result in a `Mate Circuit Pack Unequipped` but in a `Circuit Pack Unequipped/Missing` alarm to be reported.

General alarm information

The following brief overview provides important information concerning the `Mate Circuit Pack Unequipped` alarm:

Probable cause (alarm identifier)	*WaveStar* SNMS: `MCPUNEQ` *WaveStar* CIT: `REPLUNITMISS`
Alarm category	Equipment
ASAP type	Equipment

Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing Mate Circuit Pack Unequipped” (3-32).

Memory Mismatch

Meaning of the alarm

There are discrepancies between the NE database and user-originated configuration data.

General alarm information

The following brief overview provides important information concerning the `Memory Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `MMIS` *WaveStar* CIT: `DATAFLT`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Deferred
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

MSect Alarm Indication Signal

Meaning of the alarm

The incoming STM-N signal contains MS-AIS.

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

General alarm information

The following brief overview provides important information concerning the `MSect Alarm Indication Signal` alarm:

Probable cause (alarm identifier)	*WaveStar®* SNMS: `MSF_AIS` *WaveStar* CIT: `MSAIS`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	AU-AIS (for all AUs contained in the STM-N signal) is inserted in the downstream direction.
Effect on protection switching	The alarm constitutes a Signal Fail (SF) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please refer to “Clearing MSect Alarm Indication Signal” (3-34).

MSect Excessive Error

Meaning of the alarm

The bit error ratio (BER) in the multiplex section, calculated using the B2 bytes of the Multiplex Section Overhead (MSOH), has exceeded the provisioned **MS DEXC Threshold**.

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

Possible causes of the alarm

An `MSect Excessive Error` alarm can have the following causes:

- Electrical STM-1 port:
  - excessive attenuation of the electrical signal (e.g. due to using a wrong coaxial cable),
  - incorrect formation of the STM signal at the far end,
  - considerable interference in the transmission path in the receive direction.
- Optical STM-N port:
  - excessive attenuation of the optical signal (e.g. due to connectors featuring impurities) on the transmit and/or receive side,
  - incorrect formation of the STM signal at the far end,
  - a defect in the optical transmitter at the far end,
  - considerable interference in the transmission path in the receive direction.

General alarm information

The following brief overview provides important information concerning the `MSect Excessive Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `MSF_EXC` *WaveStar* CIT: `MSEXC`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.

Consequent actions	Provided that **EBER AIS** is enabled: • AU-AIS is inserted in the downstream direction. • MS-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	The alarm constitutes a Signal Fail (SF) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

MSect Remote Failure Indication

Meaning of the alarm

The STM-N receive signal contains MS-RDI.

The network element at the far end of the multiplex section (in the downstream direction) has detected an error in the incoming signal and, as a consequent action, has inserted MS-RDI into the outgoing signal in the upstream direction.

MS-RDI is inserted as a result of `STM Loss of Signal`, `STM Loss of Frame`, `MSect Alarm Indication Signal` or `MSect Excessive Error`.

General alarm information

The following brief overview provides important information concerning the `MSect Remote Failure Indication` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `MSF_RDI` *WaveStar* CIT: `MSRDI`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing MSect Remote Failure Indication” (3-36).

MSect Server Signal Failure

Meaning of the alarm

An `MSect Server Signal Failure` alarm is derived from the following failure conditions:

- `STM Loss of Signal`, or
- `STM Loss of Frame`, or
- `RSect Trace Identifier Mismatch`, or
- `MSect Alarm Indication Signal`, or
- `MSect Excessive Error` (if **EBER AIS** is enabled).

General alarm information

The following brief overview provides important information concerning the `MSect Server Signal Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `MSF_SSF` *WaveStar* CIT: `MSSSF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

MSect Signal Degrade

Meaning of the alarm

The bit error ratio (BER) in the multiplex section, calculated using the B2 bytes of the Multiplex Section Overhead (MSOH), has exceeded the provisioned **MS Degrade Threshold**.

The **MS Degrade Threshold** can be set in terms of integer powers of ten between 10^{-5} and 10^{-9}. The default setting is 10^{-6}.

Please observe the required measurement times that have to elapse before a particular BER can be detected; cf. "Required measurement times" (2-86).

General alarm information

The following brief overview provides important information concerning the `MSect Signal Degrade` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `MSF_DEG` *WaveStar* CIT: `MSDEG`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	The red "FAULT" LED on the circuit pack is flashing.
Consequent actions	–
Effect on protection switching	The alarm constitutes a Signal Degrade (SD) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Required measurement times

Especially if the **MS Degrade Threshold** is set to 10^{-7}, 10^{-8} or 10^{-9}, relatively long measurement times have to be taken into account to determine the bit error ratio.

BER	Required measurement time acc. to ITU-T Rec. G.783
10^{-3}	10 ms

BER	Required measurement time acc. to ITU-T Rec. G.783
10^{-4}	100 ms
10^{-5}	1 s
10^{-6}	10 s
10^{-7}	100 s
10^{-8}	1000 s (16 min, 40 s)
10^{-9}	10000 s (2 h, 46 min, 40 s)

Node ID Mismatch

Meaning of the alarm

The node IDs in the received APS bytes (K1 and K2 bytes in the Multiplex Section Overhead (MSOH)) are inconsistent with the ring topology data stored in the node's ring map.

A Node ID Mismatch condition causes a ring topology discovery.

General alarm information

The following brief overview provides important information concerning the `Node ID Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NIDM` *WaveStar* CIT: `NID-CONFL`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Non-Volatile Memory Usage

Meaning of the alarm

The `Non-Volatile Memory Usage` alarm is reported whenever system usage of NVM has exceeded a high threshold mark indicating that in the NVM the minimum amount of space required as spare capacity has been reached.

General alarm information

The following brief overview provides important information concerning the `Non-Volatile Memory Usage` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NVMUSG` *WaveStar* CIT: `BKUPMEMO`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Deferred
Alarm source	System controller
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Non-Volatile Memory Wearout

Meaning of the alarm

The capacity of the Non-volatile memory (NVM) is exhausted.

With repeated use and over time the number of the NVM's data clusters that are marked "failed" will generally increase. Whenever the number of failed data clusters exceeds a predetermined threshold where the NVM no longer has sufficient capacity, the `Non-Volatile Memory Wearout` alarm will be reported.

General alarm information

The following brief overview provides important information concerning the `Non-Volatile Memory Wearout` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NVMW` *WaveStar* CIT: `BKUPMEMP` (Primary backup memory failure)
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

NUT Disabled

Meaning of the alarm

The protection attribute of at least one timeslot has been provisioned to “Not Protected” or “Temporarily Not Protected” in the local node, but non-preemptible unprotected traffic (NUT) is disabled because at least one node in the ring cannot handle NUT.

The alarm is reported for the node where the protection attribute has been modified.

Related information

Please also refer to the description of the NUT functionality provided subsequent to the general alarm information.

General alarm information

The following brief overview provides important information concerning the `NUT Disabled` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NUTDSBLD` *WaveStar* CIT: `NUTDSBLD`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Not Reported
Alarm source	Tributary (VC-3, VC-4, VC-4-4C, VC-4-16C)
Local indications	–
Consequent actions	–
Effect on protection switching	“Standard” MS-SPRING protection switching is possible, non-preemptible unprotected traffic (NUT) is ***not*** possible.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Non-preemptible unprotected traffic

In some network applications, layered protection can lead to excessive usage of the bandwidth. An SNCP protected path transported over an MS-SPRING protected ring would require to reserve four times the available bandwidth.

Non-preemptible unprotected traffic (NUT) offers the possibility to selectively exclude timeslots from the MS-SPRING protection.

Basic MS-SPRING protection switching offers ring protection on all timeslots (tributaries) of an optical line. Whenever a protection switch request must be executed, the switching nodes make a bridge and switch on all service/working tributaries (timeslots 1-96 for VC-3, timeslots 1-32 for VC-4) of the failed line, using the corresponding protection tributaries of the opposite line, hence looping back the traffic away from the failure and using the full protection bandwidth the other way around the ring.

Although the possibility exists to use the protection bandwidth for low priority traffic (“extra traffic”), still this traffic cannot be guaranteed because any failure anywhere in the ring will cause a loss of this traffic due to preemption.

A better availability can be achieved by making - temporarily or permanently - particular protection timeslots unaccessible for protection purposes, i.e. making the traffic in the selected timeslots “non-preemptible”. As there is a 1:1 relationship between service/working and protection timeslots, making a protection timeslot non-preemptible also means to make its corresponding service/working timeslot unprotected. Traffic contained in such timeslots is called non-preemptible unprotected traffic (NUT).

WaveStar TDM 10G (STM-64) systems make use of a proprietary algorithm to implement non-preemptible unprotected traffic.

Protection attribute

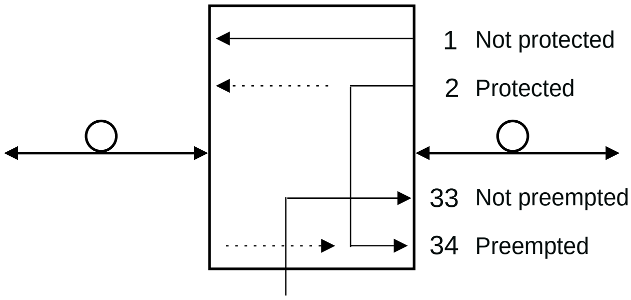
Each timeslot of an MS-SPRING protected optical line is assigned a so-called protection attribute. For service/working timeslots, the protection attribute indicates whether or not the corresponding tributary is protected by MS-SPRING. For protection timeslots, the protection attribute indicates whether or not the corresponding tributary may be preempted by MS-SPRING protection switching.

As service/working and protection timeslots are always paired, the value of the protection attribute of a service/working timeslot determines the value of this attribute for the corresponding protection timeslot.

The following table shows the possible values of the protection attribute for service/working and protection timeslots, and how they are correlated:

Service/working timeslots	Protection timeslots
Protected	Preemptible
Not Protected	Non-Preemptible
Temporarily Not Protected	Temporarily Non-Preemptible

The following figure illustrates NUT behaviour in an MS-SPRING switching node showing two pairs of service/working and protection timeslots (VC-4 tributaries) as an example.



Local NUT configuration

The local NUT configuration represents the settings of the protection attributes of all timeslots in the local node. Note that the protection attributes of service/working timeslots can be user-provisioned, while the protection attribute of the corresponding protection timeslots are automatically derived from these settings.

Operational NUT configuration

To make NUT operational, it is necessary that the local settings all nodes in the ring are identical concerning the NUT configuration.

The operational NUT configuration represents the settings of the protection attributes of all timeslots for the entire ring. The operational NUT configuration is automatically generated.

A modification of the local NUT configuration in any node of the ring is broadcasted to all other nodes in the ring via DCC. If a timeslot is set to “Not Protected” in a node, then it can only be set to “Protected” again from the same node. Consequently, if two nodes have the same timeslot set to “Not Protected”, then it must be changed back to “Protected” in both nodes before it is protected again.

Each node may have a different local NUT configuration, but all nodes must have the same operational NUT configuration.

Related alarms

These alarms are related to non-preemptible unprotected traffic:

- `Local NUT Not Operational`
- `NUT Disabled`
- `NUT Inconsistent XC Granularity`
- `Temporary NUT Provisioned`

NUT Inconsistent XC Granularity

Meaning of the alarm

The VC-4s of a concatenated signal do not have the same protection attribute in the operational NUT configuration.

Related information

Please also refer to the description of the NUT functionality (cf. “Non-preemptible unprotected traffic” (2-91)).

General alarm information

The following brief overview provides important information concerning the `NUT Inconsistent XC Granularity` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NUTINXCGRN` *WaveStar* CIT: `NUTINXCGRN`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Not Reported
Alarm source	Tributary (VC-4, VC-4-4C, VC-4-16C)
Local indications	–
Consequent actions	–
Effect on protection switching	Non-preemptible unprotected traffic (NUT) for the affected concatenated signal is ***not*** possible.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Out of Memory Error

Meaning of the alarm

The controller on the alarm-reporting circuit pack has run out of allocatable dynamic memory.

An `Out of Memory Error` results in a reset of the respective controller.

General alarm information

The following brief overview provides important information concerning the `Out of Memory Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `OMERR` *WaveStar* CIT: `WKGMEM`
Alarm category	Processing
ASAP type	System Events
Default alarm severity	Info
Alarm source	Circuit pack
Local indications	The red “FAULT” LED on the circuit pack is lit, it will be switched off during the restart.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Path Integrity Failure

Not relevant! Although the `Path Integrity Failure` alarm is part of the "BLSR/MS SPRing Protection Switch" ASAP, it has no relevance for the present *WaveStar*® TDM 10G (STM-64) release.

Path Switch Active

Meaning of the alarm

A path protection switch occurred.

The `Path Switch Active` message is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `Path Switch Active` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `PSACT` *WaveStar* CIT: `PSA`
Alarm category	Communication
ASAP type	Path Protection Switch
Default alarm severity	Not Reported
Alarm source	Path protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures.

Path Switch Failure

Meaning of the alarm

A path protection switch could not be performed due to insufficient signal quality in the protection path.

General alarm information

The following brief overview provides important information concerning the `Path Switch Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `PSFAIL` *WaveStar* CIT: `PSF`
Alarm category	Communication
ASAP type	Path Protection Switch
Default alarm severity	Info
Alarm source	Path protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Path Switch Inhibited

Meaning of the alarm

General alarm information

The following brief overview provides important information concerning the `Path Switch Inhibited` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `PSINH` *WaveStar* CIT: `PSI`
Alarm category	Communication
ASAP type	Path Protection Switch
Default alarm severity	Info
Alarm source	Path protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Power/Fuse Failure

Meaning of the alarm

One of the primary voltages (“Feeder A” or “Feeder B”) has failed. The redundancy of the primary voltage circuits is no longer ensured.

If, deliberately, only one of the primary voltage circuits is used, the alarm for the unused voltage supply can be ignored.

General alarm information

The following brief overview provides important information concerning the `Power/Fuse Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `FUSE` *WaveStar* CIT: `PWR`
Alarm category	Equipment
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	Shelf
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Resource Usage

Meaning of the alarm

The controller on the alarm-reporting circuit pack is overloaded, at least one of its resources is nearly exhausted. Examples of exhaustible resources are CPU, DRAM or buffers. The type of overloaded resource is indicated in the alarm message.

The first detected resource overload situation causes the `Resource Usage` alarm to be reported for the corresponding overloaded resource. The detection of any subsequent resource overload situation does not lead to a new `Resource Usage` alarm. Instead the first reported alarm will remain active as long as there is at least one resource overloaded.

General alarm information

The following brief overview provides important information concerning the `Resource Usage` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RSCUSG` *WaveStar* CIT: `PROCROVLD-1` (processor overload error 1)
Alarm category	Processing
ASAP type	Equipment
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Major • Non-Service Affecting (NSA): Deferred
Alarm source	Circuit pack
Local indications	The red “FAULT” LED on the circuit pack is lit.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Ring Circuit Alarm Suppressed

Not relevant! Although the `Ring Circuit Validation Suspended` alarm is part of the “BLSR/MS SPRing Protection Switch” ASAP, it has no relevance for the present *WaveStar*® TDM 10G (STM-64) release because ring circuit validation (also known as ring circuit audits) is not supported.

Ring Circuit Validation Suspended

Not relevant! Although the `Ring Circuit Validation Suspended` alarm is part of the “BLSR/MS SPRing Protection Switch” ASAP, it has no relevance for the present *WaveStar*® TDM 10G (STM-64) release because ring circuit validation (also known as ring circuit audits) is not supported.

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.

General alarm information

The following brief overview provides important information concerning the `Ring Discovery in Progress` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RDIP` *WaveStar* CIT: `RNG-DSCVY`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Info
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is 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” (3-38).

Automatic discovery of the ring topology

As a prerequisite for MS-SPRing protection switching the topology of the ring must be known at each ring node. *WaveStar* TDM 10G (STM-64) network elements have a proprietary algorithm implemented to discover the ring topology automatically.

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” (2-43)).

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

Please also refer to “Link identification information” (2-66).

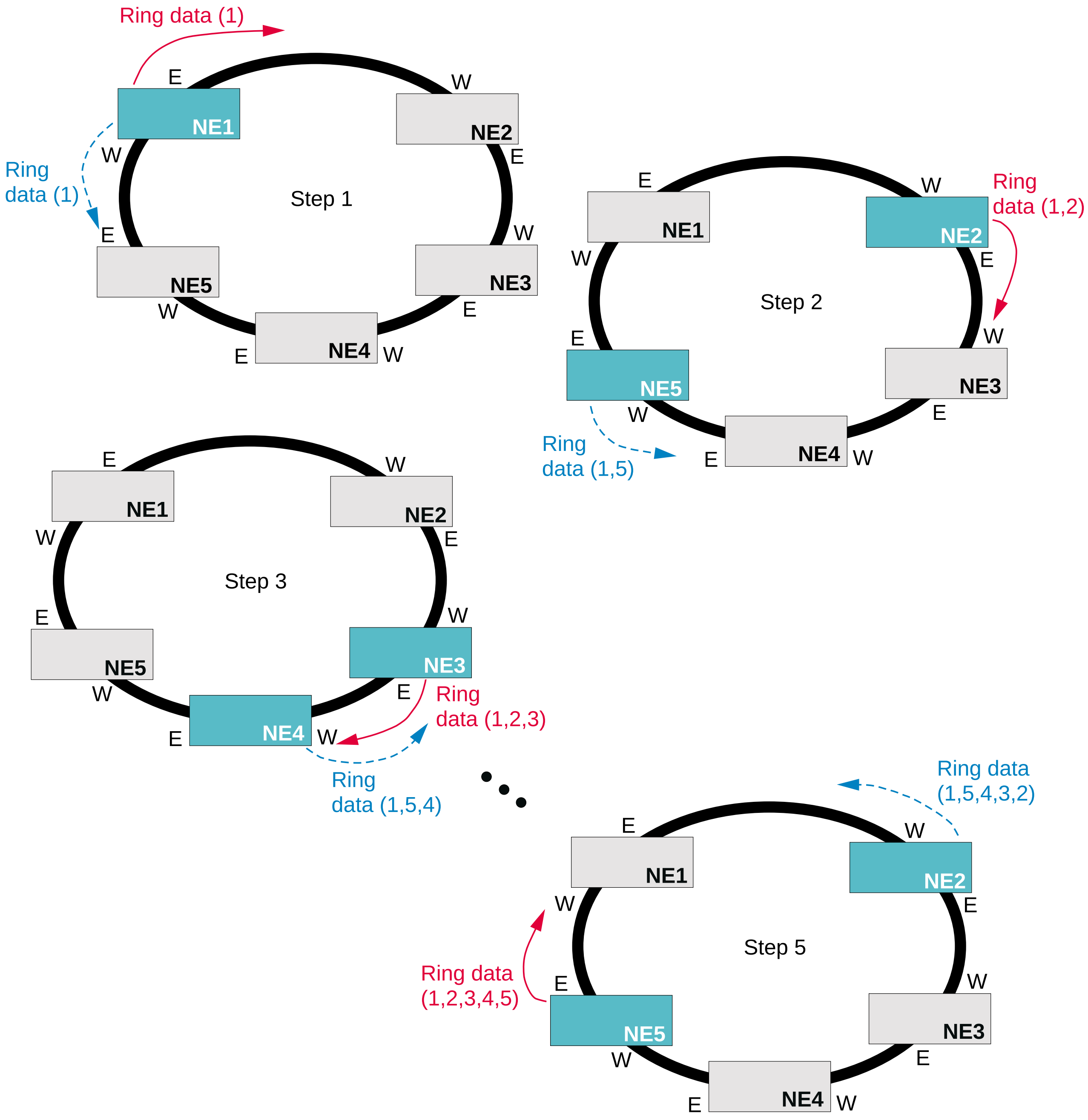
This way, at each ring node sufficient information is available to form a ring map representing the ring topology.

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 MS-SPRing port protection group, or when the local DCC controller (ADJCTL/DCCEI circuit pack) 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

The following alarms are related to the ring topology discovery:

- `Ring Discovery in Progress`
- `Ring Incomplete`
- `E/W Cable Error`

Ring Incomplete

Meaning of the alarm

A `Ring Incomplete` alarm is reported if no correct ring topology can be discovered, please also refer to "Ring Discovery in Progress" (2-104).

General alarm information

The following brief overview provides important information concerning the `Ring Incomplete` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RINC` *WaveStar* CIT: `RNG-INC`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is suspended, no further MS-SPRing protection switching requests will be processed.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Ring Open

Not relevant!

Although the `Ring Open` alarm is part of the "BLSR/MS SPRing Protection Switch" ASAP, it has no relevance for *WaveStar*® TDM 10G (STM-64) systems.

The alarm is only relevant for 4-fiber MS-SPRing configurations which are not supported in the present *WaveStar* TDM 10G (STM-64) release.

Ring Prot Switching 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 Prot Switching Suspended` alarm is cleared as soon as the ring node has a valid node ID and ring map.

General alarm information

The following brief overview provides important information concerning the `Ring Prot Switching Suspended` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RPSS` *WaveStar* CIT: `OVRDSW`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Prompt, Major
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	MS-SPRing protection switching is suspended, no further MS-SPRing protection switching requests will be processed.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

RSect Trace Identifier Mismatch

Meaning of the alarm

The received RSect trace identifier in the J0 byte of the Regenerator Section Overhead (RSOH) does not match the expected RSect trace identifier.

General alarm information

The following brief overview provides important information concerning the `RSect Trace Identifier Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RSF_TIM` *WaveStar* CIT: `RSTIM`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction. MS-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	The alarm constitutes a Signal Fail (SF) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Sequence Number Mismatch

Meaning of the alarm

The accepted and the expected sequence number of at least one VC-n (n=3 or 4) in a Virtual Concatenated Group (VCG) do not match.

General alarm information

The following brief overview provides important information concerning the `Sequence Number Mismatch` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SQM` *WaveStar* CIT: `SQM`
Alarm category	Communication
ASAP type	Path Termination SDH
Default alarm severity	Prompt, Critical
Alarm source	VC-n (n=3 or 4) of a Virtual Concatenated Group (VCG)
Local indications	–
Consequent actions	AIS (all-ones signal in the affected VC-n’s) is inserted in the downstream direction.
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Sequence numbers

Sequence numbers are used to signal to the receive end in which order the VC-n’s (n=3 or 4) of the VC-n-Xv Virtual Concatenated Group (VCG) are filled with payload data and to check that ordering of the VC-n’s inside the VC-n-Xv has not been altered during transport.

Each VC-n inside a VC-n-Xv 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.

Software Error

Meaning of the alarm

A controller software error occurred on the respective circuit pack.

Two variants of the `Software Error` alarm can be distinguished:

- `Software Error, fatal`
  A fatal software error is an unexpected event that might or will jeopardize further program execution. Fatal software errors include invalid return codes, bus errors, address errors, illegal instructions and division by zero.
  Fatal software errors result in a reset of the respective circuit pack.
- `Software Error, non-fatal`
  A non-fatal software error is an unexpected event that does not jeopardize further program execution, for example, when incorrect data has been input leading to wrong or no status information to be sent.
  Non-fatal software errors do not result in a reset of the respective circuit pack.

General alarm information

The following brief overview provides important information concerning the `Software Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SWERR` *WaveStar* CIT: `SFT`
Alarm category	Processing
ASAP type	System Events
Default alarm severity	Info
Alarm source	Circuit pack
Local indications	The red “FAULT” LED on the circuit pack is lit for fatal software errors. For non-fatal software errors there are no local indications because non-fatal software errors do not result in a circuit pack reset.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Startup/Initialization Complete

Meaning of the alarm

At the completion of the system startup, the `Startup/Initialization Complete` “alarm” is reported to indicate that the system is functional and ready to accept commands.

The `Startup/Initialization Complete` message is a temporary indication; it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `Startup/Initialization Complete` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SSC` *WaveStar* CIT: `INIT-1`
Alarm category	Equipment
ASAP type	The `Startup/Initialization Complete` alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `Startup/Initialization Complete` alarm.

STM Loss of Frame

Meaning of the alarm

The position of the frame alignment bytes A1 and A2 cannot be detected correctly in the STM-N receive signal.

General alarm information

The following brief overview provides important information concerning the `STM Loss of Frame` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `RSF_LOF` *WaveStar* CIT: `STMLOF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction. MS-RDI is inserted in the upstream (opposite) direction.
Effect on protection switching	The alarm constitutes a Signal Fail (SF) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

STM Loss of Signal

Meaning of the alarm

The optical or electrical STM-N port unit indicated in the alarm message receives no signal or the signal level is too low.

Possible causes of the alarm

An `STM Loss of Signal` alarm can have the following causes:

- Electrical STM-1 port:
  - cable break along the route,
  - inputs and outputs are mixed up,
  - hardware error on the electrical STM-1 port unit or on the associated electrical STM-1 I/O-panel.
- Optical STM-N port:
  - cable break along the route,
  - inputs and outputs are mixed up,
  - connector is not terminated or features impurities,
  - signal power outside the permissible range,
  - defective optical receiver,
  - defective optical transmitter at the far end,
  - STM-N signal levels mixed up.

General alarm information

The following brief overview provides important information concerning the `STM Loss of Signal` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `STMF_LOS` *WaveStar* CIT: `STMLOS`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Prompt, Critical • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	AIS (all-ones signal) is inserted in the downstream direction. MS-RDI is inserted in the upstream (opposite) direction.

Effect on protection switching	The alarm constitutes a Signal Fail (SF) condition and is a trigger for MS protection switching (MSP or MS-SPRing, depending on the configuration).

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Sync Reference Failure

Meaning of the alarm

There is no external clock source connected to an external timing input that is assigned as timing reference, or the signal connected cannot be used for synchronisation.

General alarm information

The following brief overview provides important information concerning the `Sync Reference Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SYNCREF` *WaveStar* CIT: `SYNC`
Alarm category	Communication
ASAP type	System Timing
Default alarm severity	Prompt, Major
Alarm source	Assigned external timing reference
Local indications	The red “FAULT” LED on the circuit pack is flashing.
Consequent actions	–
Effect on protection switching	A `Line Sync Reference Failure` alarm causes a protection switch to another timing reference signal.

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

System Clock Holdover

Meaning of the alarm

The internal timing generator has entered the holdover mode.

Possible causes of the alarm

There are two possible causes of the `System Clock Holdover` alarm:

- All assigned timing references have failed. The internal timing generator is not synchronised externally, and therefore has entered the holdover mode.
- A forced switch to the holdover mode has been carried out.

General alarm information

The following brief overview provides important information concerning the `System Clock Holdover` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `HOLDOVER` *WaveStar* CIT: `HLDOVRSYNC`
Alarm category	Communication
ASAP type	System Timing
Default alarm severity	Deferred
Alarm source	System timing
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

System in Maintenance Condition

Meaning of the alarm

The system has been placed into maintenance condition either due to a user command or autonomously (if the PCMCIA card is corrupted or unavailable for example).

The `System in Maintenance Condition` alarm is a temporary indication; it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `System in Maintenance Condition` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SIMC` *WaveStar* CIT: `SCMMA`
Alarm category	Equipment
ASAP type	The `System in Maintenance Condition` alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `System in Maintenance Condition` alarm.

System in Restoration Mode

Meaning of the alarm

The system has been placed into restoration mode.

The `System in Restoration Mode` alarm is a temporary indication; it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `System in Restoration Mode` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SIRM` *WaveStar* CIT: `RCVRY`
Alarm category	Equipment
ASAP type	The `System in Restoration Mode` alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `System in Restoration Mode` alarm.

System Restart

Meaning of the alarm

The system controller is currently restarting. After the restart has completed a `Startup/Initialization Complete` alarm will be reported.

The `System Restart` alarm is a temporary indication, it is to be understood as an information rather than as an alarm.

General alarm information

The following brief overview provides important information concerning the `System Restart` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `SRST` *WaveStar* CIT: `SYSBOOT`
Alarm category	Equipment
ASAP type	The `System Restart` alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

There are no specific trouble clearing measures for the `System Restart` alarm.

Temporary NUT Provisioned

Meaning of the alarm

The protection attribute of at least one timeslot has been set to "Temporarily Not Protected" in the local NUT configuration.

Related information

Please also refer to the description of the NUT functionality (cf. "Non-preemptible unprotected traffic" (2-91)).

General alarm information

The following brief overview provides important information concerning the `Temporary NUT Provisioned` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `NUTTMPPRV` *WaveStar* CIT: `NUTTMPPRV`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Not Reported
Alarm source	Tributary (VC-3, VC-4, VC-4-4C, VC-4-16C)
Local indications	The "ABN" LED on the user panel is lit.
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Threshold crossing alerts

Meaning

The counter value of the indicated performance parameter exceeded the configured threshold.

Performance alarms give a hint that the quality of service at a certain measurement point is degraded.

General alarm information

The following brief overview provides important information concerning the `Out of Memory Error` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `TCA` *WaveStar* CIT: `T-{monitored performance parameter}`; please refer to "Monitored performance parameters" (2-123).
Alarm category	Quality of service
ASAP type	Threshold crossing alerts do not belong to a specific ASAP type, their alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	The alarm source may be either: • VC-n tributary: VC-3, VC-4, VC-4-4C, VC-4-16C, or • STM-N port: STM-1 el., STM-1 opt., STM-4, STM-16, STM-64.
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Threshold crossing alerts are cleared automatically at the end of the first complete interval during which no threshold crossing occurred.

With the exception of physical performance monitoring parameters (cf. "Physical performance monitoring" (2-124)), there are no specific trouble clearing measures for threshold crossing alerts.

Monitored performance parameters

The following table provides an overview of the monitored *WaveStar* TDM 10G (STM-64) performance parameters (marked with an "X"):

Parameter	VC-3	VC-4	VC-4-4C	VC-4-16C	STM-1 (electr.)	STM-1 (opt.)	STM-4	STM-16	STM-64
RS-N-BBE	–	–	–	–	X	X	X	X	X
RS-N-ES	–	–	–	–	X	X	X	X	X
RS-N-SES	–	–	–	–	X	X	X	X	X
RS-N-UAS	–	–	–	–	X	X	X	X	X
MS-N-BBE	–	–	–	–	X	X	X	X	X
MS-N-ES	–	–	–	–	X	X	X	X	X
MS-N-SES	–	–	–	–	X	X	X	X	X
MS-N-UAS	–	–	–	–	X	X	X	X	X
MS-F-BBE	–	–	–	–	X	X	X	X	X
MS-F-ES	–	–	–	–	X	X	X	X	X
MS-F-SES	–	–	–	–	X	X	X	X	X
MS-F-UAS	–	–	–	–	X	X	X	X	X
VC-N-BBE	X	X	X	X	–	–	–	–	–
VC-N-ES	X	X	X	X	–	–	–	–	–
VC-N-SES	X	X	X	X	–	–	–	–	–
VC-N-UAS	X	X	X	X	–	–	–	–	–
VC-F-BBE	X	X	X	X	–	–	–	–	–
VC-F-ES	X	X	X	X	–	–	–	–	–
VC-F-SES	X	X	X	X	–	–	–	–	–
VC-F-UAS	X	X	X	X	–	–	–	–	–
LBCN	–	–	–	–	–	–	–	X	X
OPT	–	–	–	–	–	–	–	X	X
OPR	–	–	–	–	–	–	–	X	X
MS-N-FECC	–	–	–	–	–	–	–	–	X
MS-N-FECU	–	–	–	–	–	–	–	–	X

Physical performance monitoring

The physical performance monitoring parameters, i.e. the normalized laser bias current (LBCN), the optical transmit power (OPT) and the optical receive power (OPR), are not measured in time intervals but in regular intervals as a snapshot in time, they indicate a degradation of the laser performance, e.g. due to aging.

Preventive actions become necessary to avoid a further deterioration. Please refer to “Resolving laser degradation problems” (3-46).

Unknown Ring Type

Meaning of the alarm

A ring configuration has been detected that is not supported, for example a mixed ring consisting of SONET network elements and SDH network elements.

General alarm information

The following brief overview provides important information concerning the `Unknown Ring Type` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `URT` *WaveStar* CIT: `RNG-URT`
Alarm category	Communication
ASAP type	BLSR/MS SPRing Protection Switch
Default alarm severity	Info
Alarm source	BLSR/MS-SPring protection group
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

Automatic discovery of the ring type

In parallel to the discovery of the ring topology (cf. “Automatic discovery of the ring topology” (2-104)), a discovery of the ring type takes place. The type of network elements involved in the ring, the transport signal level and the protection mode used is evaluated.

Related alarms

The following alarms are related to a ring type discovery:

- `Unknown Ring Type`
- `Inconsistent Ring Prot Mode`

Upgrade Failed

Meaning of the alarm

An upgrade to a new release of software failed.

General alarm information

The following brief overview provides important information concerning the `Upgrade Failed` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `UPGRDF` *WaveStar* CIT: `UPGRDF`
Alarm category	Equipment
ASAP type	The `Upgrade Failed` alarm does not belong to a specific ASAP type, its alarm severity is not provisionable.
Default alarm severity	Info
Alarm source	System
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

User-Network Side MSect Failure

Meaning of the alarm

The LAPD mode parameter is equally set at both ends of the DCC-M link associated to the STM-N port indicated in the alarm message.

General alarm information

The following brief overview provides important information concerning the `User-Network Side MSect Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `UNSMS` *WaveStar* CIT: `UNSMSF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to "Clearing User-Network Side MSect Failure" (3-42).

User-Network Side RSect Failure

Meaning of the alarm

The LAPD mode parameter is equally set at both ends of the DCC-R link associated to the STM-N port indicated in the alarm message.

General alarm information

The following brief overview provides important information concerning the `User-Network Side RSect Failure` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `UNSRS` *WaveStar* CIT: `UNSRSF`
Alarm category	Communication
ASAP type	STMn Port
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Deferred • Non-Service Affecting (NSA): Deferred
Alarm source	STM-N port
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please refer to “Clearing User-Network Side RSect Failure” (3-44).

VCG Signal Fail

Meaning of the alarm

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

General alarm information

The following brief overview provides important information concerning the `VCG Signal Fail` alarm:

Probable cause (alarm identifier)	*WaveStar*® SNMS: `VCGSF` *WaveStar* CIT: `VCGSF`
Alarm category	Communication
ASAP type	Ethernet
Default alarm severity	Depending on the affect on service: • Service Affecting (SA): Not Reported • Non-Service Affecting (NSA): Not Reported
Alarm source	Virtual Concatenated Group (VCG)
Local indications	–
Consequent actions	–
Effect on protection switching	–

Trouble clearing

Please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

3 Trouble clearing

Overview

Purpose

This chapter describes, based on the alarms that can be generated, the measures to be taken for localising and clearing faults on the *WaveStar*® TDM 10G (STM-64) network elements.

Support

For the present *WaveStar* TDM 10G (STM-64) 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:

Telephone:	+49 911 526 2846
Facsimile:	+49 911 526 3131
E-mail:	htransde@lucent.com

Contents

Clearing AU Alarm Indication Signal

Overview

Purpose

Use this procedure to clear an `AU Alarm Indication Signal` alarm.

Related information

For related information, please refer to:

- "AU Alarm Indication Signal" (2-13)

Trouble clearing procedure

Instructions Proceed as follows to clear an `AU Alarm Indication Signal` alarm.

1 Analyze the alarm state of the upstream equipment and take appropriate measures.

END OF STEPS

Clearing BLSR Default K-bytes

Overview

Purpose Use this procedure to clear a `BLSR Default K-bytes` alarm.

Related information For related information, please refer to:

- "BLSR Default K-bytes" (2-21)

Trouble clearing procedure

Before you begin

Prior to performing this task, 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

Instructions

Proceed as follows to clear a `BLSR Default K-bytes` alarm.

1 At the *WaveStar* CIT, open the **NE Alarm List** window.

2 Determine the port AID for which the alarm is reported from the **AID** column of the **NE Alarm List**.

3 Is a `Ring Incomplete` alarm reported at the same time for the same port?

IF ...	THEN ...
Yes	Clear this alarm first (please refer to the corresponding trouble clearing procedure), and proceed with Step 4.
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 `BLSR Default K-bytes` alarm persists	proceed with Step 5.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

5 Is a persistent `Ring Discovery in Progress` alarm (for longer than approx. ten minutes) reported at the same time for the same port?

IF ...	THEN ...
Yes	Clear this alarm first (please refer to the corresponding trouble clearing procedure), and proceed with Step 6.
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 `BLSR Default K-bytes` alarm persists	proceed with Step 7.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

7 Is a `Ring Prot Switching Suspended` alarm reported at the same time for the same port?

IF ...	THEN ...
Yes	Clear this alarm first (please refer to the corresponding trouble clearing procedure), and proceed with Step 8.
No	proceed with Step 9.

8 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Default K-bytes` alarm persists	proceed with Step 9.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

9 Are other transmission alarms (Signal Fail (SF) or Signal Degrade (SD) 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 proceed with Step 10.
No	proceed with Step 11.

10 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Default K-bytes` alarm persists	proceed with Step 11.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

11 Perform a Forced Switch (FS-R).

12 Update the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Default K-bytes` alarm persists	proceed with Step 13.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

13 Has the Forced Switch been executed correctly?

IF ...	THEN ...
Yes	Remove and re-insert the affected port unit, wait for the port unit to re-initialize, and proceed with Step 14.
No	Replace the affected port unit by a known good port unit of the same type.

14 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Default K-bytes` alarm persists	Replace the affected port unit by a known good port unit of the same type.
the `BLSR Default K-bytes` alarm cleared	✓ Stop! End of procedure.

15 If you need further support please contact your Lucent Technologies Local Customer Support Team (LCS) or the Lucent Technologies service hotline.

END OF STEPS

Clearing BLSR Improper APS Codes

Overview

Purpose Use this procedure to clear a `BLSR Improper APS Codes` alarm.

Related information For related information, please refer to:

- “BLSR Improper APS Codes” (2-22)
- *WaveStar® TDM 10G (STM-64) User Operations Guide*

Trouble clearing procedure

Before you begin

You or a service technician must be on-site at the NE.

Required equipment

The following equipment is required:

- *WaveStar®* CIT

Instructions

Proceed as follows to clear a `BLSR 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 alarm list.

3 Are other alarms related to MS-SPRing protection switching reported at the same time for the same port?

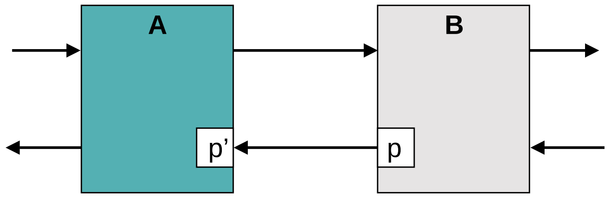
IF ...	THEN ...
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure), and proceed with Step 4.
No	proceed with Step 5

4 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Improper APS Codes` alarm persists	proceed with Step 5.
the `BLSR Improper APS Codes` alarm cleared	Stop! End of procedure.

5 Determine the AIDs of the two network elements involved.

Refer to the following figure for clarification and further reference. The `BLSR Improper APS Codes` alarm is reported on node A, port p'.



6 Check the switch status of the network elements. Are there any switch requests in the network, other than the "Lockout of protection" on node A, port p'?

IF ...	THEN ...
there are other switch requests	abort the procedure.
there are no other switch requests	proceed with Step 7.

7 Perform a Forced Switch (FS-R) at the transmitting port unit (node B, port p).

8 Check the switch status of the network elements.

IF ...	THEN ...
the Forced Switch has been executed correctly	withdraw and re-insert the transmitting port unit (node B, port p), and proceed with Step 12.
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 port unit is constantly lit.

10 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Improper APS Codes` alarm persists	proceed with Step 11.
the `BLSR Improper APS Codes` alarm cleared	proceed with “Background information” (2-70).

11 Replace the transmitting port unit (node B, port p) by a known good port unit of the same type.

12 Wait until the green “ACTIVE” LED on the faceplate of the port unit is constantly lit.

13 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Improper APS Codes` alarm persists	proceed with “Automatic discovery of the ring topology” (2-104).
the `BLSR Improper APS Codes` alarm cleared	proceed with “Background information” (2-70).

14 Replace the receiving port unit (node A, port p’) by a known good port unit of the same type.

15 Wait until the green “ACTIVE” LED on the faceplate of the port unit is constantly lit.

16 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Improper APS Codes` alarm persists	please contact your Local Customer Support team (LCS) or the Lucent Technologies service hotline.
the `BLSR Improper APS Codes` alarm cleared	proceed with “Background information” (2-70).

17 Clear the Forced Switch at the transmitting port unit (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.

END OF STEPS

Clearing BLSR Inconsistent APS Codes

Overview

Purpose

Use this procedure to clear a `BLSR Inconsistent APS Codes` alarm.

Related information

For related information, please refer to:

- "BLSR Inconsistent APS Codes" (2-24)
- *WaveStar® TDM 10G (STM-64) User Operations Guide*

Trouble clearing procedure

Before you begin

Required equipment

The following equipment is required:

- *WaveStar*® CIT

Instructions Proceed as follows to clear a `BLSR 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 alarm list.

3 Are other alarms related to 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 proceed with Step 4.
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 `BLSR Inconsistent APS Codes` alarm persists	proceed with Step 5.
the `BLSR Inconsistent APS Codes` alarm cleared	✓ Stop! End of procedure.

5 Are other transmission alarms (Signal Fail (SF) or Signal Degrade (SD) 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 proceed with Step 6.
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 `BLSR Inconsistent APS Codes` alarm persists	proceed with Step 7.
the `BLSR Inconsistent APS Codes` alarm cleared	✓ Stop! End of procedure.

7 Perform a Forced Switch (FS-R).

8 Has the Forced Switch been executed correctly?

IF ...	THEN ...
Yes	Proceed with Step 11.
No	proceed with Step 9

9 Is the traffic affected, i.e. are path-related alarms active?

IF ...	THEN ...
Yes	Remove and re-insert the affected port unit, wait for the port unit to re-initialize, and proceed with Step 11.
No	Please read the introductory note in Step 10 first. You may now simply ignore the alarm or proceed with Step 10 to resynchronize MS-SPRing protection switching by resetting the system controller.

Important! This step is optional. A system controller reset is ***not*** traffic affecting, a subsequent port unit replacement, however, ***will*** be traffic affecting. Thus, possibly intact traffic might be interrupted if you proceed.

10 Reset the system controller, wait for the system to re-initialize, and proceed with Step 11.

11 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `BLSR Inconsistent APS Codes` alarm persists	Replace the affected port unit by a known good port unit of the same type.
the `BLSR Inconsistent APS Codes` alarm cleared	✓ Stop! End of procedure.

12 If you need further support please contact your Lucent Technologies Local Customer Support Team (LCS) or the Lucent Technologies service hotline.

END OF STEPS

Clearing Circuit Pack Invalid

Overview

Purpose

Use this procedure to clear a `Circuit Pack Invalid` alarm.

Related information

For related information, please refer to:

- "Circuit Pack Invalid" (2-30)

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to perform this task:

- *WaveStar* CIT

Instructions

Proceed as follows to clear the `Circuit Pack Invalid` alarm.

1 From the "**AID**" column of the *WaveStar* CIT "**Alarm List**" determine the AID of the slot reporting the alarm.

2 From the "**Description**" column of the *WaveStar* CIT "**Alarm List**" determine which variant of the `Circuit Pack Invalid` alarm is reported.

IF ...	THEN ...
`Circuit Pack Invalid, Illegal` is reported	remove the circuit pack from the slot position obtained in Step 1 and continue with Step 5.
`Circuit Pack Invalid, Unexpected` is reported	continue with Step 3.
`Circuit Pack Invalid, Unknown` is reported	close the latches and continue with Step 5.

3 Proceed as follows depending on whether you want to provision the circuit pack in the slot position obtained in Step 1 or not:

IF ...	THEN ...
the circuit pack was mistakenly inserted into the slot	remove it from the slot.
you want to provision the circuit pack for that slot	remove it from the slot, deprovision the previously provisioned or preprovisoned circuit pack, and re-insert the desired circuit pack. Continue with Step 4

4 Wait for approx. three minutes for the just inserted circuit pack to initialize.

5 Verify that the alarm is no longer displayed in the *WaveStar* CIT "**Alarm List**".

END OF STEPS

Clearing Circuit Pack Unequipped/Missing

Overview

Purpose

Use this procedure to clear a `Circuit Pack Unequipped/Missing` alarm.

Please be aware that this alarm will unevitably occur during the first equipage of a shelf when any one of two partnering circuit packs is already provisioned while the other one is:

- either preprovisioned and not yet plugged into its slot, or
- neither preprovisioned nor provisioned.

Related Information

For related information, please refer to:

- “Circuit Pack Unequipped/Missing” (2-36)

Trouble clearing procedure

Instructions

Proceed as follows to clear a `Circuit Pack Unequipped/Missing` alarm.

1 Insert the missing circuit pack into the corresponding slot.

END OF STEPS

Clearing ClkOut Quality Failure

Overview

Purpose Use this procedure to clear a `ClkOut Quality Failure` alarm.

Related information For related information, please refer to "ClkOut Quality Failure" (2-38).

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to complete this procedure:

- *WaveStar* CIT

Instructions

Proceed as follows to clear the `ClkOut Quality Failure` alarm.

1 If other alarms are reported at the same time, clear these alarms first.

The `ClkOut Quality Failure` alarm is a possible secondary alarm for

- a `Sync Reference Failure` or a `System Clock Holdover` alarm, or
- when the timing reference is derived from the receive signal:
  - a hardware error on the associated receive circuit pack, or
  - a Signal Fail (SF) or Signal Degrade (SD) condition in the receive signal, such as `STM Loss of Signal`, `STM Loss of Frame`, `MSect Alarm Indication Signal`, `MSect Excessive Error` or `MSect Signal Degrade`.

2 Otherwise, please contact your Lucent Technologies Local Customer Support (LCS) team or the Lucent Technologies Service Hotline.

END OF STEPS

Clearing DCC Tunnel Overflow

Overview

Purpose

Use this procedure to clear a `DCC Tunnel Overflow` alarm.

Related information

For related information, please refer to “DCC Tunnel Overflow” (2-41).

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to complete this procedure:

- *WaveStar* CIT

Instructions

Proceed as follows to clear the `DCC Tunnel Overflow` alarm.

1 Free storage capacity of the routing table by deprovisioning (removing) dispensable entries.

END OF STEPS

Clearing environmental alarms

Overview

Purpose

Use this procedure to clear environmental alarms.

Related information

For related information, please refer to:

- "Environmental alarms on miscellaneous discrete inputs" (2-44).
- *WaveStar® TDM 10G (STM-64) User Operations Guide*.

Trouble clearing procedure

Instructions Proceed as follows to clear an environmental alarm.

1 Take appropriate measures depending on the specific application of the respective MDI.

END OF STEPS

Clearing HP Remote Defect Indication

Overview

Purpose Use this procedure to clear an `HP Remote Defect Indication` alarm.

Related information For related information, please refer to:

- "HP Remote Defect Indication" (2-54)

Trouble clearing procedure

Instructions

Proceed as follows to clear an `HP Remote Defect Indication` alarm.

1 Analyze the alarm state of the downstream equipment an take appropriate measures.

END OF STEPS

Clearing Mate Circuit Pack Unequipped

Overview

Purpose

Use this procedure to clear a `Mate Circuit Pack Unequipped` alarm.

Please be aware that this alarm will unevitably occur during the first equipage of a shelf when any one of two partnering circuit packs is already provisioned while the other one is:

- either preprovisioned and not yet plugged into its slot, or
- neither preprovisioned nor provisioned.

Related Information

For related information, please refer to:

- “Mate Circuit Pack Unequipped” (2-78)

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to perform this task:

- *WaveStar* CIT
- Depending on which circuit pack reports the alarm, an OC192/STM64 or a PPROC/STS192 circuit pack will be required.

Instructions

Proceed as follows to clear a `Mate Circuit Pack Unequipped` alarm.

1 From the **AID** column of the *WaveStar* CIT alarm list determine the slot AID of the circuit pack reporting the alarm.

2 Proceed as follows depending on which circuit pack reports the alarm:

If the alarm is reported by ...	then insert ...
the OC192/STM64 circuit pack in the "tre" slot	the PPROC/STS192 circuit pack into the "pproce" slot and close the latches.
the OC192/STM64 circuit pack in the "trw" slot	the PPROC/STS192 circuit pack into the "pprocw" slot and close the latches.
the PPROC/STS192 circuit pack in the "pproce" slot	the OC192/STM64 circuit pack into the "tre" slot and close the latches.
the PPROC/STS192 circuit pack in the "pprocw" slot	the OC192/STM64 circuit pack into the "trw" slot and close the latches.

3 Wait for approx. two minutes for the just inserted circuit pack to initialize.

END OF STEPS

Clearing MSect Alarm Indication Signal

Overview

Purpose

Use this procedure to clear an `MSect Alarm Indication Signal` alarm.

Related information

For related information, please refer to:

- "MSect Alarm Indication Signal" (2-81)

Trouble clearing procedure

Instructions Complete the following steps to clear an `MSect Alarm Indication Signal` alarm.

1 Analyze the alarm state of the upstream equipment and take appropriate measures.

END OF STEPS

Clearing MSect Remote Failure Indication

Overview

Purpose Use this procedure to clear an `MSect Remote Failure Indication` alarm.

Related information For related information, please refer to:

- “MSect Remote Failure Indication” (2-84)

Trouble clearing procedure

Instructions Proceed as follows to clear an `MSect Remote Failure Indication` alarm.

1 Analyze the alarm state of the downstream equipment and take appropriate measures.

END OF STEPS

Clearing Ring Discovery in Progress

Overview

Purpose

Use this procedure to clear a persistent `Ring Discovery in Progress` alarm.

Related information

For related information, please refer to:

- "Ring Discovery in Progress" (2-104)

Trouble clearing procedure

Before you begin

Prior to performing this task, 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

Instructions

Proceed as follows to clear a persistent `Ring Discovery in Progress` alarm.

1 At the *WaveStar* CIT, open the alarm list.

2 Reset the system controller, and wait for the system to re-initialize.

3 Update the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `Ring Discovery in Progress` alarm persists	Contact your Lucent Technologies Local Customer Support Team (LCS) or the Lucent Technologies service hotline.
the `Ring Discovery in Progress` alarm cleared	✓ Stop! End of procedure.

END OF STEPS

Clearing Ring Prot Switching Suspended

Overview

Purpose

Use this procedure to clear a `Ring Prot Switching Suspended` alarm.

Related information

For related information, please refer to:

- "Ring Prot Switching Suspended" (2-109)

Trouble clearing procedure

Before you begin

Prior to performing this task, 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

Instructions

Proceed as follows to clear a `Ring Prot Switching Suspended` alarm.

1 At the *WaveStar* CIT, open the alarm list.

2 Are other alarms related to MS-SPRing protection switching reported at the same time?

IF ...	THEN ...
Yes	Clear these alarms first (please refer to the corresponding trouble clearing procedure).
No	Reset the system controller and wait for the system to re-initialize.

3 Refresh the alarm list display by pressing the **Refresh** button of the **NE Alarm List** window. Check the alarm list.

IF ...	THEN ...
the `Ring Prot Switching Suspended` alarm persists	contact your Lucent Technologies Local Customer Support Team (LCS) or the Lucent Technologies service hotline.
the `Ring Prot Switching Suspended` alarm cleared	✓ Stop! End of procedure.

END OF STEPS

Clearing User-Network Side MSect Failure

Overview

Purpose

Use this procedure to clear a `User-Network Side MSect Failure` alarm.

Related information

For related information, please refer to:

- "User-Network Side MSect Failure" (2-127)
- *WaveStar® TDM 10G (STM-64) User Operations Guide*

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to perform this task:

- *WaveStar* CIT

Required privilege

You must have at least a privilege code of **S3**.

Instructions

Proceed as follows to clear a `User-Network Side MSect Failure` alarm.

1 At the *WaveStar* CIT, invoke the **Configure DCC Terminations** window from the **System View** or **Shelf View** main menu via **Configuration** → **DCC Terminations...**

2 Select the DCC controller (ADJCTL/DCCEI circuit pack) of the shelf in which the affected port unit resides by means of the equipment selection part of the window.

3 In the **Select a port for Current Termination** group box, select the optical interface port indicated in the alarm message and select the **Line DCC** tab.

4 In the **DCC Channel Parameters** group box, determine the current setting of the **LAPD mode** parameter.

IF the current setting is ...	THEN change it to ...
USER-SIDE	**NETWORK-SIDE**
NETWORK-SIDE	**USER-SIDE**

END OF STEPS

Clearing User-Network Side RSect Failure

Overview

Purpose

Use this procedure to clear a `User-Network Side RSect Failure` alarm.

Related information

For related information, please refer to:

- “User-Network Side RSect Failure” (2-128)
- *WaveStar® TDM 10G (STM-64) User Operations Guide*

Trouble clearing procedure

Before you begin

Prior to performing this task, 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 to perform this task:

- *WaveStar* CIT

Required privilege

You must have at least a privilege code of **S3**.

Instructions

Proceed as follows to clear a `User-Network Side RSect Failure` alarm.

1 At the *WaveStar* CIT, invoke the **Configure DCC Terminations** window from the **System View** or **Shelf View** main menu via **Configuration** → **DCC Terminations...**

2 Select the DCC controller (ADJCTL/DCCEI circuit pack) of the shelf in which the affected port unit resides by means of the equipment selection part of the window.

3 In the **Select a port for Current Termination** group box, select the optical interface port indicated in the alarm message and select the **Section DCC** tab.

4 In the **DCC Channel Parameters** group box, determine the current setting of the **LAPD mode** parameter.

IF the current setting is ...	THEN change it to ...
USER-SIDE	**NETWORK-SIDE**
NETWORK-SIDE	**USER-SIDE**

END OF STEPS

Resolving laser degradation problems

Overview

Purpose

Use this procedure to take preventive actions if a normalized laser bias current (LBCN), optical transmit power (OPT) or optical receive power (OPR) threshold crossing alert is reported.

Related information

For related information, please refer to:

- *WaveStar*® TDM 10G (STM-64) User Operations Guide,
- “Threshold crossing alerts” (2-123)

Trouble clearing procedure

Before you begin

Required equipment

The following equipment is required to perform this task:

- Depending on the type of threshold crossing alert, a replacement port unit will be required.

Instructions

Complete the following steps to clear laser degradation problems.

1 Depending on the type of threshold crossing alert:

IF ...	THEN ...
an LBCN or OPT threshold crossing alert is reported	replace the port unit concerned.
an OPR threshold crossing alert is reported	continue with Step 2.

2 At the same time, a transmission alarm should be reported in that case, for example:

- `STM Loss of Signal`,
- `STM Loss of Frame`,
- `MSect Excessive Error` or
- `MSect Signal Degrade`.

Check the alarm list for active alarms (especially for the alarms listed above), and clear these alarms first.

END OF STEPS

4 Supporting procedures

Overview

Purpose

The present chapter contains descriptions of supporting procedures that are helpful for maintenance and trouble clearing activities.

Contents

Retrieving a list of current alarms

Overview

Purpose

Use this procedure to retrieve detailled information about the current alarm status of a *WaveStar*® TDM 10G (STM-64) NE by using the *WaveStar* CIT.

The *WaveStar* CIT NE alarm list

Please refer to “The *WaveStar* CIT NE Alarm List” (4-4).

The *WaveStar* SNMS alarm list

Please refer to the *WaveStar SNMS Provisioning Guide for WaveStar TDM 10G (STM-64)*.

How to retrieve the *WaveStar*® CIT NE Alarm List

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 List**.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

Proceed as follows to retrieve the **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** or **Shelf View** window, or
- selecting **Fault** → **NE Alarm List** in the **System View** or **Shelf View** main menu, or
- selecting **Reports** → **NE Alarm List** in the **System View** or **Shelf View** main menu.

Result:

The **NE Alarm List** window will be opened.

Important! 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

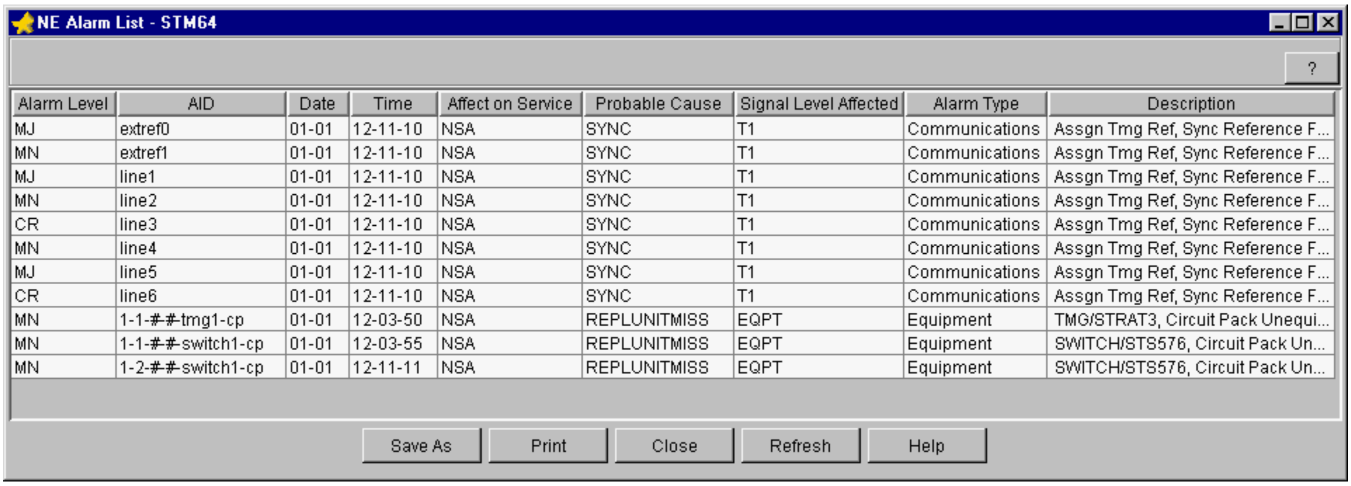
as soon as you observe changes in the alarm status display in the lower left corner of the **System View** or **Shelf View** window, or if you are unsure whether the alarm list is still synchronized to the current alarm status.

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 *WaveStar* TDM 10G (STM-64) NE.



NE Alarm List - STM64

Alarm Level	AID	Date	Time	Affect on Service	Probable Cause	Signal Level Affected	Alarm Type	Description
MJ	extref0	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MN	extref1	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MJ	line1	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MN	line2	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
CR	line3	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MN	line4	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MJ	line5	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
CR	line6	01-01	12-11-10	NSA	SYNC	T1	Communications	Assgn Tmg Ref, Sync Reference F...
MN	1-1-#-#-tmg1-cp	01-01	12-03-50	NSA	REPLUNITMISS	EQPT	Equipment	TMG/STRAT3, Circuit Pack Unequi...
MN	1-1-#-#-switch1-cp	01-01	12-03-55	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit Pack Un...
MN	1-2-#-#-switch1-cp	01-01	12-11-11	NSA	REPLUNITMISS	EQPT	Equipment	SWITCH/STS576, Circuit Pack Un...

Save As | Print | Close | Refresh | Help

Structure of the “NE Alarm List”

The following table explains the structure of the *WaveStar* CIT **NE Alarm List**.

Column	Meaning
Alarm Level	This column indicates the alarm severity. Possible values are (depending on the **Preferences** setting): • Critical/Major/Minor (**CR/MJ/MN**) or • Prompt/Deferred/Info (**PR/DF/INF**). The latter is recommended for *WaveStar* TDM 10G (STM-64) systems.
AID	This column indicates the alarm issue point, i.e. the access identifier (AID) of the equipment component or facility for which an alarm is being reported. A special format is used for tributary AIDs, please refer to “Tributary AID format” (4-7).
Date **Time**	These two columns indicate the date and time of occurrence, i.e. the date and time the alarm was reported by the NE. The date and time format depends on the country in which the *WaveStar* CIT is being used.

Column	Meaning
Affect on Service	This column indicates whether the corresponding alarm is service affecting or not. Possible values are: • service affecting (***SA***), • non-service affecting (***NSA***), • not applicable (-).
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 alarm category otherwise. Possible values are: • **EQPT** Equipment (alarm category) • **T-1** STM port timing input • **STM-1E** electrical STM-1 transport signal (155 Mbit/s) • **STM-1** optical STM-1 transport signal (155 Mbit/s) • **STM-4** optical STM-4 transport signal (622 Mbit/s) • **STM-16** optical STM-16 transport signal (2.5 Gbit/s) • **STM-64** optical STM-64 transport signal (10 Gbit/s) • **VC-3** VC-3 payload signal • **VC-4** VC-4 payload signal • **VC-4-4C** VC-4-4C payload signal • **VC-4-16C** VC-4-16C payload signal
Alarm Type	This column indicates the alarm category. Possible values are: • Communications, • Environmental, • Equipment, • Processing, • Quality of service.

Column	Meaning
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.

Tributary AID format

Background

In the *WaveStar*® CIT **NE Alarm List**, a special representation is used for VC-3, VC-4, VC-4-4C and VC-4-16C tributaries, see the following examples:

1-3-u-#-06-1-**20	STM-16 port: VC-4 in the second STM-1 of the first STM-4 within the STM-16 frame
1-3-u-#-04-1-***3	STM-16 port: Third VC-3 in the first STM-1 of the first STM-4 within the STM-16 frame

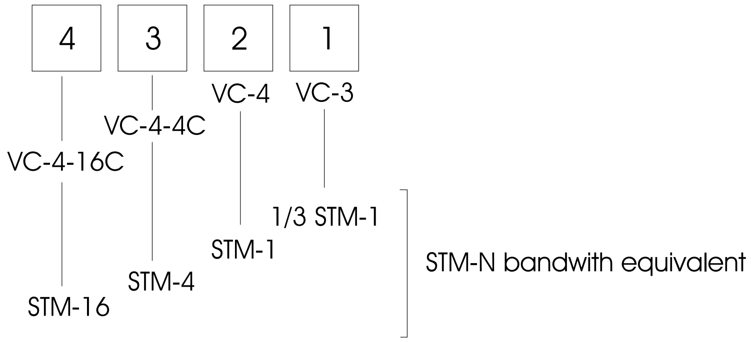
Tributary numbering scheme

The following tributary numbering scheme is used for *WaveStar* TDM 10G (STM-64) systems:

	VC-4-16C	VC-4-4C	VC-4	VC-3
STM-64 port	1000, 2000, 3000, 4000	1100, 1200, 1300, 1400, 2100, 2200, 2300, … 4300, 4400	1110, 1120, 1130, 1140, 1210, 1220, 1230, 1240, 1310, 1320, … 4410, 4420, 4430, 4440	1111, 1112, 1113, 1121, 1122, 1123,
STM-16 port	000	100, 200, 300, 400	110, 120, 130, 140, 210, 220, 230, 240, 310, 320, … 410, 420, 430, 440	111, 112, 113, 121, 122, 123, 131, 132, … 441, 442, 443
STM-4 port	insufficient bandwith	00	10, 20, 30, 40	11, 12, 13, 21, 22, 23, 31, 32, … 41, 42, 43
STM-1 port	insufficient bandwith	insufficient bandwith	0	1, 2, 3

Tributary representation in the *WaveStar* CIT NE Alarm List

A four-digit representation is used for SDH tributary AIDs in the *WaveStar* CIT **NE Alarm List**. Each of the four digits represents a particular VC-N level.



The possible values of the individual digits are as follows:

1. 0: no VC-3,
   1, 2 or 3: the first, second or third VC-3 within an STM-1 frame
2. 0: no VC-4,
   1, 2, 3 or 4: the first, second, third or fourth VC-4 within the corresponding STM-N frame
   An asterisk ("*") represents either a "1" or a fill character (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-N frame
   An asterisk ("*") represents either a "1" or a fill character (if the third digit is not required, in the case of an STM-1 or STM-4 interface port for example).
4. 1, 2, 3 or 4: the first, second, third or fourth VC-4-16C within the corresponding STM-N frame
   An asterisk ("*") represents either a "1" or a fill character (if the fourth digit is not required, in the case of an STM-1, STM-4 or STM-16 interface port for example).

Required number of digits

Depending on the STM level, a different number of digits is required to uniquely identify the tributaries contained.

STM-64 interface port	All four digits are required.
STM-16 interface port	Three digits are required.

STM-4 interface port	Two digits are required.
STM-1 interface port	Only the last digit is required.

How to determine the correct tributary

Proceed as follows to determine the correct tributary from the tributary AID representation in the *WaveStar* CIT **NE Alarm List**:

1. Determine the port unit type by means of the slot info in the AID and by using office records or the *WaveStar* CIT **Shelf View** window for example.
2. Depending on the port unit type, determine the number of required digits in the tributary AID representation.
   All ***required*** digits with an asterisk respresent a “1”, all other digits with an asterisk can be ignored.

Retrieving a list of history alarms

Overview

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 *WaveStar* TDM 10G (STM-64) 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 identical to that of the NE alarm list; please refer to "The *WaveStar* CIT NE Alarm List" (4-4).

The *WaveStar* SNMS alarm history

Please refer to the *WaveStar SNMS Provisioning Guide for WaveStar TDM 10G (STM-64)*for information about the *WaveStar* SNMS alarm history ("Alarm browser").

How to retrieve the *WaveStar*® CIT NE Alarm Log

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** or **Shelf View** main menu, or
- selecting **Reports** → **NE Alarm Log...** in the **System View** or **Shelf View** main menu.

Result:

The **NE Alarm Log** window will be opened.

END OF STEPS

Restoring the NE database

Overview

Purpose

Use this procedure to restore a database to a network element (NE) after:

- a known or suspected database corruption,
- the replacement of a nonvolatile memory (NVM) card for a simplex controller.

Changes since the last database backup

Important! Depending on the number of database changes that have occurred since the last database backup, manually applying recent changes after a restore can be a time-intensive process. Make absolutely sure that a restore is necessary before performing this task.

Related information

For related information, please refer to:

- the *WaveStar® TDM 10G (STM-64) User Operations Guide*.

How to restore a 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 *WaveStar* TDM 10G (STM-64) network element (NE) where the database is to be restored.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Safety precautions

To assure both personal safety and the proper functioning of the *WaveStar* TDM 10G (STM-64) system, it is imperative to review and understand these warnings and precautions prior to performing this task.

CAUTION

Electrostatic discharge

Handling circuit packs or working on a WaveStar TDM 10G (STM-64) system can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar TDM 10G (STM-64) 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

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:** Continue with Step 5.
the connection to the NE is direct TCP/IP,	select **FTP** in the **Restore From/Via** drop down list box. **Reference:** Continue with Step 6.
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. The File Transfer Translation Device (FTTD) is an FTAM-FTP gateway which translates the File Transfer Access and Management (FTAM) protocol over an OSI network to the File Transfer Protocol (FTP) over an TCP/IP network. **Reference:** Continue with Step 7.

5 Select “CIT” in the **Look in** field and double click successively on *C:*, *Program Files*, *Lucent Technologies*, *Wavestar CIT*, and *backups*.

Continue with Step 9.

6 Specify the **Server** (IP address or server name), port information (optional), User name (optional) and password (optional) for the FTP information.

Continue with Step 9.

7 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.

8 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.

Continue with Step 9.

Important! Be careful to select the correct backup files to restore to the NE.

9 Specify the path to the folder where the backup files reside.

10 Verify your settings and correct if necessary. Then click **Restore**.

11 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.

12 Connect to the NE again.

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

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

Important! The *WaveStar* TDM 10G (STM-64) 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 fan unit

Overview

Purpose Perform this task ***only*** when instructed to replace a fan unit as part of a trouble-clearing task.

How to replace a fan unit

Before you begin The following equipment is required to perform this task:

- A replacement fan unit

Instructions

CAUTION

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 for more than 15 minutes can cause the associated network element to fail.

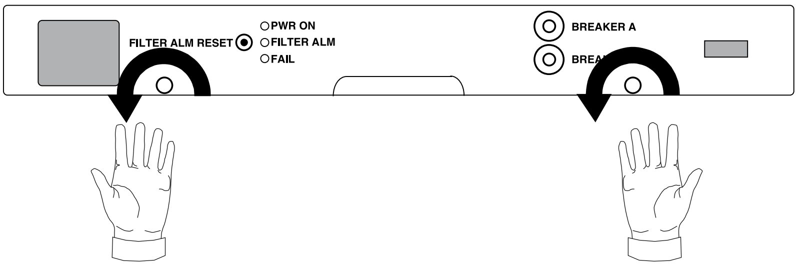
Proceed as follows to replace the fan unit.

1 Physically locate the replacement fan unit near, and within easy reach, of the corresponding NE/shelf.

2 Disconnect the two power conncetors at the rear side of the fan unit to be replaced.

3 If applicable, remove the front cover of the corresponding NE/shelf.

4 With your fingers, unscrew (turn counter-clockwise) the two captive type thumb-screws that are located on the front (one right and one left) of the fan unit.

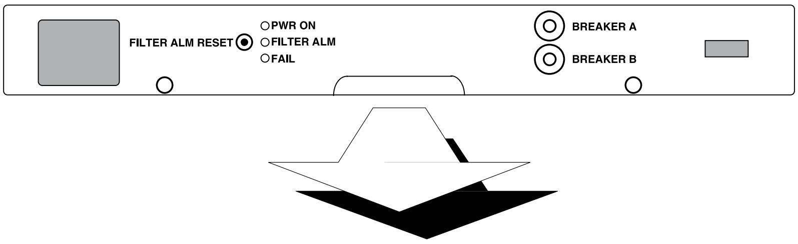


CAUTION

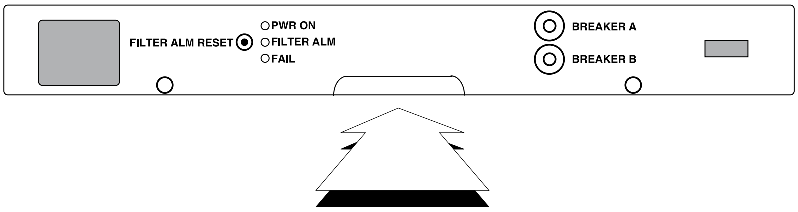
Leaving the fan unit out for more than 15 minutes can cause the associated network element to fail.

It is critical that you complete this procedure - as well as the referencing trouble-clearing procedure - soon after performing this step.

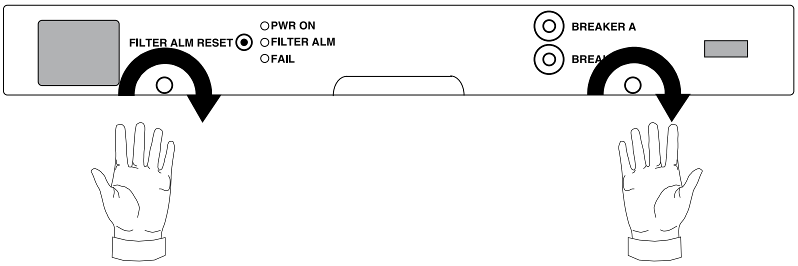
5 ***Gently*** and by applying an ***even force*** to both the left and right sides, pull the fan unit forward with the center mounted handle in order to remove it from the shelf.



6 ***Carefully***, insert the replacement new fan unit into the shelf. Again, use the center mounted handle to push the “self-aligning” fan unit into the shelf.



7 With your fingers, tighten (turn clock-wise) the two thumb screws in order to secure the fan unit into the shelf.



8 Connect the two power conncetors at the rear side of the fan unit.

9 Return to the trouble-clearing task that referred you to this task.

END OF STEPS

Replacing a fan filter

Overview

Purpose

Use this procedure to replace a fan filter:

- every six months, as part of routine fan maintenance, or
- when instructed to do so as part of a trouble-clearing procedure.

Related information

Please also refer to “Fan Failure” (2-47).

How to replace a fan filter

Before you begin

The following equipment is required to perform this task:

- A replacement fan filter.

Instructions

CAUTION

Risk of fire due to overheating.

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

Therefore, ensure that the fans of a fan unit are not obstructed and strictly observe the six-month periodic fan filter replacement interval to avoid clogging of the filter and to always ensure a sufficient air flow!

Proceed as follows to replace a fan filter:

1 Remove the shelf front covers (please refer to the *WaveStar® TDM 10G (STM-64) Installation Manual*).

2 Remove the fan filter by grasping the two pull tabs and pulling the fan filter out of the shelf.

3 Insert the replacement fan filter so that the two pull tabs are positioned at the front of the shelf.

4 Mount the shelf front covers.

5 Discard the dirty fan filter.

END OF STEPS

Cleaning optical fiber connectors and couplings

Overview

Purpose

Use this procedure to clean optical fiber connectors and/or couplings when instructed to do so as part of a trouble-clearing procedure, or when impurities are discovered or assumed.

The following procedures describe the Lucent Technologies recommended method for the cleaning and inspection of optical fiber connectors and couplings using specific tools and materials that have been proven to be effective in the assembly and testing of optical transmission equipment.

It is critical that the connector endfaces are clean and free from particular contamination to assure proper performance and reliability of lightwave systems. With the modern high speed, high power and wider bandwidth optical transmission systems, clean connectors along the optical path are absolutely essential for successful operation.

How to clean 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.

WaveStar® TDM 10G (STM-64) 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” (1-5)).

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

How to clean 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.

WaveStar® TDM 10G (STM-64) 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" (1-5)).

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

Overview

Purpose Use the following procedures to perform cross connection loopbacks.

Related information

For background information, please refer to:

- "Cross connection loopbacks" (4-33)

How to operate cross connection loopbacks

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 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 Proceed according to one of the following options to invoke the **Crossconnect Loopback - STM64** window from the *WaveStar* CIT:

- Option 1
  - Select **Fault** → **Analysis** → **Cross-Connect Loopback…** from the **System View** or **Shelf View** main menu,
  - choose the tributary for which you want to operate a cross connection loopback from the **Crossconnect Loopback** equipment selection window that will be opened, and
  - click **Select**.
- Option 2
  - Open the **Shelf View** for **Shelf 1** (“2.5G Main Shelf”), and
  - right-click on the port on which you want to select a tributary.
  - choose the tributary for which you want to operate a cross connection loopback from the **Crossconnect Loopback** equipment selection window that will be opened, and
  - click **Select**.

Result:

The **Crossconnect Loopback - STM64** window will be opened.

2 By means of the read-only fields, verify that you selected the desired tributary, and that no loopback is currently active.

The read-only fields have the following meanings:

Tributary AID	The AID of the selected tributary
Port Type/Rate	The selected port type
Cross Connect Status	If there exists a provisioned cross connection for the selected tributary then the indication is **Yes**, otherwise it is **No**.
Test Access Status	This field is not relevant for *WaveStar* TDM 10G (STM-64) systems.
Cross Connect Loopback Status	If there already exists an active cross connection loopback for the selected tributary then the indication is **Loopback Running**, otherwise it is **No Loopback**.

3 Select the VC-N level of the cross connection loopback to be operated in the **Loopback Rate** drop-down list box.

4 Proceed as follows depending on whether there exists a cross connection for the selected tributary or not:

If…	Then…
there exists a cross connection for the selected tributary (**Cross Connect Status: Yes**)	Click the **Force…** button and continue with Step 5.
there exists no cross connection for the selected tributary (**Cross Connect Status: No**)	Click the **Operate** button and confirm your selection in the confirmation window that will be opened. Stop! End of procedure.

CAUTION

Forcing a cross connection loopback on a tributary which already has a cross connection established ***will be service affecting****.*

5 If you want to proceed anyway, again click the **Force…** button and confirm your selection in the confirmation window that will be opened.

END OF STEPS

How to dismantle a cross connection 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*** **P2** ***and*** **M3** to perform cross connection loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to dismantle a cross connection loopback:

1 Proceed according to one of the following options to invoke the **Crossconnect Loopback - STM64** window from the *WaveStar* CIT:

- Option 1
  - Select **Fault** → **Analysis** → **Cross-Connect Loopback...** from the **System View** or **Shelf View** main menu,
  - choose the tributary for which you want to dismantle a cross connection loopback from the **Crossconnect Loopback** equipment selection window that will be opened, and
  - click **Select**.
- Option 2
  - Open the **Shelf View** for **Shelf 1** (“2.5G Main Shelf”), and
  - right-click on the port on which you want to select a tributary.
  - choose the tributary for which you want to dismantle a cross connection loopback from the **Crossconnect Loopback** equipment selection window that will be opened, and
  - click **Select**.

Result:

The **Crossconnect Loopback - STM64** window will be opened.

2 By means of the read-only fields, verify that you selected the desired tributary and that the **Cross Connect Loopback Status** is **Loopback Running** (see below).

The read-only fields have the following meanings:

Tributary AID	The AID of the selected tributary
Port Type/Rate	The selected port type
Cross Connect Status	If there exists a provisioned cross connection for the selected tributary then the indication is **Yes**, otherwise it is **No**.
Test Access Status	This field is not relevant for *WaveStar* TDM 10G (STM-64) systems.
Cross Connect Loopback Status	If there already exists an active cross connection loopback for the selected tributary then the indication is **Loopback Running**, otherwise it is **No Loopback**.

3 Click the **Release** button to dismantle the indicated cross connection loopback.

END OF STEPS

Cross connection loopbacks

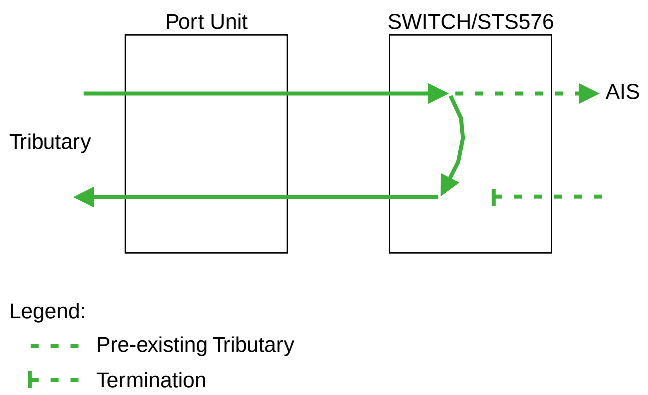
Purpose of cross connection loopbacks

Cross connection loopbacks (also referred to as “XC loopbacks”) make it possible to loop an input tributary back to the output of the same tributary. The selected input tributary is looped back in the switch unit (SWITCH/STS576 circuit pack).

Cross connection loopbacks can be used for testing purposes.

Functional principle

The following schematical diagram depicts the functional principle of cross connection loopbacks.



A cross connection loopback can be regarded as a temporary cross connection of indeterminate duration. If a cross connection already exists on the selected tributary, an alarm indication signal (AIS) is inserted downstream during the loopback. If a cross connection exists in the opposite direction, the signal is terminated during the loopback. When the cross connection loopback is released, any cross connections that were affected by the loopback are automatically re-established and the insertion of AIS is brought to a termination.

Active cross connection loopbacks are indicated via the ABN LED on the user panel.

Permitted signal levels

Cross connection loopbacks can be performed on any tributary regardless of whether there exists a cross connection for the selected tributary or not.

The permitted signal level of the tributary to be looped back depends on the respective port unit, possible signal levels are:

STM-1 port units (opt. or electr.)	VC-3 or VC-4

STM-4 port units	VC-3, VC-4 or VC-4-4C
STM-16 port units	VC-3, VC-4, VC-4-4C or VC-4-16C
STM-64 port units	VC-3, VC-4, VC-4-4C or VC-4-16C

Performing facility loopbacks

Overview

Purpose

Use the following procedures to perform a near-side or far-side facility loopback.

Facility loopbacks

Facility loopbacks make it possible to verify the correct system operation and may facilitate troubleshooting of problems.

Facility loopbacks can be operated even if the corresponding port is currently carrying traffic.

Please note, that facility loopbacks are ***not*** supported on STM-64 aggregate ports.

Related information

For further information, please refer to:

- “Near-side facility loopbacks” (4-39)
- “Far-side facility loopbacks” (4-41)

How to operate near-side or far-side facility loopbacks

Before you begin

Prior to performing this task, you must:

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

Required privilege

You must have at least privilege codes of **S1** ***and*** **P1** ***and*** **M3** to perform facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to operate a near-side or far-side facility loopback:

1 Proceed according to one of the following options to invoke the **Facility Loopback - STM64** window from the *WaveStar* CIT:

- Option 1
  - Select **Fault** → **Analysis** → **Facility Loopback…** from the **System View** or **Shelf View** main menu,
  - choose the port for which you want to operate a facility loopback from the equipment selection window that will be opened, and
  - click **Select**.
- Option 2
  - Open the **Shelf View** for **Shelf 1** (“2.5G Main Shelf”), and
  - right-click on the port on which you want to operate a facility loopback.

Result:

The **Facility Loopback - STM64** window will be opened.

2 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.

3 Select the type of facility loopback to be operated:

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

4 Click the button in the lower area 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!

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

END OF STEPS

How to dismantle a facility loopback

Before you begin

Prior to performing this task, you must:

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

Required privilege

You must have at least privilege codes of **S1** ***and*** **P1** ***and*** **M3** to perform facility loopbacks.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to operate a near-side or far-side 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** or **Shelf 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
  - Open the **Shelf View** for **Shelf 1** (“2.5G Main Shelf”), and
  - right-click on the port on which you want to dismantle a facility loopback.

Result:

The **Facility Loopback - STM64** 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. 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

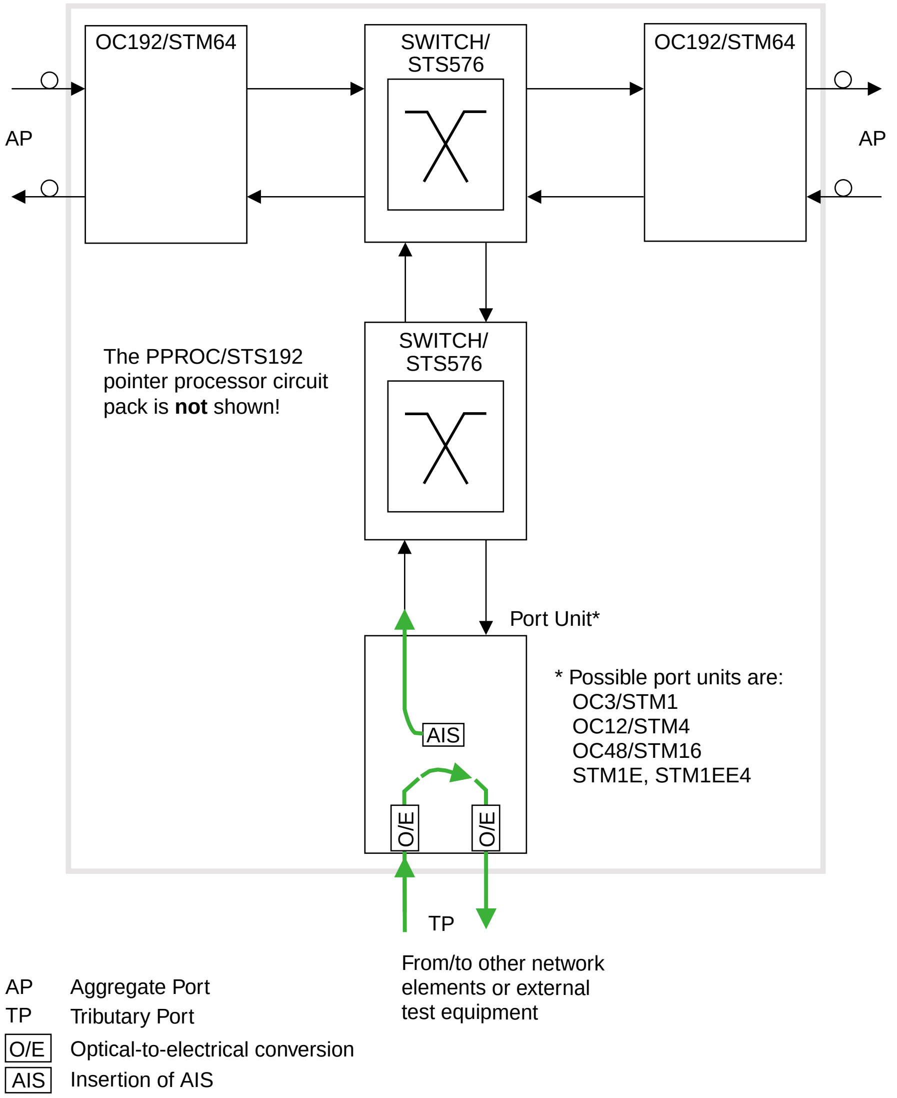
Near-side facility loopbacks

Purpose of near-side facility loopbacks

Near-side facility loopbacks can be used to test the correct cabling between two network elements including the involved port unit's physical interfaces.

Functional principle

The following schematical diagram depicts the functional principle of near-side facility loopbacks. For simplification, only one tributary port unit is shown.



The incoming signal at the port unit input is, where appropriate after optical-to-electrical conversion, entirely looped back to the port unit output.

Non-transparent and complete

Near-side facility loopbacks are non-transparent and complete. “Non-transparent” means that the signal transmitted in the original (downstream) direction is different from the signal looped back. “Complete” means that the signal is not changed before it is looped back. AIS is inserted in the downstream direction after the near-side facility loopback.

Supported port unit types

Near-side facility loopbacks are supported on all optical or electrical tributary port units (STM1E, STM1EE4, OC3/STM1, OC12/STM4, OC48/STM16) but ***not*** on OC192/STM64 aggregate port units.

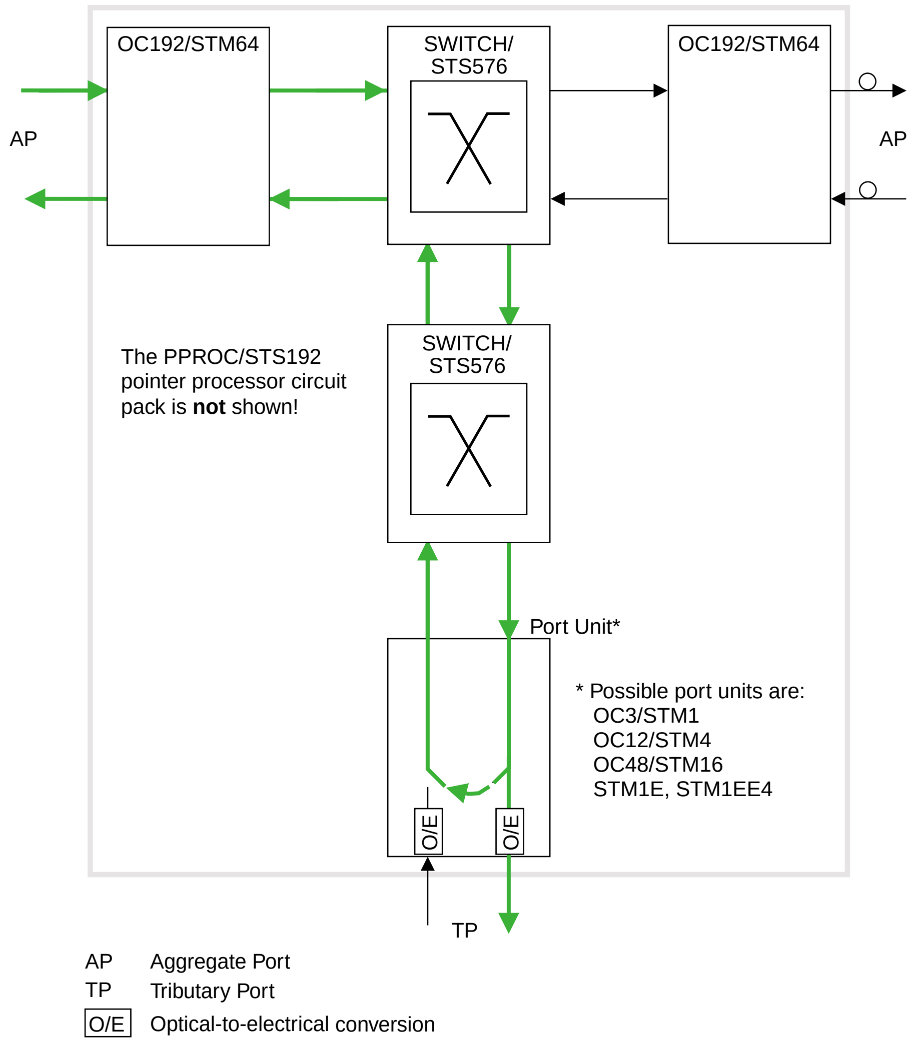
Far-side facility loopbacks

Purpose of far-side facility loopbacks

Far-side facility loopbacks can be used to test paths through a network element.

Functional principle

The following schematical diagram depicts the functional principle of far-side facility loopbacks. For simplification, only one tributary port unit is shown.



The electrical transmission signal at the port unit output, on both electrical and optical port units, is looped back to the corresponding port unit input with passing through as many equipment components as possible.

Transparent and complete for optical port units

For all supported optical port unit types, far-side facility loopbacks are transparent and complete. For electrical tributary port units, far-side facility loopbacks are non-transparent and complete.

“Transparent” means that the signal is both looped back and continued in the original direction. “Non-transparent” means that the signal transmitted in the original (downstream) direction is different from the signal looped back due to the insertion of AIS after the loopback. “Complete” means that the signal is not changed before it is looped back.

Supported port unit types

Far-side facility loopbacks are supported on all optical or electrical tributary port units (STM1E, STM1EE4, OC3/STM1, OC12/STM4, OC48/STM16) but ***not*** on OC192/STM64 aggregate port units.

Manually performing optical loopbacks

Overview

Purpose

Front access to the optical connectors on the port unit faceplates allows manual optical loopbacks. These loopbacks are performed by connecting the optical output of a port unit to the optical input of the same port unit.

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.

How to perform optical loopbacks manually

Before you begin

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,
- A standard Single-Mode (SM) non-dispersion shifted fiber (“loopback cable”),
- Suitable lightguide build-out (LBO) connectors for optical attenuation.

Instructions

DANGER

Injury to eyes caused by invisible laser radiation.

WaveStar® TDM 10G (STM-64) 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” (1-5)).

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 port unit type (please refer to “Optical port unit parameters” (4-46)).

2 At the faceplate of the port unit, remove the optical connections (including LBO connectors, if equipped) 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 Depending on the recommended attenuation:

IF ...	THEN ...
the recommended attenuation exceeds 15 dB	use two LBO connectors of the correct type (LC-type for OC192/STM64/DWDM…, ST-type, FC-type, or SC-type for all other types of port units). The sum of the attenuation values should match the recommended value. Continue with Step 4.
the recommended attenuation does not exceed 15 dB	use a corresponding LBO connector. Continue with Step 5.

4 Mount one of the two LBO connectors at the port unit's optical input, the other one at the optical output and cover them with protection caps. Continue with Step 6.

5 Mount the LBO connector at the port unit's optical input and cover it with a protection cap. Continue with Step 6.

6 Equip the loopback cable with optical connectors of the appropriate type.

7 Clean all optical fiber endfaces, connectors and couplings (please refer to "Cleaning optical fiber connectors and couplings" (4-23)).

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

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

END OF STEPS

Optical port unit 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 port units as well as a recommendation for the optical attenuation that should be used when performing manual loopbacks.

OC192/STM64 port units

These are the relevant optical parameters of the OC192/STM64 port units:

App. Code	Port unit	Transmitter output power range [dBm]	Permitted receiver input power range [dBm]	Recommended attenuation
LEY67	OC192/STM64/1.5SR1	−4 … +2	−18.5 … −13	15 dB
LEY69	OC192/STM64/1.5IR1	−1 … +2	−21 … −8	15 dB
LEY97	OC192/STM64/1.5IRS1	−1 … +2	−14 … −3	10 dB
LEY201 … LEY240	OC192/STM64/DWDM…	−6.2 … −4.8	−20 … −12.5	20 dB
LEY284 … LEY299	OC192/STM64/POU…	−1 … +2	−21 … −8	15 dB
LEY97 + SEN3	OC192/STM64/1.5LR1 (OC192/STM64/1.5IRS1 with Optical Booster Amplifier, OBA)	+10 … +13	−14 … −3	20 dB
LEY228(AE) + SEN4	OC192/STM64/DWDM28 with Optical Booster and Pre-Amplifier (OBPA)	+10 … +13	−25 … −9	25 dB

OC48/STM16 port units

These are the relevant optical parameters of the OC48/STM16 port units:

App. Code	Port unit	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
LEY7	OC48/STM16/1.3LR1	−2 … +3	−27 … −9	15 - 20 dB
LEY8	OC48/STM16/1.5LR1	−2 … +3	−28 … −9	15 - 20 dB
LEY182	OC48/STM16/1.3SR1	−10 … −3	−18 … −3	5 dB
OC48/STM16/DWDM… (OLS80G compatible)				
LEY50	OC48/STM16/DWDM01	−4.0 ± 0.7	−22 … −12	15 dB

App. Code	Port unit	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
LEY51	OC48/STM16/DWDM02	−5.3 ± 0.7	−22 … −12	10 - 15 dB
LEY52	OC48/STM16/DWDM03	−6.5 ± 0.7	−22 … −12	10 dB
LEY53	OC48/STM16/DWDM04	−7.2 ± 0.7	−22 … −12	10 dB
LEY54	OC48/STM16/DWDM05	−7.7 ± 0.7	−22 … −12	10 dB
LEY55	OC48/STM16/DWDM06	−8.2 ± 0.7	−22 … −12	10 dB
LEY56	OC48/STM16/DWDM07	−8.0 ± 0.7	−22 … −12	10 dB
LEY57	OC48/STM16/DWDM08	−6.5 ± 0.7	−22 … −12	10 dB
LEY58	OC48/STM16/DWDM09	−2.0 ± 0.7	−22 … −12	15 dB
LEY59	OC48/STM16/DWDM10	−4.6 ± 0.7	−22 … −12	10 - 15 dB
LEY60	OC48/STM16/DWDM11	−5.8 ± 0.7	−22 … −12	10 - 15 dB
LEY61	OC48/STM16/DWDM12	−6.8 ± 0.7	−22 … −12	10 dB
LEY62	OC48/STM16/DWDM13	−7.4 ± 0.7	−22 … −12	10 dB
LEY63	OC48/STM16/DWDM14	−7.9 ± 0.7	−22 … −12	10 dB
LEY64	OC48/STM16/DWDM15	−8.1 ± 0.7	−22 … −12	10 dB
LEY65	OC48/STM16/DWDM16	−7.2 ± 0.7	−22 … −12	10 dB
OC48/STM16 port unit with passive optics				
LEY80 … LEY95	OC48/STM16/POU…	−2.8 … +1	−28 … −9	15 - 20 dB

OC12/STM4 port units

These are the relevant optical parameters of the OC12/STM4 port units:

App. Code	Port unit	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
LEY14	OC12/STM4/1.3SR2	−15 … −8	−28 … −8	7 dB
LEY190	OC12/STM4/1.5LR2	−3 … +2	−28 … −8	15 dB

OC3/STM1 port units

These are the relevant optical parameters of the OC3/STM1 port units:

App. Code	Port unit	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
LEY16 (4 ports)	OC3/STM1/1.3SR4	−15 … −8	−28 … −8	7 dB

App. Code	Port unit	Transmitter output power range [dBm]	Receiver input power range [dBm]	Recommended attenuation
LEY23 (8 ports)	OC3/STM1/1.3IR-SR8	−15 … −8	−28 … −8	7 dB
LEY15 (4 ports)	OC3/STM1/1.3LR4	−5 … 0	−34 … −10	15 dB

Related information

For related information, please refer to:

- *WaveStar® TDM 10G (STM-64) Installation Manual* (available LBO connectors),
- *WaveStar TDM 10G (STM-64) Applications and Planning Guide* (ordering information, port unit data sheets).

Restarting the laser after an Automatic Laser Shutdown

Overview

Purpose

Use this procedure to restart the laser for test purposes after an Automatic Laser Shutdown (ALS).

Related information

For related information, please refer to:

- "Automatic Laser Shutdown" (2-18).

How to restart the laser after an automatic laser shutdown

Before you begin

Prior to performing this task, you must:

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

Required privilege

You must have at least privilege codes of **S4 *and* P1** to restart the laser.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

Proceed as follows to perform a laser restart:

1 From the **System View** or **Shelf View** main menu of the *WaveStar* CIT, select **Fault** → **Laser Restart...** .

Result:

An equipment selection window will be opened.

2 In the **Shelf 2 (10G I/O)** select an optical port from a port unit supporting the ALS functionality.

The following circuit packs, where applicable in connection with optical amplifiers (OBA10G, OBPA10G), support the ALS funtionality:

- OC192/STM64/1.5R1 (LEY69),
- OC192/STM64/1.5RS1 (LEY97),
- OC192/STM64/DWDM28 (LEY228).

3 Click the **Select** pushbutton.

Result:

The **Laser Restart** window will be opened.

4 Select the desired value (2 seconds or 90 seconds) in the **Laser Restart Period** field.

5 Click **Apply** and, in the case of a 90 seconds period, confirm your selection by clicking **Yes** in the confirmation window that will be opened.

END OF STEPS

Glossary

μ
Microns

NUMERICS

0x1 Line Operation
0x1 means unprotected operation. The connection between network elements has one bidirectional line (no protection line).

1+1 Line Protection
A protection architecture in which the transmitting equipment transmits a valid signal on both the working and protection lines. The receiving equipment monitors both lines. Based on performance criteria and OS control, the receiving equipment chooses one line as the active line and designates the other as the standby line.

1xN Equipment Protection
1xN protection pertains to N number of circuit pack/port units protected by one circuit pack or port unit. When a protection switch occurs, the working signals are routed from the failed pack to the protection pack. When the fault clears, the signals revert to the working port unit.

12NC (12-digit Numerical Code)
Used to uniquely identify an item or product. The first ten digits uniquely identify an item. The eleventh digit is used to specify the particular variant of an item. The twelfth digit is used for the revision issue. Items with the first eleven digits the same, are functionally equal and may be exchanged.

A

ABN
Abnormal (condition)

ABS (Absent)
Used to indicate that a given circuit pack is not installed.

AC
Alternating Current

ACO (Alarm Cut-Off)

A button on the user panel used to silence audible alarms.

ACT (Active)
Used to indicate that a circuit pack or module is in-service and currently providing service functions.

ADM (Add/Drop Multiplexer)
The term for a synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

AEL
Accessible Emission Limits

Agent
Performs operations on managed objects and issues events on behalf of these managed objects. All SDH managed objects will support at least an agent. Control of distant agents is possible via local "Managers".

AGNE
Alarm Gateway Network Element

AID (Access Identifier)
A technical specification for explicitly naming entities (both physical and logical) of an NE using a grammar comprised of ASCII text, keywords, and grammar rules.

AIS (Alarm Indication Signal)
A code transmitted downstream in a digital network that indicates that an upstream failure has been detected and alarmed if the upstream alarm has not been suppressed.

AITS
Acknowledged Information Transfer Service: Confirmed mode of operation of the LAPD protocol.

Alarm
Visible or audible signal indicating that an equipment failure or significant event/condition has occurred.

Alarm Correlation
The search for a directly-reported alarm that can account for a given symptomatic condition.

Alarm Severity
An attribute defining the priority of the alarm message. The way alarms are processed depends on the severity.

Alarm Suppression
Selective removal of alarm messages from being forwarded to the GUI or to network management layer OSs.

Alarm Throttling
A feature that automatically or manually suppresses autonomous messages that are not priority alarms.

Aligning
Indicating the head of a virtual container by means of a pointer, for example, creating an Administrative Unit (AU) or a Tributary Unit (TU).

AMI (Alternate Mark Inversion)
A line code that employs a ternary signal to convert binary digits, in which successive binary ones are represented by signal elements that are normally of alternative positive and negative polarity but equal in amplitude and in which binary zeros are represented by signal elements that have zero amplitude.

Anomaly
A difference between the actual and desired operation of a function.

ANSI
American National Standards Institute

APD
Avalanche Photo Diode

APS (Automatic Protection Switch)
A protection switch that occurs automatically in response to an automatically detected fault condition.

ASCII (American Standard Code for Information Interchange)
A standard 7-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

ASN.1
Abstract Syntax Notation 1

Assembly
Gathering together of payload data with overhead and pointer information (an indication of the direction of the signal).

Association
A logical connection between manager and agent through which management information can be exchanged.

Asynchronous
The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

ATM (Asynchronous Transfer Mode)
A high-speed transmission technology characterized by high bandwidth and low delay. It utilizes a packet switching and multiplexing technique which allocates bandwidth on demand.

Attribute
Alarm indication level: critical, major, minor, or no alarm.

AU (Administrative Unit)
Carrier for TUs.

AU PTR (Administrative Unit Pointer)
Indicates the phase alignment of the VC-N with respect to the STM-N frame. The pointer position is fixed with respect to the STM-N frame.

AUG
Administrative Unit Group

AUTO (Automatic)
One possible state of a port or slot. When a port is in the AUTO state and a good signal is detected, the port automatically enters the IS (in-service) state. When a slot is in the AUTO state and a circuit pack is detected, the slot automatically enters the EQ (equipped) state.

Autolock
Action taken by the system in the event of circuit pack failure/trouble. System switches to protection and prevents a return to the working circuit pack even if the trouble clears. Multiple protection switches on a circuit pack during a short period of time cause the system to autolock the pack.

Autonomous Message
A message transmitted from the controlled Network Element to the SNMS which was not a response to an SNMS originated command.

AVAIL
Available

B

Bandwidth
The difference in Hz between the highest and lowest frequencies in a transmission channel. The data rate that can be carried by a given communications circuit.

Baud Rate
Transmission rate of data (bits per second) on a network link.

BER (Bit Error Rate)
The ratio of error bits received to the total number of bits transmitted.

Bidirectional Line
A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bidirectional Ring
A ring in which both directions of traffic between any two nodes travel through the same network elements (although in opposite directions).

Bidirectional Switch
Protection switching performed in both the transmit and receive directions.

BIP-N (Bit Interleaved Parity-N)
A method of error monitoring over a specified number of bits (BIP-3 or BIP-8).

Bit
The smallest unit of information in a computer, with a value of either 0 or 1.

Bit Error Rate Threshold
The point at which an alarm is issued for bit errors.

BLD OUT LG
Build-Out Lightguide

Bridge Cross-Connection
The setting up of a cross-connection leg with the same input tributary as that of an existing cross-connection leg. Thus, forming a 1:2 bridge from an input tributary to two output tributaries.

Broadband Communications
Voice, data, and/or video communications at greater than 2 Mb/s rates.

Broadband Service Transport
STM-1 concatenation transport over the *WaveStar*® TDM 10G (STM-64) for ATM applications.

Byte
Refers to a group of eight consecutive binary digits.

C

C
Container

C2SL
C2 Signal Label

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

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 (Customer Interface Terminal)
The user interface terminal used by craft personnel to communicate with a network element.

CL
Clear

CLEI
Common Language Equipment Identifier

Client
Computer in a computer network that generally offers a user interface to a server.

CLLI
Common Language Location Identifier

Closed Ring Network
A network formed of a ring-shaped configuration of network elements. Each network element connects to two others, one on each side.

CM (Configuration Management)
Subsystem that configures the network and processes messages from the network.

CMI
Coded Mark Inversion

CMIP
Common Management Information Protocol. OSI standard protocol for OAM&P information exchange.

CMISE
Common Management Information Service Element

CO (Central Office)
A building where common carriers terminate customer circuits.

Co-Resident
A hardware configuration where two applications can be active at the same time independently on the same hardware and software platform without interfering with each others functioning.

Collocated
System elements that are located in the same location.

Command Group
An administrator-defined group that defines commands to which a user has access.

Concatenation
A procedure whereby multiple virtual containers are associated one with each other resulting in a combined capacity that can be used as a single container across which bit sequence integrity is maintained.

Correlation
A process where related hard failure alarms are identified.

CP
Circuit Pack

CPE
Customer Premises Equipment

CR (Critical (alarm))
Alarm that indicates a severe, service-affecting condition.

CRC
Cyclical Redundancy Check

Cross-Connect Map
Connection map for an SDH Network Element; contains information about how signals are connected between high speed time slots and low speed tributaries.

Crosstalk
An unwanted signal introduced into one transmission line from another.

CSMA/CD
Carrier Sense Multiple Access with Collision Detection

CTIP
Customer Training and Information Products

CTS
Customer Technical Support within Lucent Technologies

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 Rate)
The calculated average bit error rate 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)
Subsystem of *WaveStar* SNMS that processes and logs event reports of the network.

EMC (Electromagnetic Compatibility)
A measure of equipment tolerance to external electromagnetic fields.

EMI (Electromagnetic Interference)
High-energy, electrically induced magnetic fields that cause data corruption in cables passing through the fields.

EMS
Element Management System

Entity
A specific piece of hardware (usually a circuit pack, slot, or module) that has been assigned a name recognized by the system.

Entity Identifier
The name used by the system to refer to a circuit pack, memory device, or communications link.

EoS (Ethernet over SDH)
Generic name for the mapping of MAC 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.

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.

FTAM
File Transfer Access and Management

FTP
File Transfer Protocol

FTTD
File Transfer Translation Device

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

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.

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.

IP
Internet Protocol

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.

LO
Low Order

Location
An identifier for a specific circuit pack, interface module, interface port, or communications link.

Lockout of Protection
The *WaveStar* CIT command that prevents the system from switching traffic to the protection line from a working line. If the protection line is active when a “Lockout of Protection” is entered – this command causes the working line to be selected. The protection line is then locked from any Automatic, Manual, or Forced protection switches.

Lockout State
The Lockout State shall be defined for each working or protection circuit pack. The two permitted states are: None – meaning no lockout is set for the circuit pack, set meaning the circuit pack has been locked out. The values (None & Set) shall be taken independently for each working or protection circuit pack.

LOF (Loss of Frame)
A failure to synchronize to an incoming signal.

LOM
Loss Of Multiframe

Loop Timing
A special case of line timing. It applies to network elements that have only one OC-N/STM-N interface. For example, terminating nodes in a linear network are loop timed.

Loopback
Type of diagnostic test used to compare an original transmitted signal with the resulting received signal. A loopback is established when the received optical or electrical external transmission signal is sent from a port or tributary input directly back toward the output.

LOP (Loss of Pointer)
A failure to extract good data from a signal payload.

LOS (Loss of Signal)
The complete absence of an incoming signal.

Loss Budget
Loss (in dB) of optical power due to the span transmission medium (includes fiber loss and splice losses).

LPA (Lower order Path Adaptation)
Function that adapts a PDH signal to a synchronous network by mapping the signal into or de-mapping the signal out of a synchronous container.

LPC (Lower Order Path Connection)
Function that provides for flexible assignment of lower order VCs in a higher order VC.

LPT (Lower Order Path Termination)
Function that terminates a lower order path by generating and adding the appropriate VC POH to the relevant container at the path source and removing the VC POH and reading it at the path sink.

LS
Low Speed

LTE
Line Terminating Equipment

M

µm
Micrometer

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

MS
Multiplexer Section

ms
Millisecond

MS-SPRING (Multiplexer Section Shared Protection Ring)
A protection method used in Add-Drop Multiplexer Network Elements.

MSOH (Multiplexer Section OverHead)
Part of the Section Overhead. Is accessible only at line terminals and multiplexers.

MSP (Multiplexer Section Protection)
Provides capability for switching a signal from a working to a protection section.

MST (Multiplexer Section Termination)
Function that generates the Multiplexer Section OverHead in the transmit direction and terminates the part of the Multiplexer Section overhead that is acceptable in the receive direction.

MTBF
Mean Time Between Failures

MTBMA
Mean Time Between Maintenance Activities

MTIE
Maximum Time Interval Error

MTPI
Multiplexer Timing Physical Interface

MTS (Multiplexer Timing Source)
Function that provides timing reference to the relevant component parts of the multiplex equipment and represents the SDH Network Element clock.

MTTR
Mean Time To Repair

Multiplexer
A device (circuit pack) that combines two or more transmission signals into a combined signal on a shared medium.

Multiplexing
A procedure by which multiple lower order path layer signals are adapted into a higher order path, or the multiple higher order path layer signals are adapted into a multiplex section.

N

NA
Not Applicable

NE (Network Element)
A node in a telecommunication network that supports network transport services and is directly manageable by a management system.

NEBS
Network Equipment-Building System

NIM
Non-intrusive Monitoring

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.

NORM
Normal

NPI
Null Pointer Indication

NPPA (Non-Preemptible Protection Access)
Non-preemptible protection access increases the available span capacity for traffic which does not require protection by a ring, but which cannot be preempted.

NRZ
Nonreturn to Zero

NSA
Non-Service Affecting

NSAP Address (Network Service Access Point Address)
Network Service Access Point Address (used in the OSI network layer 3). An automatically assigned number that uniquely identifies a Network Element for the purposes of routing DCC messages.

NVM (Non-Volatile Memory)

Memory that retains its stored data after power has been removed. An example of NVM would be a hard disk.

O **O&M**
Operation and Maintenance

OA
Optical Amplifier

OAM&P
Operations, Administration, Maintenance, and Provisioning

OC, OC-n
Optical Carrier

OC-12
Optical Carrier, Level 12 Signal (622.08 Mbit/s)

OC-192
Optical Carrier, Level 192 (9953.28 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

OOF
Out-of-Frame

OOS (Out-of-Service)
The circuit pack is not providing its normal service function (removed from either the working or protection state) either because of a system problem or because the pack has been removed from service.

Open Ring Network
A network formed of a linear chain-shaped configuration of network elements. Each network element connects to two others, one on each side, except for two network elements at the ends which are connected on only one side. A closed ring can be formed by adding a connection between the two end nodes.

Operations Interface
Any interface providing you with information on the system behavior or control. These include the equipment LEDs, user panel, *WaveStar* CIT, office alarms, and all telemetry interfaces.

Operator
A user of the system with operator-level user privileges.

Optical Line Signal
A multiplexed optical signal containing multiple wavelengths or channels.

Original Value Provisioning
Preprogramming of a system's original values at the factory. These values can be overridden using local or remote provisioning.

OS (Operations System)
A central computer-based system used to provide operations, administration, and maintenance functions.

OSF
Open Software Foundation Operations System Function

OSI (Open Systems Interconnection)
Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Outage
A disruption of service that lasts for more than 1 second.

OW (Orderwire)
A dedicated voice-grade line for communications between maintenance and repair personnel.

P

Parameter
A variable that is given a value for a specified application. A constant, variable, or expression that is used to pass values between components.

Parity Check
Tests whether the number of ones (or zeros) in an array of binary bits is odd or even; used to determine that the received signal is the same as the transmitted signal.

Pass-Through
Paths that are cross-connected directly across an intermediate node in a network.

Path
A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Terminating Equipment
Network elements in which the path overhead is terminated.

PCB
Printed Circuit Board

PCM
Pulse Code Modulation

PDH
Plesiochronous Digital Hierarchy

PI
Physical Interface

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).

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.

SL
Signal Label

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 1310 nm or 1550 nm.

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 Networ)
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 Marker

SSU_L
Synchronization Supply Unit — Local

SSU_T
Synchronization Supply Unit — Transit

Standby Path
One of two signals entering a constituent path selector, the standby path is the path not currently being selected.

State
The state of a circuit pack indicates whether it is defective or normal (ready for normal use).

Station Clock Input
An external clock may be connected to a Station Clock Input.

Status
The indication of a short-term change in the system.

STBY (Standby)
The circuit pack is in service but is not providing service functions. It is ready to be used to replace a similar circuit pack either by protection or by duplex switching.

STM
Synchronous Transport Module (SDH)

STM-N (Synchronous Transport Module, Level N)
A building block information structure that supports SDH section layer connections, where N represents a multiple of 155.52 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
Target Identifiers Address Resolution Protocol

TCA (Threshold-Crossing Alert)
A message type sent from a Network Element that indicates that a certain performance monitoring parameter has exceeded a specified threshold.

TCP
Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

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