Lucent Technologies
Bell Labs Innovations

WaveStar® TDM 10G (STM-64)

User Operations Guide

Notice

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

Mandatory customer information

Always observe the Safety Instructions given in Chapter 1 when operating the system.

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.

Windows 2000 is a registered trademark of Microsoft Corporation.

Ordering information

The order number of this document is 365-371-522 (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

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

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

365-371-522   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)
User Operations Guide

365-371-522   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:
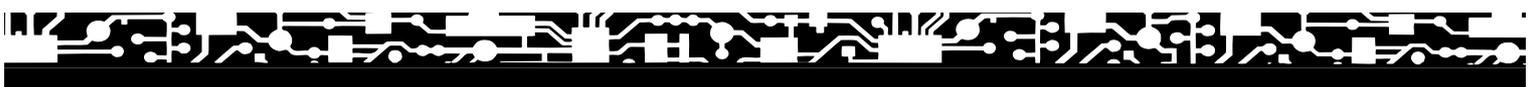
Name: _____   Date: _____

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

....

....

3   Management communication setup

....

....

C O N T E N T S   **Lucent Technologies**   365-371-522
v i   Issue b, October 2001

5 Alarm management

....

8   Traffic maintenance

....

....

9   Performance Monitoring

....

11   Database backup

12   Periodic activities

13   Security and administration concepts

....

14   Management communication setup concepts

....

15   Equipment provisioning concepts

....

....

16   Alarm management concepts

....

17   Timing provisioning concepts

18   Traffic provisioning concepts

19   Traffic maintenance concepts

....

C O N T E N T S   **Lucent Technologies**   365-371-522
x x i v   Issue b, October 2001

About this information product

Purpose   This User Operations Guide provides operations, administration and maintenance information about the *WaveStar*® TDM 10G (STM-64).

Reason for reissue   The present Issue b is a revised version of this manual containing adaptations and updates for Release 4.0.

Safety labels   The present manual contains basic safety instructions which have to be strictly observed when handling the equipment and systems described.

The most important safety instructions are collected in the "Safety" chapter in Fascicle 1 of this manual.

Strictly observe the warnings and safety instructions described in Fascicle 1 ("Safety") before carrying out work of any kind on the equipment and systems described.

All safety instructions include a signal word that classifies the danger and a text block that contains descriptions of the type and cause of the danger, the consequences of ignoring the safety instruction and the measures that can be taken to minimize the danger. In some safety instructions, a warning symbol is placed underneath the signal word.

Example:

⚠ DANGER

Arcing on removing or inserting a live power supply plug.

Arcing can cause burns to the hands and damage to the eyes. Ensure that the line circuit-breaker on the fuse panel is in the ″OFF″ position before removing or inserting the power supply plug.

Classification of hazards

There are three classes of hazards. They are designated using the head words "Danger", "Warning" and "Caution". Their meaning is as follows:

- *Danger*
  is used to mark safety warnings which, if not followed, will certainly or with a very high degree of probability result in death or extremely serious injury.

- *Warning*
  is used to mark safety warnings which, if not followed, can lead to serious injury or permanent damage to the health of an individual or to property.

- *Caution*
  is used to mark safety warnings which, if not followed, can lead to injury or property damage - including financial losses due to extensive operational impairment.

Warning symbols

The examples below show the warning symbols used.

⚠ DANGER

Example of a general warning about a danger.

⚠ DANGER

Example of a warning about laser radiation.

DANGER

Warning about devices sensitive to electrostatic discharge (ESD)

The safety instructions for the classes "Danger", "Warning" and "Caution" always have a warning symbol, the "Important" and "Notice" safety instructions can, but do not always have a warning symbol.

Conventions used

These conventions are used in this document:

Numbering

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

Cross-references

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

Keyword blocks

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

Typographical conventions

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

- Elements of the graphical user interface (GUI)
  These are examples of text that appears on a graphical user interface (GUI), such as menu options, window titles or push-buttons:
  - **Provision…**, **Delete**, **Apply**, **Close**, **OK** (push-button)
  - **Provision Timing/Sync** (window title)
  - **View Equipment Details…** (menu option)
  - **Administration** → **Security** → **User Provisioning…** (path for invoking a window)

- File names and system path information

These are examples of file names and system path information:

- *setup.exe*

- *C:\Program Files\Lucent Technologies*

- Keyboard entries
  These are examples of keyboard entries:

  - **F1**, **Esc X**, **Alt-F**, **Ctrl-D**, **Ctrl-Alt-Del** (simple keyboard entries)
    A hyphen between two keys means that both keys have to be pressed simultaneously. Otherwise, a single key has to be pressed, or several keys have to be pressed in sequence.

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

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

  - Loss of Signal

  - Circuit Pack Failure

  - HP-UNEQ, MS-AIS, LOS, LOF

  - Not enough disk space available

Abbreviations

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

Related documentation

This section briefly describes the documents that are included in the *WaveStar* TDM 10G 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) Applications, Planning, and Ordering Guide (APOG) is for use by network planners, analysts and managers. It is also for use by the Lucent Account Team. It presents a detailed overview of the system, describes its applications, gives planning requirements, engineering rules, ordering information, and technical specifications.

- User Operations Guide

The *WaveStar* TDM 10G (STM-64) User Operations Guide provides step-by-step information for use in daily system operations. The manual demonstrates how to perform system provisioning, operations, and administrative tasks by use of *WaveStar* CIT.

- Alarm Messages and Trouble Clearing Guide
  The *WaveStar* TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide gives detailed information on each possible alarm message. Furthermore, it provides procedures for routine maintenance, troubleshooting, diagnostics, and component replacement.

- 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* 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
109149773 (365-371-521)	*WaveStar* TDM 10G (STM-64) Applications and Planning Guide
109149781 (365-371-522)	*WaveStar* TDM 10G (STM-64) User Operations Guide
109149799 (365-371-523)	*WaveStar* TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide
109149823 (365-371-525)	*WaveStar* TDM 10G (STM-64) Installation Manual
109149831 (365-371-526)	*WaveStar* TDM 10G (STM-64) TL1 Reference Manual
109149807 (365-371-524)	*WaveStar* SNMS Provisioning Guide (Application *WaveStar* TDM 10G (STM-64))
109149815	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 **CLASS 1 LASER PRODUCT**

❸

DANGER

INVISIBLE LASER RADIATION WHEN OPEN AND FIBER DISCONNECTED

Avoid direct exposure to beam

Do not view beam directly with optical instruments

848301669
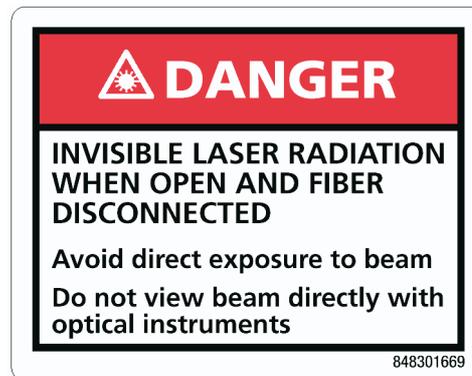
Legend

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.			

Lucent Technologies

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 Security administration

Overview

Purpose This chapter describes the security administration tasks.

Contents

Administering user logins

Overview

Purpose   User administration basically consists of:

- "Creating a user login" (2-7),
- "Modifying a user login" (2-10),
- "Deleting a user login" (2-11),
- "Disabling user logins" (2-12),
- "Enabling user logins" (2-14).

It is suggested to use "User administration tasks" (2-3) as an entry point for user administration activities.

Furthermore, it is recommended to have a list prepared of all the users that probably will need to have access to the *WaveStar*® CIT and the NEs, especially if several user logins are to be created or modified for different NEs. The list should contain the designated user IDs, associated passwords, access privileges and other related security parameters, and should be as complete as possible.

Related information   For related information, please refer to:

- "User administration" (13-3).
- Chapter 24, "*WaveStar* CIT Tutorial"

Contents

User administration tasks

User privilege   You must be a security administrator with a user privilege code of *S5* to create, modify or delete user logins.

User administration diagram   The following figure gives an outline of the main points of user administration as an overview. The diagram is based on the assumption that a new user or an existing user has or shall have access to both the *WaveStar*® CIT and the NEs.

Changes in the NE security database due to user administration activities in the NE **User Provisioning** window can also be saved to the *WaveStar* CIT security database (cf. "Creating a user login" (2-7) and "Modifying a user login" (2-10)).

User administration for the *WaveStar* CIT can be done by means of the *WaveStar* CIT **User Provisioning** window (cf. "The network element User Provisioning window" (2-6)).

```
                    ┌──────────────────────────┐   LUC01
                    │ Login to the WaveStar™ CIT│   LUC02
                    └──────────────────────────┘   Security administrator (S5)
                                 │
                                 ▼
                    ┌──────────────────────────┐
                    │ Connect to the respective NE│
                    └──────────────────────────┘
                                 │
                                 ▼
                    ┌──────────────────────────┐
                    │ Invoke the NE User        │
                    │ Provisioning window       │
                    └──────────────────────────┘
                                 │
            ┌────────────────────┼────────────────────┐
            ▼                    ▼                    ▼
    ┌───────────────┐   ┌───────────────┐   ┌───────────────┐
    │ Create a user │   │ Modify a user │   │ Delete a user │
    └───────────────┘   └───────────────┘   └───────────────┘
            └────────────────────┼────────────────────┘
                                 ▼
                          ╱─────────────╲
                         ╱ Several user   ╲   Yes
                         ╲ logins?        ╱───────
                          ╲─────────────╱
                                 │ No
                                 ▼
                    ┌──────────────────────────┐
                    │ Disconnect from the NE   │
                    └──────────────────────────┘
                                 │
                                 ▼
                          ╱─────────────╲
                         ╱ Several NEs?   ╲   Yes
                         ╲               ╱───────
                          ╲─────────────╱
                                 │ No
                                 ▼
                    ┌──────────────────────────┐
                    │ Logout from the WaveStar™ │
                    │ CIT                       │
                    └──────────────────────────┘
```
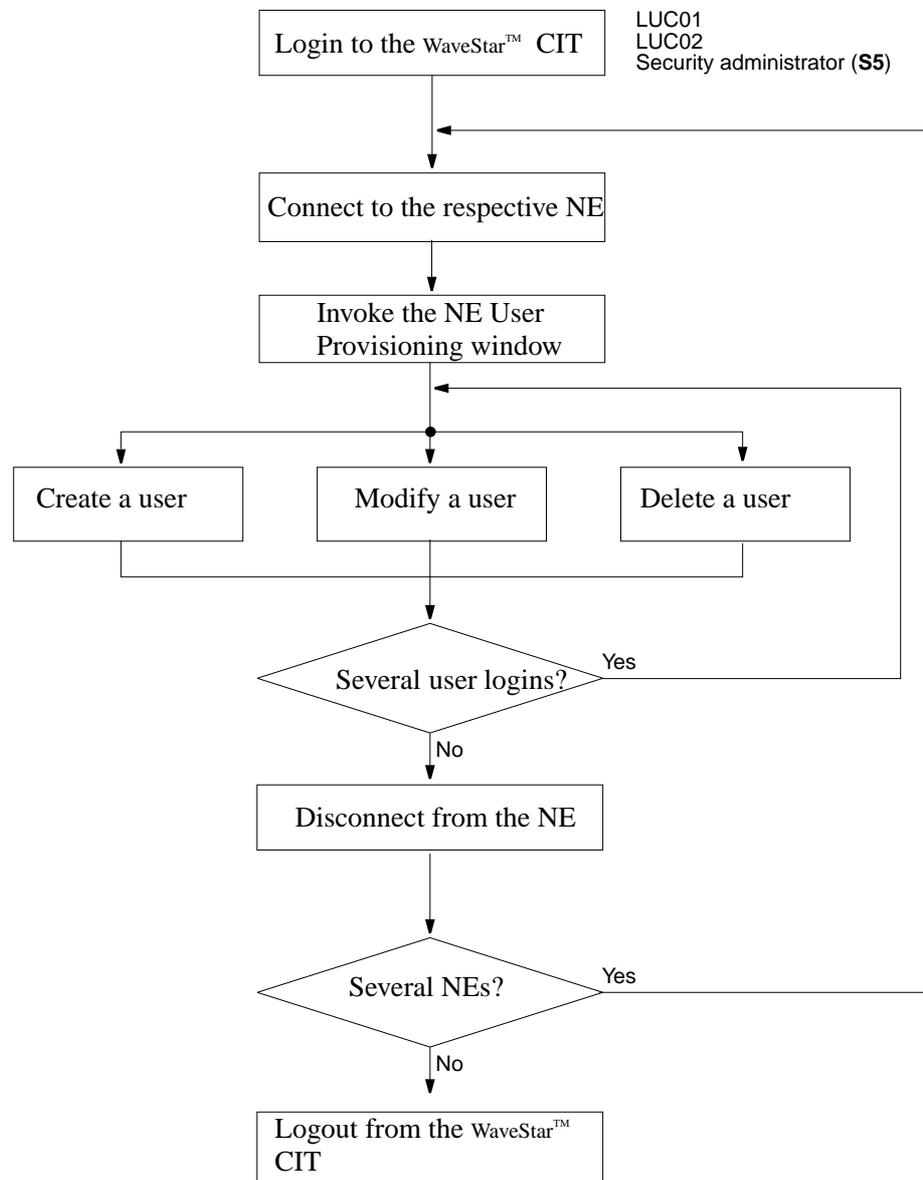
Required equipment The following equipment is required to perform these tasks:

- *WaveStar* CIT

....

2 - 4   **Lucent Technologies**   365-371-522
                                                                                            Issue b, October 2001

The *WaveStar CIT User Provisioning* window

The *WaveStar* **CIT User Provisioning** window can be invoked from the *WaveStar* CIT main window via **Administration → Security → User Provisioning...**.

Use this window to create, modify or delete a user login for a user which has or shall have a user ID, password and access privileges for the *WaveStar* CIT.

The network element *User Provisioning* window

The NE **User Provisioning** window can be invoked from the **System View** or **Shelf View** main menu via **Administration** → **Security** → **User Provisioning...** .

Use this window to create, modify or delete a user login for a user which has or shall have a user ID, password, password aging, inactivity timeout and access privileges for the network element you are currently connected to.

Creating a user login

....

Before you begin   The starting point for the following procedure is according to "User administration tasks" (2-3). The procedure itself is limited to the necessary steps to create a new user login using the NE **User Provisioning** window.

Important! Please note that any user administration changes will take effect not before the next login session.

Procedure   Complete the following steps to create a new user login.

....

1   In the NE **User Provisioning** window, select **New User**, place the cursor in the associated text box and type in the user ID.

> **Reference:**
>
> Please refer to "Valid user login" (13-3) .

....

2   Place the cursor in the **Enter Password** text box and type in the password assigned to the new user.

The password may be preliminary. Each user is permitted to change her/his own password.

> **Reference:**
>
> Please refer to "Valid password" (13-3) .

....

3   Confirm the password by typing it in again in the **Confirm Password** text box.

....

4   Assign a user type to the new user by using the **User Type** drop-down list box:

IF …	THEN …
you choose a predefined user type	the corresponding user privilege codes will be assigned automatically for the five functional categories.
you choose "Others"	you will have to assign the user privilege codes manually by using the corresponding drop-down list boxes.

....

5   Assign a command priority level to the new user by using the up/down arrows of the **Priority Level** spin box or typing it in directly.

....

The priority level range of values is from one to five. The highest priority level is five, the default priority level is one.

....

6 Specify the notifications a user may receive by using the **Change Notification** form. To invoke the **Change Notification** form click on the **Modify** button in the **Notification List** area.

....

7 Select if the *Password Aging Interval* function should be enabled or disabled.

IF ...	THEN ...
you want to enable the *Password Aging Interval*	select the right check box. You can set the *Password Aging Interval* by using the up/down arrows of the **Days** spin box or typing it in directly. **Reference:** Please refer to "Password aging" (13-6).
you want to disable the *Password Aging Interval*	select **Disable**.

....

8 Select if the *Inactivity Timeout* function should be enabled or disabled.

IF ...	THEN ...
you want to enable *Inactivity Timeout*	select the right check box. You can set value for **Inactivity Timeout** by using the up/down arrows of the **Minutes** spin box or typing it in directly. **Reference:** Please refer to "Inactivity time-out period" (13-5).
you want to disable *Inactivity Timeout*	select **Disable**.

....

9 Select if *Initialization Observability* should be enabled or disabled.

....

10 Make sure that the settings in the NE **User Provisioning** window are correct.

....

....

11   Click **Add** to add the new user login.

....

12   Confirm your changes in the confirmation window by clicking **Yes**.

Result:

Another window opens with the question: ***"Do you want to save the security changes in the CIT security database?"***

You may now:

1.   Click **Yes** to save the new user login and related security parameters also to the *WaveStar*® CIT security database, or

2.   Click **No** to close that window without adopting the *WaveStar* CIT security database.

E ND OF S TEPS
....

⌐

....

365-371-522
Issue b, October 2001

Lucent Technologies

2 - 9

Modifying a user login

Before you begin The starting point for the following procedure is according to "User administration tasks" (2-3). The procedure itself is limited to the necessary steps to modify an existing user login using the NE **User Provisioning** window.

Important! Any user administration changes will take effect not before the next login session.

Prcocedure Complete the following steps to modify an existing user login.

1 In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.

2 Modify the related security parameters according to your needs by changing only the parameters to be modified.

> **Example:**
>
> If you only want to assign another priority level then it is not necessary to enter the user's password.

3 Make sure that the settings in the NE **User Provisioning** window are correct.

4 Click **Modify** to change the user login.

5 Confirm your changes in the confirmation window by clicking **Yes**.

> **Result:**
>
> Another window opens with the question: ***"Do you want to save the security changes in the CIT security database?"***
>
> You may now:
>
> 1. Click **Yes** to save the user related security parameters also to the *WaveStar*® CIT security database, or
>
> 2. Click **No** to close that window without adopting the *WaveStar* CIT security database.

E N D   O F   S T E P S

Deleting a user login

Before you begin   The starting point for the following procedure is according to "User administration diagram" (2-4). The procedure itself is limited to the necessary steps to delete an existing user login using the NE **User Provisioning** window.

Important! Any user administration changes will take effect not before the next login session.

Instructions   Complete the following steps to modify an existing user login.

1   In the NE **User Provisioning** window, select **Existing User** and specify the user ID by using the associated drop-down list box.

2   Click **Delete** to delete the user login and confirm the deletion in the confirmation window by clicking **Yes**.

3   A window opens with the information that the user data was deleted. Click **OK** to dismiss that window.

Notice that the deleted user login will still be visible in the **Existing User** list because user administration changes take effect not before the next login session.

E N D   O F   S T E P S

Disabling user logins

....

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

Required privilege code

You must be a security administrator with a user privilege code of S5
to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions **Important!** Any user administration changes will take effect not
before the next login session.

Complete the following steps to disable existing user logins.
....

1 From **the System View** or **Shelf View** main menu select
Administration → **Security** → **Disable User Login ...**.

      Result:

      The *WaveStar* CIT **Disable User Login** window is displayed. It
      shows a list of all provisioned users (except the superusers) and
      their login status.

....

2 You can disable a single or all users logins.

IF ...	THEN ....
you want to disable all user logins,	select the radio button **Disable all the user logins**.
you want to disable a single user login,	select a user login and select the radio button **Disable only the selected user login**.

....

3 Click **OK**.

      Result:

      A confirmation screen pops up asking you to confirm your
      selection.

....

4 Click Yes.

....

Result:

The **Disable User Login** window is dismissed.

E N D   O F   S T E P S

Enabling user logins

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

Required privilege code

You must be a security administrator with a user privilege code of S5
to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   **Important!** Any user administration changes will take effect not
before the next login session.

Complete the following steps to enable existing user logins.

....

1   From **the System View** or **Shelf View** main menu select
Administration → **Security** → **Enable User Login ..**.

Result:

The *WaveStar* CIT **Enable User Login** window is displayed. It
shows a list of all currently disabled users and their login status.

....

2   You can enable a single or all users logins.

IF ...	THEN ....
you want to enable all user logins,	select the radio button **Enable all the user logins**.
you want to enable a single user login,	select a user login and select the radio button **Enable only the selected user login**.

3   Click **OK**.

Result:

A confirmation screen pops up asking you to confirm your
selection.

....

4   Click Yes.

Result:

The **Enable User Login** window is dismissed.

E N D   O F   S T E P S

Changing super user ids

Overview

Purpose   Use the following procedures to change super user ids either on the *WaveStar*® CIT or on the NE .

⌐

Changing super user ids on the *WaveStar*® CIT

When to use Use this procedure to change super user ids on the *WaveStar* CIT.

Before you begin Prior to performing this task, you must be logged into the *WaveStar* CIT Only a superuser is permitted to change a super user id.

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to change your password.

1 From **the System View** or **Shelf View** main men, select
Administration → **Security** → **Change Superuser Login ID...**

     Result:

     The **Change Super User ID** form is displayed:

2 Select the super user Login ID you want to change. Click on the respective radio button.

3 Key in the new Login ID.

     Note

     Login IDsare case sensitive and must start with a letter.

4 Click **OK**.

     Result:

     The super user Login ID is updated and the **Change Super User ID** form is dismissed.

     The changed super user Login ID will take effect the next time you log into the *WaveStar* CIT.

E N D   O F   S T E P S

Changing super user IDs on the NE

When to use   Use this procedure to change your own password on the NE (for the user ID currently logged in with).

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

Required privilege code

You must have a user privilege code of S5 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to change your password.

1   From **the System View** or **Shelf View** main men, select
     Administration → Security → Change Superuser Login ID...

     Result:

     The **Change Super User ID** form is displayed:

2   Select the super user Login ID you want to change. Click on the respective radio button.

3   Key in the new Login ID.

     Note

     Login IDsare case sensitive and must start with a letter.

4   Click **OK**.

     Result:

     The super user Login ID is updated and the **Change Super User ID** form is dismissed.

     The changed super user Login ID will take effect the next time you log into the NE.

     E N D   O F   S T E P S

Changing your password

Overview

....

Purpose
Use this procedure to change your own password (for the user ID currently logged in with).

Please note, to administer passwords and other login information for other users, please refer to "Administering user logins" (2-2).

Valid password
The following characters are allowed in a password:

- Upper-case letters ('A' .. 'Z')

- Lower-case letters ('a' .. 'z')

- Digits ('0' .. '9')

- Special characters:

  - Plus sign ('+')

  - Percent sign ('%')

  - Number sign ('#')

Furthermore, a valid password ...

- ... consists of a sequence of six to ten characters.

- ... must start with a letter.

- ... must contain at least one of the special characters ('+', '%' or '#').

Please note that passwords are case sensitive.

Related information
For related information, please refer to:

- Chapter 13, "Security and administration concepts".

- Chapter 24, " *WaveStar*® CIT Tutorial"

⌐

....

Procedure

....

Before you begin   Each user is permitted to change her/his own password.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to change your password.
....

1   From the *WaveStar* CIT main window, select **Administration** →
Change Password...

> **Result:**
>
> The **Change Password** form is displayed:

....

2   Place the cursor into the **Old Password** field and key in the password
you are currently using.

....

3   Place the cursor into the **New Password** field and key in the new
password.

> **Note**
>
> Passwords are case sensitive and must start with a letter.
>
> The new password cannot be a password used for this login in
> the past.

....

4   Place the cursor into the **Confirm Password** field and key in the new
password a second time.

....

5   Click **OK**.

> **Result:**
>
> The password is updated and the **Change Password** form is
> dismissed.
>
> The changed password will take effect the next time you log
> into the *WaveStar* CIT.

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

Modifying user security parameters

Overview

....

Purpose   Use this procedure to change the variables for the *User Id Lockout*
function.

Related information   For related information, please refer to:

- "User id lockout threshold" (13-6).
- "User id lockout period" (13-6).
- "User id lockout aging period" (13-7).
- "User id aging period" (13-7).
- Chapter 24, " *WaveStar*® CIT Tutorial"

....

Procedure

....

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

Required privilege code

You must be a security administrator with a user privilege code of S5
to perform this task.

Required equipment

The following equipment is required to perform this task:

• *WaveStar* CIT

Instructions   Complete the following steps to modify the User ID Lockout
parameters.

....

1   From the **System View** or **Shelf View** main menu select
Administration → **Security** → **Security Provisioning...**.

> **Result:**

> The **Provision NE Security** form is displayed:

....

2   Define the parameters by using the up/down arrows of the spin boxes
or typing it in directly.

....

3   Click **OK**.

> **Result:**

> The parameters are updated and the **Provision NE Security**
> form is dismissed.

....

The modification will take effect only with the next login.

E N D   O F   S T E P S

Modifying user notification

Overview

....

Purpose   Use this procedure to change your notification list, if you cannot access the NE **User Provisioning** window to do so because you are no super user.

Related information   For related information, please refer to:

- "Notification list" (13-5).
- "Administering user logins" (2-2)
- Chapter 24, " *WaveStar*® CIT Tutorial"

❒

....

Procedure

....

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

Required privilege code

You must be at least a general user with a user privilege code of S1 to
perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to modify the User notifications.
....

1   From the **System View** or **Shelf View** main menu select
Administration → **Change Notifications ...**.

Result:

The **Change Notification** form is displayed:

....

2   Define the notification types you want to receive.

....

3   Click **OK**.

....

Result:

The notification list is updated and the **Change Notification** form is dismissed.

The modification will take effect only with the next login.

E N D   O F   S T E P S

Logging out NE users

Overview

....

Purpose   Use this procedure to terminate another user's login association with an NE.

The *Log Out User* window   The *WaveStar*® CIT **Log Out User** window can be invoked from the *WaveStar* CIT **System View** or **Shelf View** main menu via **Administration → Security → Logout NE User ...**.

Related information   For related information, please refer to:

- Chapter 24, "*WaveStar* CIT Tutorial"

....

Lucent Technologies

Procedure

....

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

Required privilege code

You must be a security administrator with a user privilege code of S5
to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to log out users from the NE.
....

1   From the **System View** or **Shelf View** main menu select
Administration → **Security** → **Logout NE User ..**.

> **Result:**
>
> The *WaveStar* CIT **Log Out User** window is displayed. It shows
> a list of all users currently logged into the NE.

The CIT does not display your own UID, because this screen cannot
be used to log out yourself.

....

2   You can log out a single or all users from the NE.

IF ...	THEN ....
you want to logout all users,	click **Logout All**.
you want to logout a single user,	select a user and click **Logout One**.

> **Result:**
>
> A confirmation screen pops up asking you to confirm your
> selection.

....

3   Click Yes.

> **Result:**
>
> The **Log Out User** form is dismissed.

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

....

Displaying login information

Overview

Purpose   Use this procedure to display a list of all users logged into an NE and to get information on all logins into an NE.

The *View User Logins* window   The *WaveStar*® CIT **View User Logins** window can be invoked from the *WaveStar* CIT **System View** or **Shelf View** main menu via **Administration** → **Security** → **View User Logins ....**

Lucent Technologies

The *View Logged In User* window

The *WaveStar* CIT **View Logged In User** window can be invoked from the *WaveStar* **System View** or **Shelf View** main menu via **Administration** → **Security** → **View Logged**-**In Users ...**.

Related information

For related information, please refer to:

- Chapter 24, "*WaveStar* CIT Tutorial"
- Chapter 13, "Security and administration concepts"

Procedure

....

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

Required privilege code

You must have a user privilege code of S1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to get information on the logins
into the actual NE.

....

1

IF ...	THEN ...
you want to display a list of all users currently logged into the NE.	from the **System View** or **Shelf View** main menu select **Administration** → **Security** → **View User Logins ..**.
	Result:
	The *WaveStar* CIT "View User Logins" window is displayed. It shows a list of all users currently logged into the NE.
you want to display information to all User Logins into the NE	from the **System View** or **Shelf View** main menu select **Administration** → **Security** → **View User Logins ..**.
	Result:
	The *WaveStar* CIT **View Logged In Users** window is displayed. It shows information on all users currently logged into the NE.
	Reference:
	Refer to Chapter 13, "Security and administration concepts".

E ND OF S TEPS
....

⌐

....

3 Management communication setup

Overview

Purpose This chapter describes the procedures which have to be performed for the management communication setup.

Contents

Changing the NE name (TID)

Overview

Purpose Use this procedure to change an NE's name (also referred to as the target identifier, TID).

NE names NE names must be unique within a network to guarantee the reachability by management systems and the proper interworking of NEs.

Related information For related information, please refer to:

- "NE name administration" (14-32).
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

Before you begin   Prior to performing this task, you must:

- have a valid user login and password,

- be connected to the subject NE, and

- have proper access privileges to perform this task.

Required privilege codes

You must have at least privilege codes of S4 and M4 and P1 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to change a network element's name.

....

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

....

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

....

3   Invoke the **Provision TID/NE Name** window from the **System View** main menu via **Administration → Set TID...**

....

4   Place the cursor in the **New TID/NE Name** text box and key in the new TID observing the following configuration rules:

- Each NE name must be unique within the network.

- The following characters are allowed in an NE name:

  - Upper-case letters ("A" .. "Z"),

  - Lower-case letters ("a" .. "z"),

  - Special characters("-", "+", "_", ".", "/"),

  - Digits ("0" .. "9").

- An NE name must not end and begin with an special character.

- Each NE name must be maximally 20 characters in length.

- The NE name may contain segments separated by hyphens ("-") or slashes ("/"), but each segment must begin with a letter.

....

Please note that NE names are case-insensitive.

....

5 Make sure that the new TID is correct.

IF …	THEN …
the new TID is correct,	continue with Step 6.
the new TID is not correct,	correct the entry in the **New TID/NE Name** text box and continue with Step 6.

....

6 Place the cursor in the **Confirm TID/NE Name** text box and key in the new TID again.

Important! Take a note of the TID you are going to assign to the NE!

....

7 Click **OK** to assign the new TID and to dismiss the window.

....

8 From the **System View** main menu, invoke the **Enter/Exit Maintenance Condition window vi**a **Fault** → **Enter/Exit Maintenance Condition...** → **Exit Maintenance Condition...**.

....

9 Confirm the resulting system message by clicking **Yes**.
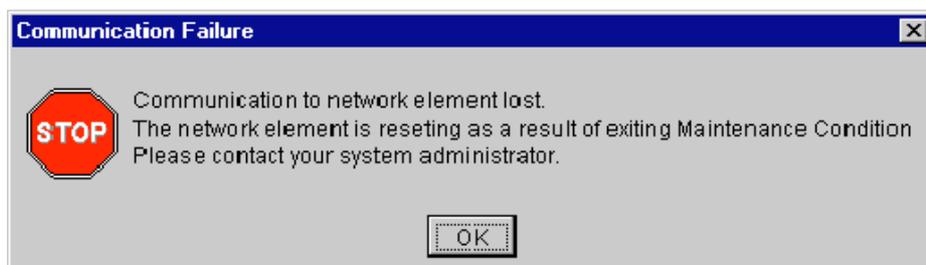
Result:

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, now using the new TID.

....

Make sure that the *WaveStar* CIT's static routing table
(Name/Address List) always reflects the correct assignment of
NE names to NSAP addresses.

E N D   O F   S T E P S

Configuring the data communication network

Overview

Purpose   This task description serves as an overview of the individual procedures that must be carried out to configure the Data Communication Network (DCN) for *WaveStar*® TDM 10G (STM-64) network elements and the *WaveStar* CIT.

Related information   For related information, please refer to:

- Chapter 14, "Management communication setup concepts"

- Chapter 24, "*WaveStar* CIT Tutorial"

Procedure

....

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

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

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

....

365-371-522
Issue b, October 2001

Lucent Technologies

3 - 7

Configuring the Data Communication Network (DCN) for *WaveStar* TDM 10G (STM-64) network elements and the *WaveStar* CIT consists of the procedures listed below.

Configuring the Data Communication Network (DCN)

Configuring the basic DCN parameters for the WaveStar® CIT

Configuring the LDB timers for the WaveStar® CIT

Administering the address list at the WaveStar® CIT

Configuring the basic DCN parameters for a network element:
- Enabling/Disabling the IAO-LAN
- Modifying a node's area address
- Specifying a node's IS characteristics
- Setting the CLNP PDU lifetime

Configuring Data Communication Channels

Configuring the TARP parameters for a network element

Assigning TARP manual adjacencies

References

For brief descriptions of the individual procedures refer to:

- "Configuring the basic DCN parameters for the *WaveStar* CIT" (3-10)

- "Configuring the LDB timers for the *WaveStar* CIT" (3-16)

- "Administering the address list at the *WaveStar* CIT" (3-19)
- "Configuring the basic DCN parameters for an NE" (3-31)
- "Configuring data communication channels" (3-39)
- "Configuring the TARP parameters for an NE" (3-47)
- "Assigning TARP manual adjacencies" (3-52)

⌐

Configuring the basic DCN parameters for the *WaveStar*® CIT

Overview

Purpose This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Use this procedure to configure the network layer parameters relevant to the *WaveStar* CIT.

Related information For related information, please refer to:

- Chapter 14, "Management communication setup concepts"
- Chapter 24, "*WaveStar* CIT Tutorial"

Procedure

....

Before you begin   Prior to performing this task, you must:

- have a valid user login and password for the *WaveStar*® CIT,

- be logged into the subject *WaveStar* CIT, and

- have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to configure the network layer parameters relevant to the *WaveStar* CIT.
....

1   From the *WaveStar* CIT main menu select **Administration** → **Data Communications...**.

> **Result:**
>
> The **CIT Data Communication** window opens.

....

2   Select the **Network Layer** tab.

....

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

If you like to change the area address:

1. Disable the Auto-Learn NSAP function, and

2. Select **Modify...** in the **Primary Area Address** segment.

> **Result:**
>
> The **Modify Primary Area Address** window opens.

....

4   In the **Modify Primary Area Address** window, you can now

1. either override the area address as a whole or in parts in the **Manual Area Address** text box, or

2. change each area address field individually in the **AFI**, **IDI** etc. text boxes.

Click **OK** to confirm your changes.

....

Result:

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

....

5   If desired, change the maximum value of the routing metric in the
Max Link Metric spin box.

....

6   If desired, change the value of ESCT in the **End System Config.
Timer** spin box.

....

7   You may now proceed working in the **CIT Data Communication**
window to configure the TARP loop detection buffer (LDB) timers for
the *WaveStar* CIT, or you may save your changes and close the
window.

IF ...	THEN ...
you want to proceed configuring the TARP loop detection buffer (LDB) timers,	click **Apply** and confirm your changes in the confirmation window, and refer to "Configuring the LDB timers for the *WaveStar* CIT" (3-16). END OF STEPS
you want to save your changes and close the window,	click **OK** and continue with Step 8.

....

8   Close and restart the *WaveStar* CIT application for your changes to
take effect.
E N D   O F   S T E P S
....

Supporting information

....

The *Network Layer* tab

The **Network Layer** tab of the **CIT Data Communication** window
enables you to

- view and modify the *WaveStar*® CIT's area address
  (**Primary Area Address**).

- set the maximum value of the routing metric (**Max Link Metric**).

- set the *WaveStar* CIT's ESCT (**End System Config. Timer**).
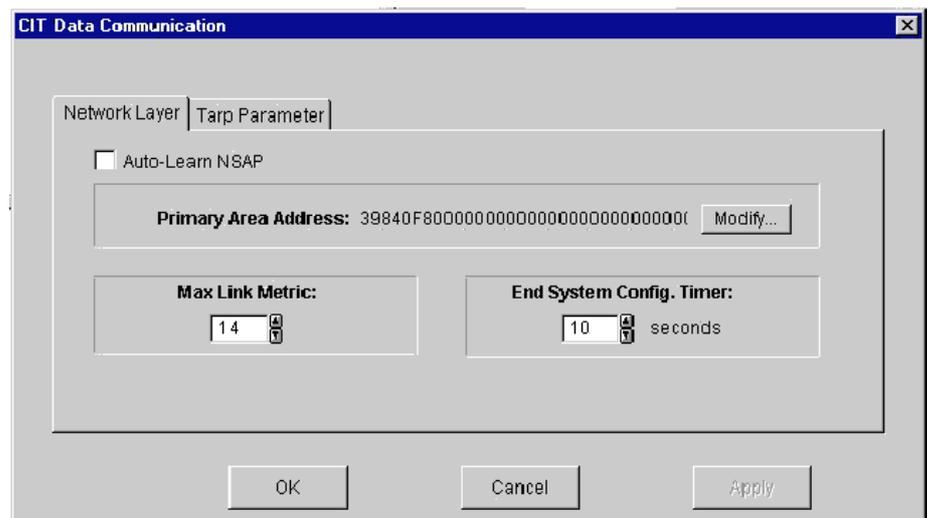
Window elements

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

Window element	Meaning	Value range	Default setting
Auto-Learn NSAP	This function enables the *WaveStar* CIT to automatically "learn" its area address by requesting the area address of the connected network elements. Please refer to the explanation below.		enabled
Primary Area Address	The complete area address in hexadecimal representation.		
Modify...	Click this button to invoke a configuration window for the **Primary Area Address**. This button will be greyed-out as long as the Auto-Learn NSAP function is enabled.		
Max Link Metric	The maximum value of the routing metric	1 to 63	14

....

Window element	Meaning	Value range	Default setting
End System Config. Timer	The *WaveStar* CIT's ESCT	1 to 1000 seconds	10 seconds

ESCT: end systems periodically generate ES Hellos (ESHs). The interval between two ESHs is determined by the End System Configuration Timer (ESCT).

"Auto-Learn NSAP" function

When the *WaveStar* CIT application is started it initially has no NSAP address. If the Auto-Learn NSAP function is enabled, it is possible to request the area address of the connected network elements automatically. However, a precondition is that the *WaveStar* CIT is physically connected to an NE. The *WaveStar* CIT adopts the retrieved area address because the *WaveStar* CIT and the NEs on the LAN must have the same area address. The system identifier of the *WaveStar* CIT's NSAP address depends on the PC hardware.

If the Auto-Learn NSAP function is disabled, you have to enter the *WaveStar* CIT's NSAP address manually, either directly in the **Primary Area Address** field or by using the **Modify Primary Area Address** window. Notice that manually modifying the NSAP address is not possible as long as the Auto-Learn NSAP function is enabled.

The *Modify Primary Area Address* window

In the **Modify Primary Area Address** window, you can change the *WaveStar* CIT's area address.
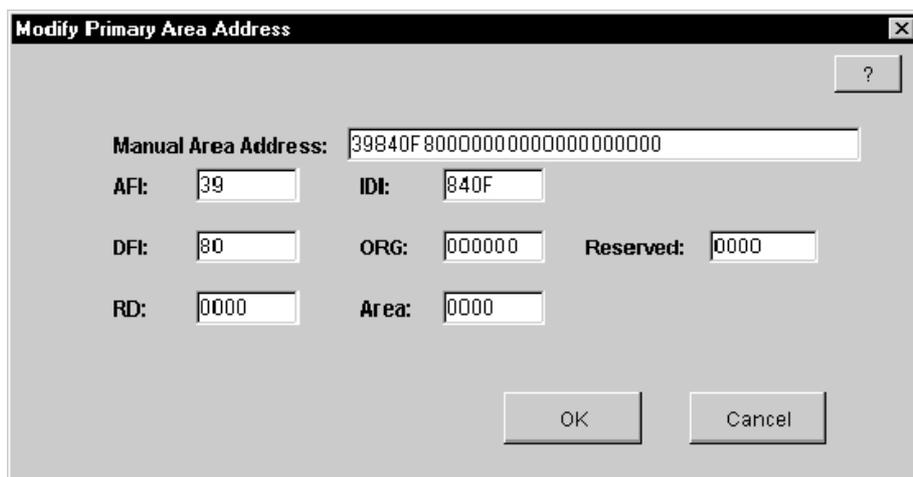
You can invoke the **Modify Primary Area Address** window by selecting **Modify...** in the **Primary Area Address** segment of the **Network Layer** tab of the **CIT Data Communication** window.

Please refer to "NSAP address format" (14-16), for a description of
the individual area address fields.

⌐

Configuring the LDB timers for the *WaveStar*® CIT

Overview

....

Purpose   This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Use this procedure to configure the TARP loop detection buffer (LDB) entry timer and flush timer for the *WaveStar* CIT.

Related information   For related information, please refer to:

- Chapter 14, "Management communication setup concepts"
- Chapter 24, "*WaveStar* CIT Tutorial"

....

3 - 1 6   **Lucent Technologies**   365-371-522
                                                                                  Issue b, October 2001

Procedure

Before you begin Prior to performing this task, you must:

- have a valid user login and password for the *WaveStar*® CIT,

- be logged into the subject *WaveStar* CIT, and

- have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

1 From the *WaveStar* CIT main menu select **Administration** → **Data Communications...**.

> **Result:**
>
> The **CIT Data Communication** window opens.

2 Select the **TARP Parameters** tab.

3 If desired, set the LDB timer values according to your needs.

Please note that the default timer values conform to the Telcordia Technologies GR-253 standard.

4 Close and restart the *WaveStar* CIT application for your changes to take effect.

E N D O F S T E P S

Supporting information

***WaveStar*® CIT TARP functionality**	The *WaveStar* CIT supports the TARP originator functionality which cannot be disabled. The related timers (T1, T2, T3 and T4) are permanently preset according to the Telcordia Technologies (formerly Bellcore) GR-253 standard.

The *TARP Parameters* tab

The **TARP Parameters** tab of the **CIT Data Communication** window enables you to set the TARP loop detection buffer timers:

- The LDB entry timer determines the time interval in minutes during which a previously processed and again received TARP PDU will be discarded. Possible values are 1 to 10 minutes, the default value is 5 minutes.

- The LDB flush timer serves to periodically re-initialize the loop detection buffer. Possible values are 1 to 1440 minutes (24 hours), the default value is 5 minutes.

⌐

Administering the address list at the *WaveStar*® CIT

Overview

Purpose   Use this procedure to generate and maintain a local CIT file containing the TIDs and NSAPs and/or IP addresses for NEs that might be connected to the CIT via OSI or via TCP/IP. Provisioning IP addresses into this local CIT file does not set or change the NE's IP address, but provides a method for giving the *WaveStar* CIT the IP addresses of an NE to which the CIT is to be connected in the absence of a DNS. This is necessary since there is no equivalent in TCP/IP to the OSI/TARP capability to broadcast a TID on the network and receive back the NSAP from the NE that has that TID.

For systems that have no access to an SDS database and which do not support TARP for Name/Address resolution, it is necessary to provide a mechanism to manually enter a list of TID/NSAP pairs.

This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Related information   For related information, please refer to:

- Chapter 14, "Management communication setup concepts"
- Chapter 24, "*WaveStar* CIT Tutorial"

Procedure

Important! *Each DCC controller exchange needs to be reflected in the static routing tables of all WaveStar® CITs managing the NEs!* The IEEE 802.3 MAC address, stored on the DCC controller (ADJCTL/DCCEI) circuit pack during the manufacturing process, is used as the system identifier in the NE's NSAP address (cf. "NSAP address fields" (14-17)). Hence, when a new DCC controller is inserted, then the system identifier, and so the NSAP address, automatically changes. After a DCC controller exchange the static routing tables in *all WaveStar* CITs managing the NEs need to be adapted.

Before you begin Due to the fact that the static routing tables of *all WaveStar* CITs managing the NEs must reflect the current network situation and must be synchronised, it might be useful to generate and maintain a routing information text file which can be imported into all *WaveStar* CITs concerned.

Prior to performing this task, you must:

• have a valid user login and password for the *WaveStar* CIT,

• be logged into the subject *WaveStar* CIT, and

• have proper access privileges to perform this task.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

• *WaveStar* CIT

Instructions Complete the following steps to administer the static routing table (**Address List**) at the *WaveStar* CIT.

1 From the *WaveStar* CIT main menu select **Administration** → **Address List...**.

Result:

The **Address Provisioning** window opens.

2 Depending on the action you want to perform:

IF ...	THEN ...
you want to add new entries to the list,	continue with Step 3.
you want to remove entries from the list,	continue with Step 7.
you want to modify entries in the list,	continue with Step 10.
you want to import a list from a text file,	continue with Step 15.
you want to export the **Address List** into a text file,	continue with Step 18.

3 Click **Add**.

      Result:

      The **Protocol Provisioning** window opens.

4 Enter the information of the NE to be added, and verify that your entries are correct (refer to "Elements of the Protocol Provisioning window" (3-26)).

5 Click **OK** to save the new entry in the **Address List**.

6 Repeat Step 3 to Step 5 to add another NE address information.

Otherwise, click **OK** to save the **Address List** and to dismiss the window.

END OF STEPS

7 In the displayed list, select the entry to be removed.

8 Click **Delete** to remove the selected entry rom the list.

9 Repeat Step 7 and Step 8 to remove another entry from the list.

Otherwise, click **OK** to save the **Address List** and to dismiss the window.

END OF STEPS

....

10 In the displayed list, select the entry to be modified.

....

11 Click **Modify**.

> **Result:**
>
> The **Protocol Provisioning** window opens.

....

12 Modify the information for the selected entry, and verify that your entries are correct (refer to "Elements of the Protocol Provisioning window" (3-26)).

....

13 Click **OK** to save the modified information and to dismiss the window.

....

14 Repeat Step 10 to Step 13 to modify another TID/NSAP address pair.

Otherwise, click **Close** to save the **Address List** and to dismiss the window.

END OF STEPS

....

15 Click **Import...**

> **Result:**
>
> A file selection dialog window opens.

....

16 Select the file to be imported from the file selection dialog window and click **Open**.

> **Result:**
>
> The **Address List** is replaced by the imported list.

Please note that if the import file has not the expected structure (cf. "Import file format" (3-29)), then importing of the file will be rejected with a corresponding error message.

....

17 Click **OK** to save the **Address List** and to dismiss the window.

....

18 Click **Export...**

....

Result:

A file selection dialog window opens.

....

19   Select the path where the file has to be stored and enter a filename
and click **OK**.

Result:

The **Address List** is stored at the specified location and by the
specified filename.

....

20   Click **OK** to save the **Address List** and to dismiss the window.

E N D   O F   S T E P S

Supporting information

The *Address Provisioning* window

The **Name Address Resolution** window is relevant to perform this task.

The **Address Provisioning** window can be invoked from the *WaveStar*® CIT main menu via **Administration** → **Address List...**
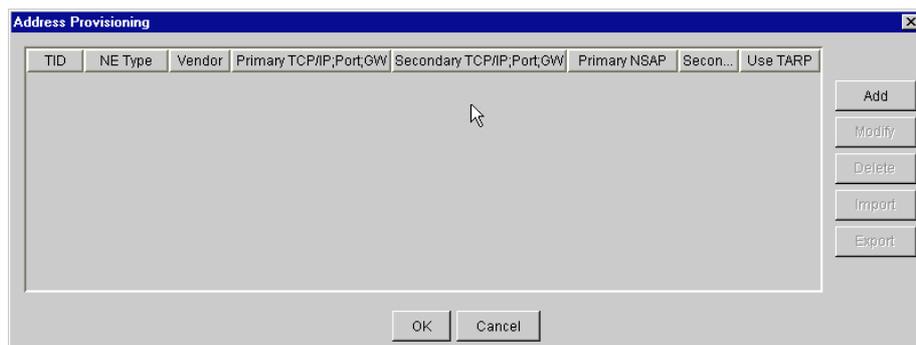
**The *Protocol Provisioning*
window**

The **Protocol Provisioning** window can be invoked from the
Address Provisioning window.
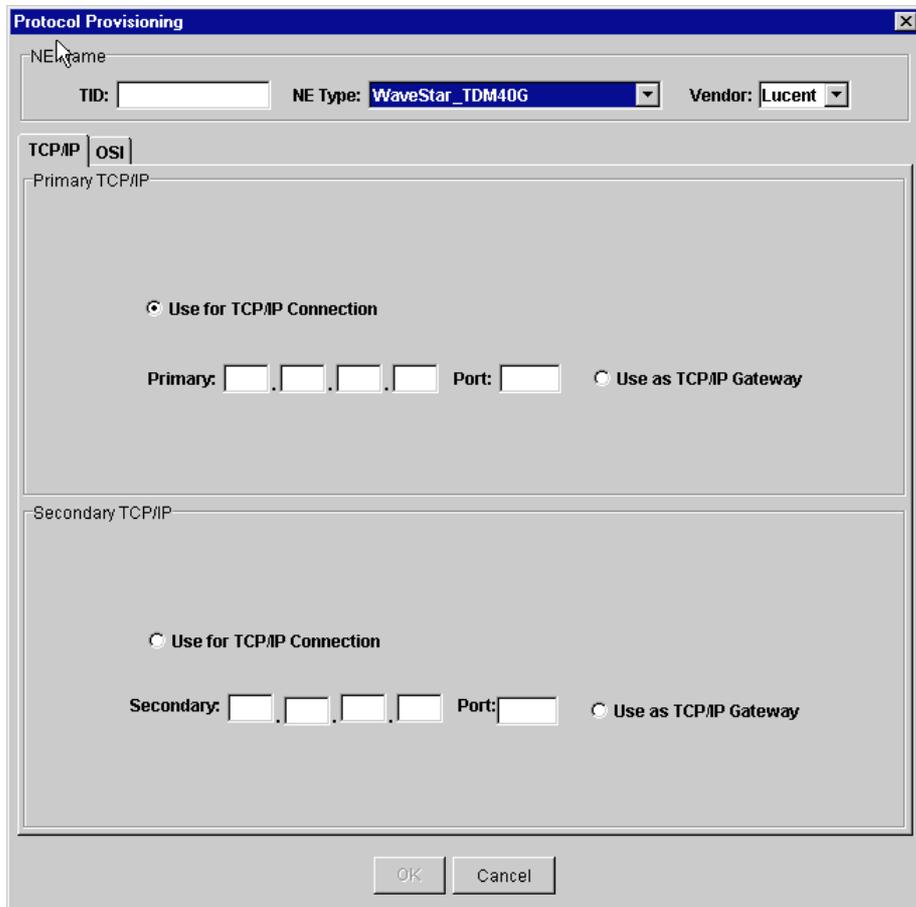
Elements of the *Protocol Provisioning* window

The elements of the **Protocol Provisioning** window and their meaning are listed in the following table.

Window element	Meaning
NE Name List	This displays a list of the existing TIDs in the CITs file and enables you to select or enter or modify a TID. Upon selection of an existing TID, the screen is filled with the current Address provisioning for that TID. If no TID is selected, the address fields are empty, ready to be filled in with the information for a new list entry.
NE Type	This field displays the NE type for the selected/entered NE name. You can also enter or modify the NE name. You can select from a list of supported NE types or Other.
	Observe the configuration rules given on page "NE name configuration rules" (3-28).
Vendor	This field displays and enables the user to enter or modify the system vendor, e.g. Lucent.

Primary TCP/IP, Direct and Gateway

Window element	Meaning
Use for TCP/IP Connection	Values Primary or Secondary (or checkbox). Default: Primary. Secondary is not applicable if no Secondary TCP/IP address is defined. The selected address is used for TCP/IP connections to this NE.
Primary TCP/IP Direct Connect Address	The 32 bit IPv4 address. The format is a dotted decimal notation: 4 dot-separated decimal numbers ranging from 0 to 255, inclusive. If no IP address has been provisioned, this is set to the Default NE IP Address.
Port Number	The 16 bit transport layer destination port number. Value range: 0 to 65535.
Secondary TCP/IP, Direct and Gateway	
Secondary TCP/IP Direct Connect Address	This field displays the 32 bit IPv4 address. The format is a dotted decimal notation: 4 dot-separated decimal numbers ranging from 0 to 255, inclusive. If no IP address has been provisioned, this is set to the Default NE IP Address.
Use for TCP/IP Connection	Values Yes or No (or checkbox), mutually exclusive with the Use for TCP/IP Connection value for Primary TCP/IP address. Default No. If Yes, this address is used for TCP/IP connections to this NE.
Port Number	This field displays the 16 bit transport layer destination port number. Value range: 0 to 65535.
OSI	
Use for OSI Connection	Values Primary or Secondary (or checkbox). Default: Primary. Secondary is not applicable if no Secondary NSAP is defined. The selected address is used for OSI connections to this NE.
Primary OSI NSAP (TARP Override)	This field displays a primary NSAP address as a 40 character NSAP entry or 20 octets. In this field the displayed NSAP address can be modified. You can enter this field either as a single string of 40 characters or in individual fields.
NSAP Address	The text boxes in this group box represent the individual fields of an NE's NSAP address. Please refer to "NSAP address format" (14-16).
	These text boxes can be used to enter an NSAP address corresponding to the TID in the **NE Name** group box.
	The **NSAP** text box at the bottom of the group box is a read-only box and indicates the complete NSAP address.
Secondary OSI NSAP (TARP Override)	This field displays a secondary NSAP address as a 40 character NSAP entry or 20 octets. In this field the displayed NSAP address can be modified. You can either write your entry into this field as a single string of 40 characters or into individual fields.

Window element	Meaning
NSAP Address	The text boxes in this group box represent the individual fields of an NE's NSAP address. Please refer to "NSAP address format" (14-16).
	These text boxes can be used to enter an NSAP address corresponding to the TID in the **NE Name** group box.
	The **NSAP** text box at the bottom of the group box is a read-only box and indicates the complete NSAP address.
NE name configuration rules	The following NE name configuration rules must be observed:
	• The following characters are allowed in an NE name:
	- Upper-case letters ('A' .. 'Z'),
	- Lower-case letters ('a' .. 'z'),
	- Digits ('0' .. '9'),
	- Hyphen ("-").
	• Each NE name must be unique within the network.
	• Each NE name must be maximally 20 characters in length.
	• The NE name may contain segments separated by hyphens ("-"), but each segment must begin with a letter.
	Please note that NE names are case-insensitive.
Pushbuttons	The **Address Provisioning** window provides the following pushbuttons:
	Close Use this button to dismiss the window.
	Add Use this button to add a new new NE Name with its accompanying data. This option is dimmed if the you select an existing entry in the list.
	Delete Use this button to remove an existing NE Name with its accompanying data. This option is dimmed until you select an existing entry in the list.
	Modify Use this button to modify an existing NE Name and its accompanying data. This option is dimmed until you select an existing entry in the list.
	Apply Use this button to apply changes to the static routing table.

Import...   Use this button to import a standard text file (cf. "Import file format" (3-29)) containing a list of NE Names with their accompanying data. The imported list will replace the existing static routing table of the *WaveStar* CIT. Clicking on this field invokes a Microsoft Windows standard browser window from which you can select a file, which is then be used to replace the existing Address List on the CIT. It is your responsibility to build this file in the proper manner.

Export...   Enables you to select a file to be generated with the fields supported above. Clicking on this field invokes a Microsoft Windows Standard Browser window from which you can select a file. Selection will cause the Address List to be entered into that file name in the format below.

Import file format   The file to be imported must have the following structure:

- The import file may be a standard text file.

- Each line shall represent a single NE.
  Fields on each line shall be semicolon separated and as follows:

  - The first field represents the TID. The TID format must be in accordance with the TID configuration rules (cf. "Elements of the Protocol Provisioning window" (3-26)).

  - NE Type..

  - Vendor, e.g. Lucent

  - A primary IP address,

  - For a primary TCP/IP Gateway NE only, an integer field is required which is the port number, ranging from 0 to 65535, inclusive. If this field is missing or an invalid integer, the primary TCP/IP Gatewayis set to Disable, even it this overrides the value in the primary TCP/IP Gateway Enable field (since the port number is needed to enable the Gateway).

  - For a TCP/IP Gateway NE only, an integer field to enable or disable the primary TCP/IP Gateway. 0 implies Disable, 1 implies Enable. If fields 6 and 7 are not filled in, i.e. '-', then primary TCP/IP Gateway is Disable.

- A secondary IP address

- For a secondary TCP/IP Gateway NE only, an integer field is required which is the port number, ranging from 0 to 65535, inclusive. If this field is missing or an invalid integer, the secondary TCP/IP Gateway is set to Disable, even if this overrides the value in the secondary TCP/IP Gateway Enable field (since the port number is needed to enable the Gateway).

- For a TCP/IP Gateway NE only, an integer field to enable or disable the secondary TCP/IP Gateway. 0 implies Disable, 1 implies Enable. If fields 8 and 9 are not filled in, i.e. '-', then secondary TCP/IP Gateway is Disable.

- A Primary NSAP (in accordance with the ISO-DCC NSAP address format). Please refer to "NSAP address format" (14-16).

- A Secondary NSAP (in accordance with the ISO-DCC NSAP address format). Please refer to "NSAP address format" (14-16).

- Comments can be added to the file as needed. Comments are designated by the pound '#' character.

- All fields must be present. A dash '-' is used if values do not apply.

Important! If any given import file has not the expected structure, then importing of the file will be rejected with a corresponding error message.

Configuring the basic DCN parameters for an NE

Overview

....

Purpose   This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Use this procedure to configure the basic DCN parameters for a network element. Configuring the basic DCN parameters includes:

- Enabling/Disabling the Intraoffice LAN (IAO-LAN),

- Modifying a node's area address (the area address is the configurable part of the NSAP address),

- Specifying the node's intermediate system (IS) characteristics,

- Setting the CLNP PDU lifetime.

Related information   For related information, please refer to:

- "NSAP address format" (14-16)

- Chapter 14, "Management communication setup concepts"

- Chapter 24, " *WaveStar*® CIT Tutorial"

....

365-371-522
Issue b, October 2001

Lucent Technologies

3 - 3 1

Procedure

....

Before you begin Prior to performing this task, you must:

1. log into the *WaveStar*® CIT, and

2. connect to the NE.

Required privilege code

You must have at least a privilege code of:

*   S4
    to enable or disable the IAO-LAN,

*   S3
    to modify a node's area address, specify the node's IS
    characteristics and/or specify the CLNP PDU lifetime.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar* CIT

Instructions Complete the following steps to configure the basic DCN
parameters for an NE.
....

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

> **Result:**
>
> The equipment selection window opens.

....

2 By means of the equipment selection window, select the DCC
controller (ADJCTL/DCCEI circuit pack) of the shelf for which you
want to configure the basic DCN parameters.

> **Result:**
>
> The **Data Communications** window opens.

....

3 If you like to view (and possibly change) the LAN status, then select
the **LAN Management** tab.

Otherwise continue with Step 9.

....

....

4 You may now enable or disable the LAN access to the external LAN (IAO-LAN for the high speed part) and/or the internal LAN of the main shelf.

Important! The attempt to disable the LAN access to the IAO-LAN for the low-speed part of the main shelf is rejected by the NE because the current association between the *WaveStar* CIT and the NE would be lost in that case, and only remote associations via DCC would be possible.

....

5 If desired, change the value for the LAN Router Priority by means of the **LAN Router Priority** spin box. The possible values range from 1 to 127.

....

6 If desired, change the value for the Internal Max Link Metric parameter by means of the **Internal Max Link Metric** spin box. The possible values range from 1 to 63.

....

7 If desired, change the value for the External Max Link Metric parameter by means of the **External Max Link Metric** spin box. The possible values range from 1 to 63.

....

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

....

9 Select the **Network Layer** tab.

....

10 Check the actual setting of the area address in the **Network Service Access Point** segment.

IF ...	THEN ...
you like to change the node's area address,	select **Modify...** and continue with Step 11.
you want to leave the node's area address unchanged,	continue with Step 12.

....

11 In the **NSAP/Area Address Provision** window, you can now change each area address field individually in the **AFI**, **IDI** etc. text boxes.

....

Click **OK** to confirm your changes.

Result:

The **NSAP/Area Address Provision** window is closed.

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

....

12   Specify the node's IS routing capability by means of the **Routing
Capability** check boxes in the **Intermediate System** group box
depending on whether the node shall act as a **Level 1** or **Level 1&2**
router.

....

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

....

14   You may now select another tab of the **Data Communications**
window to configure TARP parameters or manual adjacencies for
example, or you may save your changes and close the window.

IF ...	THEN ...
you want to save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description.
you want to save your changes and close the **Data Communications** window,	click **OK** and then **Close** and confirm your changes in the confirmation window. Please note that subsequently the DCC controller is restarted. Wait until the restart has finished.

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

⌐

Supporting information

....

**Network elements and
nodes**

A distinction has to be made between network elements and nodes.
Network elements can be identified by their target identifier (TID), i.e.
their NE name ("NE name" and "TID" are used synonymously
throughout this User Operations Guide), whereas a node is identified
by its Network Service Access Point (NSAP) address. Each NSAP
address within a network constitutes a node which can individually be
addressed.

**The *Data Communications*
window**

The **LAN Management**, the **Transport Layer** and the **Network Layer**
tabs of the **Data Communications** window are relevant to perform
this task.

The *LAN Management* tab

The **LAN Management** tab of the **Data Communications** window
makes it possible to enable or disable the LAN access to the internal
LAN, the so-called Operations Network (ON), and to the external
LAN (Intraoffice LAN (IAO-LAN)) for a selected DCC controller
(ADJCTL/DCCEI circuit pack). The LAN access is enabled in the
basic configuration. The **LAN Management** tab also offers the
opportunity to modify the LAN Router Priority and the Max Link
Metric parameters for both LAN types.
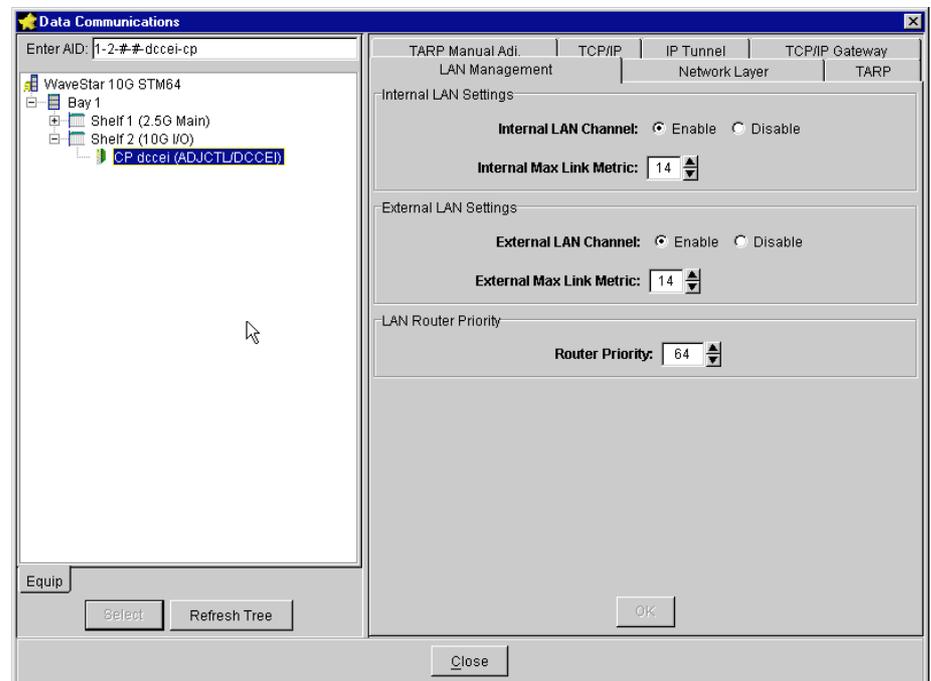
**Elements of the *Lan Layer*
tab**

The elements of the **Lan Layer** tab and their meaning are listed in the
following table. If applicable, the permitted value range as well as the

....

default settings of the parameters are given.

Window element	Meaning	Value range	Default setting
LAN Router Priority	Indicates the priority of the router connected to the LAN. A higher number has priority over a lower one. From all routers connected to the LAN, the router with the highest priority is selected as the Designated router. The designated Router takes care of routing of packets in the Q-LAN.	0- 127	64
Internal Max Link Metric		1 to 63	14
External Max Link Metric		1 to 63	14

The *Network Layer* tab

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

Elements of the *Network Layer* tab

The elements of the **Network Layer** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range	Default setting
NSAP	The complete area address in hexadecimal representation	dependent on the actual setting of the configurable NSAP address fields	read-only; please refer to "NSAP address fields" (14-17)
Modify...	Click this button to invoke a configuration window for the **Primary Area Address**.		
Intermediate System Routing Capability	The node's IS routing capability	**Level 1** **Level 1&2** **Level 1&2 w/Partition repair**	**Level 1**

Notes on the table:

- Intermediate systems periodically generate IS Hellos (ISHs). The interval between two ISHs is determined by the Intermediate System Configuration Timer (ISCT).

- The CLNP PDU lifetime specifies the maximum number of hops permitted for a PDU. If this PDU lifetime control parameter is exceeded, the PDU will not be forwarded further. A direct transmission link between two nodes is referred to as a hop.

⌐

Configuring data communication channels

Overview

Purpose Use this procedure to create new or modify existing DCC terminations.

This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Related information For related information, please refer to:

- Chapter 14, "Management communication setup concepts"
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

Before you begin   Prior to performing this task, you must have an overview of the current network topology.

Furthermore, you must:

1.   log into the *WaveStar*® CIT, and

2.   connect to the NE.

Required privilege codes

You must have at least a privilege code of:

*   S1
    to view the currently enabled DCC terminations,

*   S3
    to create new or modify existing DCC terminations.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar* CIT

Instructions   Complete the following steps to create a new DCC termination or to modify an existing DCC termination.

....

1   At the *WaveStar*CIT, open the **View DCC Terminations** window and verify that at least one LAPD channel is indicated available by checking the **Remaining Channels** field (cf. "The View DCC Terminations window" (3-42)).

....

2

IF ...	THEN ...
there is at least one LAPD channel available,	continue with Step 3.
there are no LAPD channels available,	disable dispensable DCC channels, and continue with Step 3.

....

3   Invoke the **Configure DCC Terminations** window from the **System View** main menu via **Configuration → DCC Terminations...**; see "The Configure DCC Terminations window" (3-44).

....

4   Select the DCC controller (ADJCTL/DCCEI circuit pack) for which you want to configure the DCC terminations by means of the equipment selection part of the window.

....

....

5 In the parameter part, select the action you want to perform

....

6

If you want to...	then ...
create a new DCC termination,	select **New Termination** and continue with Step 7.
modify an existing DCC termination,	select **Current Terminations** and continue with Step 8.
disable a currently enabled DCC termination,	select **Current Terminations** and continue with Step 11.

....

7 In the **Select a port for New Termination** group box, select the working optical interface port, and continue with Step 9.

....

8 In the **Select a port for Current Termination** group box, select the working optical interface port, and continue with Step 9.

....

9 In the **DCC Channel Parameters** group box, chose the LAPD mode in the **LAPD:** drop down list box.

Important! The LAPD mode setting must be different at both ends of a DCC link. Otherwise, an alarm (either "User-Network Side RSect Failure" or "User-Network Side MSect Failure") will be generated.

....

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

END OF STEPS

....

11 In the **Select a port for Current Termination** group box, select the working optical interface port for which you want to disable the DCC communication.

....

12 Disable the DCC termination by selecting the **Disabled** option in the **DCC Channel Parameters** group box.

Important! Disabling a previously enabled DCC at an NE needs to be coordinated with disabling the same DCC at the opposite end of the DCC link (remote NE) to avoid persistent alarms from the remote NE.

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

....

365-371-522   **Lucent Technologies**   3 - 4 1
Issue b, October 2001

Supporting information

....

Preconditions for enabling a DCC

You are permitted to enable a DCC if all of the following preconditions are fulfilled:

- The corresponding optical interface port is provisioned (configured) or at least pre-provisioned.
- The type of DCC (either DCC-R or DCC-M) is supported on the corresponding optical interface (cf. "Supported data communication channels" (14-20)).
- The DCC is not yet enabled.
- There are LAPD channels available. Please refer to "Max. number of active DCC links" (3-42) below.

Max. number of active DCC links

The maximum number of simultaneously supported LAPD channels per DCC controller is 32. Each DCC controller thus can support up to 32 active DCC links. Upon circuit pack insertion, DCCs will automatically be enabled and a LAPD channel assigned as long as LAPD channels are available.

Preconditions for disabling a DCC

You should disable a DCC only if *all* of the following preconditions are fulfilled:

- The DCC is currently enabled.
- The DCC is currently not needed for MS-SPRing management.
- The DCC is not the only management connection to remote NEs.

Relevant windows

The following *WaveStar*® CIT windows are relevant to perform this task:

- **View DCC Terminations**
- **Configure DCC Terminations**

The *View DCC Terminations* window

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

There are two possible ways to invoke this window:

- By selecting the **DCC Terminations** option from the pop-up menu that opens when you right-click on a DCC controller (ADJCTL/DCCEI circuit pack) in the shelf display of the **System View** window.
- By selecting **View → DCC Terminations...** in the **System View** main menu.

....

Please note that you must specify the DCC controller first (by entering the respective AID or selecting the DCC controller from the **Equipment Selection** window) before the **View DCC Terminations** window opens.
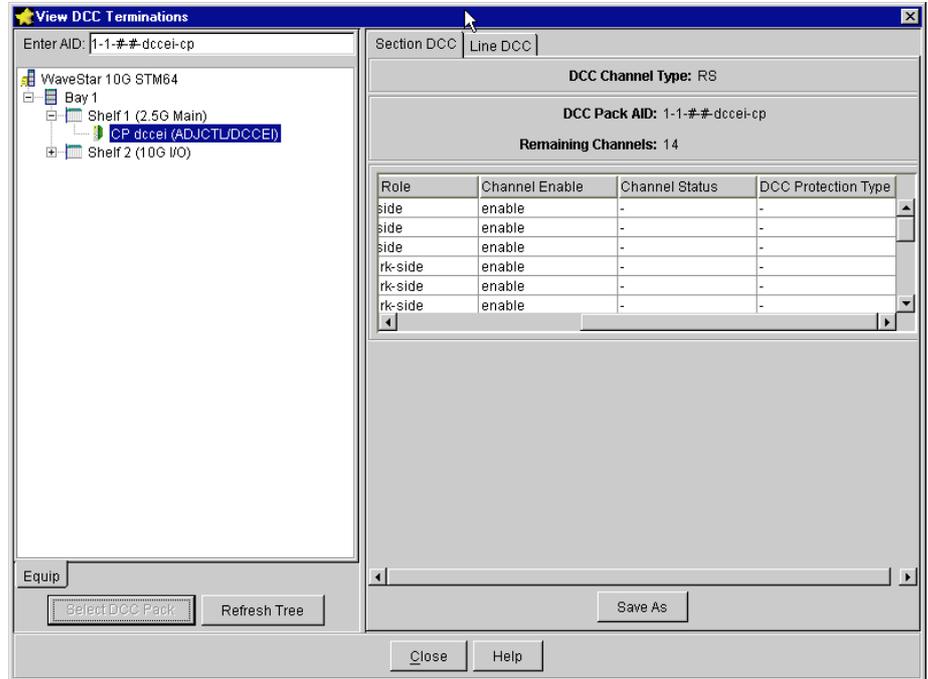
Elements of the *View DCC Terminations* window

The window elements of the **View DCC Terminations** window and their meaning are listed in the following table (please also refer to "Data communication channels" (14-20)). These window elements are displayed for each LAPD channel terminated on the ADJCTL/DCCEI circuit pack.

The following table lists the window elements of the **View DCC Terminations** window and explains their meaning.

Parameter	Meaning
DCC Channel Type	**RS** (DCC-R) or **MS** (DCC-M)
DCC Pack AID	The AID of the selected DCC controller (ADJCTL/DCCEI circuit pack).
Remaining Channels	The number of available LAPD channels.
Scrollable table with details on enabled DCC links:	
Port AID	The AID of the optical interface port.
	All optical interface ports with DCC enabled are considered to be "working" ports.

Parameter	Meaning
Port Type	The type of the associated optical interface port.
	This can be either **STM1**, **STM16** or **STM64**.
LAPD Role	The assigned LAPD role.
	This can be either **USER-SIDE** or **NETWORK-SIDE** with **USER-SIDE** being the default setting.
Channel Enable	The current status of the corresponding DCC channel. **Notice:** Since only enabled DCC channels are listed in the table the status will always be **Enabled**.
Channel Status	This can be either **Unequipped**, **Good**, **Failed**, or **Unknown**.
DCC Protection Type	This can be either • Unprotected • 1X1 Bidirectional Revertive • 1XN Bidirectional Revertive • 1+1 Unidirectional Non-Revertive • 1+1 Bidirectional Revertive • 1+1 Bidirectional Non-Revertive

The *Configure DCC Terminations* window

In the **Configure DCC Terminations** window, you can set all the parameters required for the operation of data communication channels.

The **Configure DCC Terminations** window can be invoked from the **System View** or **Shelf View** main menu via **Configuration** → **DCC Terminations...**

Equipment selection
After you have opened the **Configure DCC Terminations** window, only the equipment selection part on the left-hand side of the window is displayed. The parameter part on the right-hand side is not displayed until after you have selected a DCC controller (ADJCTL/DCCEI circuit pack) by either entering its AID directly in the **Enter AID:** field or selecting it from the equipment tree.

Parameter part
The parameter part on the right-hand side of the **Configure DCC Terminations** window contains two tabs, one for the **Section DCC** (RS DCC) and one for the **Line DCC** (MS DCC).

Elements of the *Configure DCC Terminations* window
The window elements of the parameter part of the **Configure DCC Terminations** window are listed in the following table (please also refer to "Data communication channels" (14-20)). If applicable, the permitted value range as well as the default setting of the parameters are also given.

Window element	Meaning/Value range	Default Setting
DCC Pack AID	dependent on the previous selection	no default setting; read-only

Window element	Meaning/Value range	Default Setting
DCC Channel Type	**RS** (DCC-R) or **MS** (DCC-M)	no default setting; dependent on the tab selection; read-only
Selection group box (**Select One**)	**Current Terminations** or **New Termination**	**Current Terminations**
Port AID	Displays a port terminated on the DCC or alternatively enables the user to select a new port to terminate, dependent on the previous selection	only selectable optical interface ports are listed
Port Type	dependent on the selected optical interface port: **STM1**, **STM16** or **STM64**	no default setting; read-only
LAPD Role	**USER-SIDE** or **NETWORK-SIDE**	**USER-SIDE**
Radio buttons (**DCC Termination**)	**Enabled** or **Disabled**	**Enabled** (as long as the upper limit of 32 DCCs has not been reached)

⌐

Configuring the TARP parameters for an NE

Overview

Purpose This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Use this procedure to

- enable or disable the TARP propagation functionality,

- enable or disable the TARP responder functionality, or to

- set the TARP loop detection buffer (LDB) entry timer and flush timer

for a selected node.

Related information For related information, please refer to:

- Chapter 14, "Management communication setup concepts"

- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to configure the TARP parameters
for an NE:

....

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

> **Result:**
>
> The equipment selection window opens.

....

2   By means of the equipment selection window, select the DCC
controller (ADJCTL/DCCEI circuit pack) of the shelf for which you
want to configure the TARP parameters.

> **Result:**
>
> The **Data Communications** window opens.

....

3   Select the **TARP** tab of the **Data Communications** window.

....

4   Enable or disable the TARP propagation functionality according to
your needs by selecting the corresponding check box in the **TARP
Propagation** group box. The TARP propagation functionality is
enabled by default.

Important! It is recommended to have the TARP propagation
functionality enabled for the low-speed part of the main shelf.

....

5   Enable or disable the TARP responder functionality according to your
needs by selecting the corresponding check box in the **TARP
Responder** group box. The TARP responder functionality is enabled
by default.

....

Important! It is recommended to have the TARP responder functionality enabled for the low-speed part of the main shelf.

....

6 If desired, set the LDB timer values according to your needs.

Important! The default timer values conform to the Telcordia Technologies GR-253 standard.

....

7 You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

If you want to ...	then ...
save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS
save your changes and close the **Data Communications** window,	click **OK** and then **Close.** and confirm your changes in the confirmation window. END OF STEPS

E ND OF S TEPS

Supporting information

The *Data Communications* window

The **TARP** tab of the **Data Communications** window is relevant to perform this task.
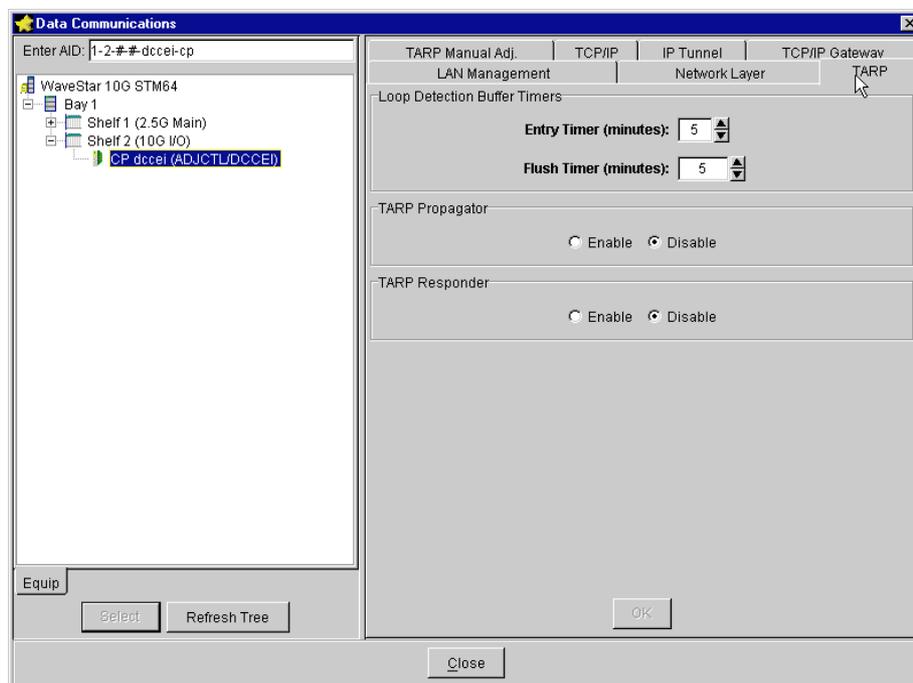
The **TARP** tab of the **Data Communications** window makes it possible to

- enable or disable the TARP propagation functionality,
- enable or disable the TARP responder functionality, or to
- set the TARP loop detection buffer timers

for a selected node.

Invoking the window

The **Data Communications** window can be invoked from the **System View** or **Shelf View** main menu via **Administration** → **Data Communications...**

LDB entry timer

The LDB entry timer determines the time interval in minutes during which a previously processed and again received TARP PDU will be discarded. Possible values are 1 to 10 minutes, the default value is 5 minutes.

LDB flush timer The LDB flush timer serves to periodically re-initialize the loop detection buffer. Possible values are 1 to 1440 minutes (24 hours), the default value is 5 minutes.

⌐

Assigning TARP manual adjacencies

Overview

Purpose
This procedure is part of the DCN configuration; please refer to "Configuring the data communication network" (3-6).

Use this procedure to manually assign adjacent nodes that support TARP ("TARP manual adjacencies") by entering their Network Entity Title (NET).

Two TARP manual adjacencies can be created for one DCC.

The area address together with the system identifier (SYSTEM field) of the NSAP address is also called the Network Entity Title (NET; cf. "ISO-DCC NSAP address format" (14-16)).

Related information
For related information, please refer to:

- Chapter 14, "Management communication setup concepts"

- Chapter 24, " *WaveStar*® CIT Tutorial"

⌐

Procedure

....

Before you begin Prior to performing this task, you must:

1. log into the *WaveStar*® CIT, and

2. connect to the NE.

Take notes of the NSAP addresses of the TARP manual adjacencies you are going to assign.

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar* CIT

Instructions Complete the following steps to assign TARP manual adjacencies:
....

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

> **Result:**
>
> The equipment selection window opens.

....

2 By means of the equipment selection window, select the DCC controller (ADJCTL/DCCEI circuit pack) of the shelf for which you want to configure TARP manual adjacencies.

> **Result:**
>
> The **Data Communications** window opens.

....

3 Select the **TARP Manual Adj.** tab of the **Data Communications** window.

....

4 Depending on whether you want to assign a new, modify or delete an existing TARP manual adjacency:

....

If you want to ...	then ...
add a manual adjacency, there must be an empty **TARP Manual Adjacency** (between the field **MAJ1:** or **MAJ2:** and the corresponding **Modify** button no Network Entity Title (NET) has to be displayed).	continue with Step 5.
modify an existing manual adjacency,	continue with Step 9.
delete an existing manual adjacency,	continue with Step 13.

5 Click **Modify** beside the empty **TARP Manual Adjacency.**

   Result:

   The **NSAP/Area Address Provision** window opens.
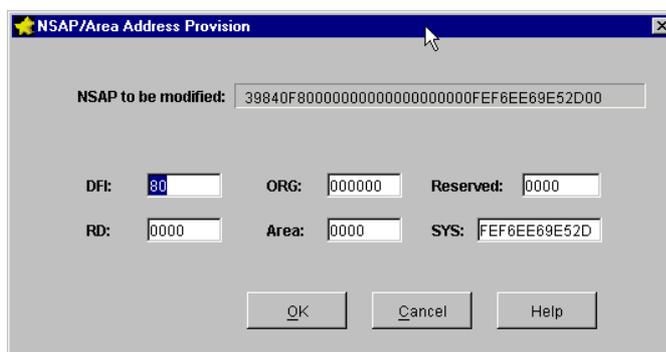
6 Enter the individual fields of the TARP manual adjacency's NET into the corresponding text boxes in the **NSAP/Area Address Provision** window.

7 Make sure that the NET is correct.

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

....

8   Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

....

9   Click **Modify...** beside the text box of the MAJx you want to modify.

Result:

The **NSAP/Area Address Provision** window opens.

In principle the window is the same as the window used in Step 5.

....

10   Enter the individual fields of the TARP manual adjacency's NET into the corresponding text boxes in the **NSAP/Area Address Provision** window.

....

11   Make sure that the NET is correct.

IF …	THEN …
the NET is correct,	continue with Step 12.
the NET is not correct,	correct the corresponding entries and continue with Step 12.

....

12   Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

....

13   Click **Modify** beside the **TARP Manual Adjacency** you want to delete.

Result:

The **NSAP/Area Address Provision** window opens.

In principle the window is the same as the window used in Step 5.

....

14   Remove all the entries in the individual fields of the TARP manual adjacency's NET in the **NSAP/Area Address Provision** window.

....

....

15   Click **OK** in the **NSAP/Area Address Provision** window.

Result:

The **NSAP/Area Address Provision** window is closed.

Continue with Step 16.

....

16   You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

IF ...	THEN ...
you want to save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS
you want to save your changes and close the **Data Communications** window,	click **OK** and then **Close.** and confirm your changes in the confirmation window. END OF STEPS

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

Lucent Technologies

Supporting information

....

The *Data Communications*   The **TARP MAJ** tab of the **Data Communications** window is relevant
window   to perform this task.

The **TARP Manual Adj.** tab of the **Data Communications** window
makes it possible to enter new or modify existing TARP manual
adjacencies.
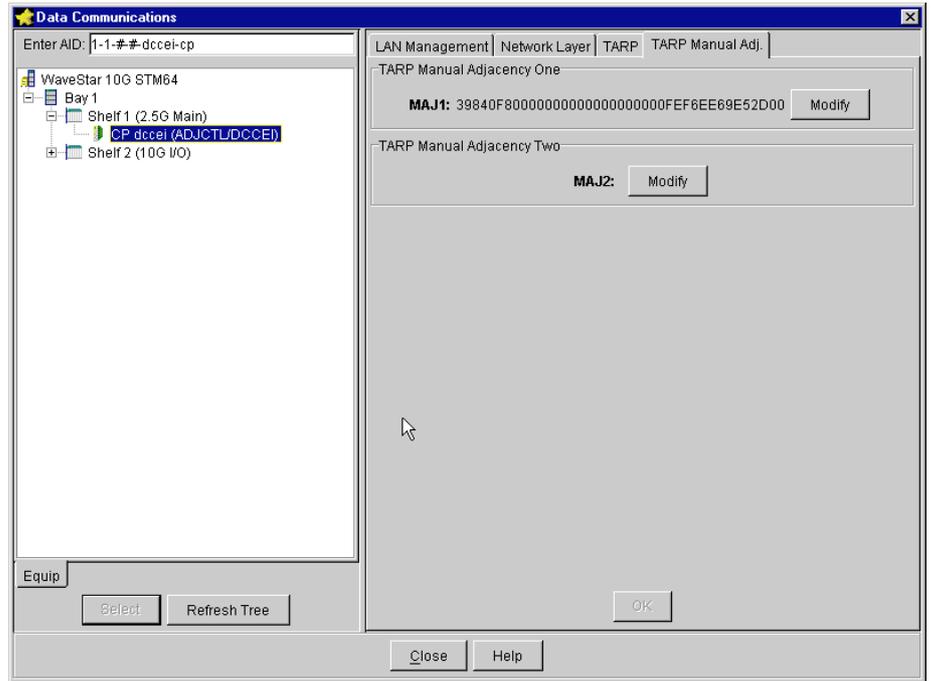
The **Data Communications** window can be invoked from the
System View or **Shelf View** main menu via **Administration → Data
Communications...**

....

Configuring the TCP/IP network address

Overview

Purpose   Use this procedure to configure the TCP/IP network address for a selected node.

Related information   For related information, please refer to:

- "DCN protocols and services" (14-11)
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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

Required privilege code

You must have at least a privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to configure the TCP/IP network
address:

....

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

Result:

The equipment selection window opens.

....

2   By means of the equipment selection window, select the DCC
controller (ADJCTL/DCCEI circuit pack) of the shelf for which you
want to configure the TCP/IP network address.

Result:

The **Data Communications** window opens.

....

3   Select the **TCP/IP** tab of the **Data Communications** window.

....

4   To configure the IP address click **Modify** beside **IP Address**.

Result:

The **IP Address Provisioning** window opens.

....

5   Enter theIP address into the corresponding fields in the **IP Address
Provisioning** window and click **OK**.

....

6   To configure the IP subnet mask click **Modify** beside **IP Subnet
Mask**.

....

> **Result:**
>
> The **IP Subnet Mask Provisioning** window opens.

....

7   Enter theIP subnet mask into the corresponding fields in the **IP Subnet Mask Provisioning** window and click **OK**.

....

8   To configure the IP default router address click **Modify** beside **IP Default Router Address**.

> **Result:**
>
> The **IP Default Router Address Provisioning** window opens.

....

9   Enter theIP default router address into the corresponding fields in the **IP Default Router Address Provisioning** window and click **OK**.

....

10   You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

If you want to ...	then ...
save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS
save your changes and close the **Data Communications** window,	click **OK** and then **Close.** and confirm your changes in the confirmation window. END OF STEPS

E N D   O F   S T E P S

....

⌐

Supporting information

....

The *Data Communications* window The **TCP/IP** tab of the **Data Communications** window is relevant to perform this task.
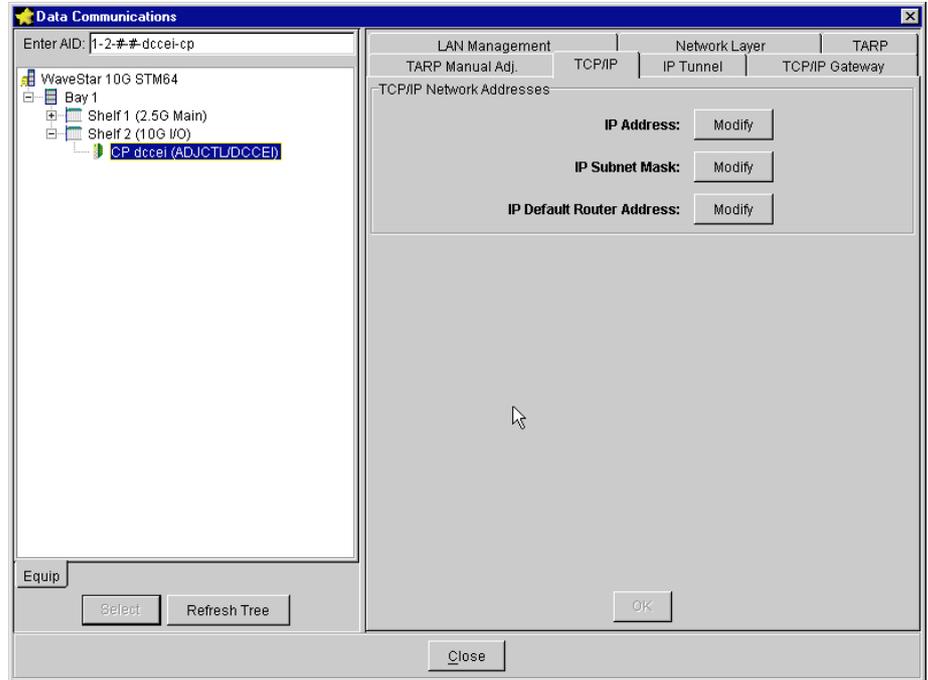
Elements of the *TCP/IP* tab The elements of the **TCP/IP** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range
IP Address	This is the 32 bit IPv4 address.	4 dot-separated decimal numbers ranging from 0 to 255. No default.

....

Window element	Meaning	Value range
IP Subnet Mask	This is the 32 bit IPv4 subnet mask.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
IP Default Router Address	This is the 32 bit IPv4 router address.	4 dot-separated decimal numbers ranging from 0 to 255. No default.

Configuring the TCP/IP gateway function

Overview

Purpose   Use this procedure to configure the TCP/IP gateway function for the selected NE.

Related information   For related information, please refer to:

- "DCN protocols and services" (14-11)
- Chapter 24, " *WaveStar*® CIT Tutorial"

⌐

Procedure

....

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

Prior to performing this task, the TCP/IP network address has to be
configured (cf. "Configuring the TCP/IP network address" (3-58)).

Required privilege code

You must have at least a privilege code of S3 to perform this task.

Required equipment

The following equipment is required to perform this task:

● *WaveStar* CIT

Instructions   Complete the following steps to configure the TCP/IP gateway
host list:
....

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

> **Result:**
>
> The equipment selection window opens.

....

2   By means of the equipment selection window, select the DCC
controller (ADJCTL/DCCEI circuit pack) of the shelf for which you
want to perform this task.

> **Result:**
>
> The **Data Communications** window opens.

....

3   Select the **TCP/IP Gateway** tab of the **Data Communications**
window.

....

4

IF	THE
you want to enable/disable theTCP/IP gateway function on the selected node,	select the respective radio button in the **TCP/IP Gateway Control** field. **Reference:** Continue with Step 6.

....

IF	THE
you want to configure Encoding Mode Port Numbers,	enter the desired values in the field **Encoding Mode Port Numbers**. **Reference:** Continue with Step 6.
you want to add/modify/delete a TCP/IP gateway host	select a list entry and click on the symbol in the very left column of the list. **Result:** The **Edit OS Name and OS Type** window opens. **Reference:** Continue with Step 5.

....

5

IF	THEN
you want to add a TCP/IP gateway host,	enter the new OS name in the respective field and select the desired OS type in the **New OS Types** spin box. Click **ADD**. **Result:** The **Edit OS Name and OS Type** window closes and the new entry is added to the list.
you want to modify the selected TCP/IP gateway host	enter the new OS name in the respective field and select the desired OS type in the **New OS Types** spin box. Click **Modify**. **Result:** The **Edit OS Name and OS Type** window closes and the entry is updated in the list.
you want to delete the selected TCP/IP gateway host,	click **Delete**. **Result:** The **Edit OS Name and OS Type** window closes and the entry is deleted in the list.

....

6   You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

....

If you want to ...	then ...
save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS
save your changes and close the **Data Communications** window,	click **OK** and then **Close.** and confirm your changes in the confirmation window. END OF STEPS

E ND OF S TEPS

Supporting information
....

**The *Data Communications*
window**

The **TCP/IP Gateway** tab of the **Data Communications** window is relevant to perform this task.
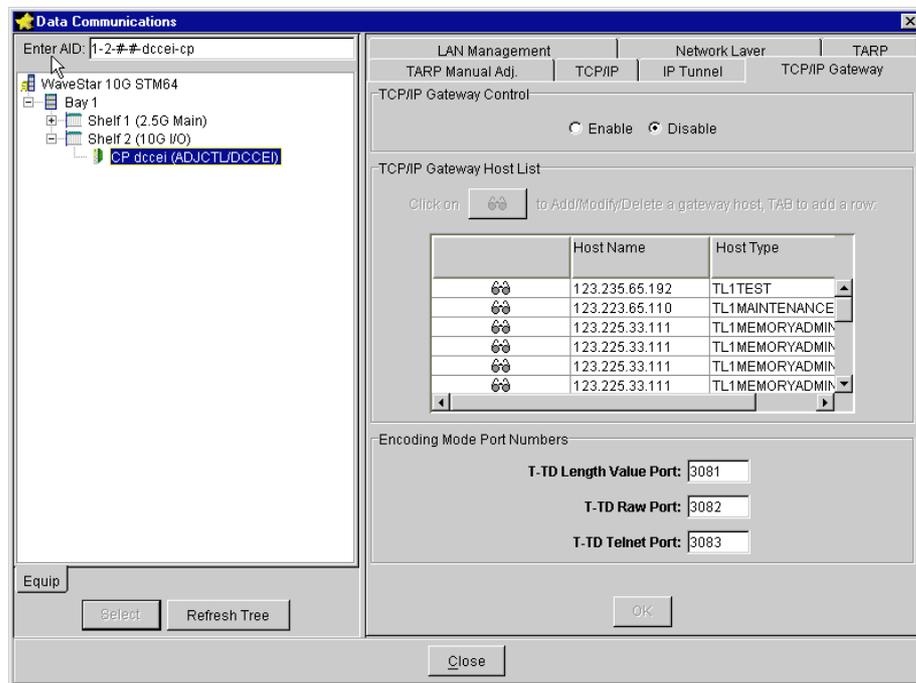
**Elements of the *TCP/IP
Gateway* tab**

The elements of the **TCP/IP Gateway** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range
TCP/IP Gateway Control	This parameter enables or disables TCP/IP to OSI conversion for the selected NE.	Enable, Disable Default: Disable
TCP/IP Gateway Host List		
Host Name	IP address of the host.	1 to 24 alphanumeric characters. Optional.

....

Window element	Meaning	Value range
Host Type	Application Context Identifier.	Possible values • Maintenance OS (TL1MAINTENANCE) • Memory Administration OS (TL1MEMORYADMIN) • Test OS (TL1TEST) • Other OS (TL1OTHER1) • Peer Communications OS (TL1PEERCOM) (Default)
Encoding Mode Port Numbers		
T-TD Length Value Port	Sets the Port Number over which the T-TD function is accessible using the length value Encoding method.	0..65535. (Default: 3081)
T-TD Raw Port	Sets the Port Number over which the T-TD function is accessible using the raw-mode encoding.	0..65535. (Default: 3082)
T-TD Telnet Port	Sets the Port Number over which the T-TD function is accessible using the Telnet encoding mode.	0..65535. (Default: 3083)

Enabling/Disabling IP tunneling

Overview

....

Purpose   Use this procedure to enable or disable IP tunneling for a selected node and to configure tunneling routes.

Related information   For related information, please refer to:

- "IP tunneling" (14-13)

- Chapter 24, " *WaveStar*® CIT Tutorial"

....

Procedure

....

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

Required privilege code

You must have at least a privilege code of S4 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to enable or disble IP tunneling for
a selected node and to configure tunneling routes.:

....

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

Result:

The equipment selection window opens.

....

2 By means of the equipment selection window, select the DCC
controller (ADJCTL/DCCEI circuit pack) of the shelf for which you
want to perform this task.

Result:

The **Data Communications** window opens.

....

3 Select the **IP Tunnel** tab of the **Data Communications** window.

Important! The routing table is split in three lists, local routes,
manual routes and TAP routes. Each list has its own editing
capabilities:

- for local routes, only the TAP advertising and TAP cost fields can
  be edited

- for manual routes, all fields can be edited, entries can be added
  and deleted.

- for TAP routes, nothing can be edited, deleted or added.

....

4

....

IF	THEN
you want to enable or disable IP tunneling through the selected node,	select the respective radio button beside **IP Tunnel Status**.
you want to configure the TAP group, to which the system belongs to,	enter the desired value into the **TAP Group** entry field.
you want to modify a route	select the route and change the parameters in the respective field.
you want to globally advertise several routes,	select the respective routing list entries and in the **TAP Properties** field select the **Enable** radio button beside **TAP Advertise**.
	This overrules all the individual **TAP Advertise** settings as displayed in the route list.
	After enabling the TAP Advertise option, all routes which have the tap_advert field set to 'Yes' will be advertised. The ones with the tap_advert field set to 'No' will NOT be advertised. If the TAP Advertise option is set to disabled, none of the routes will be advertised (including the ones with tap_advert set to 'Yes').
you want to enable the learning status for the auto provisioning protocol,	select the **Enable** radio button beside **TAP Learn**.

5 You may now select another tab of the **Data Communications** window to configure other DCN-related parameters, or you may save your changes and close the window.

If you want to ...	then ...
save your changes and select another tab of the **Data Communications** window,	click **OK** and confirm your changes in the confirmation window, and refer to the corresponding task description. END OF STEPS

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

E ND OF S TEPS

**Lucent Technologies**

Supporting information

....

The *Data Communications* window   The **IP Tunnel** tab of the **Data Communications** window is relevant to perform this task.
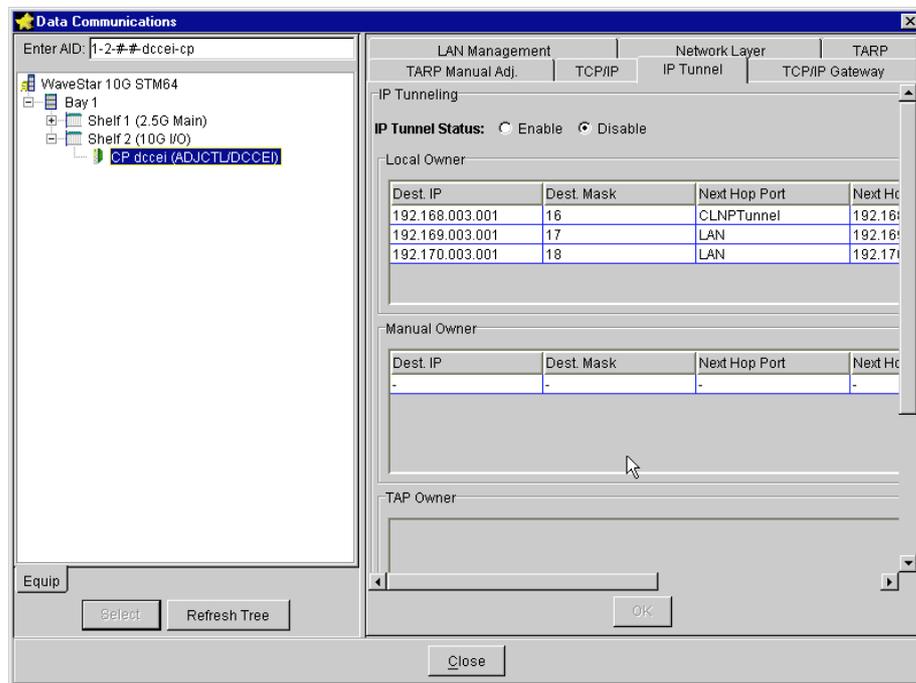
Elements of the *IP Tunnel* tab   The elements of the **IP tunnel** tab and their meaning are listed in the following table. If applicable, the permitted value range as well as the default settings of the parameters are given.

Window element	Meaning	Value range
IP Tunneling		
IP Tunnel Status	This parameter enables or disables IP tunneling.	Enable Disable Default: Disable
Local Owner route list (only the fields **TAP Advertise** and **TAP Cost** can be edited)		
Dest. IP	Destination IP address.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
Dest. Mask	Destination mask.	4 dot-separated decimal numbers ranging from 0 to 255. No default.

....

Window element	Meaning	Value range
Next Hop Port	For each route Id: type of next hop port.	**LAN** **CLNP Tunnel**
Next Hop Address	For each route Id: address of the next hop.	Values : • IP Address, • NSAP Address,
TAP Advertise	Indicates whether the route should be advertised (individual advertising).	**Yes** **No**
TAP Cost	Cost of the route.	0…65535.
Manual Owner route list (all fields can be edited, entries can be added and deleted).		
Dest. IP	Destination IP address.	4 dot-separated decimal numbers ranging from 0 to 255.
Dest. Mask	Destination mask.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
Next Hop Port	For each route Id: type of next hop port.	**LAN** **CLNP Tunnel**
Next Hop Address	For each route Id: address of the next hop.	Values : • IP Address, • NSAP Address,
TAP Advertise	Indicates whether the route should be advertised (individual advertising).	**Yes** **No**
TAP Cost	Cost of the route.	0…65535.
IP Default Router Address	This is the 32 bit IPv4 router address. The format is a dotted decimal notation. This parameter must be provisioned prior to the enabling the TCP/IP Bridge function.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
TAP Owner route list (read only)		
Dest. IP	Destination IP address.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
Dest. Mask	Destination mask.	4 dot-separated decimal numbers ranging from 0 to 255. No default.
Next Hop Port	For each route Id: type of next hop port.	**LAN** **CLNP Tunnel**

Window element	Meaning	Value range
Next Hop Address	For each route Id: address of the next hop.	Values : • IP Address, • NSAP Address,
TAP Advertise	Indicates whether the route should be advertised (individual advertising).	**Yes** **No**
TAP Cost	Cost of the route.	0…65535.
TAP Properties		
TAP Advertise	This parameter allows the user to globally enable or disable the advertising of the routes marked to be advertised (the parameter overrules all the individual TAP Advertise as displayed in the Route List).	**Enable** **Disable**
TAP Learn	This parameter controls the learning status for the auto provisioning protocol.	**Enable** **Disable**
TAP Group	Defines the TAP Group to which the system belongs.	0...65535

Setting date and time

Overview

Purpose   Use this procedure to set time and date of the system. The network element clock must be set again after each power on or reboot.

Related information   For related information, see:

- "Overview of access identifiers" (15-18)
- "Alarm severities" (16-26)

Procedure

....

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

Required privilege code(s)

You must have at least a privilege code of P3, Provisioning, or M3,
Maintenance, to set the system parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to set the date and time of the
system:
....

1   From the *WaveStar* CIT System View or Shelf View main menu,
select **Configuration** → **Provision**.

> **Result:**
>
> The window **Provision Parameters for Protection Groups or
> Equipment** opens. The **Equipment** selection tab appears on the
> left side of the window.

....

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

> **Result:**
>
> The selection window for time and date appears on the right
> side of the window.

....

3   Select the day (by clicking on the respective date), month (via the
drop-down list box) and year (via the spin-box) in the group box
Date.

....

4   Set the time in the group box **Time**.

....

5   Click the **Apply** pushbutton.

Important! The settings made in this window come into effect and
will be shown after re-opening the window.

E N D O F S T E P S

....

Supporting information

....

Relevant *WaveStar*® CIT window   The following window is used to set the date and time of the system:
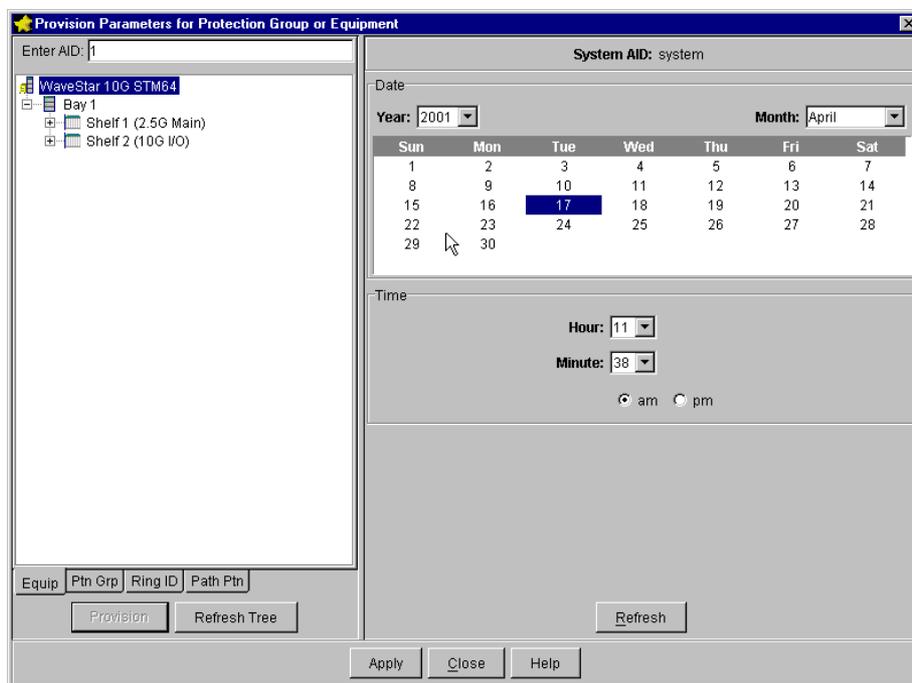
4   Equipment provisioning

Overview

Purpose

This chapter describes the procedures which have to be carried out for the provisioning of the hardware components of the *WaveStar*® TDM 10G.

Provisioning hierarchy

Some provisioning parameters relate to other provisioning parameters and must be completed in a hierarchical fashion.

Provisioning of an NE with an empty database

If an initial load to the non-volatile memory (NVM) of a newly established network element has been performed, it has an empty database, meaning that it has no configuration data. Before the NE can be managed at least the Target Identifier (TID) has to be set.

The steps of this basic provisioning are described in the chapter Chapter 3, "Management communication setup":

Configuration data

After the basic steps have been carried out, the definition of the configuration data can be carried out. This finally leads to the normal operation of an NE within a network according to the given needs.

Additionally to the setting of the configuration data for normal operation, this chapter includes procedures related to the hardware such a removing equipment from the system and the switching of equipment protections.

Download of existing data
Besides the step-by-step configuration, it is possible to download existing configuration data from a data carrier to the NE in the two following ways:

- *Starting from clean NVM*
  First copy the generics from the up directory to the NVM. You put the NVM in the system which starts in an unstable state, so you have to backup and restore the database. After that reset you can change the TID. Exit the **maintenance condition** and reset the system again. Then you can create a **high speed shelf** (On cable identifier=2) and an **extension shelf** (On cable identifier=1), it is not necessary to take a new bay.

- *Starting with download software*
  First copy the generics from the up directory to the directory *C:\program files\lucent technologies\Wavestar CIT\generics*. Select **configuration → software → download software**, a warning message appears, the download will last a long time (about 30 minutes to 1 hour). After downloading you have to activate the new software with **configuration → software → activate software**.
  Please note that all **protection groups** and **cross-connections** have to be the same as before activating software.

Contents

Initial equipment provisioning

Overview

....

Purpose   This procedure shows the provisioning steps which have to be carried out for the setting of the configuration data of the hardware components belonging to a network element with an empty database.

⌐

....

Procedure

....

| **Before you begin** | Prior to performing the following tasks, you must be logged into the *WaveStar*® CIT and a network element (directly or remotely). |

Required privilege code

The required privilege codes are described in the respective steps.

Required equipment

The following equipment is required to perform the tasks below:

- *WaveStar* CIT

| **Instructions** | .... |

1 Log into the *WaveStar* CIT and the respective NE (cf. "*WaveStar* CIT login/logout procedure" (24-12) and "Logging into an NE" (24-32))

....

2 Creation of the high-speed shelf (shelf 1-2) (cf. "Creating a new shelf" (4-8)), all mandatory circuit packs and all other circuit packs which are already plugged-in are autoprovisioned.

To create a high speed shelf it is suffcent to create a new shelf in bay 1.

....

3 Creation of the extension shelf (optional), cf. "Creating a new shelf" (4-8)

....

4 Port provisioning (including line timing), cf. Chapter 6, "Timing provisioning", "Configuring an optical port" (4-23) and "Configuring an electrical port" (4-38)

....

5 Tributary provisioning (cf. "Configuring a tributary" (4-43))

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

⌐

....

Creating a new bay

Overview

Purpose Use this procedure to add a new bay to a network element.

A bay is physically a rack, but several bays can be connected to each other and form one network element. Up to 3 bays can be provisioned per network element, up to 99 bays can be provisioned.

Related information For related information, see:

- "Provisioning of new components" (15-5)

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create
a new bay.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to create a new bay:

....

1   In the **System View** of the *WaveStar* CIT, select **Configuration** →
Create New → **Bay...**.

   Result:

   The **Create New Bay** window opens.

....

2   Set the **Bay Access Identifier** via the spin box. Values between **02**
and **99** are possible. Preferably set the Bay Access Identifier to **02** or
03. Bay 1 is autoprovisioned.

....

3   Click on **OK**. The window closes. If you wish to discard your changes
click on **Close**.

E N D   O F   S T E P S

....

....

365-371-522   **Lucent Technologies**   4 - 7
Issue b, October 2001

Creating a new shelf

Overview

....

Purpose   Use this procedure to logically add a new shelf (part) to a network element.

Related information   For related information, see:

- "Provisioning of new components" (15-5)

⌐

....

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create
a new shelf.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to create a new shelf:
....

1   In the **System View** of the *WaveStar* CIT, select **Configuration** →
Create New → **Shelf...**.

> **Result:**
>
> The **Create New Shelf** window opens.

....

2   Select the bay for which you wish to create the shelf in the
Equipment selection tab on the left side of the window.

....

3   Click on the pushbutton **Select I/O Bay**.

> **Result:**
>
> The selection fields for the new shelf become visible on the
> right side of the window.

....

4   Select the **Shelf Type** in the upper group box. Click on the radio
button **2.5G I/O** if you wish to create an extension shelf. Click on the
radio button **10G I/O** if you wish to create the high-speed part of the
main shelf.

....

5   Set the **SS Bit Override** using the respective radio button.

Important! When SS bit override is enabled, the SS bits are set to 00
for all ports on a shelf. This overrides normal SS bit provisioning
when interworking with non-compliant SONET network elements.
When SS bit override is disabled, the SS bits are set to 10 for all
ports on a shelf. The default setting is **Disabled**.

....

....

6   Select the **Shelf AID**. The first digit of the AID is defined by the bay
and is displayed in front of the spin box. Select the second digit in the
spin box. For the high-speed part you have to select **2**.

....

7   Select the **ON Cable Identifier** via the spin box in the lower group
box. Values from **1** to **4** are possible. For the high-speed part you
have to select **1**. For an expansion (extension) shelf, use **2**.

The ON Cable Identifier is the controller address of a shelf for the
connection to the low-speed part which contains the main controller
for the whole network element. The extension shelf is connected to
the main shelf via the CTL I/O Panel. There are three sockets on this
panel which are assigned to certain ON Cable Identifiers.

The expansion shelf with the ON Cable Identifier **2** hast to be
connected physically to the Socket EXP SHELF 1.

....

8   Click on **OK**. The window closes. If you wish to discard your changes
click on **Close**.

The creation of a shelf takes a few minutes. When it is finished, only
the green LED on the circuit packs of the respective shelf should be
on.

E N D   O F   S T E P S

....

Configuring a shelf

Overview

Purpose   Use this procedure to set or modify shelf parameters. This can be done during the setup of a new network element or during operation.

Related information   For related information, see:

- "Shelf provisioning" (15-26)

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to
configure shelf parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to configure the shelf parameters:
....

1 In the **System View** of the *WaveStar* CIT select **Provision Shelf**
after right-clicking on the requested shelf .

> **Result:**
>
> The shelf provisioning window appears.

....

2 Set the **SS Bit Override** using the respective radio button.

Important! When SS bit override is enabled, the SS bits are set to 00
for all ports on a shelf. This overrides normal SS bit provisioning
when interworking with non-compliant SONET network elements.
When SS bit override is disabled, the SS bits are set to 10 for all
ports on a shelf. The default setting is **Disabled**.

....

3 Select the **Alarm Severity Assignment Profile** (ASAP). In this case
you select the Equipment ASAP.

For the current release only the default ASAP is available (cf. "Alarm
severity assignment profiles" (16-28) and "Modifying an existing
alarm severity assignment profile" (5-10)).

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

....

Alternative instructions   Another possibility to configure the shelf parameters is:

....

1   In the **System View** of the CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups or Equipment** window .

Result:

The **Equipment** selection tab appears on the left side of the window.

....

2   Select a shelf in the **Equipment** selection tab and click on the pushbutton **Provision**.

Result:

The shelf provisioning window appears on the right side of the window.

....

3   Set the **SS Bit Override** using the respective radio button.

Important! When SS bit override is enabled, the SS bits are set to 00 for all ports on a shelf. This overrides normal SS bit provisioning when interworking with non-compliant *SONET network elements*. When SS bit override is disabled, the SS bits are set to 10 for all ports on a shelf. The default setting is **Disabled**.

....

4   Select the **Alarm Severity Assignment Profile** (ASAP). In this case you select the Equipment ASAP.

For the current release only the default ASAP is available (cf. "Alarm severity assignment profiles" (16-28) and "Modifying an existing alarm severity assignment profile" (5-10)).

E N D   O F   S T E P S

Configuring a slot

Overview

Purpose Use this procedure to set or modify slot parameters before the slot is equipped. This can be done during the setup of a new network element or during operation.

Related information For related information, see:

- "Slot/circuit pack provisioning" (15-27)

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to configure shelf parameters.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions	Complete the following steps to configure the slot parameters:

....

1 In the **Shelf View** of the *WaveStar* CIT select **Provision Slot** after right-clicking on the requested slot.

> **Result:**
>
> The slot provisioning window appears. This is possible only for empty slots. The slot AID is displayed.

....

2 Select the **Alarm Severity Assignment Profile** (ASAP). In this case you select the Equipment ASAP.

For the current release only the default ASAP is available (cf. "Alarm severity assignment profiles" (16-28) and "Modifying an existing alarm severity assignment profile" (5-10)).

....

3 Define in the drop-down list box **Apply To:**, whether the setting shall be applied to the selected slot only, or to all slots in the shelf.

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

....

365-371-522   **Lucent Technologies**   4 - 1 5
Issue b, October 2001

Alternative instructions   Another possibility to configure the slot parameters is:

....

1   In the **System View** of the CIT, via **Configuration** → **Provision** call
up the **Provision Parameters for Protection Groups or Equipment**
window .

Result:

The **Equipment** selection tab appears on the left side of the
window.

....

2   Select a shelf in the **Equipment** selection tab and click on **+**.

Result:

The equipped and the empty slots of the shelf are displayed.

....

3   Select the desired slot (equipped or unequipped) and click on the
pushbutton **Provision**.

Result:

If you have selected an equipped slot two tabs become visible
on the right side of the window. Select the tab **Slot**.

....

4   Select the **Alarm Severity Assignment Profile** (ASAP). In this case
you select the Equipment ASAP.

For the current release only the default ASAP is available, but it is
possible to change settings within the ASAP (cf. "Alarm severity
assignment profiles" (16-28) and "Modifying an existing alarm
severity assignment profile" (5-10)).

....

5   Define in the drop-down list box **Apply To:**, whether the setting shall
be applied to the selected slot only, or to all slots in the shelf.
E N D   O F   S T E P S

⌐

....

Lucent Technologies

Creating a new circuit pack

Overview

Purpose   Use this procedure to define a new circuit pack for a certain slot in a network element (pre-provisioning).

Related information   For related information, see:

- "Provisioning of new components" (15-5)

┐

Procedure

....

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

                         Required privilege code

                         You must have at least a privilege code of P3, Provisioning, to create
                         a new shelf.

                         Required equipment

                         The following equipment is required to perform this task:

                         • *WaveStar* CIT

Instructions   Complete the following steps to create a new circuit pack:
                         ....

1   In the **Shelf View** of the *WaveStar* CIT select **Create New Circuit
                         Pack** after right-clicking on the requested slot.

                              Result:

                              The window **Establish Circuit Pack** opens.

                         ....

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

                         ....

3   Select the **Equipment Alarm Severity Assignment Profile** and the
                         System Event Alarm Severity Assignment Profile in the respective
                         drop-down list boxes.

                         By clicking on the pushbuttons **View Details** you can call up a table
                         with details on the ASAPs. Please refer to "Alarm severity assignment
                         profiles" (16-28) and "Modifying an existing alarm severity
                         assignment profile" (5-10).

                         For the current release only the default Alarm Severity Assignment
                         Profiles (ASAPs) are available.

                         ....

4   Click on **OK** to apply your settings. The window closes. If you wish
                         to discard your changes, click on **Close**.

                              Result:

                              The window closes. and the selected circuit pack type is
                              displayed in the **Shelf View**.

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

....

Alternative instructions   Another possiblity to create a new circuit pack is:

....

1   In the **System View** of the *WaveStar* CIT, select **Configuration** →
Create New → **Circuit Pack...**.

Result:

The **Create New Circuit Pack** window opens.

....

2   Select the shelf for which you wish to create the circuit pack in the
Equipment selection tab on the left side of the window.

....

3   Select the slot for which you wish to create the circuit pack.

....

4   Click on the pushbutton **Select Slot**.

Result:

The selection fields for the new circuit pack become visible on
the right side of the window.

....

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

....

6   Select the **Equipment Alarm Severity Assignment Profile** and the
System Event Alarm Severity Assignment Profile in the respective
drop-down list boxes.

By clicking on the pushbuttons **View Details** you can call up a table
with details on the ASAPs. Please refer to "Alarm severity assignment
profiles" (16-28) and "Modifying an existing alarm severity
assignment profile" (5-10).

For the current release only the default Alarm Severity Assignment
Profiles (ASAPs) are available.

....

7   Click on **Apply**. The window closes. If you wish to discard your
changes, click on **Close**.

E ND OF S TEPS

....

Reassigning a circuit pack

Overview

....

Purpose   Use this procedure to change the assignment of a slot, i.e. another
type of circuit pack than currently provisioned. This can only be done
for slots where different types of circuit packs are allowed (e.g. all
slots for tributary port units).

Related information   For related information, see:

- "Slot/circuit pack provisioning" (15-27)
- "Deleting a cross-connection" (7-26)
- "Deleting a protection group" (7-88)

⌐

....

Lucent Technologies

Procedure

....

Before you begin Prior to performing this task, you must:

- Delete cross-connections the equipment you want to remove is involved in (cf. "Deleting a cross-connection" (7-26))

- Delete protection groups the equipment you want to delete is involved in (cf. "Deleting a protection group" (7-88))

Please note that reassignment of required (core) circuit packs is not possible.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to configure a circuit pack.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

⚠ **CAUTION**

Deletion of provisioned equipment will remove all parameter settings. Removing or modifying a working circuit pack will interrupt service! In order to prevent service interruptions, you should verify that the respective circuit pack is out of service.

Complete the following steps to configure circuit pack parameters:

....

1 Physically remove the current circuit pack.

....

2 In the **System View** of the *WaveStar* CIT call up the **Shelf View** of the respective shelf where the circuit pack is removed from by double-clicking on it.

> **Result:**

> The circuit pack is displayed with several diagonal grey lines to show that the slot is still assigned to this circuit pack.

....

....

3   Select the desired circuit pack in the **Shelf View**, click the right
mouse button and select the option **Delete Circuit Pack** in the pop-up
menu.

> **Result:**
>
> A confirmation window opens containing a warning that all
> provisioned parameters will be lost.

....

4   Click on **Yes** to confirm your changes.

....

5   Physically insert the new circuit pack.

> **Result:**
>
> The slot will be autoprovisioned for the new circuit pack.

E ND   OF   S TEPS

....

Configuring an optical port

Overview

Purpose   Use this procedure to configure one or more optical port(s) of the same type for the operation of a *WaveStar*® TDM 10G (STM-64) system.

Related information   For related information, see:

- "Port and tributary provisioning" (15-28)
- "Reassigning a circuit pack" (4-20)
- "Regenerator section trace" (19-2)
- "Path trace" (19-3)
- "Setting regenerator section trace" (8-17)
- "Viewing regenerator section trace" (8-22)
- "Viewing path trace" (8-26)

Procedure

....

Before you begin   Prior to performing this task, you must insert the optical port unit you want to configure into the correct slot of a shelf. Furthermore, the circuit pack provisioning must be completed before a certain port can be configured (cf. "Slot/circuit pack provisioning" (15-27) and "Reassigning a circuit pack" (4-20)).

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

Required privilege code

You must have at least a privilege code of S3+P3+M1 to configure an optical port.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps in order to configure the parameters of one or more optical port(s):

....

1   In the **System View** of the *WaveStar* CIT, via **Configuration** → **Provision** call up the **Provision Parameters for Protection Groups of Equipment** window.

   Result:

   On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double click on the shelf or click on the **+** in front of the shelf name.

   Result:

   The list of circuit packs and slots which are availabe becomes visible below the shelf name.

....

3   Select the desired optical port unit. Double click on the port unit or click on the **+** in front of the unit name.

....

4   Select the desired port (type). Click on the **Provision** pushbutton.

....

Result:

On the right side of the window the provisionable parameters are displayed.

....

5 Set the parameters according to your needs. Please refer to "Setting the parameters of optical ports" (4-27) for hints on the selection of the parameter values.

....

6 For substructuring the input signal click on the button **Use Form** next to the text box **Input Signal Rate List** in the tab **Transmission**.

Result:

The window **Signal Rate Entry Form for Input Signal Rate List** opens.

The substructuring is a prerequisite for the cross-connection switching. Configure the substructue according to the cross-connection plan for the respective network element.

First select a signal rate, then select all tributaries which are necessary to fill the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**.

Substructuring should be made by clustering

- VC-3, VC-4 for STM 1

- VC-3, VC-4, VC4–4C for STM 4

- VC-3, VC-4, VC4–4C, 4–16C for STM 16 and STM 64

tributaries, i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Input Signal Rate List**. Please refer to "Setting the parameters of optical ports" (4-27) for the meaning of the display.

....

7 For substructuring the output signal click on the button **Use Form** next to the text box **Unequipped Output Signal**.

Result:

The window **Signal Rate Entry Form for Unequipped Output Signal** opens.

First select a signal rate, then select all tributaries which are necessary for the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**. Substructuring should be made by clustering VC-3, VC-4, VC4–4C, or 4–16C channels, i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Unequipped Output Signal**. Please refer to

....

"Setting the parameters of optical ports" (4-27) for the meaning of the display.

....

8   Select the Alarm Severity Profile in the tab **Fault Management** list box. You can choose between the default and a specific ASAP. Via the push-button View Details... you can retrieve more detailed information on the ASAPs. There is also a tab **Timing** in which **Force DUS** can be enabled or disabled.

....

9   Select the destination port(s) in the **Apply To:** drop-down listbox. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack or to all ports on this type in the shelf. By using the latter options, you can decrease your provisioning time significantly.

....

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

E N D   O F   S T E P S

Setting the parameters of optical ports

Purpose Use this procedure to configure the optical ports according to the needs of the network environment. Especially the correct transmission rate, the alarm behavior, the transmission of timing information and the laser state are concerned. The following settings can all be carried out in the **Provision Parameters for Protection Groups or Equipment** window.

Setting the *Port Mode* in the group box *Transmission*

IF	THEN
you want the port to cause alarms during normal operation, but not if there is no valid signal present at the port, e.g. during preprovisioning,	set the **Port Mode** to **Auto**. This is the default value.
there is a valid signal present at the port and you want the port to cause alarms,	set the **Port Mode** to **Monitored**.
you do not want the port to cause alarms,	set the **Port Mode** to **Not Monitored**.

Substructuring

IF	THEN
it is necessary to create a substructure for the input or output signal,	click on the button Use Form and define the substructure according to the required cross-connections.

First select a signal rate, then select all tributaries which are necessary to fill the respective rate by clicking on the desired timeslots in the structure diagram in the group box **Tributaries**. Substructuring should be made by clustering VC-3, VC-4, VC4–4C, VC4–16C tributaries, i.e. using subsequent time slots in the signal. The final substructure is displayed in the text box **Input Signal Rate List** or **Unequipped Output Signal** respectively in the following form **<NX-NX-NX-...>**. X= **3**, **4**, **4c**, **16c**. X is the transmission rate (VC-3, VC-4, VC-4-4c (four concatenated VC-4) and VC-4-16c (16 concatenated VC-4). N is the number of subsequent X.

Example:

64–303 for an STM-16 port designates a substructure of 6 VC-4 (timeslots 111 to 221) and 30 VC-3 (timeslots 231 to 443).

Nonexample:

The following figure shows the **Signal Rate Entry Form for Input Signal Rate List** window. It shows the substructure of an STM-16 signal with 12 VC-3, 8 VC-4 and 1 VC-4-4c.

Timing **settings**	IF	THEN
	you wish to prevent the optical line from being used for synchronization, e.g. because a timing loop might occur,	set the parameter **Force DUS** to **Enabled**.
	you wish the optical line to be used for synchronization,	set the parameter **Force DUS** to Disabled, in this case the current timing marker information for that line is transmitted.

Setting the *Fault Management* **parameters**	IF	THEN
	you wish AIS (Alarm Indication Signal) to be inserted as consequent action of the EBER alarm (Excessive Bit Error Ratio),	set **EBER AIS Enable** to **Enabled**.
	you wish to enable Forward Error Correction for an STM-64 port,	set **FEC Enable** to **Enabled**. For further information on the FEC types, please refer to "Forward error correction" (16-40).
	the Forward Error Correction is enabled via **FEC Enable** and you wish to start or stop the FEC bit error correction at any time,	set the parameter **FEC Correction Enable** to **Enabled** or **Disabled**, respectively.
	you wish that the redundant information is stored and transported in previously unused overhead bytes, so that the framing structure as well as the bit rate remain unchanged,	set the parameter **FEC Type** to **In-Band**.

IF	**THEN**
you wish that the redundant information is appended to the original signal resulting in an optical signal with a modified framing structure and extended bit rate.	set the parameter **FEC Type** to **Out-Band**. The bit rate is increased by approx. 7%. The new signal format is referred to as "Optical Channel" at the corresponding bit rate.
you wish to change the threshold for the Excessive Bit Error Ratio (EXC or EBER) related to the Multiplex Section,	select the required value in the drop-down list box **MS DEXC Threshold**. The values **10E-5**, **10E-4** and **10E-3** (default value) are possible.
you wish to change the threshold for the tolerable signal degradation,	select the required value in the drop-down list box MS Degarde Threshold. The values **10E-5**, **10E-6** (default value), **10E-7**, **10E-8**, **10E-9** are possible.

⌐

Configuring a Gigabit Ethernet port

Overview

....

Purpose   Use this procedure to configure a port of the Gigabit Ethernet
(GE1/SX2) interface.

Related information   For related information, see:

*   "Gigabit Ethernet (GE1/SX2) Interface" (15-29)

....

Procedure

....

Prior to performing this task, the respective slot must at least be preprovisioned for a Gigabit Ethernet interface or an interface must be inserted.

Required privilege code

You must have at least privilege codes of P3 + M1 for port provisioning.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions for LAN ports Complete the following steps in order to configure the parameters of one or more Gigabit Ethernet port(s):

....

1 In the **System View** of the *WaveStar* CIT, via **Configuration** →
Provision... call up the **Provision Parameters for Protection Groups or Equipment** window.

> **Result:**
>
> On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2 Select the desired shelf. Double click on the shelf or click on the **+** in front of the shelf name.

> **Result:**
>
> The list of circuit packs and slots which are availabe becomes visible below the shelf name.

....

3 Select the desired port unit (GE1/SX2). Double click on the port unit or click on the **+** in front of the unit name.

....

4 Select the desired LAN port. Click on the **Provision** pushbutton.

> **Result:**
>
> On the right side of the window 3 tabs containing the provisionable parameters are displayed.

....

5 Select the **Port Mode** in the group box **Fault** of the tab **Port Data**.

....

Lucent Technologies

The following values are possible:

- **AUTO**

- **Monitored**

- **Not Monitored**

....

6 Select the **Default Priority**. This is the priority for untagged incoming frames.

The following values are possible:

- **Not Applicable**

- **High**

- **Low**

....

7 Select the **Flow Control Mode**.

The following values are possible:

- **Disable**

- **AUTO**

On the same tab the **Flow Control Mode Operation** is displayed. The values **Enable**, **Disable** and **Unavailable** are possible.

....

8 Select the **Alarm Severity Profile** in the respective drop-down list box. You can choose between the default and a specific ASAP. Via the push-button **View Details...** you can retrieve more detailed information on the ASAPs.

....

9 Define whether **Untagged VLAN Frames** are admitted by clicking on the respective check box on the tab **Admitted Frame Types**.

....

10 If untagged VLAN frames are admitted, insert a **Port VLAN Identifier**. Insert an integer in the range **1** ... **4093**.

....

11 Edit the valid VLAN list in the respective text box. A VLAN identifier is an integer with values form **1** to **4093**. Several identifiers can be seperated by a comma. A VLAN range is denoted with two VLAN identifiers separated by a dash. In the group box **Edit VLAN List** click on the radio button **Add** in order to add the edited VLAN list to the valid VLAN list or click on the radio button **Delete** to remove it. If you wish to retrieve details on a selected VLAN click on

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 3 3

the button **VLAN Overview** in order to open the **VLAN Overview** window.

....

12   In the drop-down list box **Apply to:** select whether the changes shall affect only the selected port, all ports of the present type on the selected circuit pack, or all ports of the present type in the selected shelf.

....

13   Click on **Apply** in order to activate your changes. If you wish to discard your changes, click on **Close**. For the configuration of the VCG tributaries please refer to "Configuring a tributary" (4-43).
E N D   O F   S T E P S

....

Instructions for WAN ports   ....

1   In the **System View** of the *WaveStar* CIT, via **Configuration** → **Provision...** call up the **Provision Parameters for Protection Groups or Equipment** window.

       Result:

       On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double click on the shelf or click on the **+** in front of the shelf name.

       Result:

       The list of circuit packs and slots which are availabe becomes visible below the shelf name.

....

3   Select the desired port unit (GE1/SX2). Double click on the port unit or click on the **+** in front of the unit name.

....

4   Select the desired WAN port. Click on the **Provision** pushbutton.

       Result:

       On the right side of the window 2 tabs containing the provisionable parameters are displayed.

....

5   Select the **Port Mode** in the group box **Fault** of the tab **VCG Data**.

....

4 - 3 4   **Lucent Technologies**   365-371-522
Issue b, October 2001

The following values are possible:

- **Monitored**

- **Not Monitored**

....

6 Select the **Alarm Severity Profile** in the respective drop-down list box. You can choose between the default and a specific ASAP. Via the push-button **View Details...** you can retrieve more detailed information on the ASAPs.

....

7 In the drop-down list box **Apply to:** select whether the changes shall affect only the selected VCG port, all VCG ports of the present type on the selected circuit pack, or all VCG ports of the present type in the selected shelf.

E ND OF S TEPS
....

Viewing VLAN data

Overview

Purpose Use this procedure to retrieve information on ethernet ports and VC Groups on an NE basis, which are part of a specified VLAN.

Related information

For related information, see:

- "Gigabit Ethernet (GE1/SX2) Interface" (15-29)
- "Configuring a Gigabit Ethernet port" (4-31)

Lucent Technologies

Procedure

....

Before you begin   Prior to performing this task you must be connected to the *WaveStar*®
CIT and the respective network element.

Required privilege code

You must have at least privilege codes of P1 + M1 for viewing
VLAN data.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   ....

1   In the **System View** of the *WaveStar* CIT via **View** → **VLAN
Topology** call up the window **VLAN Overview**. Alternatively you can
click on the **VLAN Overview** button on the Ethernet port provisioning
window.

....

2   Select a VLAN ID from the data selection screen or a slot AID from
the equipment selection screen.

   Result:

   The following values are displayed:

   - **VLAN ID**
   - **Ethernet Port AID**
   - **VCG AID**
   - **VCG Rate**
   - **VCG Size**

E N D   O F   S T E P S

....

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 3 7

Configuring an electrical port

Overview

Purpose Use this procedure to configure an electrical port for the operation of a *WaveStar*® TDM 10G system.

Related information For related information, see:

- "Port and tributary provisioning" (15-28)
- "Reassigning a circuit pack" (4-20)
- "Regenerator section trace" (19-2)
- "Path trace" (19-3)
- "Setting regenerator section trace" (8-17)
- "Viewing regenerator section trace" (8-22)
- "Viewing path trace" (8-26)

Procedure

....

Before you begin   Prior to performing this task, you must insert the electrical port unit you want to configure into the correct slot of the shelf. Furthermore the circuit pack provisioning must be completed before a certain port can be configured (cf. "Reassigning a circuit pack" (4-20)).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to configure an electrical port.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps in order to configure the parameters of one or more electrical port(s):

....

1   In the **System View** of the *WaveStar* CIT, via **Configuration** → **Provision** call up the window **Provision Parameters for Protection Groups of Equipment**.

   Result:

   On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double-click on the shelf or click on the **+** in front of the shelf name.

   Result:

   The list of circuit packs and slots which are available becomes visible below the shelf name.

....

3   Select the desired electrical port unit. Double click on the port unit or click on the **+** in front of the unit name.

....

4   Select the desired port (type). Click the **Provision** pushbutton.

   Result:

   On the right side of the window, the provisionable parameters are displayed.

....

....

5   Set the parameters according to your needs. Please refer to "Provisionable parameters of electrical ports" (4-41) for the description of the parameters.

Substructuring (via **Tributary Rate Lists**) should be made by clustering VC-3 or VC-4 channels, i.e. using subsequent time slots in the signal.

....

6   Select the destination port(s) in the **Apply To:** drop-down list box. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack or to all ports of this type in the shelf. By using the latter options, you can decrease your provisioning time significantly.

....

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

E N D   O F   S T E P S

....

Provisionable parameters of electrical ports

Important settings Configure the electrical ports according to the needs of the network environment. Especially the correct transmission rate and, the alarm behaviour are concerned.

The following table shows which parameters are provisionable, and explains their meaning:

Parameter	Values	Meaning
Transmission parameters		
Port Mode		The Port Mode defines whether a port causes alarms or not.
	Auto (default)	If a valid signal is present at the port, the Port Mode is set to *MON* automatically
	Monitored (MON)	The port causes alarms, if necessary
	Not Monitored (NMON)	The port does not cause alarms
Tributary Rate Lists		
Tributary Input Signal Rate List	*<NX-NX-NX-...>*	This parameter defines the VC-N signal substructure across the port's bandwidth for the input signal. X=*3*, *4*, N= number of subsequent X, e.g. *33* designates a substructure of 3 VC-3 in one STM-1 signal
Tributary Unequipped Output Signal	*<NX-NX-NX-...>*	This parameter defines the VC-n signal substructure across the port's bandwidth for an output signal which does not contain real traffic. X=*3*, *4*, N= number of subsequent X, e.g. designates a substructure of one VC-4 in an STM-1 signal
Fault Management		
EBER AIS Enable	*Enabled* *Disabled*	When this parameter is set to *Enabled*, AIS (Alarm Indication Signal) will be inserted as consequent action of the alarm EBER (Excessive Bit Error Ratio)

Parameter	Values	Meaning
MS DEXC Threshold	*10E-5* *10E-4* *10E-3* (default value)	This parameter defines the threshold for the Excessive Bit Error Ratio (EBER or EXC) related to the Multiplex Section. If the threshold is exceeded Signal Fail (SF) is signalled.
MS Degrade Threshold	*10E-5* *10E-6*(default) *10E-7* *10E-8* *10E-9*	This parameter defines the threshold for the tolerable signal degradation. If the threshold is exceeded Signal Degrade (SD) is signalled.
Alarm Severity Profile	*<ASAP name>* (24 charac- ters max.), *Default*	Selection between the default and a specific ASAP

Configuring a tributary

Overview

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

Related information   For related information, see:

- "Reassigning a circuit pack" (4-20)

- "Configuring an optical port" (4-23)

- "Configuring an electrical port" (4-38)

Procedure

....

Purpose   Use this procedure to configure tributaries belonging to optical or
electrical SDH signals.

Before you begin   Prior to performing this task, you must insert the port unit you want
to configure into the correct slot of a shelf. Furthermore, the circuit
pack provisioning and the port provisioning must be completed before
a certain tributary can be configured (cf. "Reassigning a circuit pack"
(4-20) and "Configuring an optical port" (4-23)).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to
configure tributaries.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps in order to configure the parameters
of a tributary:

....

1   In the **System View** of the *WaveStar* CIT, via **Configuration** →
Provision call up the **Provision Parameters for Protection Groups
or Equipment** window.

Result:

On the left side of the window, the **Equipment** selection tab is
displayed. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double-click on the shelf or click on the **+** in
front of the shelf name.

Result:

The list of circuit packs and slots which are availabe becomes
visible below the shelf name.

....

3   Select the desired port unit. Double click on the port unit or click on
the **+** in front of the unit name.

Result:

The list of ports which are available becomes visible below the
port unit name.

....

....

4   Select the desired port. Double click on the port or click on the **+** in front of the port.

>   **Result:**

>   The list of tributaries which are available becomes visible below the port.

....

5   Select the desired tributary (type).

>   **Result:**

>   On the right side of the window, the provisionable parameters are displayed.

....

6   Set the parameters according to your needs. Please refer to "Provisionable parameters of tributaries" (4-46) for the description of the parameters.

....

7   Select the destination tributary(s) in the **Apply To:** drop-down list-box. Here, you can specify whether the settings should apply only to the above selected tributary or to all tributaries of the respective port or to all tributaries on the respective circuit pack. By using the latter options, you can decrease your provisioning time significantly.

....

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

E ND   OF   S TEPS
....

⌐

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 4 5

Provisionable parameters of tributaries

Important settings

Configure the tributary according to the needs of the network environment. Especially the alarm behaviour is concerned.

The following table shows which parameters are provisionable, and explains them:

Parameter	Values	Meaning
Fault Management		
Tributary Monitoring Mode	*Monitored (MON)*	An alarm is caused, if necessary
	Not Monitored (NMON-)(default)	No alarms are caused.
Tributary Alarm Severity Profile	*<ASAP name>* (24 characters max.), *Default*	Selection between the default and a specific ASAP
HP Degraded Threshold	*0 ... 100* in steps of 5, initial value: *30*	Threshold value for the signal degradation of tributaries belonging to electrical STM-1 ports. This parameter is related to the Higher Order path.
HP DEXC Threshold	*10E-5, 10E-4, 10E-3* (default)	This parameter defines the threshold for the Excessive Bit Error Ratio (EBER or EXC) related to the Higher Order path. If the threshold is exceeded HP-EXC is signalled. This parameter only applies to tributaries belonging to optical ports.
HP Degraded Threshold	*10E-5, 10E-6*(default), *10E-7*, *10E-8*, *10E-9*	This parameter defines the threshold for the tolerable signal degradation related to the Highe Order path. If the threshold is exceeded HP-DEG is signalled. This parameter only applies to tributaries belonging to optical ports.

Parameter	Values	Meaning
HP Degraded Interval	*2 ... 10 in steps of 1, initial value 7*	Only for electrical STM 1 ports

Removing equipment from the system

Overview

Purpose   Use this procedure to de-provision (delete) equipment which has been provisioned for the system. This can be necessary, for example, in the event of a reconfiguration.

      Lucent Technologies

Procedure

....

Before you begin   Prior to performing this task, you must:

- Delete cross-connections in which the equipment you want to remove is involved (cf. "Deleting a cross-connection" (7-26))

- Delete protection groups in which the equipment you want to delete is involved (cf. "Deleting a protection group" (7-88))

- Physically remove the equipment.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to remove equipment from the system.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

⚠ CAUTION

Deletion of provisioned equipment will remove all parameter settings. Removing or modifying a working circuit pack will interrupt the service! In order to prevent service interruptions, you should verify that the respective circuit pack is out of service.

Complete the following steps to remove equipment from the system:

....

1   In the **System View** of the *WaveStar*CIT, via **Configuration** → **Delete...** call up the **Delete** window.

> **Result:**
>
> The **Delete** window appears.

....

2   Select the component you want to delete in the tab **Equipment**. You can delete the following types of component:

- Circuit Packs (when they are removed and no cross-connections and protection is at this pack)

- Bay

- Shelf

In the tab **Protection** you can delete a protection group.

....

....

3   Click on **Select** to apply your changes. A confirmation window opens
containing the warning that all provisioned parameters will be lost.
Click on **Yes** to confirm your changes. Click on **No** to discard your
changes.

E ND   OF   S TEPS

....

⌐

Exchanging a circuit pack

Overview

....

Purpose   Use this procedure to exchange circuit packs by functionally equivalent or compatible circuit packs.

Functionally equivalent or compatible circuit packs can be exchanged via the TL1 command ed-eqpt while the circuit pack is still **active**. This can be done in **cut-through** or **menu mode**.

Related information   For related information, see:

- "Exchangeability of circuit packs" (15-7)
- "Cut Through view" (24-62).

⌐

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 5 1

Procedure

....

Before you begin   Prior to performing this task, you must be logged into the *WaveStar*®
CIT.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Important! The **strong FEC** capability is recognized only at
initialization of a new pack. This might lead to a not desirable
configuration. To avoid this, first disable **strong FEC** (bilateral
impact: far-end too) (refer to "Configuring an optical port" (4-23)),
exchange the pack and set **strong FEC** again.

Instructions   ....

1   Pull the desired active circuit pack.

Important! The current software is not able to handle repeated open
close events of the latch. If the latch is opened, always extract the
circuit pack after the protection switch has happened.

....

2   Call up the **Cut-Through** window from the main menu via **Network
Element** → **Cut-Through** (see also "Cut Through view" (24-62))

....

3

IF	THEN
you want to reprovision the relevant slot	use the TL1 command ed-eqpt and specify the circuit pack to be inserted. **Reference:** "Exchangeability table" (15-7).
you want to choose a pack from the acceptable circuit pack list	use the TL1 command rtrv-eqpt to retrieve this list and pick an exchangeable pack. **Reference:** "Exchangeability table" (15-7).

....

4   Insert the new circuit pack.

The NE software checks if the removed circuit pack and the new
circuit pack share the same exchangeability group. The NE only
accepts the specified one.

....

Result:

If you have specified an empty slot instead of a new circuit pack the database will be updated.

E N D   O F   S T E P S

Upgrade In-Service Switch/STS576 to Switch/STS768

Overview

....

Purpose Use this procedure to upgrade in-service the Switch/STS576 to a Switch/STS768.

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

CAUTION

Electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar system, to prevent electrostatic discharge damage to sensitive components.

CAUTION

Do not rock circuit packs back and forth when removing and installing them. Carefully slide circuit packs into or out of the shelf .

Related information For related information, see:

- "Main shelf configuration" (15-9)

- Chapter 24, "*WaveStar* CIT Tutorial".

....
Lucent Technologies

Procedure

....

Before you begin   Before you begin this task, verify that a *WaveStar*® CIT is connected
and logged in to the *WaveStar* TDM 10G (STM-64) system. Prior to
performing this task, you must be logged into the *WaveStar* CIT.

Required privilege code

A privilege code of at least M4 is required to perform a protection
switch. A privilege code of at least S1 is required to view the
protection switch status.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT (Release 6.0.0)

- Wrist strap

- 2 replacement SWITCH/STS768 circuit packs for the SWITCH/
  STS576 circuit packs in slot SWITCH 0 and SWITCH 1 of the
  high-speed part of the main shelf

- 2 replacement PPROC/STS384 circuit packs for the PPROC/
  STS192 circuit packs in slot PPROC 0 and PPROC 1 of the
  high-speed part of the main shelf.

Important! The *WaveStar* system must be equipped with Release
4.0.0 or later software. Earlier software releases do not support the
Switch/STS768.

**Upgrading in-service
Switch/STS576 to
Switch/STS768**   Complete the following steps to upgrade in-service the
Switch/STS576 to a Switch/STS768.

....

1   At the *WaveStar* CIT, select **Fault → NE Alarm List...** or click on
Alarm List to obtain an **NE Alarm List**.

....

2   View the NE Alarm List.

IF THERE ARE…	THEN…
no alarms listed,	go to Step 3.
alarms listed,	refer to *WaveStar* TDM 10G (STM-64), Alarm Messages and Trouble Clearing Guide and clear all alarms before proceeding to Step 3.

....

....

3 Determine the status (*Active Side* and *Switch Request State*) of the
576x576 switch protection group (*1+1 Equipment esysswitchgrp*).

"Viewing the status of the 576x576 Switch Protection Group" (4-57)

....

4 Replace the standby (non-active) SWITCH/STS576 and PPROC/
STS192 circuit packs in the high-speed part of the main shelf with the
SWITCH/STS768 and PPROC/STS384 circuit packs.

> **Reference:**
>
> "Replacing standby SWITCH/STS576 and PPROC/STS192
> circuit packs" (4-58)

....

5 Perform a protection switch from the Active switch side to the
Standby (non-active) switch side using the **Fault** → **Protection
Switch...** command.

> **Reference:**
>
> "Switching a 1+1 equipment protection" (4-67)

....

6 Replace the standby (non-active) SWITCH/STS576 and PPROC/
STS192 circuit packs in the high-speed part of the main shelf with the
SWITCH/STS768 and PPROC/STS384 circuit packs.

> **Reference:**
>
> "Replacing standby SWITCH/STS576 and PPROC/STS192
> circuit packs" (4-58)

....

7 Perform a protection switch from the Active switch side to the
Standby (non-active) switch side using the **Fault** → **Protection
Switch...** command to verify the Standby switch side operates
correctly.

> **Reference:**
>
> "Switching a 1+1 equipment protection" (4-67)

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

**Viewing the status of the
576x576 Switch Protection
Group**

Perform the following steps to determine the current status
(***Active Side*** and ***Switch Request State***) of the 576x576 switch
protection group (***1+1 Equipment esysswitchgrp***).

....

1   In the **System View** of the *WaveStar* CIT, via the menu **View** →
Protection... call up the **View Protection** window.

Result:

The **View Protection** window opens.

....

2   Click on the **Ptn Grp** tab (if required). Then click on **1+1 Equipment
esysswitchgrp** and **Select**.

Result:

The protection information appears for the 576x576 switch
protection group.

....

Important! The 576x576 switch protection group consists of Side 0
circuit packs and Side 1 circuit packs. One side is active and the other
side is standby.

3   Verify the **Protection Group AID** and note the **Active Side**.
Determine the active SWITCH/STS576 circuit pack and the standby
SWITCH/ STS576 circuit pack on the high-speed part of the main
shelf (shelf 1-2).

Important! The Shelf View screen of the high-speed part of the main
shelf also shows the Active and Standby SWITCH/STS576 circuit
packs. An (**A**) is shown on the Active SWITCH/STS576 circuit pack
and an (**S**) is shown on the Standby SWITCH/STS576 circuit pack.

....

4   Observe the **Switch Request State**.

....

IF the Switch Request State is ...	THEN click on Close and ...
Forced Switch,	Clear the forced switch by performing the following: 1. At the WaveStar CIT, select **Fault → Protection Switch...** . (The Switch Protection screen appears.) 2. Click on the **Ptn Grp** tab (if required). Then click on **1+1 Equipment esysswitchgrp** and **Select**. (The protection switch information appears for the switch protection group.) 3. Verify the information on the screen (note the current **Active Side**) and select *Clear Forced* in the **Switch Type:** field. Click on **Apply**. (A dialog box appears asking you to confirm executing this command.) 4. Click on **Yes**. The protection switch is cleared. Click on **Close**.
Equipment Fail,	refer to *WaveStar* TDM 10G (STM-64), Alarm Messages and Trouble Clearing Guide. Clear all alarms before proceeding.
Equipment Fail,	proceed.

E N D   O F   S T E P S

Replacing standby SWITCH/STS576 and PPROC/STS192 circuit packs

Perform the following steps to replace the standby SWITCH/STS576 and PPROC/STS192 circuit packs in the high-speed part of the main shelf with SWITCH/STS768 and PPROC/STS384 circuit packs.

⚠ **CAUTION**

Damages at the slot guides and the shelf.

Do not rock the circuit pack back and forth. To avoid damage, carefully place the replacement circuit pack into the slot guides and slowly slide it into the shelf (using BOTH hands) until the latch is fully engaged

1   Locate the Standby (non-active) SWITCH/STS576 circuit pack,
unlock the circuit pack latches, and remove the circuit pack.

Important! The **Shelf View** screen shows an (**A**) on an Active circuit
pack and an (**S**) on a Standby circuit pack.

....

2   Install the replacement SWITCH/STS768 circuit pack in the slot.

Result:

The SWITCH/STS768 circuit pack initializes.

....

⚠️ **CAUTION**

Damages at the slot guides and the shelf.

*Do not rock the circuit pack back and forth. To avoid
damage, carefully place the replacement circuit pack into
the slot guides and slowly slide it into the shelf (using
BOTH hands) until the latch is fully engaged*

3   Locate the Standby (non-active) PPROC/STS192 circuit pack in slot
PPROC 0 or **PPROC 1**, unlock the circuit pack latches, and remove
the circuit pack.

Important! The **Shelf View** screen shows an (**A**) on an Active circuit
pack and an (**S**) on a Standby circuit pack.

....

4   Install the replacement SWITCH/STS384 circuit pack in the slot.

Result:

The SWITCH/STS384 circuit pack initializes.

....

5   Wait several minutes for the SWITCH/STS768 and PPROC/STS384
circuit packs to stabilize.

E N D   O F   S T E P S

❐

Viewing an equipment protection group

Overview

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

Related information   For related information, see:

- "Protection mechanisms" (18-10)
- "Protection configurations" (18-35)
- "Equipment protection" (15-31)

Lucent Technologies

Procedure
....

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

Required privilege code

You must have at least a privilege code of S1, Security, to query an
equipment protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the status of a protection
group
....

1 In the **System View** of the *WaveStar* CIT, via the menu **View** $\rightarrow$
Protection... call up the **View Protection** window.

Result:

The **View Protection** window opens.

....

2 Select the components of the required protection group in the tab **Ptn
Grp** on the left side of the window.

E ND OF S TEPS
....

$\beth$

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 6 1

Parameters for a 1+1 equipment protection

Status data The following table shows the status data which are shown in the **View Protection** window for a 1+1 equipment protection of timing or switch circuit packs.

Information field	Possible value	Meaning
Protection Group AID	cf. "Overview of access identifiers" (15-18)	The AID defined for the selected protection group.
Protection Type	**Switch Fabric**	
Circuit Pack Type(s)	**TMG/STRAT3**or **SWITCH/STS576 PPROC/STS192**	The circuit pack type for which the equipment protection has been established.
Side 0 AID(s)	cf. "Overview of access identifiers" (15-18)	The circuit pack AID(s) of one circuit pack belonging to the protection group (designated as side 0).
Side 1 AID(s)	cf. "Overview of access identifiers" (15-18)	The circuit pack AID(s) of one circuit pack belonging to the protection group (designated as side 1).
Side 0 Alarm Status/Side 1 Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)**or**Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm status associated with side 0/side 1. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preference** window (cf. Chapter 24, " *WaveStar*® CIT Tutorial").
Active Side	**0**, **1**	The side (circuit pack) which is currently working
Switch Request State	**No Request, Forced Switch, Equipment Failed**	Last switch request which caused a switch between the two circuit packs.

Parameters for a 1:N equipment protection

Status data   The following table shows the status data which are shown in the
View Protection window for a 1:N equipment protection of STM1E/4
circuit packs.

Information field	Possible value	Meaning
Protection Group AID	cf. "Overview of access identifiers" (15-18)	The AID defined for the selected protection group.
Protection Type	**1xN Electrical**	—
Circuit Pack Type	**STM1E/4**	—
Protection Pack AID	cf. "Overview of access identifiers" (15-18)	The AID of the circuit pack for the selected protection group.
Working Pack List	cf. "Overview of access identifiers" (15-18)	The list of the working circuit packs of the selected protection group.
Circuit Pack Alarm Status	**Critical (CR), Major (MJ), Minor (MN) or Not Alarmed (NA)**	The alarm status of each working circuit pack.
Protection Pack Alarm Status	**Critical (CR), Major (MJ), Minor (MN) or Not Alarmed (NA)**	The alarm status of the protection circuit pack.
Pack Being Protected	**<circuit pack AID> <circuit pack type>, —**	Failed circuit pack if a protection switch has occurred.
Switch Request State	**No request, Lockout, Forced, Equipment Fail, Wait to Restore**	Last switch request which caused traffic to be carried on the protection circuit pack
Locked Out Pack	**<circuit pack AID>**	List of AIDs of all circuit packs belonging to the protection group which are in the Lockout state
Wait To Restore	**0 ... 12 minutes, infinite**	The working circuit pack is operable again. Traffic is still carried on the protection circuit pack. A wait is made for a defined time (wait-to-restore time) to see whether the working section is stable before traffic is switched back.

⌐

Creating a 1:N STM-1(e) equipment protection group

Overview

....

Purpose   Use this procedure to create a new equipment protection group for STM-1 electrical port units (STM1E/4).

Related information   For related information, see

- "Equipment protection" (15-31)
- "Viewing an equipment protection group" (4-60)
- "Switching a 1:N equipment protection" (4-70)
- "Configuring an electrical port" (4-38)

┐

....

Procedure

....

Before you begin Before you perform the procedure below, make sure that:

- No STM1E/4 or EPS-64 (shown as SWITCH/STM1EE4 in *WaveStar*® CIT) circuit packs are provisioned or pre-provisioned in the dedicated slots (1–1)eprn and (1–1)eprotsw. Check by using *WaveStar* CIT.

- Please note that there are two variants of electrical STM-1 interface circuit packs:

   - STM1EE4/4 (LEY40, used in former releases, should not be used in protection applications and therefore has to be manually excluded)

   - STM1E/4 (LEY44, new for Release 2, supports protection). Your NE can be equipped with both types, the STM1EE4/4, however, will not be part of the protection group.

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create a new equipment protection group.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to create a new equipment protection group:
....

1 Insert an STM1E/4 port unit into the slot (1–1)eprn.

   Result:

   The pack is validated and initialized.
   ....

2 Insert an EPS-64 circuit pack (shown as SWITCH/STM1EE4 in the *WaveStar* CIT) into the slot (1–1)eprotsw.

   Result:

   The pack is validated and initialized. The electrical protection group becomes fully functional to the user. All STM-1(e) interface circuit packs (STM1E/4 and STM1EE4/4) become members of the protection group.

....
365-371-522
Issue b, October 2001

Lucent Technologies

4 - 6 5

....

3   Configure all STM1EE4/4 circuit packs to be in the ***Lockout of
        Working*** state. Please refer to "Viewing an equipment protection
        group" (4-60).

        Result:

        Switch requests from this circuit pack (e.g. failures or extracting
        the circuit pack form the slot) will no longer cause a protection
        switch.

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

Switching a 1+1 equipment protection

Overview

Purpose Use this procedure to switch from one circuit pack to the other in a 1+1 equipment protection of timing or switch circuit packs.

Related information For related information, see:

- "Protection mechanisms" (18-10)
- "Protection configurations" (18-35)
- "Viewing an equipment protection group" (4-60)

Procedure

....

Before you begin   Please note that a forced switch to a faulty circuit pack may cause a traffic interruption. Make sure that a forced switch is only carried out to a circuit pack that is working correctly.

Required privilege code

You must have at least a privilege code of M4, Maintenance, to switch a 1+1 equipment protection.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to switch a 1+1 equipment protection:
....

1   Call up the **Protection Switch** window either in the System View via **Fault** → **Protection Switch**, or in the **Shelf View** by right-clicking on the requested circuit pack, then selecting Protection Switch.

> **Result:**
>
> The **Protection Switch** window opens.

....

2   Select the respective equipment protection in the tab **Ptn Group** on the left side of the window.

> **Result:**
>
> Some data of the protection group are displayed.

....

3   The desired **Switch Type** depends on the type of protection. The following options are possible:

- For switch packs
    - Manual To Side 0
    - Manual To Side 1
    - Forced to Side 0

....

- Forced to Side 1
- Clear
- For timing packs
  - Manual To Side 0
  - Manual To Side 1
  - Clear

....

4   Click on **OK**.

E N D   O F   S T E P S

....

Switching a 1:N equipment protection

Overview

....

Purpose   Use this procedure to switch from one circuit pack to the other in a 1:N equipment protection of STM1E/4 circuit packs, or to lockout specific STM-1E/4 or STM-1EE4/4 circuit packs from protection.

Related information   For related information, see:

- "Protection mechanisms" (18-10)

- "Protection configurations" (18-35)

- "Viewing an equipment protection group" (4-60)

⌐

....

Switching a 1:N equipment protection

4 - 7 0   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

Before you begin Please note that only STM1E/4 circuit packs can be used properly in a protection configuration. If STM1EE4/4 circuit packs are plugged, these have to be manually locked out from the protection group (always should remain in the switch state **Lockout of Working**)

Required privilege code

You must have at least a privilege code of M4, Maintenance, to switch a 1:N equipment protection.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to switch a 1:N equipment protection, or to lockout specific circuit packs:

....

1 Call up the **Protection Switch** window either in the System View via **Fault** → **Protection Switch**, or in the **Shelf View** by right-clicking on the requested circuit pack, then selecting Protection Switch.

> **Result:**
>
> The **Protection Switch** window opens.

....

2 Select one working port unit of the respective equipment protection in the tab **Ptn Group** on the left side of the window.

> **Result:**
>
> Some data of the protection group are displayed.

....

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

- **Clear**
- **Clear Lockout of Working**
- **Lockout of Working**
- **Lockout of Protection**
- **Forced**
- **Manual**

....

4 Click on **Apply**.

E N D   O F   S T E P S

....

Configuring Miscellaneous Discrete Inputs and Outputs

Overview

Purpose   Use this procedure to set the parameters for the operation of the Miscellaneous Discrete Inputs (MDIs) and Outputs (MDOs).

Related information   For related information, see:

- "Miscellaneous Discrete Inputs and Outputs" (15-33)

Procedure

....

Before you begin   Prior to performing this task, you must be logged into the *WaveStar*®
CIT and the respective network element. The MDIs and MDOs which
are to be used have to be connected to a device, via the MDI/MDO
output of the NE.

Required privilege code

You must have at least a privilege code M3, Maintenance, to
configure MDIs and MDOs.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to configure the MDIs and MDOs:
....

1   In the **System View** of the *WaveStar* CIT via **Configuration** → **Misc.
Discretes...** call up the window **Configure Miscellaneous Discretes.**

....

2   Select in the **Equip** tab the MDI or MDO you wish to configure.
MDIs and MDOs become visible in the list as soon as they are
connected to a device.

....

3   If necessary, change the name of an MDI or MDO in the text box
Name:.

....

4   If you are configuring an MDI select an **Alarm Severity Assignment
Profile** (ASAP) in the respective drop-down list box. You can select
among all ASAPs of the type **Environmental**. Proceed to Step 7.

If you are configuring an MDO proceed to Step 5.

....

5   If you are configuring an MDO select the **Initial State** by clicking on
the respective radion button. The values **Operated** and **Released** are
possible. If the **Initial State** is **Released** the MDO is default **not
activated**, otherwise default is **activated**.

....

6   If you are configuring an MDO set its **Duration Mode** by clicking on
the respective radio button. This defines whether the relay contact is

....

opened or closed continuously or momentarily with a fixed period of
300 ms.

The possible values are:

- **Continuously**
  if any equipment is connected which needs a continuous signal

- **Momentarily**
  if equipment is connected which only needs a short pulse.

....

7   Click on **Apply** to activate your changes.

> **Result:**
>
> A warning appears which indicates that the NE service may be
> affected by the changes.

....

8   Click on **Yes** to execute the command.

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

Viewing Miscellaneous Discrete Inputs and Outputs

Overview

....

Purpose   Use this procedure to retrieve the parameters for the operation of the Miscellaneous Discrete Inputs (MDIs) and Outputs (MDOs).

Related information   For related information, see:

- "Miscellaneous Discrete Inputs and Outputs" (15-33)
- "Configuring Miscellaneous Discrete Inputs and Outputs" (4-72)

┐

....

Procedure

....

Before you begin   Prior to performing this task, you must be logged into the *WaveStar*®
CIT and the respective network element. The MDIs and MDOs which
are to be used have to be connected to a device.

Required privilege code

You must have at least a privilege code M1, Maintenance, to retrieve
parameters of MDIs and MDOs.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to configure the MDIs and MDOs:
....

1   In the **System View** of the *WaveStar* CIT via **View → Misc.
Discretes...** call up the window **View Miscellaneous Discretes.**

....

2   Select in the **Equip** tab the MDI or MDO of which you wish to
retreive the parameters. MDIs and MDOs become visible in the list as
soon as they are connected to a device.

....

3   If you are viewing an MDI the configured **Alarm Severity
Assignment Profile** (ASAP) is displayed in the respective group box.
The possible ASAPs are of the type **Environmental**. Proceed to Step
5.

If you are configuring an MDO proceed to Step 4.

....

4   If you are viewing an MDO the **Initial State** is displayed. The
possible values **Operated** and **Released** indicate the default situation.

Furthermore the **Duration Mode** is displayed. It defines whether the
relay contact is opened or closed continously or momentarily with a
fixed period of 300 ms. Thus the values **Continuously** and
Momentarily are possible.

The **Control Status** can be **set On** or **Off** via **Fault → Operate MDO
Screen**.

....

5   Click on **Close** to quit the window.
E N D   O F   S T E P S
....

....

Operating Miscellaneous Discrete Outputs

Overview

Purpose Use this procedure to set the **Control Status** of the Miscellaneous Discrete Outputs (MDOs) to *on* or *off*.

Related information For related information, see:

- "Miscellaneous Discrete Inputs and Outputs" (15-33)

Procedure

....

Before you begin Prior to performing this task, you must be logged into the *WaveStar*®
CIT and the respective network element. The MDOs which are to be
used have to be connected to a device.

Required privilege code

You must have at least a privilege code M3, Maintenance, to operate
an MDO.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to set the **Control Status** of an
MDO:
....

1 In the **System View** of the *WaveStar* CIT via **Fault** → **Operate
Output Misc. Discretes...** call up the window **Operate
Miscellaneous Discrete Outputs.**

....

2 Select in the **Equip** tab the MDO you wish to operate.

....

3 Set the **Control Status** of the selected MDO.

Depending on the **Duration Mode** and the **Initial State** defined for the
selected MDO the following different values for the **Control Status**
are selectable.

If the **Duration Mode** of the selected MDO is set to **Continuously**,
the following values are selectable:

- **On**

- **Off**.

If the **Duration Mode** of the selected MDO is set to **Momentarily**, the
the following values are selectable:

- **Initial State** On

  - **On**

  - **Momentary Off**

- **Initial State** Off

  - **Off**

  - **Momentary On**

....

The **Duration Mode** of an MDO defines whether the relay contact is opened or closed continously or momentarily with a fixed period of 300 ms.

....

4   Click on **Apply** to activate your changes.

Result:

A warning appears which indicates that the NE service may be affected by the changes.

....

5   Click on **Yes** to execute the command.

E ND   OF   S TEPS
....

....

365-371-522
Issue b, October 2001

Lucent Technologies

4 - 7 9

Lucent Technologies
Bell Labs Innovations

5   Alarm management

Overview

Purpose   This chapter describes the procedures which have to be performed for the alarm management of the *WaveStar*® TDM 10G (STM-64).

Contents

⌐

Creating a new alarm severity assignment profile

Overview

....

Purpose   Use this procedure to create a new Alarm Severity Assignment Profile
(ASAP).

Note

In the present *WaveStar*® TDM 10G (STM-64) release, apart from the
"STMn Port" and "VC-N(c) Tributary" ASAP types, only the default
ASAP of each ASAP type can be assigned to a functional system
component.

Related information   For related information, see:

- "Alarm severity assignment profiles" (16-28)

- Chapter 24, "*WaveStar* CIT Tutorial"

⌐

....

5 - 2   **Lucent Technologies**   365-371-522
                                                                                     Issue b, October 2001

Procedure

....

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 code

You must have at least a privilege code of:

- M1
  to view ASAPs,

- M3
  to create or provision ASAPs.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new ASAP:

....

1   From the *WaveStar* CIT **System View** or **Shelf View** main menu, select **Configuration** → **Alarms** → **Alarm Severity Assignment Profiles ...**

> **Result:**
>
> The **Provision Alarm Severity Profile** window opens. Initially, only the ASAP selection part ("ASAP tree") on the left-hand side of the window is displayed, the right-hand side of the window is blank.

....

2   Select the desired ASAP type (for example: **ASAP Type STMn Port**) in the ASAP tree and press the **New ASAP** button.

> **Result:**
>
> The ASAP details part is displayed on the right-hand side of the window. The displayed alarm severity assignments correspond to the default ASAP for the selected ASAP type.

....

3   Enter the desired name for the new ASAP into the **ASAP Name** textbox.

An ASAP name may consist of up to 24 alphanumeric characters.

....

4 Modify the assigned alarm severities for the individual alarms in the **Probable Cause** column by clicking on the respective entry in the **SA Alarm Level** or **NSA Alarm Level** column and selecting the desired alarm severity from the list of possible alarm severities that pops up.

5 Verify that all your settings are correct.

6 Apply your changes by pressing the **Apply** button.

7 Press the **Close** button to dismiss the **Provision Alarm Severity Profile** window.

E N D   O F   S T E P S

Supporting information

Relevant *WaveStar*® CIT window

The following figure shows the **Provision Alarm Severity Profile** window.

Creating a non-reporting alarm severity assignment profile

Overview

....
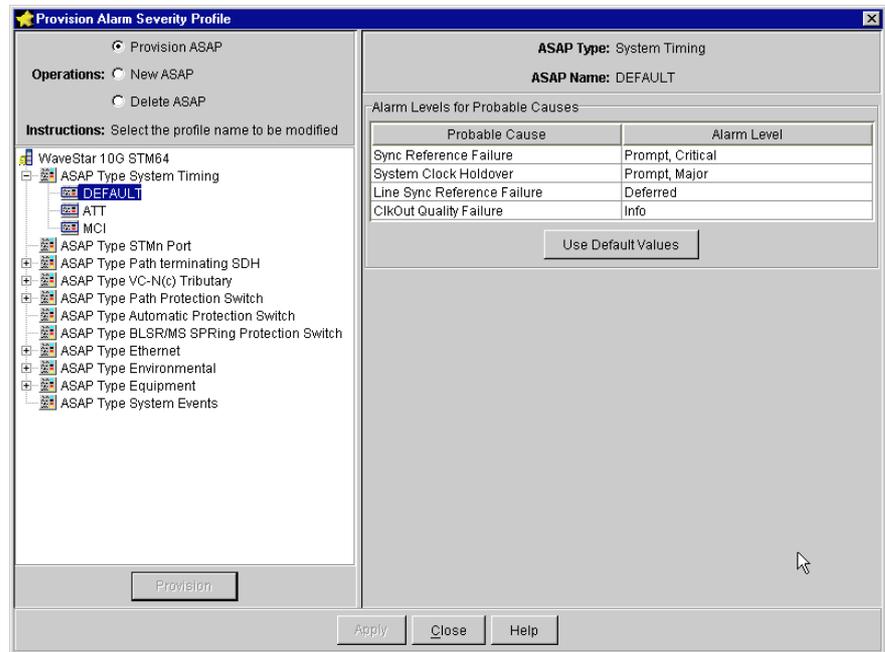
Purpose   Use this procedure to create a non-reporting Alarm Severity Assignment Profile (ASAP) for an ASAP of the "STMn Port" or "VC-N(c) Tributary" type.

Related information   For related information, see:

- "Alarm severity assignment profiles" (16-28)
- Chapter 24, " *WaveStar*® CIT Tutorial"

⌐

....

5 - 6   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

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 code

You must have at least a privilege code of:

- M1
  to view alarm severity assignment profiles,

- M3
  to provision alarm severity assignment profiles.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a non-reporting ASAP:

....

1   From the *WaveStar* CIT **System View** or **Shelf View** main menu,
select **Configuration** → **Alarms** → **Create NonReporting ASAPs ...**.

> **Result:**
>
> The **Create NonReporting ASAP Profiles** window opens.

....

2   Move all those ASAP types for which you want to create a
non-reporting ASAP from the **Available ASAP Types** list on the left
to the **Selected ASAP Types** list on the right.

You can either move single ASAP types one by one or all listed
ASAP types at once.

1. To move a single ASAP type, select the desired ASAP type from
   the **Available ASAP Types** list and press the **Add** button.
   Alternatively, you can also double click on the desired ASAP
   type.

2. To move all listed ASAP types at once, press the **Add All** button.

....

3   When the **Selected ASAP Types** list contains all those ASAP types
for which you want to create a non-reporting ASAP, click **OK** and
confirm your selection by clicking **Yes** in the confirmation window.

....

Result:

For all ASAPs in the **Selected ASAP Types** list a new ASAP
named "NonReporting" is created.

....

4 Click **Close** to dismiss the **Create NonReporting ASAP Profiles**
window.

E N D   O F   S T E P S

....

⌐

Supporting information

Relevant *WaveStar*® CIT window   The follwowing figure shows the **Create NonReporting ASAP Profiles** window.
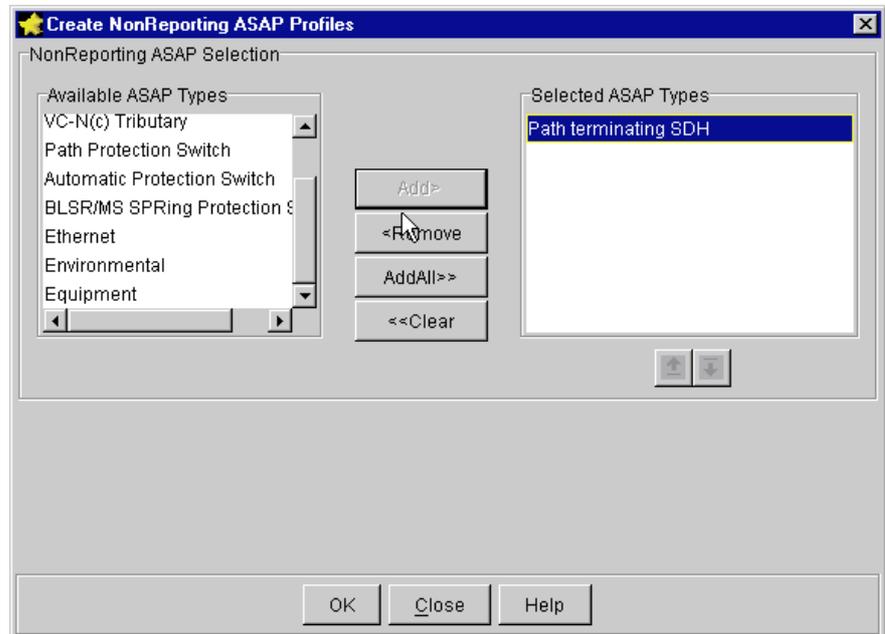
Modifying an existing alarm severity assignment profile

Overview

Purpose   Use this procedure to modify alarm severity assignments.

Note

In the present WaveStar™ TDM 10G (STM-64) release, apart from the "STMn Port" and "VC-N(c) Tributary" ASAP types, only the default ASAP of each ASAP type can be assigned to a functional system component.

Related information   For related information, see:

* "Alarm severity assignment profiles" (16-28)

* Chapter 24, " *WaveStar*® CIT Tutorial"

Lucent Technologies

Procedure

....

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 code

You must have at least a privilege code of:

- M1
  to view ASAPs,

- M3
  to create or provision ASAPs.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to modify an existing ASAP:

....

1 From the *WaveStar* CIT **System View** or **Shelf View** main menu,
select **Configuration** → **Alarms** → **Alarm Severity Assignment
Profiles ...**

   Result:

   The **Provision Alarm Severity Profile** window opens.

   Initially, only the ASAP selection part ("ASAP tree") on the
   left-hand side of the window is displayed, the right-hand side of
   the window is blank.

....

2 Select the ASAP to be modified in the ASAP tree by clicking on the
'+' sign next to the respective ASAP type and selecting the ASAP
from the expanded list.

....

3 Press the **Provision** button to rename the ASAP and/or modify the
alarm severity assignments.

   Result:

   The ASAP details part is displayed on the right-hand side of the
   window. The displayed alarm severity assignments correspond to
   the selected ASAP type.

....

....

4   To rename the ASAP, enter the new ASAP name into the **New Name** textbox.

Important! It is not possible to rename the *DEFAULT* ASAP.

An ASAP name may consist of up to 24 alphanumeric characters.

....

5   To modify alarm severity assignments for the individual alarms in the **Probable Cause** column, click on the respective entry in the **SA Alarm Level** or **NSA Alarm Level** column and select the desired alarm severity from the list of possible alarm severities that pops up.

....

6   Verify that all your settings are correct.

....

7   Apply your changes by pressing the **Apply** button.

....

8   Press the **Close** button to close the **Provision Alarm Severity Profile** window.

E ND OF S TEPS
....

....

Supporting information

Relevant *WaveStar*® CIT window

The follwowing figure shows the **Provision Alarm Severity Profile** window.
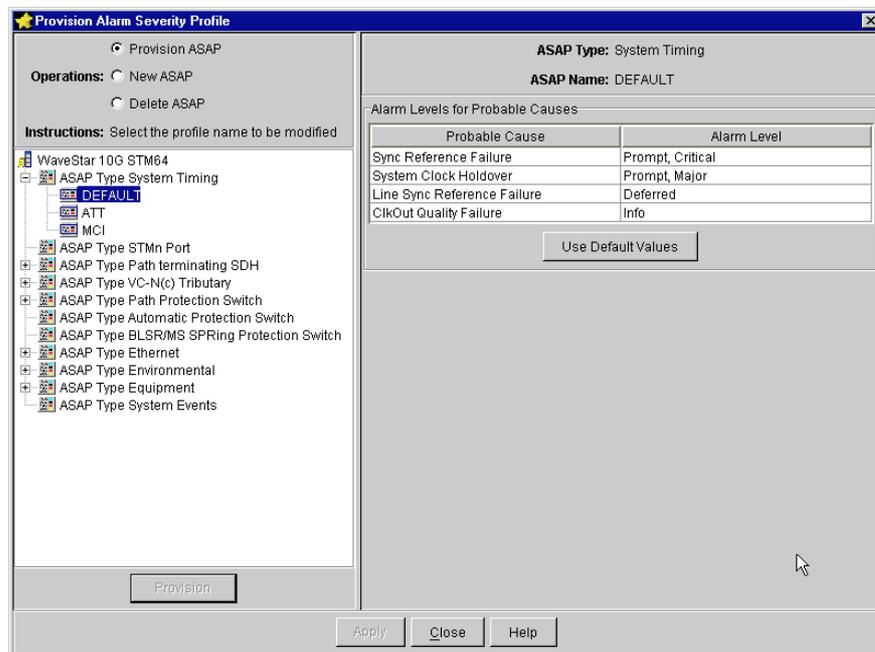
Configuring validation times and office alarm signalling

Overview

Purpose   Use this procedure to:

- configure validation times for communication (facility) and
  equipment alarms,
  and/or

- to enable or disable office alarm signalling.

Related information   For related information, please refer to:

- "Office alarms interface" (16-52)

- "Fault management" (16-2)

- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least a privilege code of M3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to enable or disable office alarm
signalling.

....

1 From the **System View** main menu select **Configuration** → **Alarms**
→ **Alarm Configuration...**

....

2 According to your needs, enable or disable office alarm signalling by
either selecting **Enabled** or **Disabled** in the **Office Alarm** group box.

Important! The remaining group boxes in this window are for
configuring validation times for communication (facility) and
equipment alarms.

....

3 You may now proceed working in the **Alarm Configuration
Provisioning** window to configure validation times for
communication and equipment alarms.

IF ...	THEN ...
you only want to enable or disable office alarm signalling	click **OK** to apply your changes and to dismiss the window. Stop! End of Task.
you also want to configure validation times	continue with Step 4.

....

4 Configure the **Alarm-Generate Delay** and **Alarm-Clear Delay**
parameters in accordance with the configuration guidelines given in
"Configuration guidelines" (5-17).

....

....

5   Click **OK** to apply your changes and to dismiss the window.

E ND OF S TEPS

....

Supporting information

....

You may use the **Alarm Configuration Provisioning** window to
specify, generate and clear validation times (**Alarm-Generate Delay**,
Alarm-Clear Delay) for both equipment and communication (facility)
faults, and to enable or disable office alarms signalling.
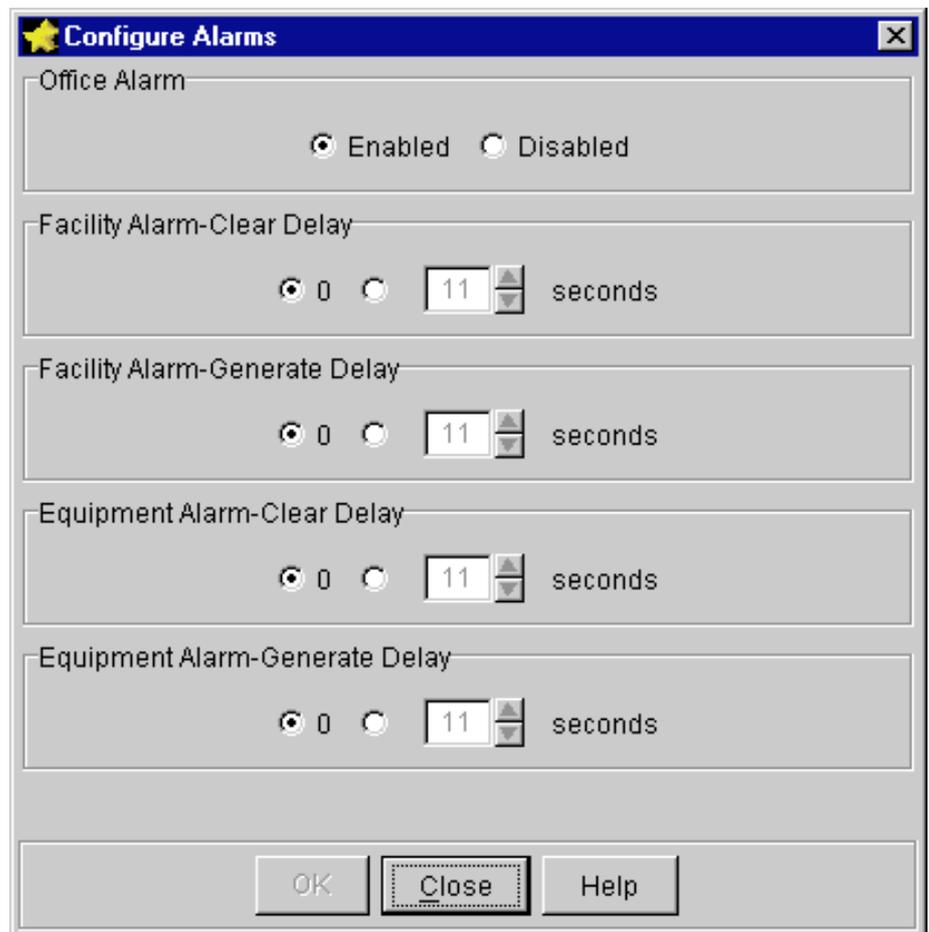
Configuration guidelines

Important! The facility **Alarm-Generate Delay** and **Alarm-Clear
Delay** parameters must be set to equal values in order to maintain
simultaneous clearing of a masked lower-priority facility alarm when
a masking higher-priority alarm occurs. Otherwise, a corresponding
error message is displayed, and the configuration attempt is rejected.

....

The following rules apply to the permitted value range of the
validation times:

- All **Alarm-Generate Delay** and **Alarm-Clear Delay** parameters
  can be either 0 seconds or any value between 11 and 60 seconds
  (in steps of one second).

- **Facility Alarm-Generate Delay** must be less than or equal to
  Facility Alarm-Clear Delay.

- **Equipment Alarm-Generate Delay** must be less than or equal to
  Facility Alarm-Clear Delay.

- **Equipment Alarm-Generate Delay** must be less than or equal to
  Equipment Alarm-Clear Delay.

- The default setting for all **Alarm-Generate Delay** and
  Alarm-Clear Delay parameters is 0 seconds.

Input Data Error ✕

⚠ Data Validation failed:
Invalid value for Equipment Alarm-Generate Delay,
valid range is from 11 to 60, and must not be
greater than neither the Facility Alarm-Clear Delay
value, nor the Equipment Alarm-Clear Delay value.

OK
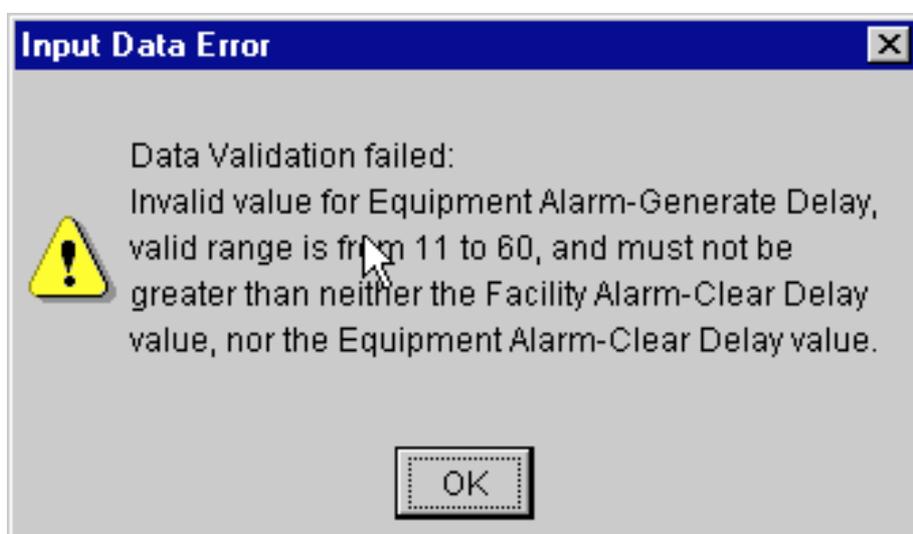
Setting the port monitoring mode

Overview

Purpose Use this procedure to configure the port monitoring mode for a port unit.

Related information For related information, please refer to:

- "Port and tributary provisioning" (15-28)
- "Port monitoring mode" (16-39)
- Chapter 24, " *WaveStar*® CIT Tutorial"

....

365-371-522
Issue b, October 2001

Lucent Technologies

5 - 1 9

Procedure

....

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 code

You must have at least a privilege code of P3 to configure the port monitoring mode.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to configure the port monitoring mode for a port unit:
....

1   Invoke any one of the two relevant *WaveStar* CIT windows.

- From the **System View** main menu select **Configuration** →
  Provision...to invoke the **Provision Parameters for Protection
  Group or Equipment** window. Subsequently an SDH port must
  be specified by using the Windows-style Explorer or by entering
  the relevant AID.

- In the shelf display right-click on the alarm LED of a port unit.
  In the now open pop-up menu select the **Provision Port #** menu
  item to invoke the **Provision Port** window.

The **Port Mode** drop-down list box indicates the actual setting of the
port monitoring mode.

....

2   Set the port monitoring mode according to your needs to either **Auto**,
Monitored or **Not Monitored**.

Auto	Port monitoring is disabled. However, as soon as a valid input signal is detected, the port monitoring mode is automatically switched to **Monitored**.
Monitored	The incoming port signal is monitored for defects.
Not Monitored	Port monitoring is disabled.

....

....

3   In the **Apply To** drop-down list box, you may now choose whether
the settings you made shall apply:

- only to the selected port (**This Port Only**),

- to all ports of the specified type on the selected circuit pack (**All
Ports of this type, This Pack**), or

- to all ports of the specified type within the selected shelf (**All
Ports of this type**, **This Shelf**).

If you choose one of the latter two options you will next have the
opportunity to apply either only the previously changed settings or all
settings currently valid.

....

4   Click **Apply** in the **Provision Parameters for Protection Group or
Equipment** window or **OK** in the **Provision Port** window.

....

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

E ND   OF   S TEPS
....

....

Supporting information

Relevant *WaveStar*® CIT window for an STM-1 port unit

The following figure shows the **Provision Parameters for Protection Group or Equipment** window for an STM-1 port unit as an example.
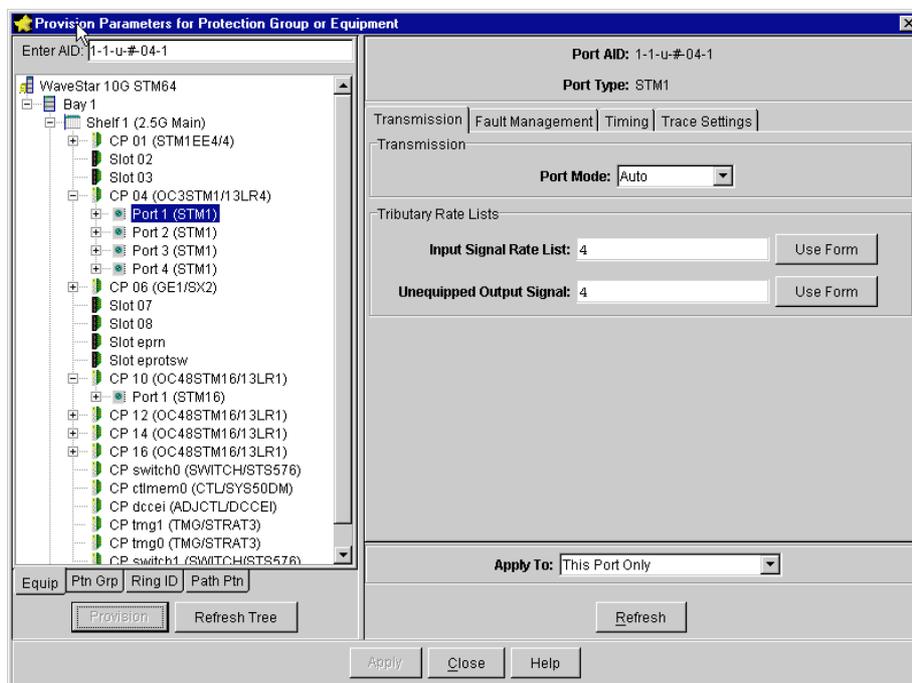
Relevant *WaveStar* CIT window for an STM-16 port unit

The following figure shows the **Provision Parameters for Protection Group or Equipment** window for an STM-16 port unit as an example.
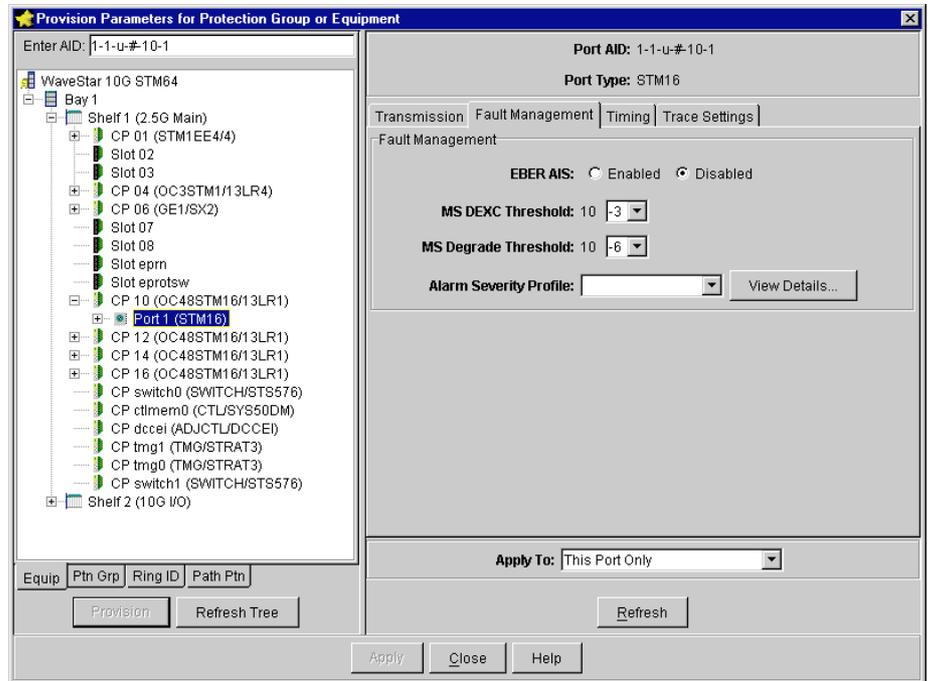
Configuring port-related fault management parameters for an STM-N port

Overview

Purpose   Use this procedure to perform the following:

- Enable/disable consequent actions (insertion of AIS and RDI) in case of an excessive bit error ratio in the Multiplex Section,

- Configure all relevant Forward Error Correction (FEC) parameters (only relevant for STM-64 ports),

- Configure thresholds for bit error monitoring in the Multiplex Section,

- Assign an Alarm Severity Assignment Profile (ASAP) to the selected port.

Related information   For related information, please refer to:

- "Alarm provisioning" (16-25)

- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least a privilege code of P3 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to configure port-related fault
management parameters:

....

1 Invoke any one of the two relevant *WaveStar* CIT windows.

- From the **System View** main menu select **Configuration** →
  Provision...to invoke the **Provision Parameters for Protection
  Group or Equipment** window. Subsequently an SDH port must
  be specified by using the Windows-style Explorer or by entering
  the relevant AID.

- In the shelf display right-click on the alarm LED of a port unit.
  In the now open pop-up menu select the **Provision Port #** menu
  item to invoke the **Provision Port** window.

The **Port Mode** drop-down list box indicates the actual setting of the
port monitoring mode.

....

2 Select the **Fault management** tab.

....

3

IF ...	THEN ...
you wish an excessive bit error ratio in the Multiplex Section to cause consequent actions (insertion of AIS and RDI)	select the **Enabled** option for **EBER AIS**.

....

Configuring port-related fault management
parameters for an STM-N port
Procedure

Alarm management

IF ...	THEN ...
you wish an excessive bit error ratio in the Multiplex Section to **not** cause consequent actions (insertion of AIS and RDI)	select the **Disabled** option for **EBER AIS**. This is the default setting.

....

4 Please continue with Step 10 for ports of any type other than
STM-64.

....

5 For STM-64 ports, you may now configure all relevant Forward Error
Correction (FEC) parameters.

Important! Modifying the FEC parameters during operation may be
traffic affecting. Therefore, it is recommended to configure all FEC
parameters prior to putting the corresponding OC192/STM64 circuit
pack into operation and leave them unchanged during operation, if
possible.

> **Reference:**
>
> Please refer to "Forward error correction" (16-40) for related
> information.

....

6 Please refer to Step 7 to Step 9 for configuring the FEC parameters
for an STM-64 port. Otherwise, please continue with Step 10.

....

7 Enable or disable the **Forward Error Correction** (FEC) by selecting
the **Enabled** or **Disabled** option, respectively, for **FEC Enable**.

Enabling the FEC mode means that the required FEC information will
be calculated and processed.

Important! In the case of in-band FEC, enabling the FEC decoder at
the receiver while no BCH-encoded signal is transmitted leads to B1
bit errors being detected erroneously. Therefore, make sure that the
FEC decoder is enabled only if a BCH-encoded signal is transmitted.
The reporting of RS-SES and RS-UAS threshold crossing alarms may
be an indicator for a wrong FEC configuration.

....

8 Define the type of FEC to be applied by means of the **FEC Type
checkboxes.**

....

Configuring port-related fault management
parameters for an STM-N port
Procedure

Alarm management

Possible values are:

- **In-band** (default value)

- **Out-band**

Important! Do not provision FEC Out-band on LEY67 CPs.

....

9   Provided that the FEC mode is enabled (cf. Step 7) you may start or
stop the FEC bit error correction at any time by selecting the **Enabled**
or **Disabled** option, respectively, for **FEC Correction Enable**.

....

10 If desired, set the **MS DEXC Threshold** to one of the following
values:

- 10^{-3} (default value)

- 10^{-4}

- 10^{-5}

The configured threshold defines the bit error ratio in the Multiplex
Section that must be exceeded before an "MSect Excessive Error"
alarm is reported.

....

11 If desired, set the **MS DEG Threshold** to one of the following values:

- 10^{-5}

- 10^{-6} (default value)

- 10^{-7}

- 10^{-8}

- 10^{-9}

The configured threshold defines the bit error ratio in the Multiplex
Section that must be exceeded before an "MSect Signal Degrade"
alarm is reported.

....

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

....

Configuring port-related fault management
parameters for an STM-N port
Procedure

Alarm management

....

13   In the **Apply To** drop-down list box, you may now choose whether
the settings you made shall apply:

- only to the selected port (**This Port Only**),

- to all ports of the specified type on the selected circuit pack
(**All Ports of this type, This Pack**), or

- to all ports of the specified type within the selected shelf
(**All Ports of this type, This Shelf**).

If you choose one of the latter two options you will next have the
opportunity to apply either only the previously changed settings or all
settings currently valid.

....

14   Click **Apply** in the **Provision Parameters for Protection Group or
Equipment** window or **OK** in the **Provision Port** window.

....

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

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

....

5 - 2 8   **Lucent Technologies**   365-371-522
                                                                                  Issue b, October 2001

Supporting information

....

Relevant *WaveStar*® CIT window for an STM-1 port unit

The following window shows the **Provision Parameters for Protection Group or Equipment** window for an STM-64 port as an example.
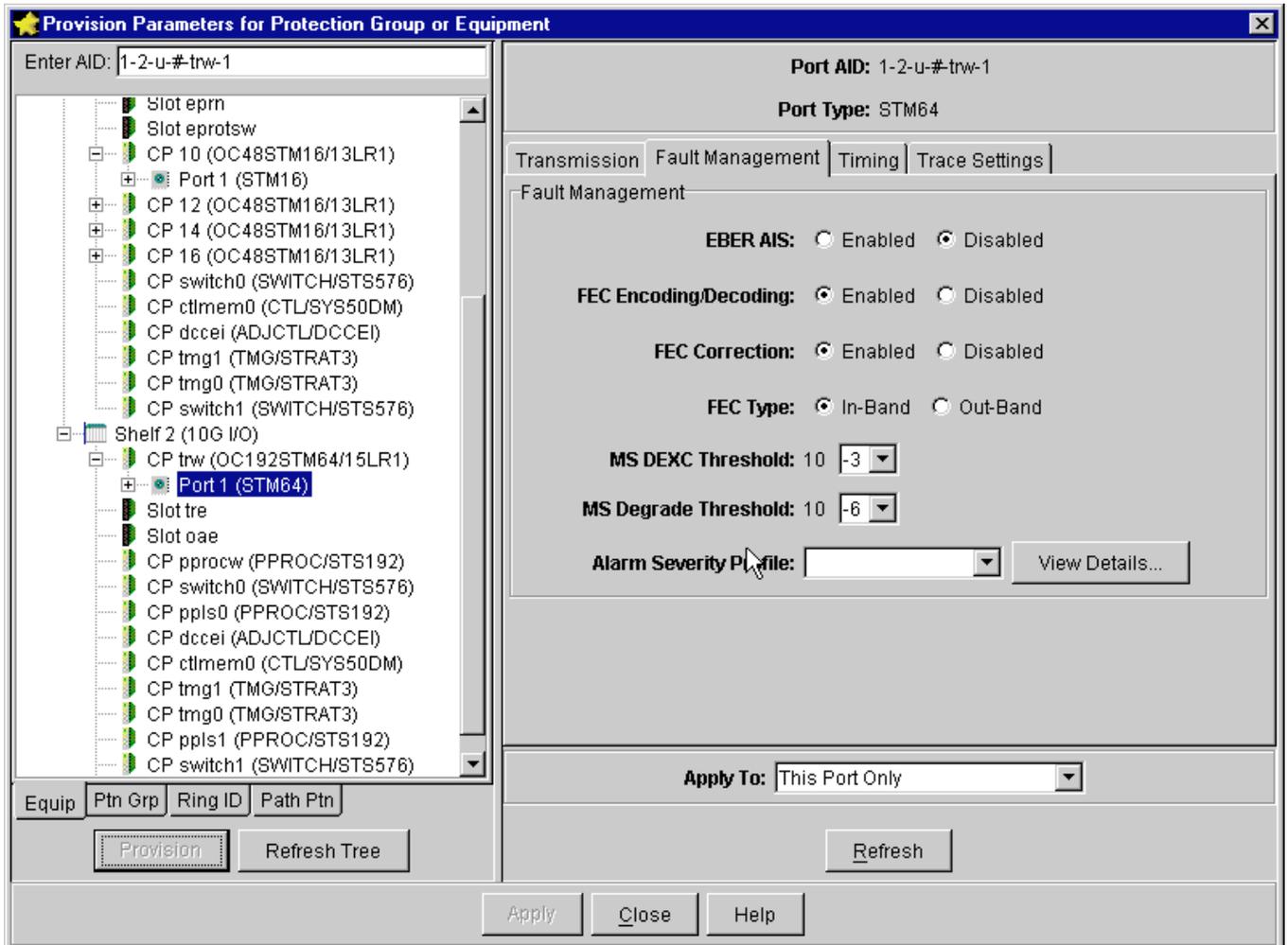
Configuring port-related fault management
parameters for an STM-N port
Supporting information

Alarm management

Relevant *WaveStar* CIT window for an STM-16 port unit

The following figure shows the **Provision Parameters for Protection Group or Equipment** window for an STM-16 port unit as an example.
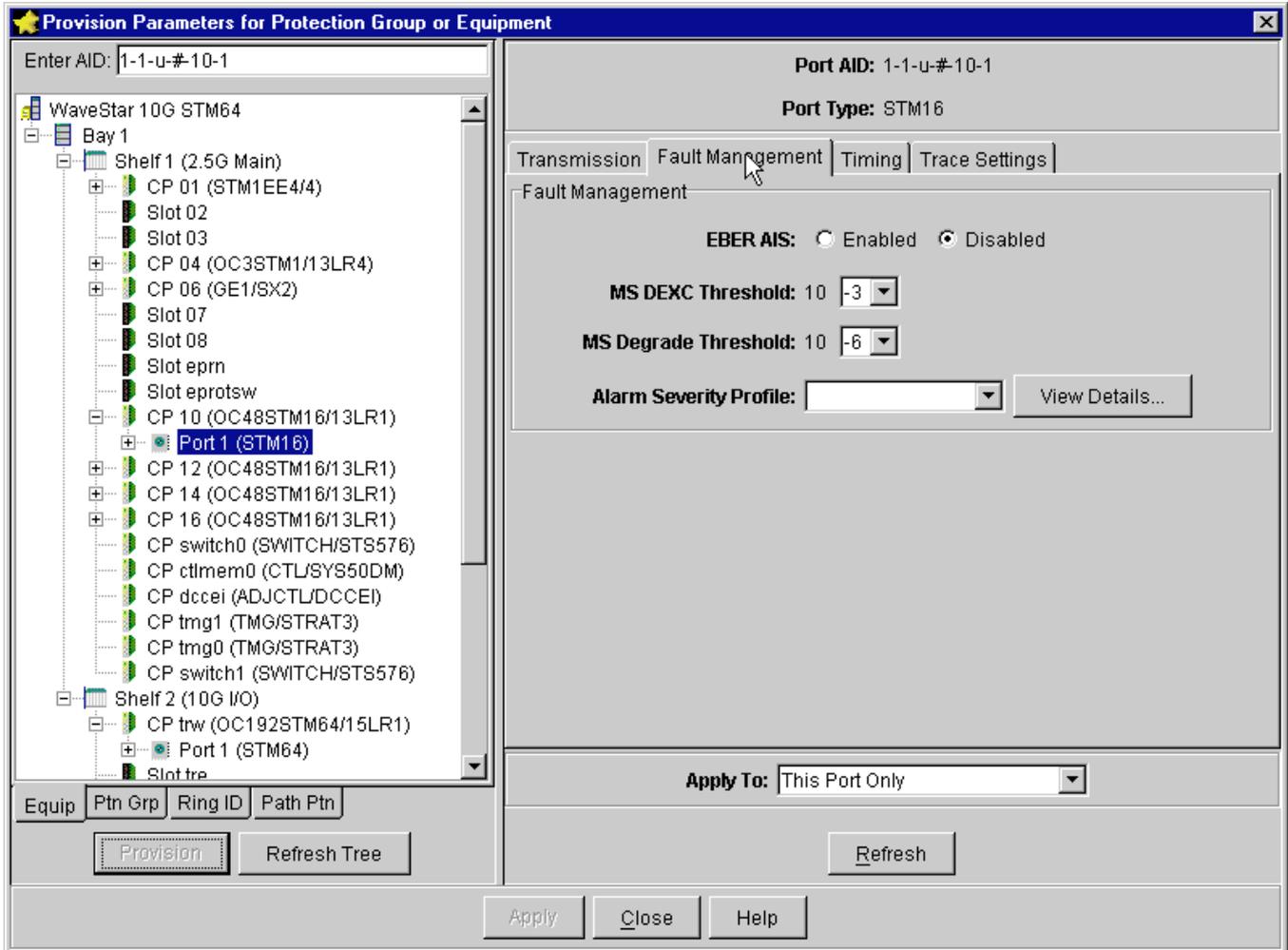
Performing an LED test

Overview

....

Purpose Use this procedure to test the correct functioning of the user panel and circuit pack LEDs.

Please note that the **PWR ON LED** on the user panel and the fan unit LEDs are not affected by the LED test.

Two possible ways There are two possible ways to perform an LED test:

- by using the *WaveStar*® CIT (please refer to "Procedure: LED test using the *WaveStar* CIT" (5-32)), or

- by pushing the LED TEST button on the user panel (please refer to "Procedure: LED test using the LED TEST button on the user panel" (5-35)).

Related information For related information, please refer to:

- "User panel" (16-43)

- Chapter 24, "*WaveStar* CIT Tutorial"

Procedure: LED test using the *WaveStar*® CIT

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 code

You must have at least a privilege code of M2 to perform this task.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions **Important!** After an LED test the restoration of the LED state before the test may be delayed for some seconds on certain circuit packs.

Complete the following steps to test the correct functioning of the user panel and circuit pack LEDs:

1 At the *WaveStar* CIT, select **Fault → Test → LED...** from the **System View** main menu.

2 Select a shelf in the **Test LED** equipment selection window, depending on which LEDs shall be tested.

3

If you want to perform the LED test for	then select the
the main shelf (user panel, low-speed part, high-speed part),	select the low-speed part of the main shelf.
the high-speed part of the main shelf only,	select the high-speed part of the main shelf.
the extension shelf,	select the extension shelf.

Performing an LED test
Procedure: LED test using the *WaveStar*®
CIT

Alarm management

....

4 Specify the **Number Of Iterations** (test cycles) by means of the associated drop-down list box. Two iterations are suggested.

....
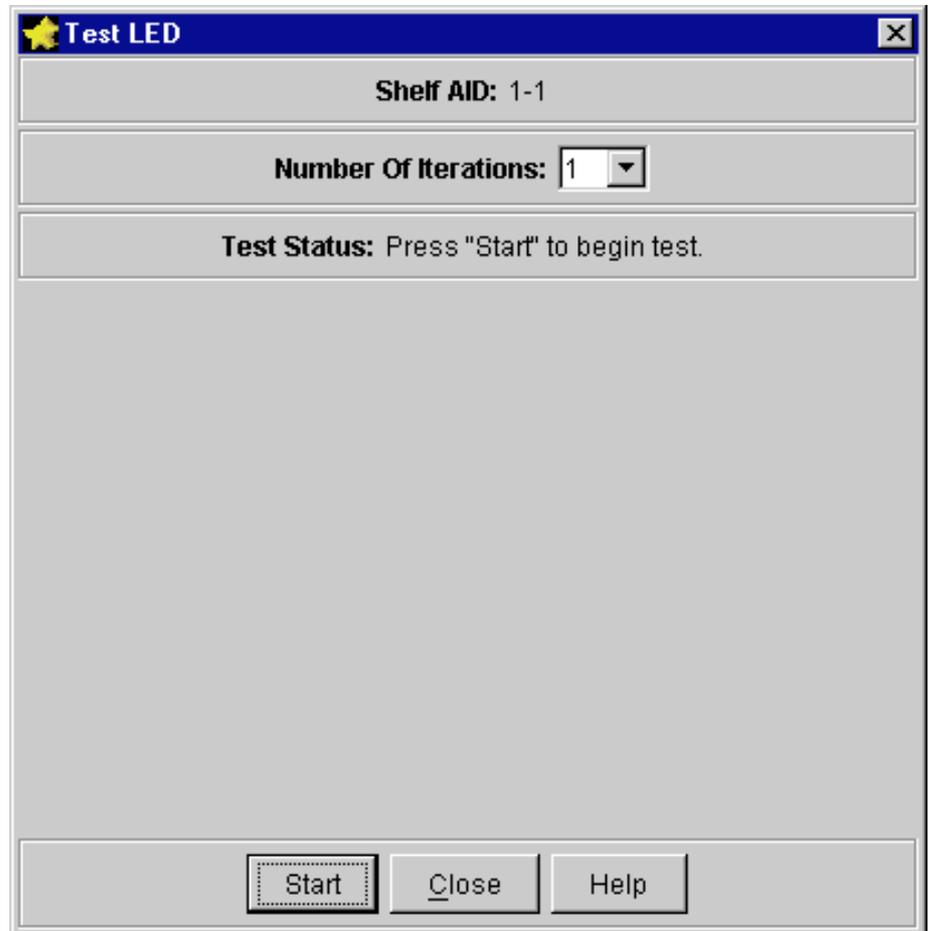
5 Click **Start** and confirm the **Test LED Confirmation** window.

....

Performing an LED test
Procedure: LED test using the *WaveStar*®
CIT

Alarm management

Result:

For each test cycle the sequence of LED indications should be as follows:

1.   When the low-speed part of the main shelf is selected:

a.   The LEDs on the main shelf's user panel (except the PWR ON LED) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

b.   The LEDs on the circuit packs of the low-speed part of the main shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

c.   The LEDs on the circuit packs of the high-speed part of the main shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

2.   When the high-speed part of the main shelf is selected:
The LEDs on the circuit packs of the high-speed part of the main shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

3.   When the extension shelf is selected:

a.   The LEDs on the extension shelf's user panel (except the PWR ON LED) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

b.   The LEDs on the circuit packs of the extension shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

The **Test LED** window is automatically closed when the test has finished.

E N D   O F   S T E P S

Procedure: LED test using the LED TEST button on the user panel

Instructions   **Important!** The number of test cycles for the LED test initiated via the LED TEST button is limited to one. After an LED test the restoration of the LED state before the test may be delayed for some seconds on certain circuit packs.

Complete the following step to test the correct functioning of the user panel and circuit pack LEDs.

1   Press the LED TEST button on the user panel.

ᴇɴᴅ ᴏꜰ Sᴛᴇᴘs

Sequence of LED indications   The sequence of LED indications should be as follows:

1. When the LED TEST button on the main shelf's user panel is pushed:

    a.   The LEDs on the main shelf's user panel (except the PWR ON LED) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence,

    b.   the LEDs on the circuit packs of the low-speed part of the main shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence,

    c.   the LEDs on the circuit packs of the high-speed part of the main shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

2. When the LED TEST button on the extension shelf's user panel is pushed:

    a.   The LEDs on the extension shelf's user panel (except the PWR ON LED) turn on for 2 seconds and subsequently off for 2 seconds three times in sequence,

    b.   the LEDs on the circuit packs of the extension shelf turn on for 2 seconds and subsequently off for 2 seconds three times in sequence.

Performing an office alarm test

Overview

Purpose   Use this procedure to perform an office alarm test.

An office alarm test serves to verify the connection of the alarming equipment, including external office alarm equipment. The alarm indicators activated by an office alarm test are the visual and audible office alarm outputs, and the CR, MJ and MN LEDs on the user panel.

Related Information   For related information, please refer to:

- "Operations interfaces" (16-42)
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least a privilege code of M2 to perform this task.

Required equipment

The following equipment is required to perform this task:

WaveStar® CIT

Instructions   Proceed as follows to complete the alarm test:

....

1   From the **System View** or **Shelf View** main menu of the *WaveStar* CIT, select **Fault → Test → Office Alarm...** .

....

2   Select a shelf in the rack for which the office alarm signalling shall be tested.

....

365-371-522   **Lucent Technologies**   5 - 3 7
Issue b, October 2001

....

3 Select the **Number Of Iterations** (test cycles) using the associated
drop-down list box. Two iterations are suggested.

....

4 Click **Start**, then **Yes** in the confirmation window.

Important! During an office alarm test a rack alarm lamp remains lit
if an alarm of the corresponding severity is present for any of the
shelves in the rack.

> **Result:**
>
> The **Test Office Alarm** window is automatically closed when the
> test has finished.

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

....

Lucent Technologies

Expected sequence of LED indications:

Please refer to "ACO interaction with an alarm test" (16-48)

Performing a laser restart

Overview

Purpose Use this procedure if you want to request a laser restart for test purposes.

Related Information For related information, please refer to:

- "Automatic laser shutdown" (16-37)
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least the privilege codes S4 and P1 to perform this task.

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 screen is displayed.
....

2   In the Shelf2 (10G I/O) select an optical port from a unit supporting the ALS function.

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/WDM9310 (LEY228)
....

3   Click the **Select** pushbutton.

    Result:

    The **Laser Restart** window is displayed.
....

4   Check if the **Provisioned Laser State** is **ON**.

To set the **Provisioned Laser State** refer to "Switching a laser permanently on" (5-47)

....

....

5 Select the desired value in the field **Laser Restart Period**.

> **Reference:**
>
> Please refer to "Supporting information" (5-43) for the description of the parameters.

....

6 Click on **Restart Laser**.

> **Result:**
>
> When the user restarts the laser for a 90 seconds period, a Laser Safety Warning Screen Confirmation is displayed.

....

7 Click on **Yes** to execute the command.

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

⌐

....

Supporting information

Provisionable parameters for *Laser Restart*

The following table shows which parameters are displayed in the **Laser Restart** window, and explains them:

Parameter	Values	Meaning
ALS Mode	Enable	displays the actual ALS mode
	Disable	
Provisioned Laser State	OFF	displays the provisioned laser state
	ON	
Actual Laser State	OFF,	displays the actual laser state.
	ON,	
	ON 2 SECONDS,	
	ON 90 SECONDS	
Laser Restart Period	2s	Selects the period for which the laser shall be restarted.
	90s	

Deactivating or activating Automatic Laser Shutdown ALS

Overview

Purpose   Use this procedure if you want to deactivate or activate Automatic Laser Shutdown ALS.

Related Information   For related information, please refer to:

- "Automatic laser shutdown" (16-37)
- Chapter 24, " *WaveStar*® CIT Tutorial"

⌐

Procedure

....

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 code

You must have at least the privilege codes S4 and P1 to perform this task.

Required equipment

The following equipment is required to perform this task:

WaveStar® CIT

Instructions   Proceed as follows to deactivate or activate Automatic Laser Shutdown ALS:

....

1   From the **System View** or **Shelf View** main menu of the *WaveStar* CIT, select **Configuration** → **Provision...** .

> **Result:**
>
> On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   In the Shelf2 (10G I/O) select an optical port from a unit supporting the ALS function.

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/WDM9310 (LEY228)

....

3   Click the **Select** pushbutton.

> **Result:**
>
> On the right side of the window several tabs containing the provisionable parameters for the selected optical port are displayed.

....

....

4 In the **ALS** tab disable or enable the **ALS Mode**.

> **Reference:**
>
> Please refer to "Supporting information" (5-43) for the
> description of the parameters.

....

5 Click on **Apply**.

E ND   OF   S TEPS
....

Switching a laser permanently on

Overview

Purpose   Use this procedure if you want to switch a laser permanently on.

Related Information   For related information, please refer to:

- "Automatic laser shutdown" (16-37)
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least the privilege codes S4 and P1 to perform this task.

Required equipment

The following equipment is required to perform this task:

WaveStar® CIT

Instructions   Proceed as follows to permanently switch a laser ***on***:

....

1   From the **System View** or **Shelf View** main menu of the *WaveStar* CIT, select **Configuration → Provision...** .

   Result:

   On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   In the Shelf2 (10G I/O) select an optical port from a unit supporting the ALS function.

   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/WDM9310 (LEY228)

....

3   Click the **Select** pushbutton.

   Result:

   On the right side of the window several tabs containing the provisionable parameters for the selected optical port are displayed.

....

....

4   In the **ALS** tab disable the **ALS Mode** and select the radiobutton **ON**
in the field **Provisioned Laser State**.

Reference:

Please refer to "Supporting information" (5-43) for the
description of the parameters.

....

5   Click on **Apply**.

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

Switching a laser permanently off

Overview

Purpose   Use this procedure if you want to switch a laser permanently off.

Related Information   For related information, please refer to:

- "Automatic laser shutdown" (16-37)
- Chapter 24, " *WaveStar*® CIT Tutorial"

Procedure

....

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 code

You must have at least the privilege codes S4 and P1 to perform this task.

Required equipment

The following equipment is required to perform this task:

WaveStar® CIT

Instructions   Proceed as follows to permanently switch a laser *off*:
....

1   From the **System View** or **Shelf View** main menu of the *WaveStar* CIT, select **Configuration** → **Provision...** .

   Result:

   On the left side of the window, the equipment selection tab becomes visible. The shelves belonging to the system are listed.

....

2   In the Shelf2 (10G I/O) select an optical port from a unit supporting the ALS function.

   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/WDM9310 (LEY228).

....

3   Click the **Select** pushbutton.

   Result:

   On the right side of the window several tabs containing the provisionable parameters for the selected optical port are displayed.

....

....

4   In the **ALS** tab disable the **ALS Mode** and select the radiobutton **OFF**
in the field **Provisioned Laser State**.

Reference:

Please refer to "Supporting information" (5-43) for the
description of the parameters.

....

5   Click on **Apply**.

E N D   O F   S T E P S

⌐

....

5 - 5 2   **Lucent Technologies**   365-371-522
                                                                                Issue b, October 2001

6 Timing provisioning

Overview

Purpose   This chapter describes the procedures which have to be performed for the configuration of the system timing of the *WaveStar*® TDM 10G (STM-64).

Contents

Viewing the timing configuration

Overview

Purpose   Use this procedure to view the configuration of the external timing input and output ports, the timing reference and the system timing.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"

Procedure

.... 6 - 3

Before you begin Prior to performing this task, verify that a *WaveStar*® CIT is connected and logged into the *WaveStar* TDM 10G system.

Required privilege code

You must have at least a privilege code of P1, Provisioning to query the data of the timing configuration.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the data of the timing configuration:

....

1 In the **System View** of the *WaveStar* CIT, select **View** → **Timing/Sync**

   Result:

   The **View Timing/Sync** window appears with the active **External Timing Input Ports** tab.

   The corresponding parameters are described in "Configuring the external timing input ports" (6-12).

....

2 Click on the tab **External Timing Output Ports** to query the data on the timing output port. The corresponding parameters are described in "Configuring the external timing output ports" (6-14).

....

3 Click on the **Timing Reference** tab to query the data on the configured timing reference source. The corresponding parameters are described in "Configuring the timing references" (6-17).

....

4 Click on the **System Timing** tab to query the data on the internal SDH Equipment Clock (SEC). The corresponding parameters are described in "Configuring the system timing" (6-21).

....

5 Click on **Close** to quit the window.

   END OF STEPS

....

365-371-522
Issue b, October 2001

Lucent Technologies

6 - 3

Parameters of the "View Timing/Sync" window

Overview The window **View Timing/Sync** contains four tabs:

- **External Timing Input Ports**
- **External Timing Output Ports**
- **Timing Reference**
- **System Timing**

The corresponding parameters are described as follows.

Pushbutton The window has one pushbutton. Via **Close** the window is closed.

The *External Timing Input Ports* tab The first tab displays the external timing input ports.

Description *WaveStar*® TDM 10G provides two external timing input ports. Thus the **External Timing Input Ports** tab consists of two group boxes, one for each port. Each group box contains two information fields.

External Timing Port AID The information field **External Timing Port AID** displays the Access Identifier (AID) of the external timing input ports. Possible values are:

- **exttmg0**
- **exttmg1**

Timing Input Format The information field **Timing Input Format** displays the format of the incoming timing signal. The displayed values can be:

- **2 MHz**
- **2 Mbit - framed**
- **2 Mbit - unframed**

Quality Level Input The information field **Quality Level Input** displays the quality of the incoming timing signal.

The following values are possible (in order from highest to lowest quality):

1. PRC (Primary Reference Clock)
2. SSUT (Synchronization Supply Clock (Transit node)
3. SSUL (Synchronization Supply Clock (Local node)
4. SEC (SDH Equipment Clock)
5. DNU (Do not use for synchronization)
6. Invalid

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

The *External Timing Output Ports* tab

WaveStar TDM 10G provides two external timing output ports. A 2 MHz or 2 Mbit/s timing signal can be derived from the internal system clock and forwarded to the output ports. A timing signal can be derived from the system clock and is forwarded to both external timing outputs in parallel. It can be used as synchronization signal for an external network. The timing signal can also be derived from the six possible line references, choosen by the selection SETG (system clock) or TLS (lines).

The tab **External Timing Output Ports** of the window **View Timing/Sync** displays data on the timing output port (**exttmg0_out**).

Timing Output Port Quality Level

This information field shows the quality (the value of the Synchronization Status Marker, SSM) of the outgoing timing signal.

The following values are possible (in order from highest to lowest quality):

1. PRC (Primary Reference Clock)

2. SSUT (Synchronization Supply Clock (Transit node)

3. SSUL (Synchronization Supply Clock (Local node)

4. SEC (SDH Equipment Clock)

5. DNU (Do not use for synchronization)

Timing Output Format

This parameter shows the signal format of the outgoing timing signal. **2 MHz**, **2 Mbit/s-framed** and **2 Mbit/s-unframed** are possible.

Derived Output Timing Enable

This parameter shows whether a timing signal is derived from the system clock and forwarded to the output port.

The values are

•   **Enable**

•   **Disable**

Provisioned Derived Output Timing Source Selection

This parameter shows from which source the external timing signal is derived.

Possible values are:

•   **TLS**
    The external timing signal is derived from one of the six line timing references.

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

The selection criteria are the same as for **system timing apply** except the following:

- signals with derived output priority enabled

- signals with derived output lockout status set to **No Lockout**

- **SETG**
  The timing output is derived from the system clock

External reference signals (extref1 and extref2) can not be selected.

Output Signal Status This parameter describes the Status of the outgoing timing signal.

It can take the values

- **Normal**

- **Disable**

- **Unacceptable**

Sync Message Force DUS/DNU Enable This parameter defines whether DNU is inserted in the outgoing timing signal.

The following values are possible

- **Enable**

- **Disable**

External Timing Port Impedance This parameter displays the impedance of the external timing input and output ports.

The following values are possible

- **120 ohms**

- **75 ohms**

The *Timing Reference* tab The **Timing Reference** tab of the **View Timing/Sync** window displays data on the configured timing reference source.

Active Timing Reference In the group box **System Timing Reference**, the information field **Active Timing Reference** displays the reference timing signal which is currently selected. The timing reference is an external signal to which the internal SDH Equipment Clock (SEC) is locked.

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

The following signals can be used as timing reference:

- 2 external net clock input signals (2048 kHz or 2048 kbit/s acc. to G.703)

- 6 reference signals derived from the incoming STM-16, STM-4 or STM-1 tributary signals or the incoming STM-64 line signals.

Thus the following values can be displayed:

- **extref1** or **extref2** for the external net clock input signals

- **line1** to **line6** for the SDH signals

Output SSM mode A limited SSM (Synchronization Status Marker) feature is supported for framed 2 Mbit/s timing output signals. If the quality level is below a defined value, the signal is replaced by AIS. 2 MHz and unframed 2 Mbit/s signals are squelched in this case.

AIS mode This parameter specifies what value shall be sent if signal is below quality acceptance or if forced DUS is enabled.

The possible values are AIS mode or QL mode.

Acceptance Quality Level for Output Threshold This parameter defines the quality level of the derived timing output signal below which AIS is inserted (in a framed 2 Mbit/s signal) or squelched respectively (2 MHz or unframed 2 Mbit/s signals).

The possible values are:

- PRC (Primary Reference Clock)

- SSUT (Synchronization Supply Clock (Transit node)

- SSUL (Synchronization Supply Clock (Local node)

- SEC (SDH Equipment Clock)

Settings The table on the tab gives an overview of the possible settings of the timing references.

Column	Possible values	Meaning
Timing Reference	**extref1**, **extref2**	Logical designation of the external timing reference signals
	line1, ..., **line6**	Designation of the SDH timing reference
Port AID	**exttmg0**, **exttmg1**	An external net clock input signal is used as timing reference
	Not connected	The respective timing reference source is not used
	<port AID of an SDH timing reference>	The respective SDH timing reference signal is used as timing reference

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

Column	Possible values	Meaning
Reference Priority	**Disable** (initial value), **1**, **2,3, ..., 8**	Configured priority of the timing reference signals
Alarm Level	**MJ** (Major), **MN** (Minor), **NA** (Not-alarmed), **CR** (Critical) or **PR** (Prompt), **DF** (Deferred), **INF** (Info)	Displays the highest alarm severity associated with this timing reference
Signal Status	**NORMAL**	The timing reference signal is fault-free.
	FAILED	The timing reference signal failed.
	WAIT-TO- RESTORE	The timing reference signal has been failed and is now restored. A wait is made for a defined time (wait-to-restore time) to see whether the signal is stable, before the system switches back to it.
	NOT-CONNECTED	The timing reference is not used.
Lockout Status	**LOCKOUT**	The clock protection is deactivated
	NO-LOCKOUT	The clock protection is activated
Timing Ref QL	**DNU**, **PRC**, **SSUT**, **SSUL**, **SEC**	This parameter shows the synchronization messaging quality level value for timing references. This is the value which is forwarded to the timing output ports.
Input QL Status	**VALID**, **INVALID**, **NOT-SUPPORTED**, **NOT-APPLICABLE**	This parameter shows if a valid timing input signal is available for the respective timing reference.
Provisioned QL	**DNU**, **PRC**, **SSUT**, **SSUL**, **SEC**, **AUTO**	This parameter is the quality level SSM value which will be receicved on the timing references.
Output Lockout State	**LOCKOUT**, **NO-LOCKOUT** empty for extref1 and extref2	This parameter shows whether a certain timing reference is locked out as reference from which the timing output signal can be derived.
Output Priority	**DISABLE**, **1 ... 6** empty for extref1 and extref2	This parameter defines the priority according to which the reference for the timing output signal is selected. **DISABLE** indicates that the reference is not used
		Only one of the timing references at a time can be selected as the active one.

The *System Timing* tab The **System Timing** tab on the **View Timing/Sync** window displays data on the internal SDH Equipment Clock (SEC).

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

Description The tab consists of three group boxes **Synchronization Signal**, **Clock** and **System Timing Reference**.

The *Synchronization Signal* group box The following table lists the information fields of the group box **Synchronization Signal**, the possible values and their meaning.

Information field	Possible value	Meaning
System Timing Signal Status	**Normal**	The system clock works correctly.
	Failed	The system clock has failed.
System Quality Level Status	**PRC**, **SSUT**, **SSUL**, **SEC**, **DNU**	The current quality level of the system clock.
Alarm Level	**MJ** (Major), **MN** (Minor), **NA** (Not-alarmed), **CR** (Critical) or **PR** (Prompt), **DF** (Deferred), **INF** (Info)	Displays the highest alarm severity associated with this timing reference.
System Timing Alarm Severity Profile	Default Provisined ASAP	Displays the correspondig ASAP. If no ASAP has been provisioned the active ASAP is the default, if ASAPs have been provisioned one can be made active.
Stratum Level Status	**SEC**	Timing quality of the internal equipment clock acc. to ITU-T Rec. G.813.

The *Clock* group box The following table lists the information fields of the **Clock** group box , the possible values and their meaning.

Information field	Possible value	Meaning
Provisioned Clock Mode	**Free Running** (initial value)	For the internal timing generator the Free Running Mode is selected. It is not locked to an external timing reference signal. The system clock is generated by an internal oscilllator.
	Locked	The Locked Mode is selected. The internal timing generator is locked to an external timing reference signal.
System Clock Mode Status	**Holdover**	The current operating system clock mode is the holdover mode. The active timing generator enters the holdover mode if all timing reference signals fail. In the holdover mode, the active timing generator keeps its internal Stratum 3 clock at the point at which it was synchronized to the last known good reference signal.
	Free Running	The internal timing generator is not locked to an external timing reference signal. The system clock is generated by an internal oscillator.
	Locked	The internal timing generator is locked to an external timing reference signal.

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

Information field	Possible value	Meaning
System Clock Switch Request State	**Forced Holdover**	A forced switch to the holdover mode has been carried out.
	All References Failed	All external timing reference signals failed.
	No Request	No switch request is currently active.
Fast Start Status	**Normal**	Fixed value.
Warm Up Status	**Normal**	The timing circuit pack works normally.
	Warming Up	After a timing circuit pack has been plugged into the shelf, a warm up period of 5 minutes has to pass before the circuit pack is operational. This is displayed via this message.

The group box *System Timing Reference*   The following table lists the information fields of the group box **System Timing Reference**, the possible values and their meaning.

Information field	Possible value	Meaning
System SSM Mode	**Disable, Enable**	The use of SSM information is disabled or enabled. This means that the selection of timing reference for the system timing is either determined only by the provisioned priority list or by the quality level given by the SSM and secondly by the priority list.
Active Reference	**extref1, extref2, line1, line2**	Shows which external reference signal is used, either one of the external clock input signal or one of the SDH signals.
Active Reference Port AID	<port AID of the active system timing reference>	—
Protection Switch Wait To Restore	**0, 20 Seconds, 1 Minute, 2 Minutes... 60 Minutes, infinite**	Selected value of the wait-to-restore time which has to pass before the system switches to another timing reference signal.
Timing Reference Switch Request State	**No Request, Manual, Forced, Wait-to-Restore, Reference Failed**	Value of the Switch Request activated by the user or initiated by the system.

The group box *Output Timing Reference*   The following table lists the information fields of the group box **Output Timing Reference**, the possible values and their meaning.

Viewing the timing configuration
Parameters of the "View Timing/Sync"
window

Timing provisioning

Information field	Possible Value	Meaning
Active derived Timing Output Reference	**Line1 upto Line6**	This field displays the active derived output timing if it is set to TLS (lines).
Active Output Reference Port AID	<port AID of the active output reference>	—
Output Timing Reference Switch request State	**No Request**,**Manual**,**Forced**, **Wait-to-Restore**,**Reference Failed**	Value of the Switch Request activated by user or initiated by the system.

Configuring the external timing input ports

Overview

Purpose   Use this procedure to configure the external timing input ports.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"
- "Viewing the timing configuration" (6-2)
- "The External Timing Input Ports tab" (6-4)

⌐

Procedure

....

Before you begin   Prior to performing this task, you must connect the external timing input ports to an external timing source.

Requires privilege code

You must have at least a privilege code of P3, Provisioning, to configure the external timing input ports.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to configure the external timing input ports:

....

1   In the **System View** of the *WaveStar* CIT select **Configuration** → **Timing/Sync**.

> **Result:**
>
> The window **Provision Timing/Sync** appears with the active tab **External Timing Input Ports.**

....

2   Select the timing input format in the group box **Timing Input Format** by clicking on the respective radio button. Select the format according to the format of the the external clock source. The following values are possible:

- **2 MHz** (initial value)
- **2 Mbit - framed**
- **2 Mbit - unframed**

....

3   Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

> **Result:**
>
> If you have clicked on **OK** or **Cancel,** the window **Provision Timing/Sync** closes. If you have clicked on **Apply,** the window remains open and you can select another tab.

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

....

Configuring the external timing output ports

Overview

Purpose   Use this procedure to configure the external timing output ports.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"

- "Viewing the timing configuration" (6-2)

- "The External Timing Output Ports tab" (6-5)

Procedure

....

Before you begin Prior to performing this task, you must connect the external timing output ports to an external timing network.

Required privilege code

You must have at least a privilege code of M3 to configure the external timing output ports.

Required equipment

The following is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to configure the external timing output ports:

....

1 Select **Configuration** → **Timing/Sync** in the **System View** of the *WaveStar* CIT.

> **Result:**
>
> The window **Provision Timing/Sync** appears with the active tab **External Timing Input Ports.**

....

2 Select the tab **External Timing Output Format**.

....

3 Select the timing output format in the group box **Timing Output Format** by clicking on the respective radio button. Select the format according to the format which is required for the external network. The following values are possible:

- **2 MHz** (initial value)

- **2 Mbit - framed**
  For framed 2 Mbit/s signals, the generation and evaluation of timing marker information on the timing quality is supported as per ITU-T Rec. G.704. If you want to use the timing marker, select **2 Mbit - framed**.

- **2 Mbit - unframed**

....

4 Enable the use of the external outputs in the group box **Derived Output Timing Enable**. Click on the radio button **Enable**.

....

Please note that there is only one timing output signal derived from the system clock or line signals which is forwarded in parallel to the two output ports which are physically available.

....

5   Select the timing output source in the group box **Provisioned Derived Output Timing Source Selection** from which the external timing signal is derived.

Possible values are:

- **TLS**
  The external timing signal is derived from one of the six line timing references.
  The selection criteria are the same as for **system timing** except the following:
  - signals with derived output priority enabled
  - signals with derived output lockout status set to **No Lockout**

- **SETG**
  The external timing signal is derived from the system clock

....

6   Set the parameter **Sync Message Force DNU**. Via this parameter you can define whether DNU is consistantly transmitted from the timing output ports.

The following values are possible:

- **Enable**

- **Disable**

....

7   Select the impedance of the external timing output ports in the group box *External Timing Port Impedance*. Click on the respective check box.

The following values are possible:

- **120 ohms**

- **75 ohms**

....

8   Apply the changes by clicking on **Apply** or **OK**. If you wish to discard the changes click on **Cancel**.

> **Result:**
>
> If you have clicked on **OK** or **Cancel,** the **Provision Timing/Sync** window closes. If you have clicked on **Apply,** the window remains open and you can select another tab.

E N D   O F   S T E P S

Configuring the timing references

Overview

....

Purpose   Use this procedure to configure the timing references.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"
- "Viewing the timing configuration" (6-2)
- "The Timing Reference tab" (6-6)

⅂

....

365-371-522
Issue b, October 2001

Lucent Technologies

6 - 1 7

Procedure

....

Before you begin Prior to performing this procedure, you must have completed the following provisioning tasks:

- Administrave tasks, such as a setup of user profiles (cf. Chapter 2, "Security administration") and provisioning of management communication via DCN (cf. Chapter 3, "Management communication setup").

- Creation of the high-speed shelf (shelf 1–2)

- Creation of the extension shelf (if required)

Required privilege code

You must have at least a privilege code of M3 to configure the timing references.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions Complete the following steps to configure the timing references:
....

1 Select **Configuration** → **Timing/Sync** in the **System View** of the *WaveStar* CIT.

> **Result:**

> The window **Provision Timing/Sync** appears.

....

2 Select the **Timing Reference** tab.

....

3 Select the timing reference source which you wish to configure in the drop-down list box **Timing Reference.**You can select the external timing signals **extref1** or **extref2** or an SDH signal via **line1** to **line6**.

....

4 Select the port AID in the drop-down-list box **Port AID**.

IF	THEN
the selected timing reference shall not be used,	select **NOT-CONNECTED**
the selected timing reference is **extref1**	select **exttmg0**

....

IF	THEN
the selected timing reference is **extref2**	select **exttmg1**
the selected timing reference is **line1** to **line6** and the corresponding SDH port is not yet assigned,	click on **Browse**... and select the SDH port which shall be used as timing reference. You can either select one STM-16 or one STM-64 signal. It is not possible to select an SDH port which belongs to the expansion shelf.
	Result: The window **Select Line Timing Port AID** opens.
the selected timing reference is **line1** to **line6** and the corresponding SDH port is already assigned,	- **Result:** the respective port AID is displayed in the drop-down list box **Port AID**.
the selected timing reference is **line1** or **line2** and you want to assign a new SDH signal as timing reference,	select **NOT-CONNECTED** first in order to disable the currently assigned SDH port, and then select the new SDH port via **Browse...**

5 Select the timing quality belonging to the timing reference in the drop-down list box **QL Provisioned**. For **line1** and **line2** select **AUTO**. This means that the timing marker is evaluated. For **extref1** and **extref2** assign the actual quality level of the external timing source. If the input format is 2mbit-framed (SSM supported) also select **AUTO**.

> **Result:**
>
> The timing references are now used in the order of their quality level.

6 Select in the drop-down list box **System Timing Reference Priority** the priority of the selected timing reference. The values can be

- **Disable** (initial value)

- **1** upto **8**

Make sure that all configured timing references have different priorities assigned.

Result:

A priority list is created for the configured timing reference signals. Initially the signal with the highest quality level is used as timing reference signal. If it fails, the system switches to the signal with the next lower quality level. If there are several timing references with the same quality level, they are used according to the priority list. If all possible timing reference signals fail, the timing generator enters the holdover mode.

....

7 Apply the changes by clicking on **Apply**. If you wish to discard the changes click on **Cancel**.

....

8 Repeat Step 3 to Step 7 until all timing references are configured. Click on **OK** to close the window.

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

Configuring the system timing

Overview

....

Purpose   Use this procedure to configure the system timing.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"

- "Viewing the timing configuration" (6-2)

- "The System Timing tab" (6-8)

❒

....

365-371-522
Issue b, October 2001

Lucent Technologies

6 - 2 1

Procedure

....

Before you begin   Prior to performing this procedure, you must have completed the
following provisioning tasks:

- Administrave tasks, such as a setup of user profiles (cf. Chapter
  2, "Security administration") and provisioning of management
  communication via DCN (cf. Chapter 3, "Management
  communication setup").

- Creation of the high-speed shelf (shelf 1–2)

- Creation of the extension shelf (if required)

Required privilege code

You must have at least a privilege code of M3 to configure the
external timing input ports.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to configure the timing references:

....

1   Select **Configuration → Timing/Sync** in the **System View** of the
WaveStar CIT.

> **Result:**
>
> The window **Provision Timing/Sync** appears.

....

2   Select the **System Timing** tab.

....

3   Select the clock mode in the group box **Provisioned Clock Mode.**
Click on the respective radio button. You can select the following
values:

- **Free Running** (The system is synchronised to the internal
  oscillator.)

- **Locked** (The system is synchronised to a timing reference
  signal.)

During normal operation in a network, the timing generator should be
locked to a timing reference signal as far as available. Normally the
free-running mode is used directly after the system start.

....

....

4   Enable or disable the use of the timing marker for the system timing
in the group box **System SSM Mode**. This means that the selection of
timing reference for the system timing is either determined only by
the provisioned priority list or by the quality level given by the timing
marker (SSM, Synchronization Status Message) and secondly by the
priority list. Click on the respective radio button.

The values can be

- **PRC**

- **SSUT**

- **SSUL**

- **SEC**

....

5   Select the wait-to-restore time in the group box **Timing Reference
Wait To Restore.** Click on the respective radio button. The values can
be:

- **0** (initial value)

- **20 Seconds**

- **1 Minutes** ... **60 Minutes** (selectable via a spin box)

- **Infinite**

The wait-to-restore time is the wait which is made before every single
switching from one timing reference to another.

....

6   Select the impedance of the external timing output ports in the group
box **Timing Port Impedance**. Click on the respective radio button.

....

7   Select the quality level of the derived timing output signal below
which AIS is inserted (in a framed 2 Mbit/s signal) or the signal is
quelched respectively (2 Mhz or unframed 2 Mbit/s signals). Click on
the respective radio button in the group box **Output Acceptance QL**.

....

8   Apply the changes by clicking on **OK**. If you wish to discard the
changes, click on **Cancel**.

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

....

Forced Switching of the timing generator to the holdover mode

Overview

Purpose   Use this procedure to switch between different clock modes:

- Clear Mode Switch
  This means that a current Forced Switch condition is reset.

- Force to Holdover
  The timing generator is switched to the holdover mode.

Related information   For related information, see:

- Chapter 17, "Timing provisioning concepts"

Procedure

....

Before you begin Prior to performing this task, verify that a *WaveStar*® CIT is connected and logged into the *WaveStar* TDM 10G system.

Required privilege code

You must have at least a privilege code of M4 to change the system clock mode.

Required equipment

The following equipment is required to perform this task:

* *WaveStar* CIT

Instructions Complete the following steps to change the clock mode:

....

1 Select **Clock Mode Switch** via **Fault → Timing/Sync Protection Switch** in the system view of the CIT.

> **Result:**
>
> The window **Clock Mode Switch** appears.

....

2 Select the switch commmand in the field **Switch Type.**You can select the following values via a radio button:

* **Clear Mode Switch**
  This command clears the Forced Switch condition. If the system clock is switched to the holdover mode by the Forced Switch command, this will be reset. The **Clear Mode Switch** command does not affect the state of the automatic protection switching based on synchronisation reference failure.

* **Force to Holdover**
  The **Force to Holdover** command causes the system clock to be switched to the holdover mode regardless of the state of the timing references.
  The mode switch is not carried out when the clock is provisioned for the free running mode.

....

3 Apply the changes by clicking on **OK**. If you wish to discard the changes, click on **Cancel**.

Important! After a switch to holdover or a clear mode switch, it takes the system about 7 minutes to stabilize the holdover filter. So don't do any further timing action during these 7 minutes.

....

Forced Switching of the timing generator to
the holdover mode
Procedure

Timing provisioning

Result:

The window **Clock Mode Switch** closes.

E ND   OF   S TEPS

Lucent Technologies

Switching to another timing reference

Overview

....

Purpose Use this procedure to switch between different timing reference signals and to apply certain switch requests to a selected reference:

- Clear Reference Switch
- Forced Switch
- Manual Switch
- Lockout
- Clear Lockout

Related information For related information, see:

- Chapter 17, "Timing provisioning concepts"
- "Configuring the timing references" (6-17)

....

Procedure

....

Before you begin   Prior to performing this task,

- verify that a *WaveStar*® CIT is connected and logged into the *WaveStar* TDM 10G system.

- configure the timing references sources for the system via Configuration → Timing/Sync → Timing Reference... (cf. "Configuring the timing references" (6-17)).

- verify that the timing generator is in the locked mode via View → Timing/Sync → System Timing (cf. "Parameters of the "View Timing/Sync" window" (6-4))

Please note that the switch requests are only applicable if the timing generator is locked to a timing reference source. When the system is provisioned to the free running mode, all present requests are cleared.

Required privilege code

You must have at least a privilege code of M4 to perform the switch commands.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to switch to another timing reference:

....

1   Select **System Timing Reference Switch** via **Fault → Timing/Sync Protection Switch** in the system view of the CIT.

        Result:

        The window **System Timing Reference Switch** appears.

....

2   Select the switch request you want to perform in the drop-down list box **Switch Type**. The following switch requests are possible:

- **Clear Reference Switch**
removes any active external request (Lockout, Forced and Manual Switch). It cannot be denied. It can also be used to clear the Wait to Restore time. The Clear Reference Switch command does not affect the state of the automatic protection switching based on synchronisation reference failure. If you select **Clear Reference Switch**, proceed to Step 4.

- **Lockout**

....

allows manual selection of individual references, or manual disabling of individual references.

- **Clear Lockout** disables the Lockout command.

- **Manual Switch to Reference**
  causes the system to be switched to the selected timing reference only if that timing reference is working fault free and no other external request is present.

- **Forced Switch to Reference**
  causes the system to be switched to the selected timing references regardless of the state of the timing reference. Only if a Clear Reference Switch or a Lockout command is present the Forced Switch is denied. A Forced Switch remains active until it is removed by a Clear Reference Switch or a Lockout command.

....

3 Select the timing reference source to which you want to perform a switch request in the drop-down-list box **Timing Reference**. This can be:

- **extref1**

- **extref2**

- **line1 to line6**

  Result:

  The AID of the respective timing reference is displayed in the **Port AID** information field. If no timing reference is defined, the drop-down list box and the information field are greyed out.

....

4 Apply the changes by clicking on **OK**. If you wish to discard the changes, click on **Cancel**.

Important! After a timing reference switch, it takes the system about 7 minutes to stabilize the holdover filter. So don't do any further timing action during these 7 minutes.

  Result:

  The window **System Timing Reference Switch** closes.

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

....

365-371-522
Issue b, October 2001

Lucent Technologies

6 - 2 9

**Switching to another
derived output timing
reference**

In the same way you can switch to another **derived output timing
reference**. Please note that **extref1** and **extref2** can not be selected.

⌐

Lucent Technologies

7 Traffic provisioning

Overview

Purpose   This chapter describes the procedures which have to be performed for the traffic provisioning. This comprises basically the functions of the Cross Connection Wizard and the setup of network protections, such as MSP, MS-SPRing and SNCP.

Contents

Viewing existing cross-connections

Overview

Purpose Use this procedure to query cross-connections in point-to-point, linear chain or ring applications. This also includes the protections on path level (DNI, SNCP, Adjunct Path Protection) belonging to the cross-connection.

Related information For related information, see:

- "Cross-connection management" (18-2)
- "2-fiber MS-SPRing" (18-13)
- "Multiplex Section Protection" (18-11)
- "Configuring an optical port" (4-23)
- "Configuring an electrical port" (4-38)
- "Configuring a tributary" (4-43)

Procedure

....

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

Required privilege code

You must have at least a privilege code of P2, Provisioning, to query
existing cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to query existing cross connections:
....

1   Call up the window **View Cross Connections** via **View → Cross
Connection...** in the **System View** of the *WaveStar* CIT.

....

2   Select in the tab **Ptn Grp** the required element for which you would
like to query the cross-connection. This can be a shelf, circuit pack,
port or tributary. Activate the selection via double click or via the
pushbutton **Select**.

Alternatively you can directly type the AID of the required element in
the text box **Enter AID**.

Result:

The window **View Cross Connections for STM64** opens. The
displayed parameters are described in the chapter "Parameters of
the window "View Cross Connections"" (7-5)

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

....

Parameters of the window "View Cross Connections"

Overview   The window **View Cross Connections** consists of three tabs which are described in this chapter.

The *Equipment* tab   The window contains three tabs. The first displays the ports.

Hierarchical structure   The network element components are organized in a tree structure from the system level down to the tributaries. Components of a lower level become visible by clicking on the "**+**" in front of a higher level component. You can select the components according to the following hierarchy:

system-bay-shelf-(protection group)-circuit pack/slot-port-tributary

This hierarchy is also used for the AIDs (cf. "Overview of access identifiers" (15-18))

The *Ptn. Grp* tab   The tab **Ptn. Grp.** is very similar to the tab **Equipment**. Shelves, circuit packs, ports and tributaries can also be selected on this tab. Additionally the tab contains information about the participation of a port in a protection group. For further information on protection, please refer to "Protection mechanisms" (18-10).

The *View Cross Connections for STM64* window   After the selection of the required element the window **View Cross Connections for STM64** opens. In this window all cross-connections belonging to the selected network element component are displayed.

Data in the information field   In the information field the following values are displayed:

Value	Meaning
Src Node NE Name	20-character TID which has been assigned to the Source Node TID (cf. Chapter 14, "Management communication setup concepts"). If a TID has not been associated with the source, "**-**" is displayed.
Src	The AID(s) for the source tributary/tributaries
Dest.	The AID(s) for the destination tributary/tributaries
Dest. Node NE Name	The 20 character TID which has been assigned to the Destination Node TID (cf. Chapter 14, "Management communication setup concepts"). If a TID has not been associated with the destination, "**-**" is displayed.

Viewing existing cross-connections
Parameters of the window "View Cross
Connections"

Traffic provisioning

Value	Meaning
Rate	The rate associated with the cross-connection. The values **VC3, VC4, VC44c, VC416c** are possible.
Type	The cross-connection type. The values **1–Way**, **2–Way**, **1–Way PP, Adj PP** are possible. In this context "path protected (PP)" means protected by Dual Node Ring Interworking.
Validity	Indicates whether the respective NE name (TID) is valid or invalid.
Role	The values **Wkg** and **Prot** are possible. This parameter shows whether a cross-connection is the working or the protection leg of a path protected cross-connection.

A certain cross-connection can be selected in the information field. Then further information on that cross-connection is displayed in the group boxes below.

The *Loopback* information field

The information field **Loopback** reflects the loopback status of a cross-connection. It indicates if any of the tributaries of the cross-connections is involved in a loop. Thus the values **Yes** or **No** are possible.

The *Output Mode* information field

The following values for the provisioned **Output Mode** are possible:

- **Normal** refers to a cross-connection which is carrying "normal" traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via the respective cross-connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.

Pushbuttons

The pushbutton **Browse** leads back to the window **View Connection** where you can select a shelf, circuit pack, port or tributary.

The pushbutton **Refresh** updates the window.

Via the pushbutton **Save As** it is possible to save the displayed data in a text file.

Via the pushbutton **View Graphic** the selected cross-connection is graphically displayed.

Via the pushbutton **Close** the window is closed.

Creating a new cross-connection

Overview

Purpose   Use this procedure to provision unprotected cross-connections in point-to-point, linear-chain or ring applications.

Related information   For related information, see:

- "Cross-connection management" (18-2)
- "2-fiber MS-SPRing" (18-13)
- "Multiplex Section Protection" (18-11)
- "Configuring an optical port" (4-23)
- "Configuring an electrical port" (4-38)
- "Configuring a tributary" (4-43)
- "Creating a cross-connection in a 2-fiber MS-SPRing network environment" (7-15)
- "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57)
- "Creating an unidirectional path protection" (7-69)
- "Creating an Adjunct Path Protection" (7-77)
- "Creating a bidirectional SNCP" (7-80)
- "Creating a bidirectional ring-to-ring SNCP" (7-84)

Procedure

....

Before you begin   Prior to performing this task, you must complete the port provisioning, including protection provisioning(not needed for 1:1 ports), for any port which is involved in the cross-connection.

Generally, an end-to-end link requires that a series of cross-connections (involving multiple ports and NEs) have to be provisioned for pre-service testing or re-arrangements. It is recommended to complete the cross-connections starting from:

1. One of the add/drop NEs,

2. continuing sequentially through all intermediate NEs, and

3. ending with the alternate add/drop NE.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar*® CIT

Instructions

CAUTION

> *cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.*

Complete the following steps to create a new cross-connection:
....

1   Call up the **Cross-Connection Wizard** via **Configuration →
     Cross-Connections...** in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Create a new cross-connection** and click
     on **Next>**.

           Result:

           Screen 1 appears.

....

....

3 Define the cross-connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

- **VC-3** (default value)

- **VC-4**

- **VC-4-4c**

- **VC-4-16c**

Please note that it is only possible for default value to proceed to the next window before selecting the cross-connection rate.

....

4 Define the type of cross-connection by clicking on the respective radio button in the group box **Type of cross-connection**. The following values are possible:

- **1 Way Point-to-Point**

- **2 Way Point-to-Point**

- **1 Way path-protected**

- **1 Way Adjunct Path Protected**

- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing Primary Node**

- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing Primary Nodes in Same NE**

- **Ring Interworking, Drop & Continue, UPSR/SNCP Node**

- **UPSR/SNCP Ring Add, Drop**

- **UPSR/SNCP Ring-to-Ring, Single Node Interconnection, Same NE**

For path-protected cross-connections please note that 1-way and 2-way path-protected cross-connections can be established as connections between two rings which are protected by an MS-SPRing or SNCP. These connections are also called Dual Node Ring Interworking (DNI) cross-connections. You have to know the network topology in detail in order to be able to create proper DNI cross-connections. The DNI can be implemented by a connection between two different nodes (primary nodes), each belonging to one of the two protected rings. The broadcast and the switch function are located in two different network elements. Furthermore there are two other network elements involved in the DNI which realize the rerouting of the protected signals (secondary nodes). The DNI can also be realized implementing the broadcast and the switch function in one network element, and there may be also only one secondary node. This variant is called DNI with collapsed nodes. For further

....

information on the DNI please refer to "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57) and "Creating an unidirectional path protection" (7-69) .

If you are creating 1-way or 2-way cross-connections within a ring which is protected by a 2-fiber MS-SPRing please note the additional hints in "Creating a cross-connection in a 2-fiber MS-SPRing network environment" (7-15).

If you are creating an adjunct path protection, additionally to an existing one, please refer to "Creating an Adjunct Path Protection" (7-77).

If you are creating a cross-connection which is protected by a Sub-Network Connection Protection (SNCP) please refer to "Creating a bidirectional SNCP" (7-80) or "Creating a bidirectional ring-to-ring SNCP" (7-84).

....

5 Click on **Next>** to proceed to the next window.

> **Result:**

> Screen 2 opens.

....

6 Click on **Select...** to select the source tributary.

> **Result:**

> The **Ptn Grp** selection tab appears. In the list box of the **Ptn Grp** selection tab the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted.

....

7 Select one port in the list or enter the AID in the text box **Enter AID:** above.

> **Result:**

> In the list box **Tributary** on the right, the AIDs of all VCs belonging to the respective port are displayed.

....

8 Select the VC which shall be used as the source and click on the **Select...** button.

....

9 Select the destination port in the **Ptn Grp** selection tab and the corresponding VC in the **Tributary** list box and click on the **Select...** button.

....

Result:

On Screen 2 both, the source and destination tributary, are displayed.

....

10   Click on the **Next>** button.

Result:

The **Screen 3** opens.

If you are creating an unprotected cross-connection you can set the values of the provisionable parameters of the specified cross-connection via this window. Configuration data is described in "Parameters of the window "View Cross Connections"" (7-5).

....

11   Select the **Output Mode** in the group boxes **Source to Destination** and **Destination to Source**. The following values are possible:

- **NORM**

- **AIS**

- **IDLE/UNEQ**

    Result:

    The selected settings have the following consequences:

    - With the setting **NORM**, a normal payload signal is transmitted.

    - With the setting **AIS**, An AIS is inserted in the signal for test and maintenance purposes.

    - With the setting **IDLE/UNEQ**, an unequipped signal is transmitted for test and maintenance purposes.

....

12   Click on the **Finish** button to apply your settings.

Result:

In case of one (or two) unprotected ports, a confirmation window appears. If you are sure, confirm.

E N D   O F   S T E P S

....

⌐

....

365-371-522
Issue b, October 2001

Lucent Technologies

7 - 1 1

Creating a bridge

Overview

....

Purpose   Use this procedure to create a cross-connection with one source and two destination ports (broadcast). This can be necessary for 1-way path protection or DNI applications.

Related information   For related information, see:

- "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57)

- "Creating an unidirectional path protection" (7-69)

⌐

....

7 - 1 2   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

Before you begin   Prior to performing this task, you must complete the port provisioning, including protection provisioning, for any port which is involved in the cross-connection. Additionally a 1-way cross-connection must already exist with the source tributary which shall be used as source of the bridge.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

CAUTION

cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both legs of the bridge.

Complete the following steps to create a new cross-connection:
....

1   Call up the **Cross-Connection Wizard** via **Configuration** → **Cross-Connections...** in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Bridge a cross-connection from a source tributary** and click on **Next>**.

>   **Result:**

>   **Screen 1** appears. The **Ptn Grp** selection tab becomes visible. In the list box of the **Ptn Grp** selection tab the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs, and ports is depicted.

....

3   Select one port in the list or enter the AID in the text box **Enter AID:** above.

....

Result:

In the table on the right, the cross-connections belonging to the respective port are displayed.

....

4   Select the 1-way cross-connection to which the bridge shall be created and click on the **Next>** button.

....

5   Click on the **Select...** button next to the **Destination** field and select the destination tributary via the **Ptn Grp** selection tab and the table on the right side of the window **Destination Tributary**.

....

6   Click on the **Select** button.

....

7   Click on the **Next>** button in **Screen 2**.

   Result:

   The **Screen 3** opens.

....

8   Select the **Output Mode** in the respective drop-down list box. The following values are possible:

   - **NORM**

   - **AIS**

   - **IDLE/UNEQ**

   Result:

   The selected settings have the following consequences:

   - With the setting **NORM**, a normal payload signal is transmitted.

   - With the setting **AIS**, An AIS is inserted in the signal for test and maintenance purposes.

   - With the setting **IDLE/UNEQ**, an unequipped signal is transmitted for test and maintenance purposes.

....

9   Click on the **Finish** button to apply your settings.

   Result:

   In case of one (or two) unprotected ports, a confirmation window appears. If you are sure, confirm.

   E N D   O F   S T E P S

....

Creating a cross-connection in a 2-fiber MS-SPRing network environment

Overview

Purpose   Use this procedure to create cross-connections for traffic which is protected via a 2-fiber MS-SPRing.

Related information   For related information, see:

- "Creating a new cross-connection" (7-7)
- "Creating a new 2-fiber MS-SPRing" (7-48)

....

365-371-522   **Lucent Technologies**   7 - 1 5
Issue b, October 2001

Procedure

....

Before you begin   You must have a detailed knowledge on the network topology of the respective ring.

If you are creating cross-connections within a 2-fiber MS-SPRing, you have to create through-connections in each network element which is part of the protected route, as shown in the example below.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Example   A bidrectional route which is protected by an MS-SPRing is established between NE A and NE D. In each NE in between a bidirectional cross-conenction has to be created in order ot route the traffic from NE A to NE D.
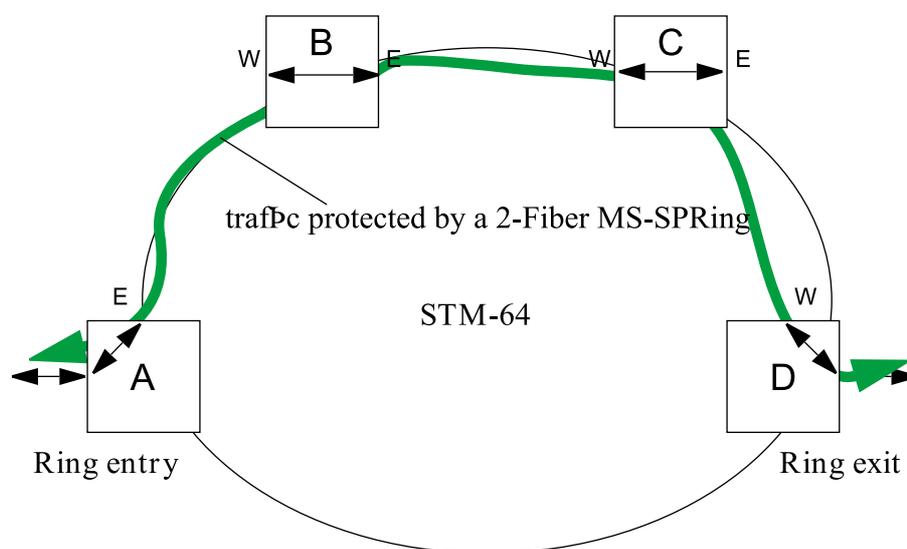
In order to avoid confusion with the source and destination of the cross-connection, which might cause traffic loss in case of a protection switch, it ist highly recommended to start at one end of the route with the creation of the cross-connections and proceed from NE to NE and to keep always the same view of source and destination for the through-connection. This means that you should always switch the cross-connection, for example, from a tributary of the west port to a tributary of the east port, even if you are creating a bidirectional

....

Creating a cross-connection in a 2-fiber
MS-SPRing network environment
Procedure

Traffic provisioning

cross-connection. Of course you could also select source and destination the other way round, but you should keep the same view for all NEs on the protected route.

Instructions

1   *NE at ring entry:*

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection **Source** the AID of a tributary belonging to the low-speed shelf (1-1...). In the example the ring entry is NE A.
the NE belongs to an STM-16 ring,	select as cross-connection **Source** the AID of a tributary belonging to a low-bitrate port (e.g. STM-4).

2

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection **Destination** the AID of a tributary belonging to the high-speed shelf (1-2...).
the NE belongs to an STM-16 ring,	select as cross-connection **Destination** the AID of a tributary belonging to the STM-16 port which is interface to the MS-SPRing.

     Result:

     The **Source NE Name** is greyed out.

3   Select the **Destination NE Name**. It must be the TID of the NE at the end of the MS-SPRing route.

In the example the cross-connection switching is started at the NE A, the **Destination NE Name** is D.

4   Repeat Step 1 to Step 3 for all cross-connections which have to be created in the NE at the ring entry.

5   *Intermediate NEs:*

Create all cross-connections in the neighbour network element by keeping the same view of source and destination or east and west, respectively. First select the **Source** AID, then the **Destination** AID

Creating a cross-connection in a 2-fiber
MS-SPRing network environment
Procedure

Traffic provisioning

of the cross-connection. Proceed to the next window and select the **Source NE Name** and **Destination NE Name** of the protected route.

In the example all cross-connections are switched from the cross-connection **Source** on the west port to the cross-connection **Destination** on the east port. Thus in NE B and NE C the **Source NE Name** is A and the **Destination NE Name** is D.

....

6 Repeat Step 5 for all NEs on the protected route.

....

7 *NE at ring exit:*

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection **Source** the AID of a tributary belonging to the high-speed shelf (**1-2...**). In the example the ring exit is NE D.
the NE belongs to an STM-16 ring,	select as cross-connection **Source** the AID of a tributary belonging to the STM-16 port which is interface to the ring.

....

8

IF	THEN
the NE belongs to an STM-64 ring,	select as cross-connection **Destination** the AID of a tributary belonging to the low-speed shelf (**1–1...**).
the NE belongs to an STM-16 ring,	select as cross-connection **Destination** the AID of a tributary belonging to a low-bitrate port.

Result:

The **Destination NE Name** is greyed out.

....

9 Select the **Source NE Name**. In the example it is A.

....

10 Repeat Step 7 to Step 9 for all cross-connections in the NE at the ring exit.

E N D   O F   S T E P S

....

Modifying a cross-connection

Overview

Purpose   Use this procedure to modify existing cross connections in point-to-point, linear-chain or ring applications.

Related information   For related information, see:

- "Cross-connection management" (18-2)
- "Viewing existing cross-connections" (7-3)

Procedure

....

Before you begin   Check the parameters of the cross-connection you wish to modify in the window **View cross-connections**. (cf. "Viewing existing cross-connections" (7-3))

Required privilege code

You must have at least a privilege code of P3 to modify cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

 CAUTION

> *cross-connections made to the wrong ports (wrong AIDs) will cause problems during testing and service. Removing or modifying a working cross-connection will interrupt service! In order to prevent service interruptions, you should verify the integrity of both working and protection ports.*

Complete the following steps to modify a cross-connection:
....

1   Call up the **cross-connection Wizard** via **Configuration** → **cross-connection...** in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Modify parameters on an existing cross-connection** and click on **Next>**.

> **Result:**
>
> **Screen 1** appears.
>
> In the list box of the **Equipment** selection tab, the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs and ports is depicted.

....

3   Select one port in the list or enter the AID in the text box **Enter AID:** above.

....

Result:

In the list box on the right the AIDs of all sources and destinations of cross-connections belonging to the respective port are displayed.

....

4 Select the cross-connection which shall be modified and click on the **Next>** button.

Result:

Screen 2 opens. If you have selected a one-way cross-connection, go to Step 6.

....

5 Select the desired leg (two-way cross-connections have two legs) and click on the **Next>** button.

Result:

Screen 3 opens. In this window you can set the values of the provisionable parameters of the specified cross-connection.

....

6 Modify the desired parameters and click on the **Finish** button to apply your changes.

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

Rolling a cross-connection

Overview

Purpose   Use this procedure to "roll" a cross connection leg from one tributary source to another. This means you can choose a new source for an existing cross connection.

Related information   For related information, see:

- "Cross-connection management" (18-2)

- "Configuring an optical port" (4-23)

- "Configuring an electrical port" (4-38)

- "Configuring a tributary" (4-43)

⌐

Procedure

....

Before you begin   Prior to performing this task, you must complete the port
provisioning, including protection provisioning, for any port which is
involved in the cross-connection.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to roll
cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions

 CAUTION

*cross-connections made to the wrong ports (wrong AIDs) will
cause problems during testing and service. Removing or
modifying a working cross-connection will interrupt service!
In order to prevent service interruptions, you should verify
the integrity of both working and protection ports.*

Complete the following steps to roll a cross-connection:

....

1   Call up the **cross-connection Wizard** via **Configuration** →
cross-connection... in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Roll a cross-connection leg from one
tributary source to another** and click on **Next>**.

> **Result:**
>
> **Screen 1** appears.

....

3   Select the desired port on the **Ptn Grp** tab.

> **Result:**
>
> All cross-connections belonging to the respective port are
> displayed on the table on the right side of the window. The type
> and signal rate are of the cross-connections are also displayed.

....

4   Select a cross-connection on the right table. Finally click on **Next>**.

....

> **Result:**
>
> **Screen 2** appears

....

5   Click on the cross-connection leg you want to roll. You may only choose one leg. Then click on **Next>**.

Each leg of a two-way cross-connection is treated as a one-way cross-connection. If the roll function is applied for one leg, first this leg is removed and a new one is created with another tributary source. The second leg remains untouched.

> **Result:**
>
> The **New Source Tributary** window appears

....

6   Select a new source for the cross-connection. First select a port on the **Ptn Grp** tab.

> **Result:**
>
> The AID of all VCs belonging to this port are displayed on the table on the right side of the window. Furthermore it is shown whether a VC is already involved in a cross-connection and if it is protected.

Please note the following rules for the rolling of the source of a path protected cross-connection to a new one:

1.   You can select a source tributary which is located in the same shelf as the old one or

2.   you can select a source which is located in a different shelf from the old one, provided that the second source tributary of the path protected cross-connection is located in the same shelf as the destination tributary.

Other actions will be refused.

....

7   Select the tributary which shall be used as a new source and click on the **Next>** button.

> **Result:**
>
> **Screen 3** opens. In this window you can set the values of the provisionable parameters of the specified cross-connection. The **Screen 3** also contains a view of the configured changes. Furthermore configuration data is displayed.

....

....

8 Select the source and the destination TID in the drop-down list boxes
New Src NE Name: and **Destination NE Name:**

This field only applies to a leg which is part of an MS-SPRing
(Multiplex Section Shared Protection Ring).

....

9 Click on the **Finish** button to apply your settings.

E ND OF S TEPS

Deleting a cross-connection

Overview

....

Purpose   Use this procedure to delete cross connections in point-to-point, linear-chain or ring applications.

Related information   For related information, see:

- "Cross-connection management" (18-2)
- "Creating a new cross-connection" (7-7)
- "Configuring an optical port" (4-23)
- "Configuring an electrical port" (4-38)
- "Configuring a tributary" (4-43)

⌐

....

Procedure

....

Before you begin   In order to prevent a service interruption, the service provided on the subject path must have previously been removed before deleting any of the cross-connections included in that path. Again, the recommendation is that cross-connections be deleted starting from

1. one of the add/drop NEs,

2. continuing sequentially through all intermediate NEs, and

3. ending with the alternate add/drop NE.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to delete cross-connections.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar*® CIT

Instructions   Complete the following steps to delete a cross-connection:

....

1   Call up the **cross-connection Wizard** via **Configuration** → **cross-connection...** in the **System View** of the *WaveStar* CIT.

....

2   Select the option **Delete leg(s) of an existing cross-connection** and then click on the **Next>** button.

> **Result:**
>
> The **Screen 1** appears.
>
> In the list box of the **Equipment** selection tab the system is displayed. The displays can be expanded. Thus a tree of systems, bays, shelves, circuit packs and ports is depicted.

....

3   Select one port in the list or enter the AID in the text box **Enter AID:** above.

> **Result:**
>
> In the list box on the right the AIDs of all sources and destinations of cross-connections belonging to the respective port are displayed.

....

4 Select the cross-connection which shall be deleted and click on the **Next>** button.

> **Result:**
>
> 2way cross-connection → **Screen 2** opens. Proceed with next step.
>
> 1way cross-connection → **Screen 3** opens. It contains the parameters of the cross-connection that is to be deleted. Go to step 6.

5 Select the leg(s) of the cross-connection you want to delete and click on the **Next>** button

> **Result:**
>
> **Screen 3** opens. This window contains the parameters of the cross-connection which is to be deleted.

6 Review the data. Click on **<Back** to make any corrections, click on **Cancel** to discard your changes or click on **Finish>** to delete the cross-connection.

> **Result:**
>
> If you have clicked on the **Finish>** button a **Confirm** box opens.

7 Review the accuracy of the entries in the **Confirm** box and, as appropriate, check **Yes** or **No**.

E N D   O F   S T E P S

Viewing an existing protection group

Overview

Purpose   Use this procedure to query the current status of a protection group. It can be used for all kinds of protection.

Related information   For related information, see:

- "Protection mechanisms" (18-10)
- "Multiplex Section Protection" (18-11)
- "2-fiber MS-SPRing" (18-13)
- "Sub-Network Connection Protection (SNCP)" (18-19)
- "Dual Node Ring Interworking" (18-23)

Procedure

....

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

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create
new cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to query the status of a protection
group:

....

1 Call up the window **View Protection** via the menu **View** →
Protection... in the **System View** of the *WaveStar* CIT.

....

2 Select the components of the required protection group in the tab **Ptn
Grp** on the left side of the window.

E N D   O F   S T E P S

**Alternative instruction for
DNI and SNCP**

....

1 Call up the window **Path Protection Group Names** via the menu
View → **Path Protection Group Names** and select the desired path
protection group.

E N D   O F   S T E P S

⌐

....

Parameters of the window "View Protection" for a 1+1 MSP or 1:1 MSP

Status data   The following table shows the status data which is shown in the **View Protection** window for a 1+1 MSP or 1:1 MSP.

Information field	Possible value	Meaning
Protection Group AID	cf. "Overview of access identifiers" (15-18)	The AID defined for the selected protection group.
Protection Type	**1+1 MSP, 1xN Optical Port**	1xN Optical Port = 1:1 MSP
Optical Line Rate	**STM1, STM4, STM16, STM64**	SDH line rate associated with the port. For a 1:1 MSP only **STM64** is possible.
Interworking Type	**SDH**	
Protocol	**Unidirectional**	Each transmission direction is monitored separately and switched over if necessary. This can lead to a situation in which only one direction is transmitted via the main section an the other direction via the standby section.
	Bidirectional	Both transmission directions are always monitored and switched over in synchronization if necessary.
Working AID	cf. "Overview of access identifiers" (15-18)	The port AID which has been assigned to be the working port.
Protection AID	cf. "Overview of access identifiers" (15-18)	The port AID which has been assigned to be the protection port.
Protection Group Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)** or **Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm status associated with the protection group. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preference**s window (cf. Chapter 24, " *WaveStar*® CIT Tutorial").
Working Port Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)** or **Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm status associated with the working port. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preferences** window (cf. Chapter 24, "*WaveStar* CIT Tutorial").
Working Switch Fault Status	**Signal Failure, Signal Degrade, -**	Switch initiation reason associated with the working port

Viewing an existing protection group
Parameters of the window "View
Protection" for a 1+1 MSP or 1:1 MSP

Traffic provisioning

Information field	Possible value	Meaning
Protection Port Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)**or**Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm status associated with the protection port. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preferences** window (cf. Chapter 24, "*WaveStar* CIT Tutorial").
Protection Switch Fault Status	**Signal Failure, Signal Degrade, -**	Switch initiation reason associated with the protection port
Active Port	**Working (<port AID>), Protection (<port AID>)**	Indicates which port is carrying traffic
Switch Request State	**Lockout, Forced Switch , Signal Fail High, Signal Degrade High, Manual Switch, Wait to Restore (WTR), No Request, Do Not Revert, Failure of Protocol**	Indicates whether a manually or automatically initiated switch has occurred and whether the MSP is activated. For the meaning of the Switch Requests please refer to "Switch request state" (7-39).
Near-End Outgoing APS Message	**Lockout,** **Forced Switch, No request, Signal Fail High,** **Signal Degrade High, Wait To Restore, Manual Switch,** **Do Not Revert, Reverse Request**	The outgoing Automatic Protection Switch Message, please refer to "Switch request state and APS messages" (7-33).
Near-End Outgoing Request Selection	**Working (<port AID>), Protection (<port AID>), Invalid**	
Far-End Incoming APS Message	**Lockout,** **Forced Switch, No request, Signal Fail High,** **Signal Degrade High, Wait To Restore, Manual Switch,** **Do Not Revert, Reverse Request**	cf. "Switch request state and APS messages" (7-33)
Far-End Incoming Request Selection	**Working (<port AID>), Protection (<port AID>), Invalid**	

Viewing an existing protection group
Parameters of the window "View
Protection" for a 1+1 MSP or 1:1 MSP

Traffic provisioning

Information field	Possible value	Meaning
Protection Reversion	**Enabled, Disabled**	If the **Protection Reversion** is enabled, the MSP operates in revertive mode. If the **Protection Reversion** is disabled, the MSP operates in non-revertive mode. This parameter is not applicable for 1:1 MSP
Wait To Restore/Rename	**0 ... 60 minutes, infinite**	
Hold-off Time	**0 ... 10000 ms**	
Alarm Severity Assignment Profile	-	

Important! If the protection line is interrupted the K1/K2 byte protocol is no longer transmitted. Thus messages from the Far End might be incorrect. In this case the network element on the receive side marks the Far End Messages as *Invalid*.

Switch request state and APS messages

The following table shows the meaning of the switch request state and the APS (Automatic Protection Switch) messages.

Switch Request State	Meaning
Lockout	Protection switching is deactivated. Traffic is carried on the working section. No switchover occurs in the event of a section fault.
Forced Switch	A forced switchover has been made from one section to the other (user action). This action can also be carried out to a faulty section. Automatic protection switching is deactivated as long as the Forced Switch is activated.
Signal Fail High	Signal failure on a section. An automatic switchover has been carried out.
Signal Degrade High	The signal quality on a section is degraded. An automatic switchover has been carried out.
Manual	A manual switchover has been made from one section to the other (user action). This action can be carried out to a fault-free section only. Automatic protection switching remains activated.

Viewing an existing protection group
Parameters of the window "View
Protection" for a 1+1 MSP or 1:1 MSP

Traffic provisioning

Switch Request State	Meaning
Wait To Restore	The working section is operable again. Traffic is still carried on the protection section. A wait is made for a defined time (wait-to-restore time) to see whether the working section is stable before traffic is switched back. Automatic switchback is carried out only if the MSP operates in **revertive** mode. Only in this case can a wait to restore time be defined.
No Request	No switchover request exists
Do Not Revert	Can occur only if the MSP operates in non-revertive mode. The working section is restored, but traffic remains on the protection section.
Failure of Protocol	Includes all other possible errors, which are not initiated by a user switch or a signal failure.
Invalid	The Far End APS messages are no longer valid as the protection line has failed.

Parameters of the window "View Protection" for a 2-Fiber MS-SPRing

Description The **View Protection** window consists of five tabs, each describing a set of parameters:

- Protection Group
- Alarm Status
- Provisionable Parameters
- West Side
- East Side

Status data The following table shows the status data which is shown in the **View Protection** window for a 2-Fiber MS-SPRing.

Information field	Possible value	Meaning
The tab **Protection Group**		
Protection Group AID	\<two-digit character string\> (cf. "Overview of access identifiers" (15-18))	The AID defined for the selected protection group.
Protection Type	**2-Fiber MS-SPRING**	
Optical Line Rate	**STM16**, **STM64**	SDH line-rate associated with the port
Interworking Type	**SDH**	—
Ring-ID	\<ASCII character string\> (up to 15 characters)	Ring ID for the selected protection group
West Port AID/East Port AID	cf. "Overview of access identifiers" (15-18)	Port AID of the west/east side which has been provisioned for the protection group
Ring Node APS State	**IDLE, SWITCHING, PASSTHROUGH**	Switch status of the NEs of the respective MS-SPRing
The tab **Alarm Status**		
Protection Group Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)**or**Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm level of the protection group. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preference** window (cf. Chapter 24, " *WaveStar*® CIT Tutorial").
West Port AID/East Port AID	(cf. "Overview of access identifiers" (15-18))	The AID defined for the West and the East Port of the respective NE

Viewing an existing protection group
Parameters of the window "View
Protection" for a 2-Fiber MS-SPRing

Traffic provisioning

Information field	Possible value	Meaning
West AID Alarm Status/East AID Alarm Status	**Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA)**or**Prompt (PR), Deferred (DF), Info (INF)**	The highest alarm level for the West/East port. The alarm format (**CR/MJ/MN** or **PR/DF/INF**) is configurable via the **Preference** window (cf. Chapter 24, "*WaveStar* CIT Tutorial").
The tab **Provisionable Parameters**		
Wait To Restore	**0 ... 12 minutes, infinite**	Displays the selected Wait-to-Restore time of the selected protection group.
Alarm Severity Assignment Profile	**DEFAULT**	The selected Alarm Severity Assignment Profile. For the current release only the default Alarm Severity Assignment Profile is available.
The tabs **West Side** and **East Side**		
East/West Switch Request State	**LP-S Lockout of Prot.** **FS-R Forced Switch-Ring** **SF-R Signal Fail-Ring** **SD-R Signal Degrade-Ring** **MS-R Manual Switch-Ring** **WTR Wait to Restore** **RR-R Reverse Request - Ring** **NR No Request**	Switch request for the outgoing west/east side
East/West Last Protection Switch Attempt Status	**SUCCESS, DENIED, FAILED**	
East/West Switch Priority	**LP-S Lockout of Prot.** **FS-R Forced Switch-Ring** **SF-R Signal Fail-Ring** **SD-R Signal Degrade-Ring** **MS-R Manual Switch-Ring** **WTR Wait to Restore** **RR-R Reverse Request - Ring** **NR No Request**	K1 byte, bits 1-4.
East/West Destination Node ID	**0 ... 15**	Node ID associated with the protection group. K1byte, bits 5-8
East/West Source Node ID	**0 ... 15**	Node ID associated with the Far End of the fiber. K2 byte, bits 1-4

Viewing an existing protection group
Parameters of the window "View
Protection" for a 2-Fiber MS-SPRing

Traffic provisioning

Information field	Possible value	Meaning
East/West Protection Path	**Short, Long**	K2 byte, bit 5. The path of the rerouted traffic from the point of view of the regarded NE.
East/West Channel Status	**Idle**	The current channel status of the node
	Bridged	
	Bridged and Switched	
	Extra traffic	
	Not Used	
	RDI-L	
	AIS-L	

After the deletion of an MS-SPRing protection group and the following creation of a new group with the same ports in the K-Bytes to the neighbouring NEs, not the default values are sent, as would be expected, but some old values from the deleted group. After the ring discovery has been completed, the K-Byte information will be aligned to the new group.

Parameters of the window "View Protection" for DNI and SNCP

Status data   The following table shows the status data which is shown in the **View Protection** window for SNCP and DNI.

Information field	Possible value	Meaning
Protection Group AID	cf. "Overview of access identifiers" (15-18)	The AID defined for the selected protection group.
Protection Type	**Path**	
Path Protection Group Name	**<ASCII string with up to 24 characters>**	
Cross Connection Rate	**VC-3, VC-4, VC-4–4c, VC-4–16c**	
Constituent Member List		
Adjunct Output List	cf. "Overview of access identifiers" (15-18)	AID of the adjunct output which may be associated with the protection group.
Trib.	**<number>**	
CST	**VC-3, VC-4, VC-4–4c, VC-4–16c**	Cross-connection rate
Active Constituent	**Working**, **Protection**	Shows which path is actually active
Working Source	cf. "Overview of access identifiers" (15-18)	The AID of the source tributary of the working path.
Protection Source	cf. "Overview of access identifiers" (15-18)	The AID of the source tributary of the protection path.
Destination Source	cf. "Overview of access identifiers" (15-18)	The AID of the destination tributary.
Switch Request State	cf. "Switch request state" (7-39)	
Working Fault Status	Signal Failed (**SF**), Signal Degraded (**SD**), **None**	Displays the failure condition of the working path
Protection Fault Status	Signal Failed (**SF**), Signal Degraded (**SD**), **None**	Displays the failure condition of the protection path
Revertive Mode	**Enabled, Disabled**	
System Path Level Wait To Restore	**0 ... 12 minutes, infinite**	Defines the time interval before the system switches back to the working path after restoration
Holdoff Timer	**Enabled, Disabled**	

Viewing an existing protection group
Parameters of the window "View
Protection" for DNI and SNCP

Traffic provisioning

Information field	Possible value	Meaning
System Path Level Holdoff Time	**0 ... 10 s**	Defines the time during which an alarm must be detected before the system switches to the protection path.

Switch request state   The following table shows the meaning of the switch request state:

Switch Request State	Meaning
Lockout	Protection switching is deactivated. Traffic is carried on the working path. No switchover occurs in the event of a section fault.
Forced Switch	A forced switchover has been made from one path to the other (user action). This action can also be carried out to a faulty path. Automatic protection switching is deactivated as long as the Forced Switch is activated.
Signal Failed	Signal failure on a path. An automatic switchover has been carried out.
Signal Degraded	The signal quality on a section is degraded. An automatic switchover has been carried out.
Manual	A manual switchover has been made from one section to the other (user action). This action can be carried out to a fault-free section only. Automatic protection switching remains activated.
Wait To Restore	The working path is operable again. Traffic is still carried on the protection path. A wait is made for a defined time (wait-to-restore time) to see whether the working path is stable before traffic is switched back. Automatic switchback is carried out only if the protection group operates in **revertive** mode. Only in this case can a wait to restore time be defined.
No Request	No switchover request exists.

Creating a new 1+1 MSP

Overview

Purpose   Use this procedure to create a new 1+1 Multiplex Section Protection (MSP).

Related information   For related information, see:

- "Protection mechanisms" (18-10)

- "Multiplex Section Protection" (18-11)

Procedure

....

Before you begin Prior to performing this task, you must:

- Verify that all required circuit packs are installed (cf. "Main shelf configuration" (15-9), "Extension shelf configuration" (15-15), "Creating a new circuit pack" (4-17) and "Reassigning a circuit pack" (4-20)).

- Complete the port provisioning for any optical port which is involved in the protection group (cf. "Configuring an optical port" (4-23), "Configuring an electrical port" (4-38) and "Configuring a tributary" (4-43)).

- Verify that no failure (Loss of Signal, LOS) is present on the working line (cf. *WaveStar*® TDM 10G (STM-64) Alarm Messages and Trouble Clearing Guide, chapter "Retrieving a list of current alarms").

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create new cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Configuration rules An MSP can only be established between two separate circuit packs (which are of the same type), i.e. it is not allowed to establish an MSP between 2 ports on the same circuit pack. An MSP between different ports on different circuit packs can be configured independently, e.g. one port of circuit pack 1 can be protected with one port of circuit pack 2 while the second port on circuit pack 1 is protected by circuit pack 3. The MSP-related circuit packs are not restricted to specific slots.

Instructions Complete the following steps to create a new MSP:

....

1 Call up the window **Create New Protection Group** via **Configuration** → **Create New...**→ **Protection Group** in the **System View** of the CIT.

   Result:

   On the left side of the window the tab **Ptn Grp** appears. The selected system and bay and the available shelves are displayed.

....

....

2 Select the shelf in which you wish to establish the MSP and click on
the pushbutton **Select I/O Shelf**.

> **Result:**
>
> On the right side of the window the **Protection Type Selection**
> menu appears.

....

3 Select the type **1+1 MSP** in the drop-down list box **Protection Type**.

> **Result:**
>
> The parameter fields for the 1+1 MSP appear.

....

4 Define the last digit(s) of the **Protection Group AID** in the respective
text box. Insert a value from **1** to **99**.

....

5 Select the **AIDs of the Working Port** and the **Protection Port** in the
respective drop-down list boxes in the group box **Group Member**.
The values correspond to the slot designations.

For STM-16 port units, any pair combination of allowed slot positions
can be applied: 02, 04, 06, 08, 10, 12, 14, 16. For optical STM-1 port
units, any pair combination of allowed slot positions can be applied:
01...16.

....

6 Select the **Protocol**. Click on the respective radio button. You may
choose one of the following options:

- **Unidirectional** The two transmission directions are switched
  independently from each other

- **Bidirectional** The two transmission directions are always
  switched over to the other line in synchronization, even if only
  one has failed.

The option **Optimized** is only supported for STM-1.

....

7 Set the **Protection Reversion** to **Enabled** (corresponds to revertive
mode) or **Disabled** (corresponds to non-revertive mode) by clicking
on the respective radio button.

....

8 If desired, enable the DCC protection on Multiplex Section level
(DCC_M) by clicking on the radio button **Enabled** in the group box
DCC Line/MS Protection Mode.

....

....

9 If desired, enable the DCC protection on Regenerator Section level (DCC$_R$) by clicking on the radio button **Enabled** in the group box **DCC Section/RS Protection Mode**.

....

10 Set the Wait-To-Restore time in the drop-down list box **Wait to Restore:**.

Values between **1** and **12** minutes in steps of one minute are possible. Also the value **INFINITE** can be selected.

....

11 Select the **Alarm Severity Assignment Profile**.

....

12 Click on **Apply** then click on **Close**.

Result:

The window **Create New Protection Group** closes.

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

....

365-371-522
Issue b, October 2001

Lucent Technologies

7 - 4 3

Creating a new 1:1 MSP with preemptible protection access

Overview

Purpose   Use this proecedure ot create a new 1:1 Multiplex Section Protection (MSP) for an STM-64 port.

Related information   For related information, see:

- "1:1 MSP with preemptible protection access" (18-12)

⌐

Procedure

....

Before you begin   Prior to performing this task, you must:

- Verify that all required circuit packs are installed (cf. "Main shelf
  configuration" (15-9), "Extension shelf configuration" (15-15),
  "Creating a new circuit pack" (4-17) and "Reassigning a circuit
  pack" (4-20)).

- Complete the port provisioning for any optical port which is
  involved in the protection group (cf. "Configuring an optical
  port" (4-23), "Configuring an electrical port" (4-38) and
  "Configuring a tributary" (4-43)).

- Verify that no failure (Loss of Signal, LOS) is present on the
  working line (cf. *WaveStar*® TDM 10G (STM-64) Alarm
  Messages and Trouble Clearing Guide, chapter "Retrieving a list
  of current alarms").

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create
new cross-connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Configuration rules   A 1:1 MSP can only be established between two separate STM-64
circuit packs, i.e. it is not allowed to establish an MSP between 2
ports on the same circuit pack. An MSP between different ports on
different circuit packs can be configured independently, e.g. one port
of circuit pack 1 can be protected with one port of circuit pack 2
while the second port on circuit pack 1 is protected by circuit pack 3.
The MSP-related circuit packs are not restricted to specific slots.

Instructions   Complete the following steps to create a new MSP:

....

1   Call up the window **Create New Protection Group** via
Configuration → **Create New...**→ **Protection Group** in the **System
View** of the CIT.

> **Result:**
>
> On the left side of the window the tab **Ptn Grp** appears. The
> selected system and bay and the available shelves are displayed.

....

....

2   Select the shelf in which you wish to establish the MSP and click on the pushbutton **Select I/O Shelf**.

Result:

On the right side of the window the **Protection Type Selection** menu appears.

....

3   Select the type **1:1 MSP** in the drop-down list box **Protection Type**.

Result:

The parameter fields for the 1:1 MSP appear.

....

4   Define the last digit(s) of the **Protection Group AID** in the respective text box. Insert a value from **01** to **99**.

....

5   Select the AIDs of the **Working Port** and the **Protection Port** in the respective drop-down list boxes in the group box **Group Member**. The values correspond to the slot designations. The 1:1 MSP is supported for STM-64 ports only.

....

6   Select the **Protocol**. Click on the respective radio button. You may choose one of the following options:

- **Unidirectional** The two transmission directions are switched independently from each other

- **Bidirectional** The two transmission directions are always switched over to the other line in synchronization, even if only one has failed.

....

7   Set the Wait-To-Restore time in the drop-down list box **Wait to Restore:**.

Values between **1** and **60** minutes in steps of one minute are possible. Also the value **INFINITE** can be selected.

....

8   Set the **Hold-off Time** in the respective drop-down lsit box. The hold-off time defines the duration for which a failure condition has to be present before a protection switch is carried out. Thus a toggling can be avoided.

Values between **0** and **10** seconds are possible.

....

....

9 Select the **Alarm Severity Assignment Profile**.

....

10 Click on **Apply** then click on **Close**.

Result:

The window **Create New Protection Group** closes.

E N D   O F   S T E P S

Creating a new 2-fiber MS-SPRing

Overview

....

Purpose   Use this procedure to create a new 2-fiber Multiplex Section Shared Protection Ring (MS-SPRing).

Related information   For related information, see:

- "Protection mechanisms" (18-10)
- "2-fiber MS-SPRing" (18-13)
- Chapter 3, "Management communication setup"

⌐

....

7 - 4 8   **Lucent Technologies**   365-371-522
                                                                        Issue b, October 2001

Procedure

....

Before you begin   Prior to performing this task, you must:

- Verify that all required circuit packs are installed (cf. "Main shelf configuration" (15-9), "Extension shelf configuration" (15-15), "Creating a new circuit pack" (4-17) and "Reassigning a circuit pack" (4-20)).

- Complete the port provisioning for any optical port which is involved in the protection group (cf. "Configuring an optical port" (4-23), "Configuring an electrical port" (4-38) and "Configuring a tributary" (4-43)).

- Verify that no cross-connections have been made on any port to be included in the protection group (cf. "Viewing existing cross-connections" (7-3)).

- Enable the DCC channels and check in the OSI Neighbor Map that all neighbor network elements have connection (cf. Chapter 3, "Management communication setup").

Required privilege code

You must have at least a privilege code of M4, Maintenance, to create new cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new MS-SPRing:

....

1   Call up the window **Create New Protection Group** via **Configuration** → **Create New...**→ **Protection Group** in the **System View** of the CIT.

> **Result:**
>
> On the left side of the window the tab **Ptn Grp** appears. The selected system and bay and the available shelves are displayed.

....

2   Select the high-speed shelf (for the protection of an STM-64 ring) or low-speed shelf (for the protection of an STM-16 ring) to establish the MS-SPRing and click on the pushbutton **Select I/O Shelf**.

> **Result:**
>
> On the right side of the window the **Protection Type Selection** menu appears.

....

....

3   Select in the drop-down list box **Protection Type** the type **2 Fiber MS-SPRing**.

Result:

The parameter fields for the 2-fiber MS-SPRing appear.

....

4   Define the **Protection Group AID** by typing the last digit(s) in the respective text box. This can be max. two digits, a value from **1** to **99** is possible. Please note that you have to choose different AIDs for different protection groups within one network element. Within the whole ring equal Protection Group AIDs may exist.

....

5   Enter the Ring ID. The Ring ID must be defined for the whole ring. For all MS-SPRing protection groups which are defined in network elements belonging to one ring always the same Ring ID has to be inserted.

....

6   Select the AIDs of **East Port** and **West Port** in the respective drop-down list boxes in the group box **Group Member**. The values correspond to the slot designations (cf. "Main shelf configuration" (15-9), "Extension shelf configuration" (15-15) and "Overview of access identifiers" (15-18)).

Important! The MS-SPRing related STM-16 circuit pack pairs have to be plugged into the following dedicated port unit slot pairs: 02-04, 06-08, 10-12, 14-16, 02-16, 04-14, 06-12, 08-10.

....

7   Set the Wait-To-Restore time in the drop-down list box **Wait to Restore:**.

Values between **1** and **12** minutes in steps of one minute are possible. Also the value **INFINITE** can be selected.

....

8   Verify that all parameters are correct. Click on **Apply** to make the changes.

Result:

If the creation of the MS-SPRing protection group was successful, a DCC Termination Provisioning message appears indicating that the LAPD role has been set at User Side (default). This setting can be modified (cf. "Configuring data

....

communication channels" (3-39)). If there are insufficient DCC
channels available for termination, a denial message appears.

....

9 If the creation of the MS-SPRing protection group was successful
click on **OK**, then click on **Close**.

Otherwise delete one or two DCC terminations in order to create the
MS-SPRing. Two free LAPD channels are necessary (cf. "Configuring
data communication channels" (3-39)).

....

10 Repeat Step 1 to Step 9 for each network element in the ring.
E N D   O F   S T E P S

....

365-371-522
Issue b, October 2001

Lucent Technologies

7 - 5 1

Creating a Local NUT configuration

Overview

Purpose Use this procedure to create a Local NUT configuration for a local NE in an 2-fiber MS-SPRing protected ring. The Local NUT configuration defines which working timeslots shall be (temporarily) not protected or, which protection timeslots shall be (temporarily) not preempted by the MS-SPRing, respectively.

Related information For related information, see:

- "Creating a new 2-fiber MS-SPRing" (7-48)

- "2-fiber MS-SPRing with Non-preemptible Unprotected Traffic (NUT)" (18-17)

- "Viewing the Local and Operational NUT configuration" (7-55)

- "Creating a new 2-fiber MS-SPRing" (7-48)

Procedure

....

Before you begin   Prior to performing this procedure you must have a detailed
knowledge on the cross-connections switched within the ring. You
must know in detail the priority of the traffic in each timeslot.

Required privilege code

You must have at least a privilege code of M4+P1, Maintenance and
Provisioning, to create a new MS-SPRing and to configure the NUT
feature.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   ....

1   Create a 2-fiber MS-SPRing as described in "Creating a new 2-fiber
MS-SPRing" (7-48).

....

2   Select in the **System View Configuration** → **Provision....** Click on
the tab **Ptn Grp** and select the 10G ring. Click on the **Provision**
button.

> **Result:**
>
> The window **Provision Parameters for Protection Group or
> Equipment** opens. The **NUT granularity** of the ring is
> displayed.
>
> The following values are possible:
>
> - **VC-3**
>
> - **VC-4**
>
> If a ring is composed of different NE types with different
> tributary rates, the granularity corresponds to the NE with the
> highest tributary rate, because this NE cannot support the lower
> rates.

....

3   Select the **NUT rate**. This is the rate of the concatenated group of
time slots for which the **Protection Attribute** is valid.

Possible values are:

- **VC-3**

- **VC-4**

....

- **VC-4–4c**

- **VC-4–16c**

....

4 Select the **Time Slot Number**.

Possible values are:

- for VC-3: **1...96**

- for VC-4:**<3n+1>** (n = 0...31)

- for VC-4–4c: **<12n+1>** (n = 0...7)

- for VC-4–16c: **<48n+1>** (n = 0...1)

....

5 Select the **Protection Attribute**. The Protection Attrubute is applied to the working timeslot. The value for the corresponding protection timeslot is set automatically.

The following values are possible

- **Protected** (default)

- **Not Protected**

- **Temporary Not Protected**

....

6 Click on **OK** in order to apply the settings.

E ND OF S TEPS

....

....

7 - 5 4 **Lucent Technologies** 365-371-522
Issue b, October 2001

Viewing the Local and Operational NUT configuration

Overview

Purpose Use this procedure to check the Local or Operational NUT configuration.

Related information For related information, see:

- "Creating a Local NUT configuration" (7-52)

- "Creating a new 2-fiber MS-SPRing" (7-48)

- "2-fiber MS-SPRing with Non-preemptible Unprotected Traffic (NUT)" (18-17)

Procedure

....

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

Required privilege code

You must have at least a privilege code of M4+P1, Maintenance and
Provisioning, to view the configuration of an MS-SPRing and the
NUT feature.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   ....

1   Select the window **View Protection** via **View → Protection...** via in
the **System View** of the *WaveStar* CIT.

....

2   Choose the 10G ring and click on the **Select** button.

....

3   Select the tab **Provisionable Parameters** and one of the settings

- **Local** (view the settings of the local node)

- **Operational** (view the settings for the ring)

- **Both** (default)

....

4   Click on the button **View NUT**.

       Result:

       In this window you can check the settings for the NUT feature
as described in "Creating a Local NUT configuration" (7-52)
"2-fiber MS-SPRing with Non-preemptible Unprotected
Traffic (NUT)" (18-17).

E N D   O F   S T E P S

....

⌐

....

7 - 5 6   **Lucent Technologies**   365-371-522
Issue b, October 2001

Creating a bidirectional DNI between two MS-SPRing protected rings

Overview

Purpose   Use this procedure to create a bidirectional DNI (Dual Node Ring Interworking) protection between two rings with a 2-fiber MS-SPRing.

Related information   For related information, see

- "Dual Node Ring Interworking" (18-23)

Procedure

....

Before you begin   Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new cross connection:
....

1   Call up the **Cross Connection Wizard** via **Configuration** → **Cross Connections...** in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Create a new cross-connection** and click on **Next>**.

     Result:

     Screen 1 appears.

....

3   Define the cross connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

- **VC-3**(default value)
- **VC-4**
- **VC-4-4c**
- **VC-4–16c**

Please note that it is not possible to proceed to the next window before selecting the cross connection rate.

....

Creating a bidirectional DNI between two
MS-SPRing protected rings
Procedure

Traffic provisioning

....

4   Define the type of DNI by clicking on the respective radio button in
the group box **Type of Cross-Connection**. The following values are
possible:

- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing
  Primary Node** for the interconnection of two rings via four DNI
  nodes
  This type of DNI is realized by a connection between two
  different nodes (primary nodes) each belonging to one of the two
  protected rings. The broadcast and the switch function are located
  in two different network elements. Furthermore there are two or
  three other network elements involved in the DNI which realize
  the rerouting of the protected signals (secondary nodes).

- **Ring Interworking, Drop & Continue, BLSR/MS-SPRing
  Primary Node in Same NE** for a DNI with collapsed nodes
  In this type of DNI the broadcast and the switch function are
  implemented in one network element, and there may be also only
  one secondary node.

....

5   Click on **Next>** to proceed to the next window.

Result:

Screen 2 appears. A depiction of the cross connections in the
primary node (the NE to which you are connected and for which
you are creating the DNI connections) is displayed
automatically.

....

6   Select the connection to the secondary node(s) via the button
Select.... Proceed as described in the windows **From/To Secondary
(Ring1/Ring2) Node Tributary**.

Result:

The tributaries which establish the connection to the terminating
nodes (B, D) are displayed.

....

7

IF	THEN
you have selected the DNI with collapsed nodes,	go to Step 9.
you have selected the DNI with four nodes,	go to Step 8.

....

Creating a bidirectional DNI between two
MS-SPRing protected rings
Procedure

Traffic provisioning

....

8 Select the connection to the second ring (C) via the button **Select....**
Proceed as described in the window **From/To Other Ring Tributary**.

> **Result:**
>
> The complete implementation of the DNI protection is
> displayed.

....

9 Define the role of the tributaries as working or protection tributary by
clicking on the respective check box(es).

In a DNI with collapsed nodes, the STM-64 line port is the working
port!

....

10 Click on the **Next>** button.

> **Result:**
>
> **Screen 3** opens.

....

11 Select the terminating node TID and the secondary node TID in the
drop-down list boxes **Term Node NE Name:** and **Sec Node NE
Name:**.

....

12 Insert a name for the protection group in the text box **PPG Name**.

....

13 Define in the drop-down list box **PP Reversion Behavior**, whether
the DNI shall operate in revertive or in non-revertive mode .

....

14 Define in the drop-down list box **PP Holdoff Behavior**, whether a
Holdoff time shall pass before a protection switch is performed. This
is necessary to avoid a double switch of MS-SPRing and DNI.

The default value is 100 ms, but the holdoff time can be modified in
the window **Path Protection Type Provisioning**. The selected value
is valid for all path protection which are configured for the network
element.

....

15 Click on the **Finish** button to apply your settings.

....

16 If required, set the holdoff time in the window **Path Protection Type
Provisioning** which is accessible via **Configuration → Path**

....

Creating a bidirectional DNI between two
MS-SPRing protected rings
Procedure

Traffic provisioning

Protection Type.... Note that the setting is valid for all path protections in the network element.

E ND OF S TEPS

Creating an unidirectional DNI between two protected rings.

Overview

Purpose   Use this procedure to create a unidirectional DNI protection (1-way path protection) between two rings with a 2-fiber MS-SPRing or one MS-SPRing protected ring and one SNCP protected ring.

Related information   For related information, see

- "Creating a new cross-connection" (7-7)

- "Creating a bridge" (7-12)

- "Creating an unidirectional path protection" (7-69)

⌐

Procedure

....

Before you begin   Prior to performing this task, you must complete the configuration of
the rings which are involved in the DNI. Furthermore you must have
a detailed knowledge of the ring topology of the rings involved and
the paths to be protected.

You have to distinguish between several possibilities of the network
topology which are listed below:

- 2 MS-SPRing protected rings (with or without collapsed nodes)

- A MS-SPRing protected ring, 1 SNCP ring

    - with an interconnection via four NEs; the direction of the
      protected 1-way cross-connection is from SNCP ring to
      MS-SPRing

    - with an interconnection via four NEs; the direction of the
      protected 1-way cross-connection is from MS-SPRing to
      SNCP ring

    - with an interconnection via collapsed nodes; the direction of
      the protected 1-way cross-connection is from SNCP ring to
      MS-SPRing

    - with an interconnection via collapsed nodes; the direction of
      the protected 1-way cross-connection is from MS-SPRing to
      SNCP ring

Please note that for an interworking between one SNCP protected
ring and one MS-SPRing protected ring (primary node) with both
rings in the same NE (collapsed nodes), the interconnection in
the direction from the SNCP ring to the MS-SPRing has to be
realized through an external connection, i.e. through an additional
tributary interface. Note that this does not apply to the secondary
node. (cf. "Dual Node Ring Interworking between MS-SPRing
and SNCP ring" (18-29)).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create
new cross-connections and the DNI.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

....

Creating an unidirectional DNI between two
protected rings.
Procedure

Traffic provisioning

**Instructions for a DNI
between two MS-SPRing
protected rings**

....

1
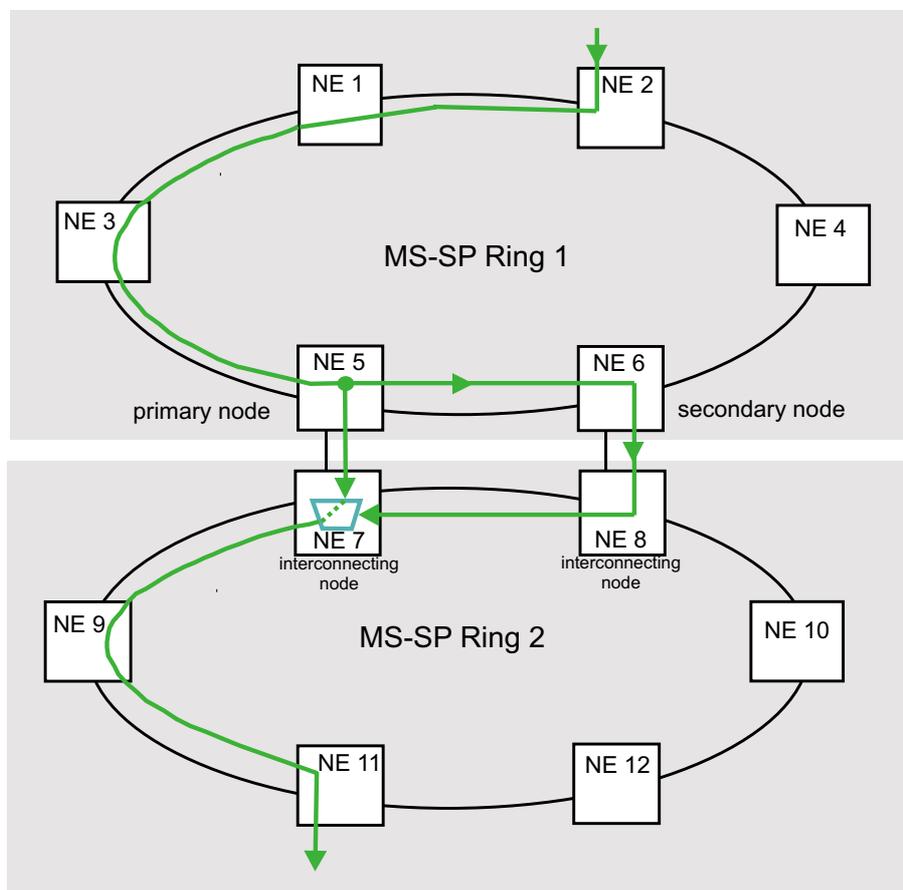
As shown in the graphic above, switch 1-way cross-connections in all
network elements (NE2, NE 1) belonging to the first ring
(MS-SPRing 1), cf. "Creating a new cross-connection" (7-7).

....

2 In the primary node (NE 5) create a broadcast (bridge) to the
secondary node (NE 6) and one interconnecting node (NE 7), cf.
"Creating a bridge" (7-12).

....

3 Create through-connections in the secondary node (NE 6) and the
second interconnecting node (NE 8), cf. "Creating a new
cross-connection" (7-7). In a network topology with collapsed nodes
only one through connection is necessary.

....

4 Create a 1-way path protection in the first interconnecting node (NE
7) which establishes the selector between the signal from the primary

....

Creating an unidirectional DNI between two
protected rings.
Procedure

Traffic provisioning

node (NE 5)and the other interconnecting node (NE 8), cf. "Creating
an unidirectional path protection" (7-69). In a network topology with
collapsed nodes, the broadcast and the 1-way path protection are in
the same network element.

....

5 Create 1-way cross-connections in all network elements (NE 9, NE
11) belonging to the second ring (MS-SPRing 2), cf. "Creating a new
cross-connection" (7-7).

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

**Instructions for a DNI
between one MS-SPRing
protected ring and one
SNCP ring via four NEs
(direction SNCP →
MS-SPRing)**

....

1
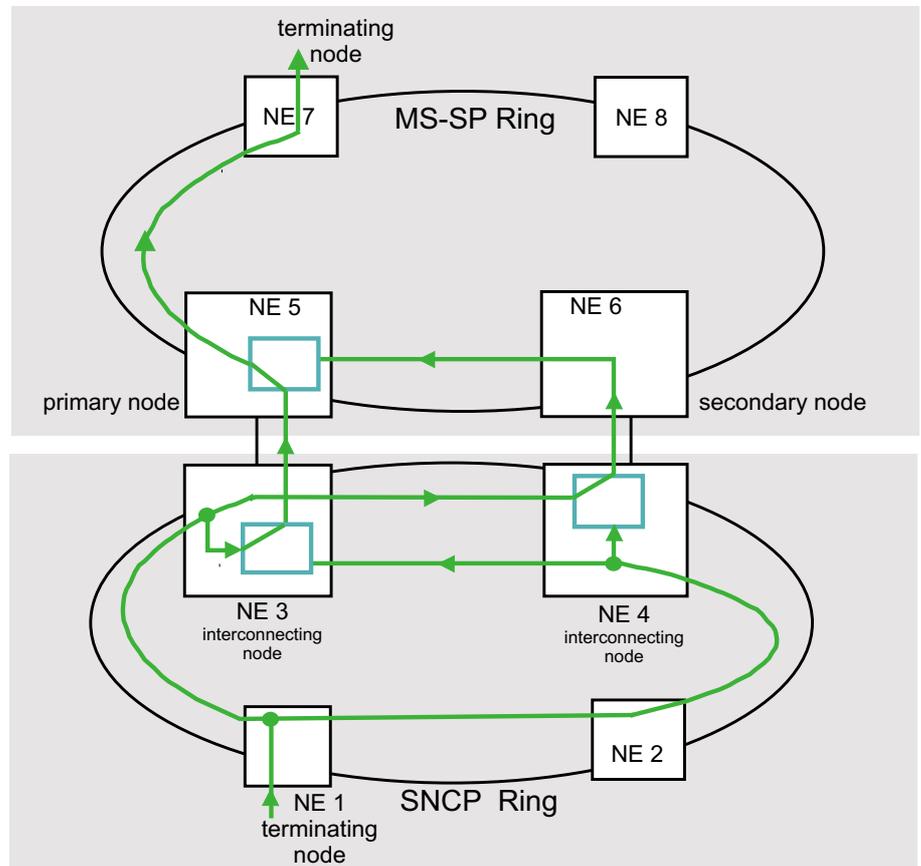
As shown in the graphic above, switch a broadcast (bridge) in the
terminating node of the SNCP ring, where the cross-connection starts
(NE 1), cf. "Creating a bridge" (7-12).

....

2 In the first interconnecting node (NE 3) create a 1-way path protection
between the two signals broadcasted at the terminating node (NE 1),
cf. "Creating an unidirectional path protection" (7-69).

....

Creating an unidirectional DNI between two
protected rings.
Procedure

Traffic provisioning

....

3 Create additionally a broadcast to the second interconnecting node
(NE 4) and the primary node (NE 5) in the same network element
(NE 3), cf. "Creating a bridge" (7-12).

....

4 Create through-connections in all network elements of the SNCP ring
which are not involved in the DNI (e.g. NE 2), cf. "Creating a new
cross-connection" (7-7).

....

5 In the second interconnecting node (NE 4) create a 1-way path
protection between the broadcasted signal from the first
interconnecting node (NE 3) and the signal which is received via the
SNCP ring (from NE 2), cf. "Creating an unidirectional path
protection" (7-69).

....

6 Create additionally a broadcast to the first interconnecting node (NE
3) and the secondary node (NE 6) in the same network element (NE
3), cf. "Creating a bridge" (7-12).

....

7 Create a through-connection in the secondary node (NE 6), cf.
"Creating a new cross-connection" (7-7).

....

8 Create a 1-way path protection between in the primary node (NE 5)
between the signal from the secondary node (NE 6) and from the
neighbour interconnecting node (NE 3), cf. "Creating an unidirectional
path protection" (7-69).

....

9 Create 1-way cross-connections in all network elements between the
primary node and the terminating node (NE 7) of the MS-SPRing
protected ring, cf. "Creating a new cross-connection" (7-7).

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

Creating an unidirectional DNI between two
protected rings.
Procedure

Traffic provisioning

**Instructions for a DNI
between one MS-SPRing
protected ring and one
SNCP ring via four NEs
(direction MS-SPRing →
SNCP)**

1
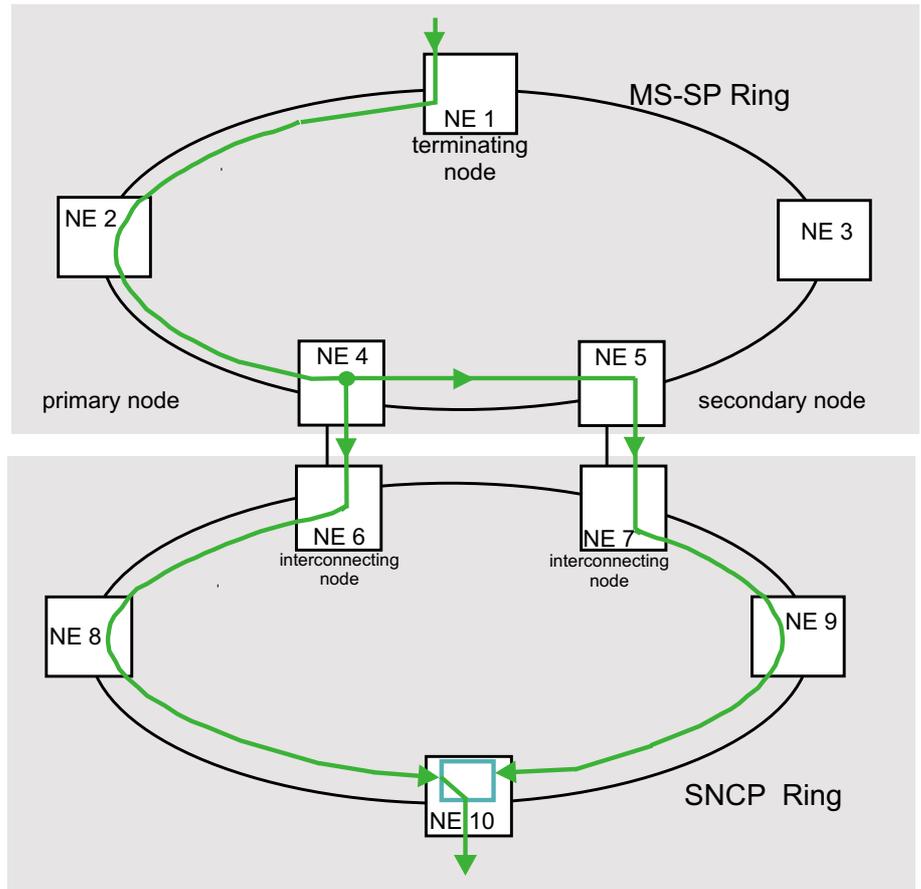
Create a 1-way cross-connection in the terminating node (NE 1) of
the MS-SPRing protected ring, cf. "Creating a new cross-connection"
(7-7).

2 Create through-connections in all network elements between the
terminating node and the primary node of the MS-SPRing protected
ring (e.g. NE 2), cf. "Creating a new cross-connection" (7-7).

3 Create a broadcast (bridge) in the primary node (NE 4) with one leg
to the secondary node (NE 5) and one to the neighbour
interconnecting node (NE 6), cf. "Creating a bridge" (7-12).

4 Create a through-connection through the secondary node (NE 5), cf.
"Creating a new cross-connection" (7-7).

Creating an unidirectional DNI between two
protected rings.
Procedure

Traffic provisioning

....

5 Create a through-connection in each interconnecting node (NE 6, NE 7) of the SNCP ring in a way that the signals are distributed via the ring in opposite directions, cf. "Creating a new cross-connection" (7-7).

....

6 Create through-connections in all network elements of the SNCP ring (e.g. NE 8, NE 9), cf. "Creating a new cross-connection" (7-7).

....

7 Create a 1-way path protection in the terminating node (NE 10) of the SNCP ring, cf. "Creating an unidirectional path protection" (7-69).

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

Instructions for a DNI between one MS-SPRing protected ring and one SNCP ring with collapsed nodes (direction SNCP → MS-SPRing)

....

1 Proceed as described in "Instructions for a DNI between one MS-SPRing protected ring and one SNCP ring via four NEs (direction SNCP → MS-SPRing)" (7-65). Please note that the primary node (NE 5) and the first interconnecting node (NE 3) are the same network element in this case.

....

2 Create a 1-way through-connection through the primary node/interconnecting node as an external connection via an additional port unit.

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

Instructions for a DNI between one MS-SPRing protected ring and one SNCP ring with collapsed nodes (direction MS-SPRing → SNCP)

....

1 Proceed as described in "Instructions for a DNI between one MS-SPRing protected ring and one SNCP ring via four NEs (direction MS-SPRing → SNCP)" (7-67). Please note that the primary node (NE 4) and the first interconnecting node (NE 6) are the same network element in this case.

....

2 Create a 1-way through-connection through the primary node/interconnecting node as an external connection via an additional port unit.

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

....

Creating an unidirectional path protection

Overview

Purpose   Use this procedure to create a 1-way path protection, e.g. as part of a DNI.

Related information   For related information, see

- "Dual Node Ring Interworking" (18-23)

⌐

Procedure
....

Before you begin　Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected. Please note that for an interworking between one SNCP protected ring and one MS-SPRing protected ring (primary node) with both rings in the same NE (collapsed nodes), the interconnection in the direction from the SNCP ring to the MS-SPRing has to be realized through an external connection, i.e. through an additional tributary interface. Note that this does not apply to the secondary node. (cf. "Dual Node Ring Interworking between MS-SPRing and SNCP ring" (18-29)).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross connections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions　Complete the following steps to create a new cross-connection:
....

1　In the **System View** of the *WaveStar* CIT, via **Configuration** → **Cross Connection...,** call up the **Cross Connection Wizard** .

....

2　Click on the radio button **Create a new cross-connection** and click on **Next>**.

　　　Result:

　　　Screen 1 appears.

....

3　Define the cross connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

- **VC-3**(default value)

- **VC-4**

- **VC-4-4c**

- **VC-4-16c**

Please note that it is not possible to proceed to the next window before selecting the cross-connection rate.

....
　Lucent Technologies

....

4   Select **1-Way Path-Protected** by clicking on the respective radio
button in the group box **Type of Cross-connection**.

....

5   Click on **Next>** to proceed to the next window.

> **Result:**
>
> **Screen 2** appears. A depiction of the DNI cross-connection in
> the NE to which you are connected is displayed.

....

6   Select the first leg source (A), the destination (B) and the second leg
source (C) as described in the window via the buttons **Select...**.
Proceed as described in the windows **First Leg Source Tributary**,
Destination Tributary and **Second Leg Source Tributary**.

....

7   Define the working leg and the protection leg by clicking on the
respective check box.

Important! In a DNI with collapsed nodes, the STM-64 line port
must be the working port!

....

8   Click on the **Next>** button.

> **Result:**
>
> **Screen 3** opens.

....

9   Select the working source NE TID, the protection source NE and the
destination NE TID in the drop-down list boxes **Wkg Source NE
Name:**, **Destination NE Name:** and **Prot Source NE Name:**.

....

10   Select the **Output Mode**. The following values are possible:

- **NORM** refers to a cross connection which carries "normal"
  traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via
  the respective cross connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped
  signal is transmitted via the respective cross connection.

....

11   Insert a name with up to 24 characters for the protection group in the
text box **PPG Name**.

....

....

12   Define in the drop-down list box **PP Reversion Behavior,** whether
the DNI shall operate in revertive or in non-revertive mode.

....

13   Define in the drop-down list box **PP Holdoff Behavior**, whether a
Holdoff time shall pass before a protection switch is performed. This
is necessary to avoid a double switch of MS-SPRing and DNI.

The default value is 100 ms, but the holdoff time can be modified in
the window **Path Protection Type Provisioning**. The selected value
is valid for all path protection which are configured for the network
element.

....

14   Click on the **Finish** button to apply your settings.

....

15   If required, set the holdoff time in the window **Path Protection Type
Provisioning** which is accessible via **Configuration → Path
Protection Type...**. Note that the setting is valid for all path
protections in the network element.

E N D   O F   S T E P S

....

Creating a bidirectional DNI between one MS-SPRing protected ring and one SNCP protected ring.

Overview

Purpose Use this procedure to create a bidirectional DNI protection (2-way path protection) between one ring which is protected by a 2-fiber MS-SPRing and one ring which is protected by an SNCP. The following procedure has to be carried out in the interconnecting nodes of the SNCP protected ring. In the primary and secondary node belonging to the MS-SPRing protected ring the DNI has to be established as described in "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57).

Related information For related information, see

- "Dual Node Ring Interworking between MS-SPRing and SNCP ring" (18-29)

- "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57)

- "Creating an unidirectional path protection" (7-69)

⌐

Creating a bidirectional DNI between one
MS-SPRing protected ring and one SNCP
protected ring.

Traffic provisioning

Procedure

....

Before you begin Prior to performing this task, you must complete the configuration of the rings which are involved in the DNI. Furthermore you must have a detailed knowledge of the ring topology of the rings involved and the paths to be protected. Please note that for a DNI with both rings in the same NE you need an additional pair of tributary ports to establish the interconnection via external connections. This procedure describes the creation of the DNI in the NEs belonging SNCP protected ring. For the complete configuration of the interworking between the two rings the creation of the DNI in the primary and secondary node belonging to the MS-SPRing protected ring as described in "Creating a bidirectional DNI between two MS-SPRing protected rings" (7-57) is necessary as well.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections and the DNI.

Required equipment

The following equipment is required to perform this task:

* *WaveStar*® CIT

Instructions Complete the following steps to create a DNI-protected cross-connection:

....

1 In the **System View** of the *WaveStar* CIT, via **Configuration** → **Cross Connection...**, call up the **Cross Connection Wizard**.

....

2 Click on the radio button **Create a new cross-connection** and click on **Next>**.

> **Result:**
>
> **Screen 1** appears.

....

3 Define the cross-connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

* **VC-3 (default value)**

* **VC-4**

* **VC-4-4c**

* **VC-4-16c**

....

Creating a bidirectional DNI between one
MS-SPRing protected ring and one SNCP
protected ring.
Procedure

Traffic provisioning

Please note that it is not possible to proceed to the next window
before selecting the cross-connection rate.

....

4 Select **Ring Interworking, Drop and Continue, UPSR/SNCP Node**
by clicking on the respective radio button in the group box **Type of
Cross-connection**.

....

5 Click on **Next>** to proceed to the next window.

   Result:

   Screen 2 appears. A depiction of the DNI cross-connection in
   the NE to which you are connected is displayed.

....

6 Via the buttons **Select...**, select the first leg source (A) defining the
connection to the terminating node where the VC has been coupled in,
the destination tributary (B) defining the connection to the
MS-SPRing protected ring and the second leg source (C) defining the
connection to the second interconnecting node.
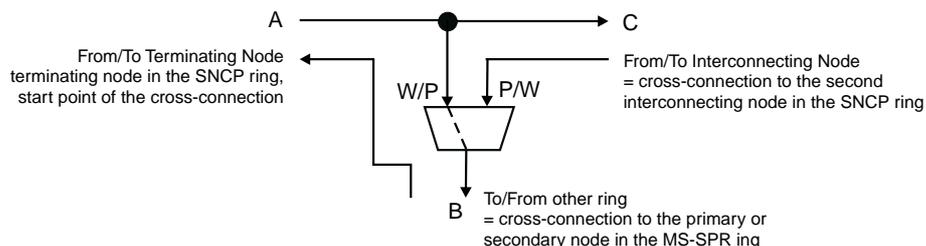
Proceed as described in the windows **From/To Terminating Node**,
From/To Interconnecting Node and **To/From Other Ring**.

....

7 Define the working leg and the protection leg by clicking on the
respective check box.

....

8 Click on the **Next>** button.

   Result:

   Screen 3 opens.

....

9 Select the **Terminating Node NE Name**, which is the TID of the
terminating node in the SNCP ring.

....

Creating a bidirectional DNI between one
MS-SPRing protected ring and one SNCP
protected ring.
Procedure

Traffic provisioning

10 Select the **Other Ring Node NE Name**, which is the TID of the terminating node in the MS-SPRing protected ring.

11 Select the **Interconnecting Node NE Name**, which is the TID of the second interconnecting node of the DNI.

12 Select the **Output Mode**. The following values are possible:

- **NORM** refers to a cross connection which carries "normal" traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via the respective cross connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross connection.

13 Insert a name with up to 24 characters for the protection group in the text box **PPG Name**.

14 Define in the drop-down list box **PP Reversion Behavior,** whether the DNI shall operate in revertive or in non-revertive mode.

15 Define in the drop-down list box **PP Holdoff Behavior**, whether a Holdoff time shall pass before a protection switch is performed.

The default value is 100 ms, but the holdoff time can be modified in the window **Path Protection Type Provisioning**. The selected value is valid for all path protection which are configured for the network element.

16 Click on the **Finish** button to apply your settings.

17 If required, set the holdoff time in the window **Path Protection Type Provisioning** which is accessible via **Configuration → Path Protection Type...**. Note that the setting is valid for all path protections in the network element.

E N D   O F   S T E P S

Creating an Adjunct Path Protection

Overview

Purpose Use this procedure to, in addition to an existing path protection, establish a function in the receiving network element, that forwards the signal to a second output.

Procedure

Before you begin   Prior to performing this task, you must complete the configuration of a unidirectional DNI (1-Way Path Protection).

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections with Adjunct path protections.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new cross-connection with an Adjunct path protection:

1   Call up the **Cross-connection Wizard** via **Configuration →**
cross-connection... in the system view of the *WaveStar* CIT.

2   Click on the radio button **Create a new cross-connection** and click
on **Next>**.

> **Result:**
>
> **Screen 1** appears.

3   Select **1-Way Adjunct Path-Protected** by clicking on the respective
radio button in the group box **Type of Cross-connection**.

4   Click on **Next>** and proceed as described in the window. Select the
path protected cross-connection to which the adjunct is to be added.

5   Click on the **Next>** button.

> **Result:**
>
> **Screen 3** opens with a depiction of the existing path-protected
> cross-connection and the unassigned adjunct output.

6   Select the adjunct output via the **Select...** button. Proceed as described
in the window **Adjunct Output Tributary**.

7   Click on the **Next>** button.

Result:

Screen 4 opens.

....

8   Select the **Wkg Source NE Name**, the **New Adjunct Output NE
Name** and the **Prot Source NE Name** in the respective drop-down list
boxes.

....

9   Select the **Output Mode**. The following values are possible:

- **NORM** refers to a cross-connection which carries "normal"
  traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via
  the respective cross-connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped
  signal is transmitted via the respective cross-connection.

....

10   Insert a name with up to 24 characters for the protection group in the
text box **PPG Name**.

....

11   Click on the **Finish** button to apply your settings.
E N D   O F   S T E P S
....

....

365-371-522
Issue b, October 2001

Lucent Technologies

7 - 7 9

Creating a bidirectional SNCP

Overview

....

Purpose   Use this procedure to create a bidirectional SNCP (Sub-Network Connection Protection). This kind of SNCP can be used to protect an SDH signal within one ring. It is realized via a broadcast in transmission direction and the protection switch in receive direction. Configure this type of SNCP for the two NEs between which the protected cross connection is to be established.

Related information   For related information, see

- "Sub-Network Connection Protection (SNCP)" (18-19)

....

7 - 8 0   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create
new cross-connections protected with an SNCP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to create a new cross-connection
protected with a bidirectional single-ring SNCP:

....

1   Call up the **Cross-connection Wizard** via **Configuration** →
cross-connection... in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Create a new cross-connection** and click
on **Next>**.

> **Result:**
>
> **Screen 1** appears.

....

3   Define the cross-connection rate in the drop-down list box **Enter
Rate:**. The following values are possible:

- **VC-3**(default value)
- **VC-4**
- **VC-4-4c**
- **VC-4–16c**

....

4   Select **UPSR/SNCP Ring Add, Drop** by clicking on the respective
radio button in the group box **Type of Cross-connection**.

....

5   Click on **Next>** to proceed to the next window.

> **Result:**
>
> **Screen 2** appears. A depiction of the cross-connection in the NE
> to which you are connected and for which you are creating the
> SNCP is displayed.

....

....

6   Select the Path 1 tributary (A), the Add/Drop (B) and the Path 2
tributary (C) as described in the window via the buttons **Select...**.
Proceed as described in the windows **Path 1 Tributary**, **Add/Drop
Tributary** and **Path 2 Tributary**.

....

7   Define the working path and the protection path by clicking on the
respective check box.

....

8   Click on the **Next>** button.

>   **Result:**

>   **Screen 3** opens.

....

9   Select the **Path 1 NE TID**, the **Add/Drop NE TID** and the **Path 2 NE
TID** in the respective drop-down list boxes. This is necessary if the
network element is part of an MS-SPRing. Otherwise proceed to Step
10.

....

10   Select the **Output Mode** for the bidirectional cross-connection in the
group boxes **Source to Destination** and **Destination to Source**. The
following values are possible:

- **NORM** refers to a cross-connection which carries "normal"
traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via
the respective cross-connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped
signal is transmitted via the respective cross-connection.

....

11   Insert a name with up to 24 characters for the protection group in the
text box **PPG Name**.

....

12   Define in the drop-down list box **PP Reversion Behavior**, whether
the SNCP shall operate in revertive or non-revertive mode.

....

13   Define in the drop-down list box **PP Holdoff Behavior**, whether a
Holdoff time shall pass before a protection switch is performed. This
is necessary to avoid a double switch of MS-SPRing and SNCP.

....

The default value is 100 ms, but the holdoff time can be modified in the window **Path Protection Type Provisioning**. The selected value is valid for all path protection which are configured for the network element.

....

14   Click on the **Finish** button to apply your settings.

....

15   If required, set the holdoff time in the window **Path Protection Type Provisioning** which is accessible via **Configuration** → **Path Protection Type...**. Note that the setting is valid for all path protections in the network element.

E N D   O F   S T E P S

....

365-371-522   **Lucent Technologies**   7 - 8 3
Issue b, October 2001

Creating a bidirectional ring-to-ring SNCP

Overview

Purpose   Use this procedure to create two SNCPs within one NE which protect a bidirectional connection that is routed via two rings. Each SNCP protects the connection in one ring.

Related information   For related information, see

- "Sub-Network Connection Protection (SNCP)" (18-19)

⌐

Procedure

....

Before you begin   Prior to performing this task, you must complete the configuration of the rings which are involved in the SNCP. Furthermore you must have a detailed knowledge on the ring topology of the rings involved and the paths to be protected.

Required privilege code

You must have at least a privilege code of P3, Provisioning, to create new cross-connections proteced with an SNCP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new cross-connection:

....

1   Call up the **cross-connection Wizard** via **Configuration** → **cross-connections...** in the **System View** of the *WaveStar* CIT.

....

2   Click on the radio button **Create a new cross-connection** and click on **Next>**.

> **Result:**
>
> **Screen 1** appears.

....

3   Define the cross-connection rate in the drop-down list box **Enter Rate:**. The following values are possible:

- **VC-3**(default value)

- **VC-4**

- **VC-4-4c**

- **VC-4–16c**

....

4   Select **UPSR/SNCP Ring-to-Ring, Single Node Interconnection, Same NE** by clicking on the respective radio button in the group box **Type of Cross-connection**.

....

5   Click on **Next>** to proceed to the next window.

....

Result:

Screen 2 appears. A depiction of the cross-connections in the
NE to which you are connected and for which you are creating
the SNCP is displayed.

....

6   Select the tributaries as described in the window via the buttons
Select.... Proceed as described in the windows **PPG2 Output
Tributary**, **Adjunct PPG2 Output Tributary**, **PPG1 Output Tributary**
and **Adjunct PPG1 Output Tributary**.

....

7   Define the two working paths by clicking on the respective check
boxes.

....

8   Click on the **Next>** button.

Result:

Screen 3 opens.

....

9   Select the **PPG1 Wkg Source NE Name**, the **PPG2 Wkg Source NE
Name**, the **PPG1 Prot Source NE Name** and the **PPG2 Prot Source
NE Name** in the respective drop-down list boxes. This is necessary, if
the network element is part of and MS-SPRing. Otherwise proceed to
Step 10.

....

10 Select the **Output Mode** for the protection groups PPG1 and PPG2 in
the respective group boxes. The following values are possible:

- **NORM** refers to a cross-connection which carries "normal"
  traffic.

- **AIS** is a test and maintenance setting. An AIS is transmitted via
  the respective cross-connection.

- **IDLE/UNEQ** is a test and maintenance setting. An unequipped
  signal is transmitted via the respective cross-connection.

....

11 Insert a name with up to 24 characters for the protection group in the
text box **PPG Name**.

....

12 Define in the drop-down list box **PP Reversion Behavior**, whether
the SNCP shall operate in revertive or in non-revertive mode.

....

....

13   Define in the drop-down list box **PP Holdoff Behavior**, whether a
Holdoff time is to expire before a protection switch is performed.

....

14   Click on the **Finish** button to apply your settings.

E N D O F S T E P S

Deleting a protection group

Overview

Purpose   Use this procedure to delete protection groups which have been provisioned for the system. This can be 1+1 MSPs, 1:1 MSPs or 2-fiber MS-SPRings (2-fiber BLSRs).

⌐

Procedure

....

Before you begin   If you intend to remove an NE completely (i.e., physically) from an MS-SPRing protected ring, perform the following before deleting the MS-SPRing protection groups in this NE and removing circuit packs or cables:

In the adjacent NEs (NE B and NE D in the example, see figure below) of the NE you want to remove (here NE A), perform a forced switch to protection (cf. "Switching a 2–fiber MS-SPRing" (8-6)). In NE B, the direction for the forced switch is East, in NE D the direction is West.
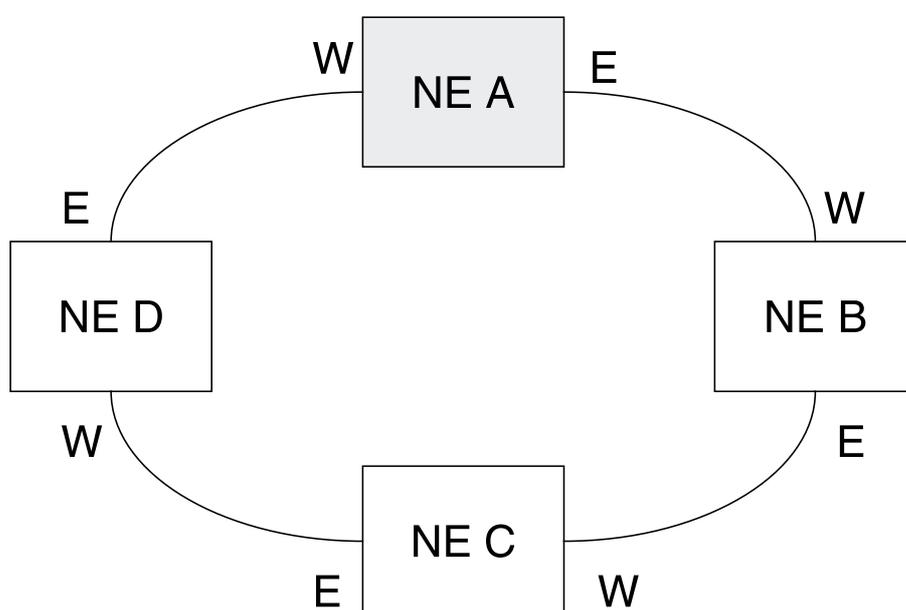
Required privilege code

You must have at least a privilege code of M4, Maintenance, to remove protection groups from the system.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to remove equipment from the system:

....

1   Call up the window **Delete** via **Configuration** → **Delete...** in the **System View** of the *WaveStar* CIT.

....

2 Select the tab **Ptn Group**.

3 Select the shelf in which the protection group is located.

4 Select the protection group

5 Click on **Select** to apply you changes. A confirmation window opens containing the name of the protection group, the protection type and the current group members. Click on **Yes** to confirm your changes. Click on **No** to discard your changes.

Deletion of a protection group which has a cross connection established of an active protection switch on one or more of the involved ports will be denied by the network element.

E N D   O F   S T E P S

8 Traffic maintenance

Overview

Purpose   This chapter describes the traffic maintenance procedures. This comprises the manual and forced switch of network protections.

Contents

Modifying the Protection Reversion parameter for an MSP

Overview

Purpose Use this procedure to modify the 1+1 MSP Protection Reversion parameter, this means to change the operation mode from revertive to non-revertive and the other way round.

Related information For related information, see:

- "Creating a new 1+1 MSP" (7-40)
- "Multiplex Section Protection" (18-11)
- "Switching an MSP" (8-4)

Procedure

....

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

Required privilege code

You must have at least a privilege code of M4, Maintenance, to
modify a 1+1 MSP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions

IF	THEN
Protection Reversion is set to **Disabled**,	select in the **System View Fault** → **Protection Switch...** and perform a protection switch **Forced to Working** in the **Protection Switch** window. After this, set the Parameter **Protection Reversion** to **Enabled** in the **Provision Parameters for Protection Group or Equipment** window. Click on **Apply**. Finally select again the **Protection Switch** window and perform a **Clear** command.**Important!** A forced switch to a faulty section could cause a traffic interruption. Perform a forced switch only to a section which is working fault-free.
Protection Reversion is set to **Enabled**,	select in the **System View Fault** → **Protection Switch...** and perform a protection switch **Lockout of Protection** in the **Protection Switch** window. After this, set the Parameter **Protection Reversion** to **Disabled** in the **Provision Parameters for Protection Group or Equipment** window. Click on **Apply**. Finally select again the **Protection Switch** window and perform a **Clear** command.

⌐

....

Switching an MSP

Overview

....

Purpose Use this procedure to switch from one section to the other in a 1+1 MSP.

Related information For related information, see:

- "Protection mechanisms" (18-10)

- "Multiplex Section Protection" (18-11)

⌐

....

8 - 4 **Lucent Technologies** 365-371-522

Issue b, October 2001

Procedure

....8 - 5

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

Required privilege code

You must have at least a privilege code of M4, Maintenance, to
switch a 1+1 MSP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to switch a 1+1 or 1:1 MSP :

1 Call up the **Protection Switch** window either in the **System View** via
Fault → Protection Switch, or in the **Shelf View,** clicking on a
specific port of a specific pack.

2 Select the working port unit of the respective MSP in the tab **Ptn
Group** on the left side of the window.

> **Result:**
>
> Some data of the protection group is displayed.

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

- **Clear**
- **Lockout of Protection**
- **Forced to Working**
- **Forced to Protection**
- **Manual to Working**
- **Manual to Protection**

Important! A forced switch to a faulty section could cause a traffic
interruption. Perform a forced switch only to a section which is
working fault-free.

4 Click on **Apply**.

E N D   O F   S T E P S

Switching a 2–fiber MS-SPRing

Overview

Purpose Use this procedure to switch from one section to the other in a 2-fiber MS-SPRing.

Related information For related information, see:

- "Protection mechanisms" (18-10)
- "2-fiber MS-SPRing" (18-13)

Procedure

....

Before you begin   Check in the menu **View** → **Rings** → **Ring Map** whether the ring discovery is finished and the ring is complete.

Please note that you do not execute manual switch commands while the ring is incomplete!

Required privilege code

You must have at least a privilege code of M4, Maintenance, to switch a 2-fiber MS-SPRing.

Required equipment

The following equipment is required to perform this task:

- *WaveStar*® CIT

Instructions   Complete the following steps to switch a 2-fiber MS-SPRing:

....

1   Call up the **Protection Switch** window either in the **System View** via **Fault** → **Protection Switch**, or in the **Shelf View,** clicking on a specific port of a specific pack.

....

2   Select the respective MS-SPRing in the tab **Ptn Group** on the left side of the window.

> **Result:**
>
> Some data of the protection group is displayed.

....

3   Select the transmission direction to which the traffic shall be switched in the field **Direction**.The following options are possible:

- **East**
- **West**

....

4   Select the desired switch request in the field **Switch Type**. The following options are possible:

- **Clear**
- **Lockout of Protection, Span**
- **Forced to Protection, Ring**
- **Manual to Protection, Ring**

....

5   Click on **Apply**.

E ND OF S TEPS

Switching a DNI or SNCP

Overview

Purpose   Use this procedure to switch from one path to the other in a DNI or SNCP.

Related information   For related information, see:

- "Dual Node Ring Interworking" (18-23)

- "Sub-Network Connection Protection (SNCP)" (18-19)

Procedure

....

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

Required privilege code

You must have at least a privilege code of M4, Maintenance, to
switch a DNI or SNCP.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions Complete the following steps to switch a DNI or SNCP:

....

1 Call up the **Protection Switch** window either in the **System View** via
Fault → Protection Switch, or in the **Shelf View,** clicking on a
specific port of a specific pack.

....

2 Select the desired DNI or SNCP in the tab **Ptn Group** on the left side
of the window.

> **Result:**
>
> The window **Path Protection Switch** opens.
>
> After selecting the **tab Path Ptn** you can choose between
> **Names** or **AID**.
>
> By giving two or more path protected crossconnections the same
> **Protection group** name, you can select the name of the **path
> protection group** and switch all crossconnections which fall in
> this group manually.

....

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

- **Clear**
- **Lockout of Protection**
- **Forced to Working**
- **Forced to Protection**
- **Manual to Working**
- **Manual to Protection**

....

....

4 Click on **Apply**.

E N D   O F   S T E P S

....

E N D   O F   S T E P S

Viewing the Intershelf Bandwidth Utilization

Overview

Purpose   Use this procedure to query how much of the available bandwidth has been assigned to the specific shelf parts.

⌐

Procedure

....

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

Required privilege code

You must have at least a privilege code of P2, Provisioning, to query
the available bandwidth.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   ....

1   Call up the **View Intershelf Bandwidth Utilization for STM64**
window via **View → Intershelf Bandwidth Utilization...** in the
System View of the CIT.

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

⌐

....

365-371-522
Issue b, October 2001

Lucent Technologies

8 - 1 3

Intershelf Bandwidth Utilization

Overview The **Intershelf Bandwidth Utilization** window allows the user to see how much of the available intershelf bandwidth has been assigned. The proportion is shown in a pie chart for each shelf.

Description The window consists of two tabs: one for the high-speed part and one for the low-speed part of the shelf. Each tab is divided into a display for the incoming (**Ingress**) capacity from other shelves and the outgoing (**Egress**) capacity to other shelves.

The capacity is displayed in VC-3 equivalents.

Data The following table shows the data which is shown in the **View Bandwidth Utilization for STM64** window.

Information field	Possible value	Meaning
The group box **Ingress**		
Total in Use:	**0 ... 192**	Number of VC-3 equivalents that are actually assigned to incoming data from other shelves to this shelf.
Remaining VC-3 Shelf Capacity:	<192 - Ingress Total in Use bandwidth>	Number of VC-3 equivalents that are actually not assigned to incoming data from other shelves to this shelf.
The group box **Egress**		
Total in Use:	**0 ... 192**	Number of VC-3 equivalents that are actually assigned to outgoing data from this shelf to other shelves.
Remaining VC-3 Shelf Capacity:	<192 - Egress Total in Use bandwidth>	Number of VC-3 equivalents that are actually not assigned to outgoing data from this shelf to other shelves.
Shared Bandwidth:	<Ingress Total in Use bandwidth (low-speed shelf) + Ingress Total in Use bandwidth (1st extension shelf) - Egress Total in Use bandwidth (high-speed shelf)	Number of VC-3 equivalents that are actually shared among the low speed shelves.

Capacity distribution The *WaveStar*® CIT displays a report on bandwidth utilization which shows how much of the inter-shelf cross-connection capacity is currently in use and how much remains available for additional cross-connections.

The following figure illustrates the capacity distribution:

Inter-shelf Cross-Connection Capacity Utilization

When LS Shelves are not configured to share the inter-shelf capacity (then b = 0 and c = a), just see shelf A
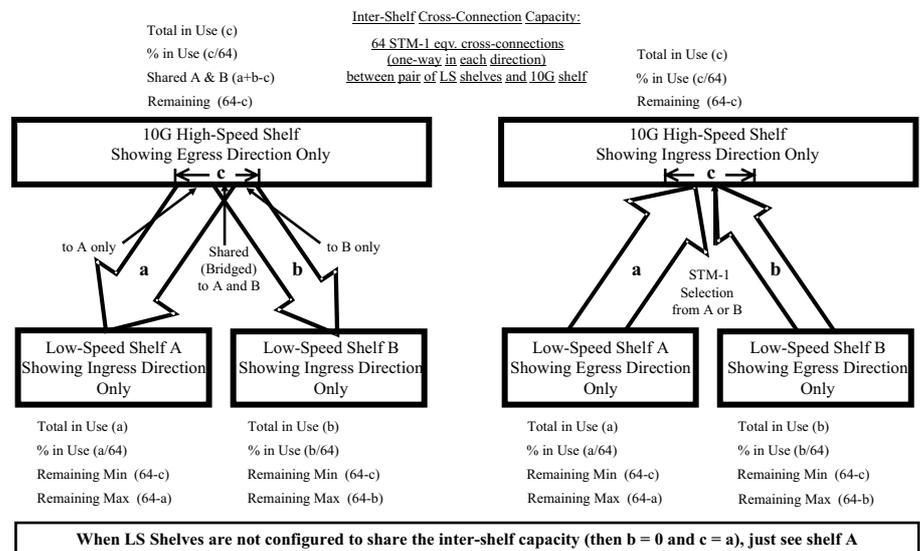
The preceding sections describe the inter-shelf cross-connection capacity and how this capacity can be used for various applications. Depending on the cabling from the low-speed shelves to the 10G shelf, an inter-shelf cross-connection capacity of 64 STM-1 equivalents can be either dedicated to one low-speed shelf or shared by a pair of low-speed shelves. When the 10G shelf is equipped with the 256 STM-1 switch fabric, the inter-shelf connection capacity is doubled, and the 10G shelf supports two separate sets of 64 STM-1 equivalents: for low-speed shelves connected to Ports A and/or B, and for low-speed shelves connected to Ports C and/or D.

Data is displayed for each low-speed shelf and for the 10G shelf (or for each of two "halves" of the 10G shelf's inter-shelf connection capacity when doubled by the larger switch fabric; but only one of them is shown in the figure above). Separate data is also displayed for each direction of transmission, into a shelf (ingress) and out of a shelf (egress), since the utilization in each direction may be different if one-way cross-connections are used.

The amount of capacity currently in use is given both as a total number of VC-3 equivalent cross-connections and as a percentage of the capacity. All percentages are based upon a capacity of 64 VC-3 equivalents since that is the number supported either to/from a low-speed shelf, or to/from the 10G shelf when equipped with the 192 STM-1 switch fabric, or to/from "one half" of the 10G shelf when equipped with the 256 STM-1 switch fabric.

In case the inter-shelf connection capacity is shared by a pair of low-speed shelves, the *WaveStar* CIT provides a range between a minimum and maximum amount of capacity that remains available both to and from each low-speed shelf. The minimum of the range is the remaining capacity to/from the 10G shelf. The maximum of the range is the remaining capacity to/from the low-speed shelf itself, based on its own utilization only. The minimum may be less than (or equal to) the maximum because the capacity in use to/from the 10G shelf may be shared by another low-speed shelf. The user can make at least the minimum number of additional cross-connections to/from this low-speed shelf, and possibly a greater number, up to the maximum, if connections were to be removed between the 10G shelf and the other low-speed shelf that shares the inter-shelf capacity. Also in case the capacity is shared by a pair of low-speed shelves, the *WaveStar* CIT specifies how much of the capacity is shared by being bridged from the 10G shelf to both of these low-speed shelves.

This bridging does not increase the utilization for the 10G shelf egress, and more capacity remains available.

When the inter-shelf connection capacity is not shared by a pair of low-speed shelves, the report is much simpler to use because the information for the 10G shelf is redundant with that for a low-speed shelf.

⌐

Setting regenerator section trace

Overview

Purpose   Use this procedure to generate a regenerator section trace.

Related information   For related information, see:

- "Regenerator section trace" (19-2)

⌐

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to
configure tributaries.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps in order to configure the trace
settings for a specific port:

....

1   Either call up the window for provisioning the desired port in the
Shelf View, clicking with the right mouse button on a specific port of
a specific circuit pack and then selecting the option **Provision Port #**
in the pop-up menu. Continue with Step 5.

or

In the **System View** of the *WaveStar* CIT, via **Configuration** →
Provision call up the **Provision Parameters for Protection Groups
or Equipment** window.

> **Result:**
>
> On the left side of the window, the **Equipment** selection tab is
> displayed. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double-click on the shelf or click on the **+** in
front of the shelf name.

> **Result:**
>
> The list of circuit packs and slots which are available becomes
> visible below the shelf name.

....

3   Select the desired port unit. Double click on the port unit or click on
the **+** in front of the unit name.

> **Result:**
>
> The list of ports which are available becomes visible below the
> port unit name.

....

....

4 Select the desired port.

> **Result:**
>
> On the right side of the window, the provisionable parameters are displayed.

....

5 Select the **Trace Settings** tab.

> **Reference:**
>
> Please refer to "Supporting information" (8-20) for the description of the parameters.

....

6 Set the parameters according to your needs.

....

7 Select the destination port(s) in the **Apply To:** drop-down list-box. Here, you can specify whether the settings should apply only to the above selected port or to all ports on the respective circuit pack. By using the latter options, you can decrease your provisioning time significantly.

....

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

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

....

Supporting information

Section trace settings tab   The following table shows which parameters are displayed in the
Trace Settings tab, and explains them:

Parameter	Values	Meaning
Write Format	**Single-byte**	A single byte (hexadecimal format using the printable T.50/ASCII character set) is repeated over and over, with no terminating/initial sequence. The default value is 0x01.
	16-byte	A 16-byte hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7. The initial value is a header byte followed by 15 0x00's (the ASCII null character).
Expected Format	**Single-byte**	A single byte (hexadecimal format using the printable T.50/ASCII character set) is repeated over and over, with no terminating/initial sequence. The default value is 0x01.
	Non-Specific-byte	A single repeating byte with hexadecimal value 0x01
	16-byte	A 16-byte hexadecimal format using the printable T.50/ASCII character set, with the first byte being a CRC-7. The initial value is a header byte followed by 15 0x00's (the ASCII null character).
Generation /Expected Identifier		
CRC Calculation	**Auto**	This button is only displayed when the write format or respectively the **Expected Format** is set to **16-byte**. The button controls the automatic calculation of the CRC-7.
		When the string is retrieved from the NE the CRC-7 is calculated over the API and compared with the retrieved CRC-7. When the comparison results in a mismatch, this control is disabled.
		If this option is selected, the field right of the **Manual** radio button is read-only. This field displays in hexadecimal representation the first byte of the 16 byte string, including the Frame Alignment Signal FAS bit (hex 0x80) . However when provisioning the Section Trace, the FAS is added to the CRC-7.
	Manual	If this option is selected, this field right of this radio button is editable by the user.
Display Mode	**ASCII** (Default)	If this option is selected, up to 15 ASCII characters (converted from the hexadecimal representation) can be displayed and entered in the **Value** field .
	Hex.	If this option is selected, the API (Access Point Identifier) in the **Value** field is displayed in hex mode.

Parameter	Values	Meaning
Value	Alphanumeric (Default), Hex (range 0..9,a..f).	Shows the value of the outgoing J0 byte section trace for the terminated STM-1.
		The value of this field can be filled in **ASCII** or in hexadecimal mode.
		This controlled by the radio buttons for **Write Format** or respectively the **Expected Format** and the settings for the **Display Mode**.
		• The default value for the **Single-byte** format is 0x01.
		• If the format is **Non-Specific-Byte** (applies only to the **Expected Identifier** area) then this field is dimmed and the value 0x01 is displayed.
		• If the format is **16-byte**, an extra field is added to the screen: a CRC-7 field displaying the CRC-7.
		• If the **Display Mode** is set to **ASCII**, up to 15 ASCII characters (converted from the hexadecimal representation) are displayed. If a series of two hexadecimal digits cannot be converted to ASCII characters, then the CIT displays a left bracket ([), the letters hex, the two hexadecimal digits, and a right bracket (]) . Trailing Nulls 0x00 or spaces 0x20 shall not be displayed at all. *Note:* editing any one of the characters of a hexadecimal representation results in the new character in place of this representation.
		• If the **Display Mode** is set to **Hex.**, the CIT displays the letters hex, a space, the two hexadecimal digits, a space, the next two hexadecimal digits, and so on until the 15 byte API is displayed. *Note:* the user is only allowed to edit the digits.
RSdTIM Monitor	**Enabled** **Disabled** (default)	*Regenerator Section trace (J0) identifier mismatch (TIM) monitor enable.*

Viewing regenerator section trace

Overview

....

Purpose   Use this procedure to view an regenerator section trace.

Related information   For related information, see:

- "Regenerator section trace" (19-2)

┓

....

Lucent Technologies

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to
configure tributaries.

Required equipment

The following equipment is required to perform this task:

* *WaveStar* CIT

Instructions   Complete the following steps in order to view the trace settings
of for a specific port:
....

1   Either call up the window for viewing the desired port in the **Shelf
View**, clicking with the right mouse button on a specific port of a
specific circuit pack and then selecting the option **View Port # Details**
in the pop-up menu. Continue with step Step 5

or

In the **System View** of the *WaveStar* CIT, via **View → View
Equipment Details…** call up the **View Equipment Details…** window.

Important! If you only want to display the actual value of the section
trace at a specific port you can also use the menu option **Fault →
Analysis → View Current Port Optical Maintenance Signal.**

Result:

On the left side of the window, the **Equipment** selection tab is
displayed. The shelves belonging to the system are listed.

....

2   Select the desired shelf. Double-click on the shelf or click on the **+** in
front of the shelf name.

Result:

The list of circuit packs and slots which are available becomes
visible below the shelf name.

....

3   Select the desired port unit. Double click on the port unit or click on
the **+** in front of the unit name.

....

Result:

The list of ports which are available becomes visible below the port unit name.

....

4   Select the desired port.

Result:

On the right side of the window, the provisionable parameters are displayed.

....

5   Select the **Trace Settings** tab.

Reference:

Please refer to "Supporting information" (8-25) for the description of the parameters.

E N D   O F   S T E P S

Supporting information

Trace Settings tab   The following table shows the **Section Trace Parameters** displayed in the **Trace Settings** tab, and explains them:

Parameter	Meaning	Values
Write Format	Displays the section trace Write Format. The current value is presented as text.	**Single-byte** **16-byte**
Generation	Shows the value of the outgoing section trace for the terminated STM-N. The value of this field can be displayed in ASCII or in Hexadecimal characters. This can be selected via the **Display Mode** radio buttons. When the Section Trace Write Format is **16-byte**, additionally a CRC-7 field is shown.	
Read Format	Displays the section trace Read Format. The current value is presented as text.	**Single-byte** **16-byte**
Retrieval	Shows the value of the received section trace for the terminated STM-N. The value of this field can be displayed in ASCII or in Hexadecimal characters. This can be selected via the **Display Mode** radio buttons. When the Section Trace Read Format is **16-byte**, additionally a CRC-7 field is shown.	
Expected Format	Displays the Expected Section Trace Format. The current value is presented as text.	**Single-byte** **Non-Specific-byte** **16-byte**
Expected Identifier	Shows the value of the expected section trace for the terminated STM-N. The value of this field can be displayed in ASCII or in Hexadecimal characters. This can be selected via a the **Display Mode** radio buttons. When the Expected Section Trace Format is **16-byte**, additionally a CRC-7 field is shown. When the Expected Section Trace Format is **Non-Specific-Byte**, then this field is dimmed with the value [hex 01].	
RSdTIM Monitor	This field displays the state of the *Regenerator Section trace (J0) identifier mismatch (TIM) monitor.* The current value is presented as text.	**Enabled** **Disabled** (default)

Viewing path trace

Overview

Purpose   Use this procedure to view path trace at a specific tributary.

Related information   For related information, see:

- "Path trace" (19-3)

Procedure

....

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

Required privilege code

You must have at least a privilege code of P3, Provisioning, to
configure tributaries.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps in order to view the path trace at a
specific tributary:

....

1   Call up the window for viewing the desired tributary in the **Shelf
View**, clicking with the right mouse button on a specific port of a
specific circuit pack and then selecting the option **View Tributary
Details** in the pop-up menu.

Continue with step Step 7

....

2   In the **System View** of the *WaveStar* CIT, via **View → View
Equipment Details…** call up the **View Equipment Details…** window.

Important! If you only want to display the actual value of the path
trace at a specific tributary you can also use the menu option **Fault →
Analysis → View Current Optical Trib. Maintenance Signal.**

    Result:

    On the left side of the window, the **Equipment** selection tab is
    displayed. The shelves belonging to the system are listed.

....

3   Select the desired shelf. Double-click on the shelf or click on the **+** in
front of the shelf name.

    Result:

    The list of circuit packs and slots which are available becomes
    visible below the shelf name.

....

4   Select the desired port unit. Double click on the port unit or click on
the **+** in front of the unit name.

....

Result:

The list of ports which are available becomes visible below the port unit name.

....

5   Select the desired port. Double click on the port or click on the **+** in front of the port.

> **Result:**
>
> The list of tributaries which are available becomes visible below the port.

....

6   Select the desired tributary (type).

> **Result:**
>
> On the right side of the window, the parameters of the selected tributary are displayed.

....

7   Select the **Trace Settings** tab.

> **Reference:**
>
> Please refer to "Supporting information" (8-29) for the description of the parameters.

E N D   O F   S T E P S

Supporting information

Trace Settings tab   The following table shows the **Path Trace Parameters** displayed in the **Trace Settings** tab, and explains them:

Parameter	Meaning	Values
Read Format	Displays the path trace Read Format. The current value is presented as text.	**Single-byte** **16-byte** **64-byte**
Retrieval	Shows the value of the received path trace for the monitored VC-N. The value of this field can be displayed in ASCII or in Hexadecimal characters. This can be selected via the **Display Mode** radio buttons. When the Path Trace Write Format is **16-byte**, additionally a CRC-7 field is shown.	
Expected Format	Displays the Expected Path Trace Format. The current value is presented as text.	**Single-byte,** **Non-Specific-byte,** **16-byte,** **64-byte**
Expected Identifier	Shows the value of the expected path trace for the terminated VC-N. The value of this field can be displayed in ASCII or in Hexadecimal characters. This can be selected via a the **Display Mode** radio buttons. If the Path Trace Expected Format is **Non-Specific-Byte**, any value between 0x00 and 0xFF is accepted.. If the Format is the **16-byte,,** then a CRC-7 field is shown. When the format is the **64 Byte** String, then the value is displayed in ASCII.	
HP TIM Monitor	This field displays the state of the *HP trace (J1) identifier mismatch (TIM) monitor.* The current value is presented as text.	**Enabled** **Disabled** (default)

⌐

9 Performance Monitoring

Overview

Purpose   This chapter describes the procedures which have to be performed for the configuration of the performance monitoring functions of the *WaveStar*® TDM 10G (STM-64).

Contents

Performance Monitoring: High-level procedure

Overview

Purpose   This high level procedure is intended to give you an idea of the sequence, in which the individual performance-monitoring-related procedures in this chapter can be performed. This is only a recommendation. There might also be cases where a different approach is necessary.

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

⌐

Procedure

....

Before you begin Prior to performing this task, you must:

- Identify the ports related to the task.

- Log into the NE with the *WaveStar*® CIT and be familiar with the functions of the *WaveStar* CIT.

Required privilege

You must have a security privilege code of at least P3 + PM4 + S3 to perform this task.

Required equipment

WaveStar Customer Interface Terminal (CIT).

Instructions Complete the following steps to obtain performance data for the selected ports or tributaries.

....

1 Enable the Performance Monitoring data collection.

Reference:

"Enable or disable Performance Monitoring (PM) data collection and TCAs" (9-5)

....

2 Initialize the respective Performance Monitoring registers.

Reference:

"Initialize Performance Monitoring (PM) registers" (9-14)

....

3 If required, create or modify a Threshold Crossing Alert (TCA) profile. When a TCA profile is in place, PM parameters that cross the thresholds defined in the profile, are alarmed.

Reference:

"Creating a new PM Threshold Crossing Alert (TCA) profile" (9-25)

....

4 Run the performance measurements (15 minutes or 1 day).

....

5 Retrieve the results of the performance measurements in the form of reports.

....

Reference:

"Display and save Performance Monitoring (PM) register
values" (9-18)

E ND   O F   S TEPS

⅂

Enable or disable Performance Monitoring (PM) data collection and TCAs

Overview

....

Purpose   Use this procedure to enable or disable all PM data collection and threshold crossing alerts for selected ports or tributaries.

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

....

365-371-522
Issue b, October 2001

Lucent Technologies

9 - 5

Procedure

Before you begin Prior to performing this task, you must:

- Identify the ports or tributaries related to the task.

- Log into the NE with the *WaveStar*® CIT and be familiar with the functions of the *WaveStar* CIT.

- Make sure that the port or tributary to be monitored has been established properly.

Required privilege

You must have a security privilege code of at least P3 + S1 to perform this task.

Required equipment

WaveStar Customer Interface Terminal (CIT).

Instructions Complete the following steps to enable or disable PM data collection for selected ports.

1

IF	THEN
you want to enable PM data collection	continue with Step 2.
you want to disable PM data collection (not applicable for Gigabit Ethernet)	continue with Step 7.

2 Before enabling PM data collection, make sure that the port monitoring mode for the required port or in case of HO VC Path PM the monitoring mode for the required tributary is set to "monitored". Therefore, on the System View toolbar, select **Configuration** → **Provision...**

> **Result:**
>
> The **Provision Parameters** window opens.

3 In the **Provision Parameters** window, open the required bay and shelf details then select the required port or tributary.

4 Click **Provision**.

Enable or disable Performance Monitoring
(PM) data collection and TCAs
Procedure

Performance Monitoring

> **Result:**
>
> The **Provision Parameters for Protection Group or
> Equipment** window opens for the port or tributary selected. The
> type of window depends on your selection.

....

5   In the **Transmission** area, select in the **Port Mode** drop-down list
(for port) or the **Tributary Monitoring Mode** drop-down list (for
tributary) the **Monitored** option.

....

6   Click the **Apply** pushbutton.

....

7   On the System View toolbar, select **Performance → Provision Ports**.

> **Result:**
>
> The **Equipment Selection** window opens.

....

8   In the **Equipment Selection** window, open the required bay and shelf
details then select the required port or tributary.

....

9   Click **Provision**.

> **Result:**
>
> The **Provision Parameters for Port Performance Monitoring**
> window opens for the port or tributary selected. The type of
> window depends on your selection.

....

10   Select the required **(RS-MS / SDH HOVC Path) PM TCA Profile**
group.

> **Result:**
>
> A list of profiles is displayed for the **PM TCA Profile** group you
> have selected.

....

11

IF	THEN
the correct profile is already assigned to the selected port or tributary	continue with the next step
the correct profile is not assigned	select the correct profile to apply to the selected port or tributary

....

Enable or disable Performance Monitoring
(PM) data collection and TCAs
Procedure

Performance Monitoring

....

12 For **(Regenerator-Near End Multiplex Section / Far End Multiplex Section / Path) PM Activation**, select **Enable** to enable performance monitoring or **Disable** to disable performance monitoring for this port or tributary. Please note that this option enables or disables all profile group performance monitoring for the selected port or tributary. See "Modifying PM Threshold Crossing Alert (TCA) profiles" (9-33) to modify a profile to disable monitoring of individual selected parameters.

....

13 From the **Apply to** list, select the required application.

> **Reference:**
>
> "Provision PM port window selection information" (9-9)

....

14 Click **Apply**, then click **Close** to exit.

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

Supporting information

**Provision PM port window
selection information**

The following is supporting information for some of the available selections in the Provision PM Ports windows:

Apply to	Description/Behavior
this port (trib) only	Enables or disables the selected PM profile parameters to only the port (tributary) you have selected.
all tribs, this port	Enables or disables the selected PM profile parameters to all the tributaries on the port that contains the tributary you have selected.
all ports (tribs) this pack	Enables or disables the selected PM profile parameters to all the ports (tributaries) on the circuit pack that contains the port (tributary) you have selected.
all ports (tribs) this type, this shelf	Enables or disables the selected PM profile parameters to all the ports (tributaries) on all the circuit packs on a shelf that have the same type port (tributary) as the one you have selected.

Viewing Performance Monitoring (PM) settings for individual ports or tributaries

Overview

Purpose Use this procedure to retrieve PM settings made for a selected port or tributary.

Related information For related information, see Chapter 20, "Performance monitoring concepts".

┐

Procedure

....

Before you begin   Prior to performing this task, you must:

- Identify the ports or tributaries related to the task.

- Log into the NE with the *WaveStar*® CIT and be familiar with the functions of the *WaveStar* CIT.

Required privilege code

You must have a security privilege code of at least PM1 to perform this task.

Required equipment

WaveStar Customer Interface Terminal (CIT).

Instructions   Complete the following steps to retrieve the PM settings for selected ports or tributaries.

....

1   On the System View toolbar, select **Performance** → **View PM Ports**.

> **Result:**
>
> The **Equipment Selection** window opens.

....

2   In the **Equipment Selection** window, open the required bay and shelf details then select the required port or tributary.

....

3   Click **Select**.

> **Result:**
>
> The **View Parameters for Port Performance Monitoring** window opens for the port or tributary selected. The type of window depends on your selection.

....

4   If a port has been selected, the following parameters can be viewed:

Parameter	Meaning
RS-MS PM TCA Profile	If a Threshold Crossing Alert (TCA) profile has been assigned to this port, the profile name is shown here.
Regenerator-Near End Multiplex Section PM Activation	Indicates whether PM in the Regenerator Section and Near-End PM in the Multiplex Section is enabled or not

....

Far End Multiplex Section PM Activation	Indicates whether Far-End PM in the Multiplex Section is enabled or not.
Multiplex Section Near End SES Threshold	Indicates the threshold set for the Severely Errored Seconds (SES) for Near-End PM in the Multiplex Section
Multiplex Section Far End SES Threshold	Indicates the threshold set for the Severely Errored Seconds (SES) for Far-End PM in the Multiplex Section
Regenerator Section Near End SES Threshold	Indicates the threshold set for the Severely Errored Seconds (SES) for Near-End PM in the Regenerator Section

....

5   If a Gigabit Ethernet port has been selected, the following parameters can be viewed:

Parameter	Meaning
Ethernet TCA Profile	If a Threshold Crossing Alert (TCA) profile has been assigned to this tributary, the profile name is shown here.
Ethernet PM Enable	Indicates whether Ethernet PM is enabled or not

....

6   If a tributary has been selected, the following parameters can be viewed:

Parameter	Meaning
SDH HOVC Path PM TCA Profile	If a Threshold Crossing Alert (TCA) profile has been assigned to this tributary, the profile name is shown here.
Path PM Activation	Indicates whether Path PM is enabled or not
Higher-order Path Far-end SES Threshold	Indicates the threshold set for the Severely Errored Seconds (SES) for Far-End Path PM
Higher-order Path Near-end SES Threshold	Indicates the threshold set for the Severely Errored Seconds (SES) for Near-End Path PM

....

7   For further details, click on the **RS-MS** (for ports) or **HO VC** (for tributary) pushbutton in the **Control Options** area. The **View TCA**

....

Profile Details window is shown. Here, the individual parameters and their values of the assigned Regenerator Section, Multiplex Section or HO VC Path PM TCA profile are displayed for the selected port or tributary.

....

8 If an STM-16 or STM-64 port has been chosen, the pushbutton **Physical** is additionally available in the **Control Options** area. A click on this pushbutton shows the **View TCA Profile Details** window for the optical performance parameters TCA profile assigned to this port.

> **Reference:**
>
> "Provision PM port window selection information" (9-9)

....

9 If an Ethernet port has been chosen, the pushbutton **Ethernet** is additionally available in the **Control Options** area. A click on this pushbutton shows the **View TCA Profile Details** window for the performance parameters TCA profile assigned to this port.

> **Reference:**
>
> "Provision PM port window selection information" (9-9)

....

10 Click **Close** to exit.

E ND OF S TEPS

....

365-371-522
Issue b, October 2001

Lucent Technologies

9 - 1 3

Initialize Performance Monitoring (PM) registers

Overview

....

Purpose   Use this procedure to set to zero (initialize) all current 15-minute or current-day Regenerator Section, Multiplex Section or HO VC Path PM registers.

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

⌐

....

9 - 1 4   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

Before you begin   Prior to performing this task, you must:

- Identify the ports or tributaries related to the task.

- Log into the NE with the *WaveStar*® CIT and be familiar with the functions of the *WaveStar* CIT.

Required privilege code

You must have a security privilege code of at least PM3 + P3 to perform this task.

Required equipment

WaveStar Customer Interface Terminal (CIT).

Workaround

Important! PM registers cannot be reset, if PM is disabled (cf. "Enable or disable Performance Monitoring (PM) data collection and TCAs" (9-5)), although the response indicates success. So after enabling PM again, there will be wrong initial values being reported as valid.

Reset PM registers only shortly before PM is disabled or immediately after PM is enabled.

Instructions   Complete the following steps to initialize selected PM registers.
....

1   On the System View toolbar, select **Performance → Initialize Registers**.

> **Result:**
>
> The **Equipment Selection** window opens.

....

2   In the **Equipment Selection** window, select the required bay, shelf, port or tributary. Click **Select**.

> **Result:**
>
> The **PM Register Initialization** window opens for the port or tributary selected.

....

3   Verify the correct port AID and port rate are displayed for the selected port.

> **Reference:**
>
> "PM register initialization window parameters" (9-17)

....

....

4 Make the required selections in the displayed window to initialize the
required register type.

....

5 Click **Apply** to make changes, then click **Close**.

E ND OF S TEPS

....

⌐

....

9 - 1 6   **Lucent Technologies**   365-371-522
Issue b, October 2001

Supporting information

PM register initialization window parameters

The following table explains some of the input parameters for the initialization of PM registers:

Parameter	Description
PM Register Type	Choose the type of register to initialize: • RS-MS may be chosen if you have selected a port. • ENET may be chosen if you have selected a ethernet port. • ALL selects both of the above registers.
Location (not used for Ethernet ports)	You may choose to initialize just the near-end registers or the far-end registers or both. • NEND — Near-end PM data only is initialized. • FEND — Far-end PM data only is initialized. • ALL — Both near-end and far-end (if applicable) PM data is initialized.
Time Period	Choose the time period: • 15-MIN — Choose to initialize the 15-minute registers. • 1-DAY — Choose to initialize the 1-Day registers. • ALL — Choose this option to initialize both types of registers.
Apply to	Choose one of the following options: • This Port Only — Choose to initialize only the port selected. • All Ports This Pack — This selection allows you to initialize all the ports on the circuit pack containing the selected port. • All Ports This Pack, This Shelf — This selection allows you to initialize all the ports on the shelf that are the same type as the selected port.

Display and save Performance Monitoring (PM) register values

Overview

Purpose   Use this procedure to display the PM register values for the following PM parameter groups when available:

- SDH Regenerator Section

- SDH Multiplex Section

- SDH Physical (optical port performance parameters for STM-16 and STM-64 port units)

- SDH Higher-Order Intermediate Path (VC-3, VC-4, VC-4-4c, VC-4-16c)

- Ethernet

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

Procedure

....

Before you begin   Prior to performing this task, you must fulfill the following
requirements:

Required privilege code

You must have a security privilege code of at least PM1 to perform
this task.

Required equipment

WaveStar® Customer Interface Terminal (CIT).

Instructions   Complete the following steps to retrieve, display, and/or save PM
register values.
....

1   Log into the system using the *WaveStar* CIT.

....

2   Select one of the following from the System View toolbar to display
the PM register values associated with the listed parameter group.

1.   SDH Physical — **Performance** → **Reports** → **SDH Physical**

2.   SDH Regenerator — **Performance** → **Reports** → **SDH
Regenerator Section**

3.   SDH Multiplex — **Performance** → **Reports** → **SDH Multiplex
Section**

4.   SDH Higher Order Path — **Performance** → **Reports** → **SDH
Path**

5.   Ethernet — **Performance** → **Reports** → **Ethernet**

  Result:

  The **Equipment Selection** window opens.

....

3   Open the bay and shelf details, then select the port for which you
want to receive a report. Click **Select**.

  Result:

  A selection window opens for the PM parameter group selected.

....

4   Select the time period, monitored date, and the PM parameters you
want to display or save to file.

....

Display and save Performance Monitoring
(PM) register values
Procedure

Performance Monitoring

Reference:

For further information on the available PM parameters, please refer to **Chapter 20, "Performance monitoring concepts"**.

....

5   Click the **Apply** pushbutton.

Important! After a change of the SES threshold (cf. "Initialize Performance Monitoring (PM) registers" (9-14)) the current PM data is not invalidated. Therefore, it is possible to retrieve valid data in one bin that is based on several different SES thresholds.

Result:

The **Report** window opens.

Reference:

"Supporting Information" (9-21)

....

6   View the report, then perform one of the following options:

IF	THEN
you want to save the results to a file,	Continue with the next step.
you want to print the results to a printer connected to your PC,	Click **Print**.
you want to refresh the screen display,	Click **Refresh**.
you do not want to save the results to a file,	Click **Close** to exit.

....

7   Select the **Save As** control option.

Result:

The file name selection window opens.

....

8   Enter a file name where you want to save the report.

....

9   Click **Apply**.

....

10   Click **Close** to exit.

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

....

Supporting Information

Explanation of Fields in the Report Windows

The following is supporting information for the PM parameters displayed in the following windows:

- **SDH Regenerator Section Nearend PM Report** window
- **SDH Multiplex Section PM Report** window
- **SDH Physical PM Report** window
- **SDH HOVC Path PM Report** window.
- **Ethernet PM Report** window.

Regenerator Section

The following are the parameters of the SDH Regenerator Section Near-end PM Reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to "Validity flag" (9-23). In addition, the NE indicates which PM registers have crossed their thresholds. For information on the value range and the default threshold values for each parameter, please refer to the task "Creating a new PM Threshold Crossing Alert (TCA) "Supporting information" (9-28).

Parameter	Description
RS_N_ES	Errored Seconds - Regenerator Section
RS_N_SES	Severely Errored Seconds - Regenerator Section
RS_N_BBE	Background Block Error - Regenerator Section
RS_N_UAS	Unavailable Seconds - Regenerator Section

Multiplex Section

The following are the parameters of the SDH Multiplex Section PM Reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to "Validity flag" (9-23). In addition, the NE indicates which PM registers have crossed their thresholds. For information on the value range and the default threshold values for each parameter, please refer to the task "Creating a new PM Threshold Crossing Alert (TCA) "Supporting information" (9-28).

Display and save Performance Monitoring
(PM) register values
Supporting Information

Performance Monitoring

Parameter	Description
MS_N_ES MS_F_ES	Errored Seconds - Multiplex Section (Near End / Far End)
MS_N_SES MS_F_SES	Severely Errored Seconds - Multiplex Section (Near End / Far End)
MS_N_BBE MS_F_BBE	Background Block Error - Multiplex Section (Near End / Far End).
MS_N_UAS MS_F_UAS	Unavailable Seconds - Multiplex Section (Near End / Far End).

SDH Physical   The following are the parameters of the SDH Physical performance data reports that are returned from the NE. For further information on the validity flag, please refer to "Validity flag" (9-23).

Parameter	Description/Behavior
LBCN	Normalized Laser Bias Current of the STM-16/STM-64 laser transmitter: LBC normal (LBCN) = LBC actual / LBC nominal. Laser transmitters In-Service and for protection (stand-by) mode are monitored. The LBC nominal value is stored when the optical pack is manufactured.
OPT	Normalized average optical output power of the STM-16/STM-64 active laser transmitter OPT normal = OPT actual / OPT nominal. Laser transmitters In-Service and for protection (stand-by) mode are monitored.
OPR	The normalized average optical power received for each active optical receiver OPR normal = OPR actual / OPR nominal. Optical receivers In-Service and for protection (stand-by) mode are monitored.

SDH Higher Order Path   The following are the parameters of the SDH HOVC Path PM Reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to "Validity flag" (9-23). In addition, the NE indicates which PM registers have crossed their thresholds. For information on the value range and the default threshold values for each parameter, please refer to the task "Creating a new PM Threshold Crossing Alert (TCA) "Supporting information" (9-28).

Display and save Performance Monitoring
(PM) register values
Supporting Information

Performance Monitoring

Parameter	Description
VC_N_ES VC_F_ES	Errored Seconds - SDH Higher Order Path (Near End / Far End)
VC_N_SES VC_F_SES	Severely Errored Seconds - SDH Higher Order Path (Near End / Far End)
VC_N_BBE VC_F_BBE	Background Block Error - SDH Higher Order Path (Near End / Far End)
VC_N_UAS VC_F_UAS	Unavailable Seconds - SDH Higher Order Path (Near End / Far End)

Ethernet The following are the parameters of the Ethernet PM Reports that are returned from the NE. In addition to the value of each parameter, the time, date, and validity of the data is returned by the NE for each parameter. For further information on the validity flag, please refer to "Validity flag" (9-23). In addition, the NE indicates which PM registers have crossed their thresholds. For information on the value range and the default threshold values for each parameter, please refer to the task "Creating a new PM Threshold Crossing Alert (TCA) "Supporting information" (9-28).

Parameter	Description
EDFC	Dropped frames - congestion
EDFE	Dropped frames - errors
EINB	Incoming number of Mbytes
EINF	Incoming number of Mframes
EONB	Outgoing number of Mbytes
EONF	Outgoing number of Mframes

Validity flag The validity flag shows the validity of the register whose value is reported. If the value is invalid, the flag is set to I-xx, where xx further explains the cause of the invalidity.

Display and save Performance Monitoring
(PM) register values
Supporting Information

Performance Monitoring

Flag	Meaning
I-01	Time/Date change to shorter interval or earlier minute, hour, day, month, or year or port unit pack (re)insertion or restart of system controller software (in the middle of an interval) or system/SRC out of service or back to service (cold boot) or system/SRC out of service or back to service (warm boot in the middle of an interval) or PU out of service or back to service
I-02	Time/Date change to longer interval or later minute, hour, day, month, or year or restart of system controller software (at boundary between intervals) or system/SRC out of service or back to service (warm boot at the boundary between intervals)
I-03	PM Enable/Disable or MON/NMON
I-08	SW processing error
I-09	Far-end parameters inhibited due to near end defects
I-10	Facility/equipment protection on failure condition
I-11	PM start change to shorter interval
I-12	PM start change to longer interval
I-13	Register initialization
I-14	Detected read error of hardware PM register by software
I-17	A change in (SDH) SES declaration threshold
I-18	Automatic Laser Shutdown (ALS)

⌐

Creating a new PM Threshold Crossing Alert (TCA) profile

Overview

Purpose   Use this procedure to create a new Threshold Crossing Alert (TCA) profile associated with the following PM parameter groups:

- SDH Regenerator Section

- SDH Multiplex Section

- SDH Physical (optical port performance parameters for STM-16 and STM-64 port units)

- SDH Higher-Order Intermediate Path (VC-3, VC-4, VC-4-4c, VC-4-16c)

- Ethernet

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

⌐

Procedure

....

Before you begin   Before performing this task:

- Identify the ports, tributaries, and TCA profiles related to the task.

Required privilege code

You must have a security privilege code of at least PM4 +S3 to perform this task.

Required equipment

The following equipment is required to perform this task.

- *WaveStar*® CIT

Instructions   Complete the following steps to create a new TCA profile.

....

1   From the System View toolbar, select the menu command required from one of the following:

1. SDH Regenerator-Multiplex profile — **Performance** → **Provision TCA Profile** → **SDH Regenerator-Multiplex**

2. SDH Physical profile — **Performance** → **Provision TCA Profile** → **SDH Physical**

3. SDH Higher Order Path profile — **Performance** → **Provision TCA Profile** → **SDH HOVC Path**

4. SDH Higher Order Path profile — **Performance** → **Provision TCA Profile** → **Ethernet**

   Result:

   The **Provision TCA Profile** window opens.

....

2   Enter a name for the new profile in the **New Profile** box. The name may be up to 24 alphanumeric characters maximum.

....

3   Click **Create** to create the new profile with default values (cf. "Supporting information" (9-28)) for the threshold parameters.

....

4

IF	THEN
you want to change the threshold parameters of your new profile,	click **Modify** and refer to "Modifying PM Threshold Crossing Alert (TCA) profiles" (9-33), Step 5.

....

IF	**THEN**
you want to keep the default values for the threshold parameters,	click **Close** to exit.
you want to rename the created profile,	click on **Rename**.

E ND OF S TEPS

┐

Supporting information

Default threshold crossing alert profile parameter settings MS, RS

The following table shows the pre-defined threshold values in the default TCA profiles for Multiplex Sections (MS) and Regenerator Sections (RS) and the range of configurable values.

Parameter	15 min default	15 min range	1 day default	1 day range
RS_N_ES	180	0–900	1500	0–86400
RS_N_SES	15	0–810	20	0–77760
RS_N_BBE	9000	1–16777215	48000	1–2147483647
RS_N_UAS	15	0–900	20	1–86400
MS_N_ES, MS_F_ES	50	0–900	150	1–86400
MS_N_SES, MS_F_SES	10	0–810	15	0–77760
MS_N_BBE, MS_F_BBE	228000 for STM-1, 912000 for STM-4, 3648000 for STM-16, 14592000 for STM-64	1–16777215	432000 for STM-1, 1728000 for STM-4, 6912000 for STM-16, 27648000 for STM-64	1–2147483647
MS_N_UAS, MS_F_UAS	15	0–900	20	0–86400

Default threshold crossing alert profile parameter settings VC-3, VC-4

The following table shows the pre-defined threshold values in the default TCA profiles for Higher Order Paths (VC-3, VC-4) and the range of configurable values.

Parameter	15 min default	15 min range	1 day default	1 day range
VC3, VC_N_ES	150	1–900	600	1–86400
VC4, VC_N_ES	180	1–900	1500	1–86400
VC_N_SES	15	1–810	20	1–77760
VC_N_BBE	36000	1–65535	48000	1–8388607
VC_N_UAS	15	1–900	20	1–86400
VC3, VC_F_ES	150	1–900	600	1–86400
VC4, VC_F_ES	180	1–900	1500	1–86400
VC_F_SES	15	1–810	20	1–77760
VC_F_BBE	36000	1–65535	48000	1–8388607

Parameter	15 min default	15 min range	1 day default	1 day range
VC_F_UAS	15	1–900	20	1–86400

Default threshold crossing alert profile parameter settings VC-4-4c, VC-4-16c   The following table shows the pre-defined threshold values in the default TCA profiles for Higher-Order Path (VC-4-4c, VC-4-16c) and the range of configurable values.

Parameter	15 min default	15 min range	1 day default	1 day range
VC_N_ES	180	1–1900	1500	1–86400
VC_N_SES	15	1–810	20	1–77760
VC_N_BBE	36000	1–16777215	48000	1–2147483647
VC_N_UAS	15	1–900	20	1–86400
VC_F_ES	180	1–1900	1500	1–86400
VC_F_SES	15	1–810	20	1–77760
VC_F_BBE	36000	1–16777215	48000	1–2147483647
VC_F_UAS	15	1–900	20	1–86400

Default threshold crossing alert profile parameter settings ethernet   The following table shows the pre-defined threshold values in the default TCA profiles for ethernet and the range of configurable values.

Parameter	15 min default	15 min range	1 day default	1 day range
EDFC	1875000	0-4294967295	9000000	0-4294967295
EDFE	1875000	0-4294967295	9000000	0-4294967295
EINB	1125	0-112500	108000	0-10800000
EINF	1	0-112500	23	0-10800000
EONB	1125	0-112500	108000	0-10800000
EONF	1	0-112500	23	0-10800000

Deleting a PM Threshold Crossing Alert (TCA) profile

Overview

Purpose Use this procedure to delete a Threshold Crossing Alert (TCA) profile. Please note that all ports provisioned with a deleted profile will revert to the default profile.

Related information For related information, see Chapter 20, "Performance monitoring concepts".

⌐

Lucent Technologies

Procedure

....

Before you begin   Before performing this task:

- Identify the ports, tributaries, and TCA profiles related to the task.

Required privilege code

You must have a security privilege code of at least PM4 + S3 to perform this task.

Required equipment

The following equipment is required to perform this task.

- *WaveStar*® CIT

Instructions   Complete the following steps to delete a TCA profile.

....

1   From the System View toolbar, select the menu command required from one of the following:

1. SDH Regenerator-Multiplex profile — **Performance** → **Provision TCA Profile** → **SDH Regenerator-Multiplex**

2. SDH Physical profile — **Performance** → **Provision TCA Profile** → **SDH Physical**

3. SDH Higher-Order Path profile — **Performance** →**Provision TCA Profile** → **SDH HOVC Path**

4. SDH Higher-Order Path profile — **Performance** →**Provision TCA Profile** → **Ethernet**

    Result:

    The **Provision TCA Profile** window opens.

....

2   Select the **Existing Profile** button.

    Result:

    The adjacent drop-down menu box activates.

....

3   In the drop-down menu box, select the profile name to delete, then click **Delete**.

    Result:

    A confirmation window opens stating that "All ports provisioned with this profile shall revert to the Default profile." Please note that the Default and Default0 profile cannot be deleted.

....

....

4 Verify the correct profile is selected, then click **OK** to delete the
profile.

E ND OF S TEPS
....

⌐

Modifying PM Threshold Crossing Alert (TCA) profiles

Overview

....

Purpose   Use this procedure to modify an existing Threshold Crossing Alert (TCA) profile for the following PM parameter groups:

- SDH Regenerator Section

- SDH Multiplex Section

- SDH Physical (optical port performance parameters for STM-16 and STM-64 port units)

- SDH Higher-Order Intermediate Path (VC-3, VC-4, VC-4-4c, VC-4-16c)

- Ethernet

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

⅂

....

Procedure

....

Before you begin Before performing this task:

- Identify the ports, tributaries, and TCA profiles related to the task.

Required privilege code

You must have a security privilege code of at least PM4 + S3 to perform this task.

Required equipment

The following equipment is required to perform this task.

- *WaveStar*® CIT

Instructions Complete the following steps to modify a TCA profile.
....

1 From the System View toolbar, select the menu command required from one of the following:

1. SDH Regenerator-Multiplex profile — **Performance** → **Provision TCA Profile** → **SDH Regenerator-Multiplex**

2. SDH Regenerator-Multiplex profile — **Performance** → **Provision TCA Profile** → **SDH Physical**

3. SDH Higher Order Intermediate Path profile — **Performance** → **Provision TCA Profile** → **SDH HOVC Path**

4. SDH Physical profile — **Performance** → **Provision TCA Profile** → **SDH Physical**

   Result:

   The **Provision TCA Profile** window opens.

....

2 Select the **Existing Profile** button.

   Result:

   The adjacent drop-down menu box activates.

....

3 In the drop-down menu box, select the profile name to modify, then click **Modify**.

   Result:

   The **Edit TCA Profile** window opens.

....

4 Verify that the correct Profile Type and Profile Name is displayed.

....

....

5   Enter or change the values under the 15-Min and 1-Day columns for each of the threshold parameters you want to enter or modify.

Please note that setting a parameter value to "0" disables thresholding for that parameter.

....

6   Click **Apply** to enter changes, then click **Close** to quit.

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

Viewing PM Threshold Crossing Alert (TCA) profiles

Overview

Purpose   Use this procedure to view all the current TCA profiles associated with the following PM parameter groups:

- SDH Regenerator Section

- SDH Multiplex Section

- SDH Physical (optical port performance parameters for STM-16 and STM-64 port units)

- SDH Higher-Order Intermediate Path (VC-3, VC-4, VC-4-4c, VC-4-16c)

- Ethernet

Related information   For related information, see Chapter 20, "Performance monitoring concepts".

Procedure

Before you begin The following eqipment is required to perform this task.

- *WaveStar®* CIT

You must have a security privilege code of at least PM1 to perform
this task.

Instructions Complete the following steps to view an existing TCA profile.

1 From the System View toolbar, select the menu command required
from one of the following:

1. SDH Regenerator-Multiplex profile — **Performance** → **View
   TCA Profile** → **SDH Regenerator-Multiplex**

2. SDH Higher Order Path profile — **Performance** → **View TCA
   Profile** → **SDH HOVC Path**

3. SDH Physical profile — **Performance** → **View TCA Profile** →
   Physical.

4. SDH Physical profile — **Performance** → **View TCA Profile** →
   Ethernet.

   Result:

   The **Select a TCA Profile** window for the selected parameter
   group opens.

2 Select the name of the profile to be displayed from the drop-down
block, then click **OK**.

   Result:

   The **View TCA Profile Details** window opens displaying the
   threshold values for each of the monitored parameters.

Please note that threshold parameter values set to "0" display as
"Reporting Disabled". Physical threshold parameter values set to "1"
display as "Reporting Enabled".

3 Click **Close** to exit.

E N D   O F   S T E P S

10   Software upgrade

Overview

Purpose   This chapter describes the procedures which have to be carried out for the software upgrade of the *WaveStar*® TDM 10G (STM-64).

Contents

Performing an initial software download using the CIT

Overview

Purpose Use this procedure to install a software generic in the NE for the first time.

The software is initially delivered to the customer on a CD-ROM (ComCode 109074625). The software generic has to be copied from the CD-ROM to the *WaveStar*® CIT PC and then to the empty PCMCIA (Personal Computer Manufacturer's Card Interface Adapter) card via *WaveStar* CIT. Afterwards, the PCMCIA card is inserted into the NE.

It is essential that the PCMCIA card has to remain in the CTL/SYS50DM circuit pack during normal operation!

Related information For related information, please refer to:

- Chapter 22, "Software upgrade concepts"
- Chapter 24, "*WaveStar* CIT Tutorial".

Procedure

....

Before you begin   Prior to performing this task, you must:

1. Have a valid login on both the *WaveStar*® CIT and all subject NE(s) within the ring.

2. Acquire the CD-ROM that contains the new generic/version of the NE software ("*WaveStar* TDM 10G (STM-64) Release 4.0 NE Software", ComCode 109074625).

3. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.

Required privilege code

You must have at least a privilege code of S4 .

Required equipment

The following equipment is required to perform this task:

- Empty 220 Mb PCMCIA card (as delivered from manufacturer)

- CD-ROM that contains the new generic/version of the NE software

- *WaveStar* CIT with PCMCIA slot

Safety precautions   To assure both personal safety and the proper functioning of the *WaveStar* TDM 10G product, it is imperative to observe the following precaution.

 CAUTION

Electrostatic discharge damage to sensitive components

Handling circuit packs or working on a WaveStar CIT can cause electrostatic discharge damage to sensitive components.

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar CIT, to prevent electrostatic discharge damage to sensitive components.

Instructions

....

Performing an initial software download
using the CIT
Procedure

Software upgrade

 CAUTION

Improper removal of a PCMCIA card can result in damaged files and the generation of information messages such as "lost clusters" and/or "missing/damaged sectors".

Do not ever remove a PCMCIA card when the CTL/SYS50DM circuit pack's GREEN LED is ON (either steady ON or blinking).

To initially download the NE software (delivered on a CD-ROM) proceed as follows:

....

1 Power up the *WaveStar* CIT PC and log into Windows NT / Windows 2000 as Administrator. If you are already logged into Windows NT / Windows 2000, close any open window.

....

2 Install the NE software on your PC. To do this, use one of the following two methods (automatic or manual installation).

....

3

IF	THEN
You use the automatic installation method	proceed with the next step.
You use the manual installation method	proceed with Step 5

....

4 Automatic Installation:

Insert the *WaveStar* CD-ROM with the new NE software and wait for the welcoming screen to appear. If your PC does not start the CD-ROM automatically, perform the following:

- Double-click **My Computer** on your desktop.

- Right-click on your CD-ROM drive's icon.

- Click **Auto Play**.
  If Auto Play is not available in this menu list, you have to start the *setup.exe* file in the root directory of your CD-ROM.
  Click the **Next** button.

....

10 - 4 **Lucent Technologies** 365-371-522
Issue b, October 2001

Performing an initial software download
using the CIT
Procedure

Software upgrade

Wait for the software transfer to complete. You will notice that the "Decompressing Files in ..." message and also the InstallShield Wizard disappears when the operation has completed.
Continue with Step 13.

....

5 Manual Installation: Insert the *WaveStar* CD-ROM with the new NE software. If the welcoming screen appears, select **Cancel** to exit from the automatic installation procedure.

....

6 Open the Windows Explorer on your desktop.

....

7 Select the hard disk drive where *WaveStar* CIT is installed (in most cases **C:**) and click through to **Program Files** → **Lucent Technologies** → **WaveStar CIT** → **generics**.

Please note that, if the subdirectory **generics** does not exist, you must create it!

....

8 In the **generics** directory, create a new folder, preferrably stating the new software version in its name.

....

9 In the Windows Explorer, right-click the CD-ROM drive of your computer and select **Explore**. Go to the **generics** directory. This directory contains two subdirectories: **p** and **up**.

....

10 Select the complete **up** and **p** directories and copy it to the folder you created in Step 8.

....

11 To install Acrobat Reader on your system, go to the *AcrobatReader* subdirectory on your CD-ROM drive and double-click the *AcrobatReader40.exe* file.

....

12 The Software Release Description (SRD) is located in the *Documentation* subdirectory of the CD. You can read it by double-clicking the *.pdf* file in this subdirectory.

....

13 Insert the empty PCMCIA card into the PCMCIA slot of the *WaveStar* CIT PC.

....

Performing an initial software download
using the CIT
Procedure

Software upgrade

....

14   Format the PCMCIA card by performing the following:

- Double click the **My Computer** icon on your desktop

- Select the harddisk drive where the PCMCIA card is plugged and
  click through to **File** → **Format...**

- Select **FAT** in the **File System** selection box.

- Enter **Prim1** in the **Volume Label** field

- Select **Quick Format**

- Click **Start**.

....

15   Start *WaveStar* CIT.

....

16   In the *WaveStar* CIT Main Window, choose the option
Administration → **Prepare PCMCIA Disks...**.

>   **Result:**

>   The **Prepare PCMCIA Disk** window appears.

....

17   In the left list, under **Available Generics**, click the version of
network element software you are installing.

....

18   In the right list, click on the drive letter that represents the PCMCIA
slot that holds the flash disk.

....

19   Click the **Copy** button.

>   **Result:**

>   The file copy function begins and you see a "Copying files..."
>   message.

....

20   The "Coying files..." message will disappear and a **Done** button will
appear when the file transfer is complete. Click the **Done** button to
exit the **Prepare PCMCIA Disk** window.

....

21   If the PCMCIA driver software you are using requires you to stop the
PCMCIA card before ejecting it, stop the card now. If the software
you are using does not allow for this procedure, make sure that the
PCMCIA slot is not being accessed (the LED is not blinking) before
continuing.

....

Performing an initial software download
using the CIT
Procedure

Software upgrade

....

22 Eject the PCMCIA card from the PCMCIA slot of the PC.

....

23 Insert the PCMCIA card with the new software version into the
CTL/SYS50DM circuit pack located in the low speed part of the Main
Shelf (red arrow on card down and facing left). Make sure that it is
firmly seated in the CTL/SYS50DM.

Result:

The system automatically starts the download. After resetting the
system controller the red LED is illuminated for a brief moment
and after that the green LED starts flashing. When the download
is completed, all circuit packs should have the green LEDs
illuminated.

If the system does not automatically start the download, remove
both DCC controllers (ADJCTL/DCC32EI) of the Main Shelf
and insert them again. Their positions within the shelf are
described in "Main shelf configuration" (15-9).

Please note that the high speed part of the Main Shelf as well as
the Extension Shelf are not affected by this action. They have to
be assigned manually via *WaveStar* CIT (see "Creating a new
shelf" (4-8)).

Also note that the PCMCIA card has to remain in the
CTL/SYS50DM circuit pack during normal operation.

E ND   OF   S TEPS
....

❑

....

365-371-522
Issue b, October 2001

Lucent Technologies

1 0 - 7

Performing a software download for upgrade purposes using the CIT

Overview

Purpose   Use this procedure to download a new version of the NE software generic. A prerequisite for this is that a software generic is already available in the NE. If this is not the case, please refer to the task "Perform an initial software download using *WaveStar*® CIT".

Related information   For related information, please refer to:

- Chapter 22, "Software upgrade concepts"
- Chapter 24, "*WaveStar* CIT Tutorial".

Procedure

....

Before you begin   Prior to performing this task, you must:

1.   Have a valid login on both the *WaveStar*® CIT and all subject NE(s) in the ring.

2.   Acquire the CD-ROM that contains the new generic/version of the NE software ("*WaveStar* TDM 10G (STM-64) Release 4.0 NE Software", ComCode 109074625)

3.   Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.

4.   Carry out a backup of the NE database (recommended; cf. "Manually Backup Database to the *WaveStar* CIT" (11-4)).

5.   Make sure that there is no configuration (write) access to the NE from other CITs or management systems during the software download.

Required privilege code

You must have at least a privilege code of S4.

Required equipment

The following equipment is required to perform this task:

*   *WaveStar* CIT
    Please make sure that you always use the *WaveStar* CIT version corresponding to the NE release you are upgrading to. If not yet done, install *WaveStar* CIT Release 6.0.0 on your PC (cf. Chapter 24, "*WaveStar* CIT Tutorial").

Important! Do not start a software upgrade of NEs, while partition repair is active in the destination area. Software download is much slower when tunnelled through a partition repair tunnel, because the number of data packets is doubled, while more hops are used for forwarding of data packets from the management system to the destination NE. In general it is the normal procedure during network upgrades, to solve any active failure in the network, before starting (or continuing) the upgrade procedure.

Instructions   Complete the following steps to download a new version of the NE software generic.

....

1   Power up the *WaveStar* CIT PC and log into Windows NT / Windows 2000 as Administrator. If you are already logged into Windows NT / Windows 2000, close any open window.

....

Performing a software download for
upgrade purposes using the CIT
Procedure

Software upgrade

....

2 Install the NE software on your PC. To do this, use one of the
following two methods (automatic or manual installation).

....

3

IF	THEN
You use the automatic installation method	proceed with the next step.
You use the manual installation method	proceed with Step 5

....

4 Automatic Installation:

Insert the *WaveStar* CD-ROM with the new NE software and wait for
the welcoming screen to appear. If your PC does not start the
CD-ROM automatically, perform the following:

- Double-click **My Computer** on your desktop.

- Right-click on your CD-ROM drive's icon.

- Click **Auto Play**.
  If Auto Play is not available in this menu list, you have to start
  the *setup.exe* file in the root directory of your CD-ROM.
  Click the **Next** button.
  Wait for the software transfer to complete. You will notice that
  the "Decompressing Files in ..." message and also the Install
  Shield Wizard disappears when the operation has completed.
  Continue with Step 13.

....

5 Manual Installation: Insert the *WaveStar* CD-ROM with the new NE
software. If the welcoming screen appears, select **Cancel** to exit from
the automatic installation procedure.

....

6 Open the Windows Explorer on your desktop.

....

7 Select the hard disk drive where *WaveStar* CIT is installed (in most
cases **C:**) and click through to **Program Files** → **Lucent
Technologies** → **WaveStar CIT** → **generics**.

Please note that if the subdirectory **generics** does not exist, you must
create it!

....

Performing a software download for
upgrade purposes using the CIT
Procedure

Software upgrade

....

8 In the **generics** directory, create a new folder, preferrably stating the
new software version in its name.

....

9 In the Windows Explorer, right-click the CD-ROM drive of your
computer and select **Explore**. Go to the **generics** directory. This
directory contains two subdirectories: **p** and **up**.

....

10 Select the complete **up** and **p** directories and copy it to the folder you
created in Step 8.

....

11 To install Acrobat Reader on your system, go to the *AcrobatReader*
subdirectory on your CD-ROM drive and double-click the
AcrobatReader40.exe file.

....

12 The Software Release Description (SRD) is located in the
Documentation subdirectory of the CD. You can read it by double
clicking the *.pdf* file in this subdirectory.

....

13 Log into the *WaveStar* CIT.

....

14 At the *WaveStar* CIT, connect to the network element.

....

15 From the *WaveStar* CIT **System View**, select the **Configuration** →
Software → **Download Software** menu option.

> **Result:**
>
> The **Download Generic** window appears.

....

16

IF	THEN
the connection to the NE is direct TCP/IP, the software is to be downloaded via FTP,	in the **Download from** drop down list box select **FTP**. **Reference:** Continue with step Step 18.

....

Performing a software download for
upgrade purposes using the CIT
Procedure

Software upgrade

IF	THEN
the connection to the NE is through a TCP/IP Gateway which does NOT support IP Tunneling,	in the **Download from** drop down list box select **FTTD**. **Reference:** Continue with step Step 17.
you want to download the software directly from the CIT,	in the **Download from** drop down list box select **CIT**. **Result:** A file selection screen appears showing that the software will downloaded from C:\Program Files\Lucent Technologies\Wavestar CIT\generics. The directory of the file selection screen is automatically pre-populated. **Reference:** Continue with step Step 20.

17   In the **FTTD** tab specify the TID, PSEL, SSEL, TSEL and NSAP for the FTTD information.

18   In the **FTP** tab specify the Server, IP or Name, Port (optional), User Name (optional) and User Password (optional) for FTP information.

19   Specify the **Source directory path**.

> **Reference:**
>
> Continue with step Step 21.

20   In the file selection window, double click the version of network element software you are upgrading to (i.e. if manual installation has been done, the name of the folder you created in Step 8), double click the **p** directory.

21   Click the **Download** push-button.

> **Result:**
>
> A warning screen appears.

22   Read the text in the warning screen and if you are sure, confirm with **OK**.

Performing a software download for
upgrade purposes using the CIT
Procedure

Software upgrade

Result:

A second warning screen appears.

....

23   Read the text in the second warning screen and confirm with **Yes**.

Result:

The new software generic is being downloaded to the NE.

A progress indicator window is shown. When the download is finished successfully, the progress indicator disappears.

Please note that downloading a full generic will take approx. 1 hour 10 minutes.

....

24   The new software generic is now available in the "PREVIOUS" area of the NE's non-volatile memory (NVM). It is not yet activated. For activating the new software, please refer to the task "Activating an NE software generic" (10-14).

E ND OF S TEPS

....

⌐

Activating an NE software generic

Overview

Purpose   Use this procedure to activate a downloaded new version of NE software generic.

Related information   For related information, please refer to:

- Chapter 22, "Software upgrade concepts"
- Chapter 24, " *WaveStar*® CIT Tutorial".

Lucent Technologies

Procedure

....

Before you begin   Prior to performing this task, you must:

1. Have a valid login on both the *WaveStar*® CIT and all subject NE(s) within the ring.

2. Connect the *WaveStar* CIT to the local area network (LAN) of the subject NE/ring.

3. Have performed a software download to the non-volatile memory of the NE before.

Required privilege code

You must have at least a privilege code of S4.

Required equipment

The following equipment is required to perform this task:

- *WaveStar* CIT

Instructions   Complete the following steps to activate a new version of the NE software generic.

....

1   Log into the *WaveStar* CIT.

....

2   At the *WaveStar* CIT, connect to the network element where you want to activate the software currently located in the "PREVIOUS" area of the non-volatile memory (NVM).

....

3   In the *WaveStar* CIT **System View**, select the menu option **Configuration → Software → Activate Software**.

....

4   The **Software Generic Activate** window appears. The window shows the currently inactive software generic in the "PREVIOUS" area of the non-volatile memory. Select the generic in the list.

....

5   Click **OK**.

> **Result:**
>
> A confirmation window appears.

....

6   If you are sure you want to activate the software, confirm by clicking **Yes**.

....

....

7 The new software generic is activated. The activation is not traffic
affecting. The NE performs a reset and it takes approx. 10 minutes
until the NE is reachable by *WaveStar* CIT again.

E ND OF S TEPS

....

Retrieving NE software generic information

Overview

....

Purpose Using the *WaveStar*® CIT you can retrieve the current software version ID. Software updates, or patches, are identified and included in the current version, if appropriate.

Software version numbering The version number of a software generic (e.g., new, point, or patch) is identified by a numeric scheme by which a new release and its subsequent point and patch releases can unambiguously be identified and related. Each field in the version numbering has two digits.

As an example of version numbering, 01.03.00, which signifies the 00 patch release to the 03 point release associated with the 01 release, corresponds to the successive edits for the first release.

NE software display window *WaveStar* CIT allows the user to view the current status of the various copies and releases of the NE software as they reside on the NE non-volatile memory (NVM). The display includes the currently active release and may include either the previous release or a newly downloaded release which might not yet be applied.

NE active software The **About NE** window which displays the currently active NE software version in the form explained above, is invoked by selecting **Help** → **About This Network Element** from the NE **System View** menu bar.

⌐

....

Procedure

....

Instructions   To invoke the **CIT/NE Software** display window proceed as
follows.

....

1   Select **View** → **Software Generic** from the NE **System View** menu
bar.

> **Result:**
>
> A file selection window is displayed.

With this invocation of the file selection screen, only NE software
type files stored on the CIT or on the NE are selectable.

....

2   Select a file or files or directory.
E ND OF S TEPS
....

Displayed information   The following information is displayed in the window for each file
selected by the user:

Object	Description/Behavior
Current generic	Software release which is currently active for the system.
File	Selected file. If resident on the NE, the file description indicates whether the file is • Current • Previous Otherwise it gives the directory tree and name of the specific file.
NE Type	Product type of alphanumeric characters
Release	Software release, for example: 01.03.00, which signifies the 00 patch release to the 03 point release associated with the 01 release, corresponds to the successive edits for the first release.
Supplier	Name of the supplier, currently Lucent.
Delivered	Date and end time that the software release was downloaded onto the NE, if this is an NE file, or the date and time the file was last modified if the file is not on the NE.

....

Object	Description/Behavior
Installed	Date and start time that the software release was installed onto the NE. If this release has not yet been applied, this field is "-".
Size	Size of the software in bytes.
Source	Source of the original download. Examples at this time include CIT and EMS along with a file path and file name. If the source system is either CIT or EMS and if the file is on the NE, the field additionally includes the psel, ssel, tsel, and NSAP values for those systems (for further explanation, refer to "DCN protocols and services" (14-11) and "NSAP address format" (14-16)).
Software State	State of this software release. It may take the values: • Corrupt • Downloaded • In Progress • Failed • Previous • Running • Initial.
Free NVM Space	Displays the free space available on the storage device in bytes.
Unavailable NVM Space	Displays the unavailable space available on the storage device in bytes.

11   Database backup

Overview

....

Purpose   This chapter describes the procedure which has to be carried out for a NE database backup of the *WaveStar*® TDM 10G (STM-64). Furthermore, the procedure for retrieving information on the current NE database is provided.

Contents

⌐

....

365-371-522   **Lucent Technologies**   1 1 - 1
Issue b, October 2001

Set limit to the number of saved backups

Overview

Purpose   Use this procedure to specify the maximum number of backup
directories to be saved.

⌐

Procedure

....

Before you begin   Before you begin this task:

- Obtain the work instructions for this task.

- Verify that a *WaveStar*® CIT is connected and logged into the *WaveStar* TDM 10G (STM-64) system.

Required equipment

The following equipment is required to perform this task.

- *WaveStar* Customer Interface Terminal (*WaveStar* CIT)

Instructions   Complete the following steps to manually backup the network element database (current program and data) to the *WaveStar* CIT.

....

1   At the *WaveStar* CIT, select **Configuration**→ **Software** → **Remote Backup**.

....

2   In the **Backup Database** window select **Setup**.

> **Result:**
>
> The **Provision Backup Number** screen appears.

....

3   In the **Provision Backup Number** screen specify the maximum number of backups to CIT per system.

The parameter can be set to a number from 1 to 99, or it can be set to infinite.

....

4   Click on **OK**.

E N D   O F   S T E P S

....

⌐

....

Manually Backup Database to the *WaveStar*® CIT

Overview

Purpose   Use this procedure to manually backup the network element database (current program and data) to the *WaveStar* Customer Interface Terminal (*WaveStar* CIT):

- after initial software installations/upgrades/changes

- after major provisioning data changes

- periodically according to local policy

- before software upgrades/changes

- before major provisioning data changes

Related information   For related information, see:

- Chapter 23, "Database backup concepts"

- *WaveStar* TDM 10G (STM-64) Alarm Messages and TroubleClearing Guide, "Manually Restore Database from the WaveStar™ CIT to an NE"

⌐

Procedure

....

Before you begin   Before you begin this task:

- Obtain the work instructions for this task.

- Verify that a *WaveStar*® CIT is connected and logged into the *WaveStar* TDM 10G (STM-64) system.

Required equipment

The following equipment is required to perform this task.

- *WaveStar* Customer Interface Terminal (*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 damage to sensitive components

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar TDM 10G (STM-64) system, to prevent electrostatic discharge damage to sensitive components.

Important! Do not start a database backup of NEs, while partition repair is active in the destination area. Database backup is much slower when tunnelled through a partition repair tunnel, because the number of data packets is doubled, while more hops are used for forwarding of data packets from the NE to the management system.

Instructions   Complete the following steps to manually backup the network element database (current program and data) to the *WaveStar* CIT.

....

1   At the *WaveStar* CIT, select **Configuration→ Software → Remote Backup**.

....

2

....

IF	THEN
the connection to the NE is direct TCP/IP,	in the **Backup To** drop down list box select **FTP**. **Reference:** Continue with step Step 4.
the connection to the NE is through a TCP/IP Gateway which does NOT support IP Tunneling,	in the **Backup To** drop down list box select **FTTD**. **Reference:** Continue with step Step 3.
you want to backup the database directly to the CIT,	in the **Backup To** drop down list box select **CIT**. **Result:** A file selection screen appears showing that the database will back up to a specified folder under C:\Program Files\Lucent Technologies\Wavestar CIT\.... The directory of the file selection screen is automatically pre-populated. **Reference:** Continue with step Step 6.

3   In the **FTTD** tab specify the TID, PSEL, SSEL, TSEL and NSAP for the FTTD information.

4   In the **FTP** tab specify the Server, IP or Name, Port (optional), User Name (optional) and User Password (optional) for FTP information.

5   Specify the **Destination directory path**.

6   Record the path/destination of the backup folder/files and click on **Backup**.

> **Result:**
>
> The NE Data Backup in Progress Screen appears.

7   When the NE Data Backup in Progress screen disappears and the backup is complete, select **View → NE Data...**

> **Result:**
>
> The File Selection Screen appears.

....

8   Select CIT in the Look in: field and double click on C:, Program
Files, Lucent Technologies, *WaveStar* CIT, and Backups. Then click
on the backupfoldernumber and on OK.

Result:

The Database Info Screen appears.

....

9   Verify the Last Backup Time and Last Backup Destination parameters
and click on Close.

E N D   O F   S T E P S

....

Retrieving NE database information

Overview

....

Purpose   Via the *WaveStar*® CIT you can retrieve the NE Backup status as reported by the NE as well as showing the release number of NE Data backup files resident on the CIT.

Related information   For related information, see Chapter 23, "Database backup concepts".

⌐

....

1 1 - 8   **Lucent Technologies**   365-371-522
Issue b, October 2001

Procedure

....

Instructions   To invoke the **Database Info** window proceed as follows.
....

1   Select **View** → **NE Data** from the **System View** menu bar.

   Result:

   A file selection window is displayed.

....

2   Select a file or files or directory.

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

Displayed information   The **Database Info** window displays the following information for the file(s) selected by the user:

Object	Description/Behavior
Current Generic	Version number of current NE software generic
TID	TID of the NE from which the configuration data was stored on this NVM.
Software Release	Software release corresponding to the data.
Size	Size of the file in bytes.
State	State of this data. It may take the values: • Corrupt • Failed • Initial • In Progress • Previous • Running.
Last Backup Time	Date and time when the data was backed up from the NE. If there has been no backup, this field is blank.
Last Backup Destination	Destination of the most recent backup. Examples at this time include SEC, EMS, and CIT and a file name/path. If there has been no backup, this field is blank.
Last Restore Time	Date and time when the data was restored to the NE. If there has been no restoral, this field is blank. This field only applies to files on the NE.

....

Object	Description/Behavior
Last Restore Source	Source of the most recent restore. Examples at this time include EMS and CIT plus a file name/path. If there has been no restoral, this field is blank.

⌐

12   Periodic activities

Overview

Purpose   This section describes periodic activities for maintaining the system.

Replacing the fan filter

Overview

....

Purpose Use this procedure:

- Every 6 months, as a part of routine fan maintenance
- When instructed to do so as a part of a trouble-clearing task

Related information For related information, see:

- "Operations interfaces" (16-42)

⊐

....

Lucent Technologies

Procedure

....

Before you begin   The following equipment is required to perform this task:

- A replacement fan filter

Instructions   Complete the following steps to replace the fan filter.
....

1   If required, remove the shelf cover.
....

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 into the shelf so that the two pull tabs are positioned at the front of the shelf.
....

4   Replace the shelf cover.
....

5   Discard the dirty fan filter.
E N D   O F   S T E P S
....

....

365-371-522
Issue b, October 2001

Lucent Technologies

1 2 - 3

13 Security and administration concepts

Overview

Purpose
This chapter provides information on security and administration concepts.

Contents

Security management

....

Access control   Access to the *WaveStar*® CIT and to *WaveStar* TDM 10G (STM-64) network elements is controlled by user logins and associated passwords. User access privileges are defined by authorization levels assigned when the user logins are created.

Security databases   A decentralized database concept is used to manage the related security information. The *WaveStar* CIT and the *WaveStar* TDM 10G (STM-64) network elements have separate security databases.

The following figure illustrates the decentralized database concept.

WaveStar™ CIT
security database

Network element
security database
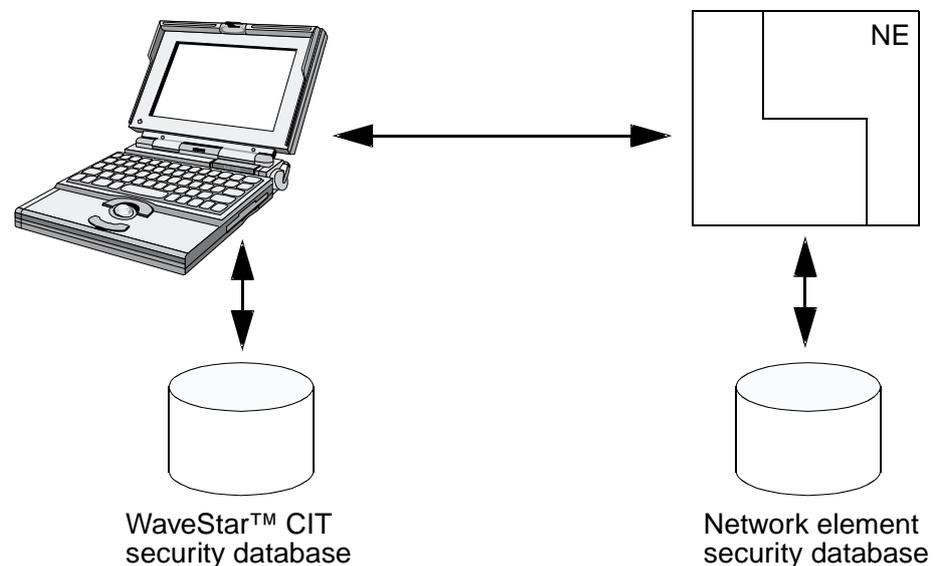
Important! Due to the decentralized database concept it is possible that a user may have different passwords for the *WaveStar* CIT and for an NE. The *WaveStar* CIT, however, may "learn" settings from an NE security database.

⌐

....

User administration

....

Overview   User administration (please refer to "Administering user logins" (2-2)) comprises the following:

- Creating, modifying or deleting user logins,

- Specifying associated passwords,

- Assigning access privileges.

User permission   Administration on the security databases can only be performed by a security administrator, i.e. a super user login or at least a user login with a security privilege code of 'S5' is required.

User login and password   Each user must enter a user identification (user login) and a password to gain access to the *WaveStar*® CIT or to a *WaveStar* TDM 10G (STM-64) NE.

To connect to a *WaveStar* TDM 10G (STM-64) NE, firstly a login attempt with the same user login and password used for the *WaveStar* CIT login will be made.

Valid user login   The following characters are allowed in a user login:

- Upper-case letters ('A' .. 'Z')

- Lower-case letters ('a' .. 'z')

- Digits ('0' .. '9')

A valid user login consists of a sequence of one to ten characters.

Important! The reserved word "ALL" in any combination of uppercase or lowercase letters cannot be used for a valid user login.

Valid password   The following characters are allowed in a password:

- Upper-case letters ('A' .. 'Z')

- Lower-case letters ('a' .. 'z')

- Digits ('0' .. '9')

- Special characters:

  - Plus sign ('+')

  - Percent sign ('%')

  - Number sign ('#')

....

Furthermore, a valid password ...

- ... consists of a sequence of six to ten characters.

- ... must start with a letter.

- ... must contain at least one of the special characters ('+', '%' or '#').

Important! Passwords are case sensitive.

User privilege codes Users are given access privileges by means of user privilege codes when the user login is created or modified. The user privilege codes determine the tasks a user is permitted to perform. They consist of a combination of one or two letters representing the functional category and a one-digit number representing the authorization level within that functional category.

The following user privilege codes are defined:

Maintenance	M0	M1	M2	M3	M4	M5
Provisioning	P0	P1	P2	P3	P4	P5
Performance Monitoring	PM0	PM1	PM2	PM3	PM4	PM5
Security	–	S1	S2	S3	S4	S5
Test	T0	T1	T2	T3	T4	T5

If a particular authorization level is '0', then there are no access privileges granted for the corresponding functional category, i.e. execution of any of the related tasks is not allowed. Notice that a user privilege code of 'S0' is not allowed and therefore not defined.

A user can be assigned any combination of user privilege codes with the only exception that apart from the two predefined super users (cf. "Super user logins and passwords" (13-7)) no other user can have an authorization level of '5' for all functional categories.

Predefined user types User types are categorized depending on the task to perform. Some users may have full access to all functions while other users have restricted access.

The six predefined user types with associated user privilege codes are as follows:

Super user	M5	P5	PM5	S5	T5
Privileged user	M5	P5	PM5	S3	T5
General user	M4	P3	PM4	S1	T4
Maintenance user	M4	P3	PM1	S1	T4

Reports only (user)	M1	P1	PM1	S1	T1
Default user	M1	P1	PM1	S1	T1

Priority level

By means of the priority level a priority for the execution of commands can be assigned. For example, if two commands are executed at the same time for the same NE, the command originating from the user with the highest priority level will be executed first.

The priority level range of values is from one to five. The highest priority level is five, the default priority level is one.

Notification list

The notification list indicates the type of notifications a user may receive. The following settings are possible:

- Database changes (DBCHG) (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

- State changes (STCHG) (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

- Protection switching changes (PSCHG) (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

- Alarm notifications (ALARMS) (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

- Responses to commands initiated by any user (RESPONS)

- Combinations of the above (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

- Responses to commands initiated by the user (OWN)
  Responses to commands initiated by the user are always included.

- ALL (only if **User receives his/her own command response only** is not selected in the **Change Notification** form.)

Inactivity time-out period

The inactivity time-out period indicates the number of minutes of inactivity before a user is logged off. The number of minutes ranges from 0 to 999. The default is 30. A value of zero disables this function.

User class

This is the class of the user, and can have the following values

- OTHER

This is the default class. For users in this class, command privileges and notifications are controlled only by their UPCs and their Notification Registration List. For users in this class, the ATAG sequence starts with 000 when they log in. Each user session has a unique ATAG sequence.

- MEMADMIN
  This is a special user class for TL1 Memory Administration OS users. For users IDs assigned to this user class, a special handling of DBCHG notifications is used. The only autonomous messages that MEMADMIN users will receive are DBCHG messages. The ATAG sequence for the autonomous messages is maintained for the entire MEMADMIN user class. In other words, the same ATAG value is used for the same autonomous message sent to all users in the MEMADMIN user class that are logged in. For MEMADMIN users, the ATAG sequence continues during an interruption.
  The ATAG sequencing continues:
  - across NE/OS loss of communication
  - across NE resets
  - or if autonomous message reporting is inhibited with the INH-MSG command.

  If MEMADMIN is selected, then the User Notification Registration List is set to *not applicable*. The Modify button in the *WaveStar* **CIT User Provisioning** window is disabled.

Password aging   Password aging is the interval before you have to change your password stored on an NE. The password aging interval range is from 7 to 999 days. The default value is 90 days. Select disable to switch off this function.

User id lockout threshold   The *User Id Lockout Threshold* indicates the number of sequential invalid login attempts after which the user id will be locked out and an *Intruder Alert Alarm* will be raised. This parameter is defined for the whole NE. The default value is 5. The number of invalid login attempts ranges from 2 to 99.

User id lockout period   The *User Id Lockout Period* indicates the number of minutes a user id will be locked out after the number of sequential login attempts exceeds the *User Id Lockout Threshold*. This parameter is defined for the whole NE. The default is 10. The number of minutes ranges from 0 to 99.

Important! Setting this parameter to 0 will eliminate User Id Lockout.

User id lockout aging period

The *User Id Lockout Aging Period* indicates the number of minutes before the NE resets a user's invalid login attempt count. This is the time period within which the counter of invalid sequential attempts are counted and starts at the first invalid login attempt. For example, if the user has 4 sequential invalid login attempts within this aging period, the invalid attempts counter is 4 and the user has not exceeded the threshold of 5 (i.e., the *User ID Lockout Threshold*). If the user then has another invalid login attempt within this aging period, the threshold will have been exceeded and the user will be locked out for the period defined by the *User Id Lockout Period*. However, if the user does not attempt another login within the lockout aging period, e.g., 60 minutes, the invalid attempts counter is reset to zero. Thus, after 60 minutes from the first invalid login attempt, the user gets another 5 attempts to login before being locked out. Note that both the invalid attempts counter and the aging period are reset to zero whenever a login attempt is successful. This parameter is defined for the whole NE. The default value is 60 minutes. The number of minutes ranges from 1 to 999 minutes.

User id aging period

The *User Id Aging Period* is a system-wide parameter. The NE provides the capability to modify this parameter. Its default value is 10 days, with a settable range from 0 days to 999 days, in increments of 1 day. The value 0 disables user ID aging.

History logs

The history logs a user can retrieve are defined by the settings in the *registration list* for the specific user.

The following table shows the correlation between the entries in the history logs and the settings in the notification registration list.

History log	DBCHG	STCHG	PSCHG	ALARMS	RESPONS
NE alarm log	–	–	–	X	–
NE protection switch activity log	–	–	X	–	–
NE user log	–	–	–	–	X
NE notification log	X	X	–	–	–

Super user logins and passwords

Two super user logins are preinstalled: "LUC01" and "LUC02".

The associated passwords are:

- For the *WaveStar* CIT:

  - "LUC+01" and "LUC+02", if the current *WaveStar* CIT release is the first *WaveStar* CIT installation on the respective PC,

  - the previously defined passwords, if previous releases of the *WaveStar* CIT have already been installed on the respective PC.

- For *WaveStar* TDM 10G (STM-64) NEs: "LUC+01" and "LUC+02".

A super user has an authorization level of '5' in all functional categories (cf. "Predefined user types" (13-4)).

The user privilege codes cannot be changed and no other user can be assigned authorization levels of '5' for all functional categories. The super user logins cannot be renamed or removed, and no other super user logins can be added. However, the default passwords can be changed.

Important! If both super user passwords are forgotten, the software containing the logins must be reloaded to recover the preinstalled logins.

⌐

History logs

Types of history logs   The *WaveStar*® TDM 10G (STM-64) system provides the following history logs:

- NE alarm log
- NE protection switch activity log
- NE user log
- NE notification log

History logs are used to display history data that is maintained in the network element database.

User dependency   Which history logs will be retrievable by a user depends on the settings in the notification registration list defined during user provisioning; please refer to "Notification list" (13-5).

NE alarm log   The NE alarm log provides a chronological history of all of the most recent anomalous behaviour detected by a *WaveStar* TDM 10G (STM-64) network element. The NE alarm log may contain up to 1024 entries.

The NE alarm log can be invoked via **Reports → NE Alarm Log...** from the **System View** or **Shelf View** main menu of the *WaveStar* CIT.

NE protection switch activity log   The NE protection switch activity log provides a chronological history of all of the most recent manual and automatic protection switching activities. The NE protection switch activity log may contain up to 512 entries.

The NE protection switch activity log can be invoked via **Reports → NE Protection Switch Activity Log...** from the **System View** or **Shelf View** main menu of the *WaveStar* CIT.

NE user log   The NE user log contains information about the previously executed commands and can thus be used to obtain the corresponding user login for any user-initiated network activity. The NE user log may contain up to 512 entries.

The NE user log can be invoked via **Reports → NE User Log...** from the **System View** or **Shelf View** main menu of the *WaveStar* CIT.

NE notification log   The NE notification log provides a chronological history of the most recent activities that caused database updates. The NE notification log may contain up to 1000 entries.

The NE notification log can be invoked via **Reports → NE Notification Log...** from the **System View** or **Shelf View** main menu of the *WaveStar* CIT.

┑

14   Management communication setup concepts

Overview

Purpose   This chapter deals with the basic theoretical background of Data Communication Networks (DCNs) and provides DCN configuration guidelines for Wave-Star™ TDM 10G (STM-64) systems.

Contents

⌐

Basic DCN principles

....

Overview   This subsection serves as an entry point, it describes the basic DCN principles. The following subsection describes common DCN configurations. DCN configuration guidelines for *WaveStar*® products, NSAP address formats and other related information are provided thereafter.

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

SDH management network   The SDH management network is an overlay network of the transmission network. A management system and the network elements together are the nodes of this network. The Q-LAN and Data Communication Channels (DCCs; cf. "Data communication channels" (14-20)) provide the physical connection between the nodes.

DCN physical components   The following figure illustrates an OSI-DCN. The illustration only gives the physical components and connections in the DCN, it does not give the logical configuration.
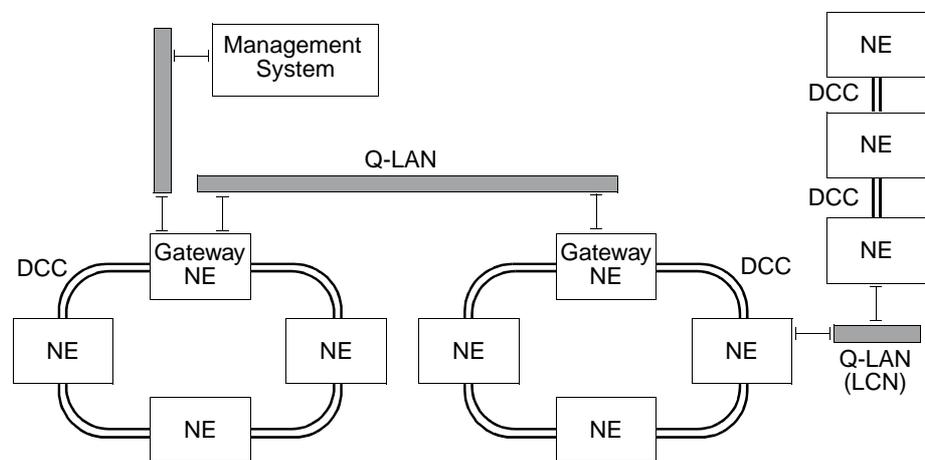
The illustration of the OSI-DCN consists of 2 Q-LANs and a number of Data Communication Channels (DCCs) in an SDH transmission network (point-to-point configuration and two ring configurations shown), with a management system (Element Management System (EMS) or Customer Interface Terminal) connected to it. The management system is connected to the transmission network via

....

Lucent Technologies

gateway network elements (GNEs) and the Q-LAN. The network elements are connected to each other by DCCs.

In the case where there is no DCC connectivity between nodes (see the right part of the illustration), a Local Communication Network (LCN) can be used to connect the nodes to each other.

"NE" versus "Node" A distinction has to be made between network elements and nodes. Network elements can be identified by their target identifier (TID), i.e. their NE name ("NE name" and "TID" are used synonymously throughout this User Operations Guide), whereas a node is identified by its Network Service Access Point (NSAP) address. Each NSAP address within a network constitutes a node which can individually be addressed.

Please note that a *WaveStar* TDM 10G (STM-64) network element has exactly one TID but up to three NSAP addresses.

Example:

A *WaveStar* TDM 10G (STM-64) network element consisting of a main shelf (with high speed part and low speed part) and an extension shelf comprises three nodes since each single part of the NE has its own DCC controller (ADJCTL/DCC32EI), i.e. its own NSAP address.
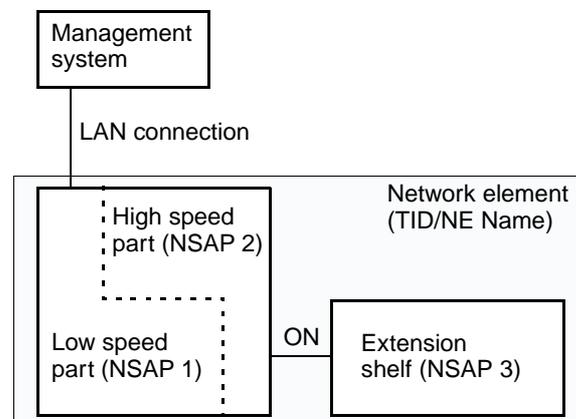
DCN protocols The Protocols used in the DCN between the nodes include:

- Media access protocols:
    - Ethernet on the Q-LAN
    - LAPD on the DCCs
- OSI network routing protocol (DCN wide)
  The OSI network routing protocol (OSI-DCN) is used for routing management data between nodes in the DCN.

ISO-OSI network protocols The network protocols used between nodes are the ISO-OSI network protocols:

- Connectionless Network Service/Connectionless Network Protocol (CLNS/CLNP) acc. to ISO 8473,

- ES-IS routing protocol acc. to ISO 9542,

- IS-IS routing protocol acc. to ISO 10589.

According to these protocols a node in the network can behave as an end system (ES) or as an intermediate system (IS, sometimes also called a router).

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

End systems (ESs) periodically generate ES Hellos (ESHs) to announce their presence. These ESHs are received and recorded by neighboring intermediate systems. The interval between two ESHs is determined by the End System Configuration Timer (ESCT).

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

Comparable to ESs, ISs periodically generate IS Hellos (ISHs). The interval between two ISHs is determined by the Intermediate System Configuration Timer (ISCT).

ES - IS protocol The end system to intermediate system protocol (ES-IS protocol) provides information to ISs on the existence of ESs within an area. This information is sent periodically to the ISs via a broadcast mechanism. The ES-IS protocol permits ESs to discover the existence and reachability of ISs and vice versa. Furthermore, the ES-IS protocol provides information to ISs supporting the computation of the shortest path first (SPF) algorithm. *WaveStar* products make use of the ES-IS protocol acc. to ISO 9542.

IS - IS protocol

The intermediate system to intermediate system protocol (IS-IS protocol) is used between intermediate systems in the DCN. The IS-IS protocol maintains the IS Routing Information Base (RIB). The information in the RIB is used by the SPF algorithm for the routing of management data packets in the DCN by the intermediate systems. *WaveStar* products make use of the IS-IS protocol acc. to ISO 10589.

Routing information base and LSPs

Each Routing Information Base comprises a number of routing tables containing information on NSAP addresses of nodes in the network and ports of the IS through which these nodes can be reached.

Intermediate systems exchange routing information regularly with one another as part of the IS-IS protocol by the use of Link State PDUs (Link State Protocol Data Units, LSPs). A Link State PDU contains information about the node itself, about its neighboring ES nodes, and about its neighboring IS nodes.

LSPs exchanged within a level-1 area are called L1-LSPs, LSPs exchanged accross level-2 areas are called L2-LSPs.

OSI routing map and OSI neighbor map

The *OSI Routing Map* and the *OSI Neighbor Map* information that can be retrieved by using the WaveStar™ CIT is derived from a node's internal routing tables and the LSP databases. The LSP database contents are equal in all nodes within an area (distributed database concept).

Please note that when a DCC controller (ADJCTL/DCC32EI) is restarted then the LSP databases and the internal routing tables may temporarily contain inconsistent information. As a consequence, the information displayed in the *OSI Routing Map* and the *OSI Neighbor Map* may also be inconsistent. After the DCC controller restart has finished Link State PDUs are exchanged to resynchronise the databases.

Management protocol: TL1

The management of *WaveStar* products is based on the use of the Transaction Language 1 (TL1, defined by Telcordia Technologies, fromerly Bellcore, standards) on the OSI application layer.

Please also refer to the *WaveStar* TDM 10G (STM-64) *TL1 Reference Manual*.

DCN configurations

....

Hierarchical routing Hierarchical routing is used for large networks when the number of NSAP entries in the RIB databases of the intermediate systems becomes too large. When this happens, it causes an exponential increase of exchanged LSPs between intermediate systems. This in turn causes the performance of the DCN to decrease due to the computation of the shortest path first (SPF) algorithm.

Definition of hierachical routing:

In hierachical routing, the addressing domain of the DCN is divided into a number of areas. Each area is assigned a unique area identifier. The value of the area identifier of the NSAP address of each node is set according to which area a node belongs (cf. "NSAP address format" (14-16)).

Level-1 IS and level-2 IS Each area contains a number of end systems as well as level-1 and level-2 intermediate systems. Level-1 intermediate systems (level-1 ISs) provide interconnectivity between nodes in an area. Level-2 intermediate systems (level-2 ISs) provide interconnectivity between areas.

Level-2 subdomain The adjacent set of level-2 ISs is also referred to as the level-2 subdomain. All areas in a network are connected via the level-2 subdomain

Area-divisioning of a DCN Divisioning is configuring the DCN in such a way that the exchange of LSPs between intermediate systems is limited.

When networks are divided into areas, the RIB databases in the systems are much smaller and hence the routing overhead is significantly reduced. Intermediate systems in an area only exchange information (L1-LSPs) on nodes with other systems in their own area. Information on other areas is exchanged by level 2 ISs only and maintained by the level-2 ISs of the area.

In this way, the load of management data in the network is strongly reduced, while keeping the dynamic re-routing capabilities of intermediate systems in case of failures intact. It is important to notice that although the DCN is divided into areas, ES-ES communication between all nodes in the DCN is still possible.

The following figure illustrates how a network can be divided into areas, connected by level-2 ISs. Each area has at least one level-2 IS

....

Lucent Technologies

assigned and can have a number of level-1 intermediate systems and end systems.
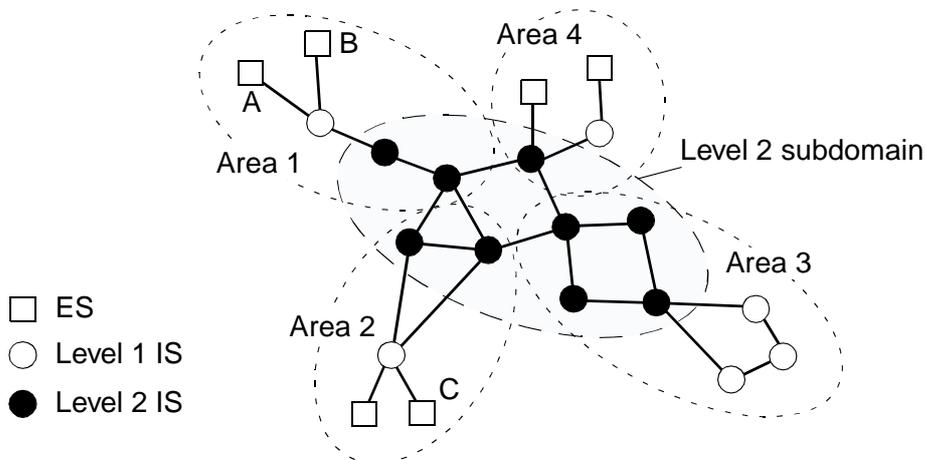
Divisioning at network protocol level

Divisioning of the DCN is usually done at the network protocol level. Communication between intermediate systems is disabled or enabled using different techniques, but this does not necessarily have to affect the physical DCN topology. The SDH transmission network should in general not be affected by DCN engineering.

Example: Routing of management data

Suppose a node "A" wants to send messages to another node. If this node is in the same area (determined by means of the area identifier of the node's NSAP address), the messages from "A" to this particular node ("B" in "Area-divisioning of a DCN" (14-7)) are routed directly using a level-1 intermediate system.

Alternatively, if the desired destination is in a different area ("C" in "Area-divisioning of a DCN" (14-7)), the messages are sent to a second, higher level (level-2) intermediate system. This level-2 IS routes the messages coming from node "A" to other level-2 ISs until they reach a level-2 intermediate system attached to the destination area of "C". From there, the messages are routed to "C" within the area using one or more level-1 ISs.

Types of OSI-DCN networks

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

• Undivided DCN, or

• IS-IS area-divided DCN.

These two types of OSI-DCN network are illustrated in the following figure.

Undivided

IS-IS Area-Divided

□ ES

○ Level 1 IS

● Level 2 IS

▬ Q-LAN

☁ (sub-) network
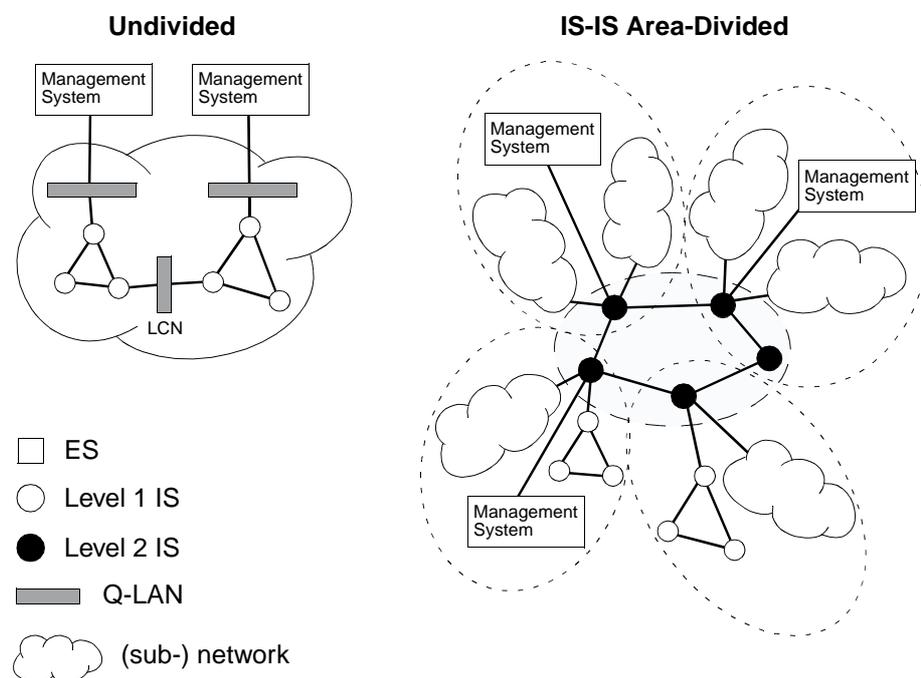
Undivided DCN   An undivided DCN consists of a single area. There is no division between the nodes on network protocol level. All nodes in the network and especially the intermediate systems can exchange routing information with each other. Although a network element can only be managed by one magement system at a time, the IS-IS protocol is running between all nodes in the network. This leads to the exchange of LSPs between all intermediate systems in the network.

IS-IS area-divided DCN   The divisioning of the DCN into areas can be accomplished by introducing level-2 intermediate systems (cf. "Area-divisioning of a DCN" (14-6)).

Advantages of areas

Among others, areas have the following advantages:

•   Management systems can be connected to any point in the DCN.

As a rule, management systems should be connected to the backbone of the DCN, i.e. to a level-2 intermediate system in the center of their management domain, to prevent them from being overloaded with too much data in the case of a failure resulting in re-routing data traffic.

- The exchange of data is still possible between **all** nodes in the DCN (cf. "Example: Routing of management data" (14-7)).

⌐

DCN configuration guidelines
....

Background information   Please refer to "Basic DCN principles" (14-2) and to "DCN configurations" (14-6). These two sections provide theoretical background information on data communication networks.

Guidelines   Please observe the following engineering guidelines when configuring a DCN with *WaveStar*® TDM 10G (STM-64) systems involved:

- A maximum of 50 nodes (i.e. NSAP addresses) is supported in an area.
  Notice that a *WaveStar* TDM 10G (STM-64) network element may **comprise up to three nodes** (please refer to ""NE" versus "Node"" (14-3)).

- A maximum of 50 areas is supported in a subnetwork.

- All nodes in an area must have the same area address (cf. "ISO-DCC NSAP address format" (14-16)).

- All nodes in an area must have DCC connectivity **within the area** to all other nodes in the same area.

- At least one level-2 IS is required per area in area-divided DCNs for communication accross area boundaries. Two level-2 ISs are recommended in each area for DCC communications redundancy to/from each area.

- All level-2 ISs must have DCC connectivity, either directly or indirectly via other level-2 ISs, to all other level-2 ISs in the subnetwork to form a single level-2 subdomain that provides connectivity to all areas.

- To distribute the load of management data in a subnetwork, it is recommended, when feasible, but not required that:

  - all area sizes be approximately the same,

  - and the number of level-2 ISs be about the same as the average area size.

  For example, a perfectly balanced subnetwork of 200 nodes would include 20 nodes per area in each of 10 areas and 20 level-2 ISs in the level-2 subdomain (two level-2 ISs per area).

Related information   Please refer to "NSAP address format" (14-16) and to "Data communication channels" (14-20) for further information.

⌐

....

Lucent Technologies

DCN protocols and services

....

Overview

WaveStar® TDM 10G (STM-64) network elements support the exchange of management information over DCC, OSI LAN, or TCP/IP. This network operations capability uses the section DCC bytes in the SDH overhead of the optical signals. *WaveStar* CIT dialogues and OS messages are transmitted in these DCC bytes.

The *WaveStar* TDM 10G (STM-64) OS interface is accessed through one of the 10BaseT Ethernet IAO LAN rear panel connectors. The *WaveStar* TDM 10G (STM-64) interface supports Transaction Language 1 (TL1) for commands/messages, and File Transfer and Access Management (FTAM) for software downloads and provisionable data backup and restore.

The *WaveStar* TDM 10G (STM-64) OS interfaces supported include the following:

- OSI LAN/WAN

- TL1 TCP/IP (using the internal gateway function)

- FTP/FTAM (for software download, etc.)

Standard 7-layer OSI stack

WaveStar TDM 10G (STM-64) network elements support the exchange of management information over the standard 7-layer OSI protocol stack over Local Area Networks (LAN) and over Data Communication Channels (DCC) acc. to the Telcordia Technologies (formerly Bellcore) GR-253 standard.

....

Protocols and services   The following figure shows how *WaveStar* TDM 10G (STM-64) network elements support the protocols and services.

```
                            TL1                    FTAM
Application
Layer        ┌──────────────────────────────────────────────┐
             │                     ACSE                      │
             └──────────────────────────────────────────────┘
                      ╭─────╮   P-SEL      ╭─────╮
                      │0xAF │              │0x02 │
                      ╰─────╯              ╰─────╯
Presentation ┌──────────────────────────────────────────────┐
Layer        │              ASN.1 BER / Kernel               │
             └──────────────────────────────────────────────┘
                              ╭───────╮
                              │ S-SEL │
                              ╰───────╯
Session      ┌──────────────────────────┐
Layer        │    Kernel / Full Duplex   │
             └──────────────────────────┘
                      ╭───────╮
                      │ T-SEL │
                      ╰───────╯
Transport    ┌──────────────────────┐   ┌──────────────────────┐
Layer        │  Transport Class 4   │   │   TARP (Responder    │
             │       (TP4)          │   │  & Propagation Function)│
             └──────────────────────┘   └──────────────────────┘
                   ╭──────╮  N-SEL            ╭──────╮
                   │ 0x1D │                   │ 0xAF │
                   ╰──────╯                   ╰──────╯
Network      ┌──────────────────────────────────────────────┐
Layer        │              CLNP, ES-IS, IS-IS               │
             └──────────────────────────────────────────────┘
Data Link    ┌──────────────────────────┐   ┌────────────────┐
Layer        │      IEEE 802.2 LLC1      │   │ LAPD (AITS/UITS)│
Physical     ├──────────────────────────┤   ├────────────────┤
Layer        │  10BASE-T / IEEE 802.3 MAC │   │  DCC-R, DCC-M  │
             └──────────────────────────┘   └────────────────┘
                        LAN                         DCC
```
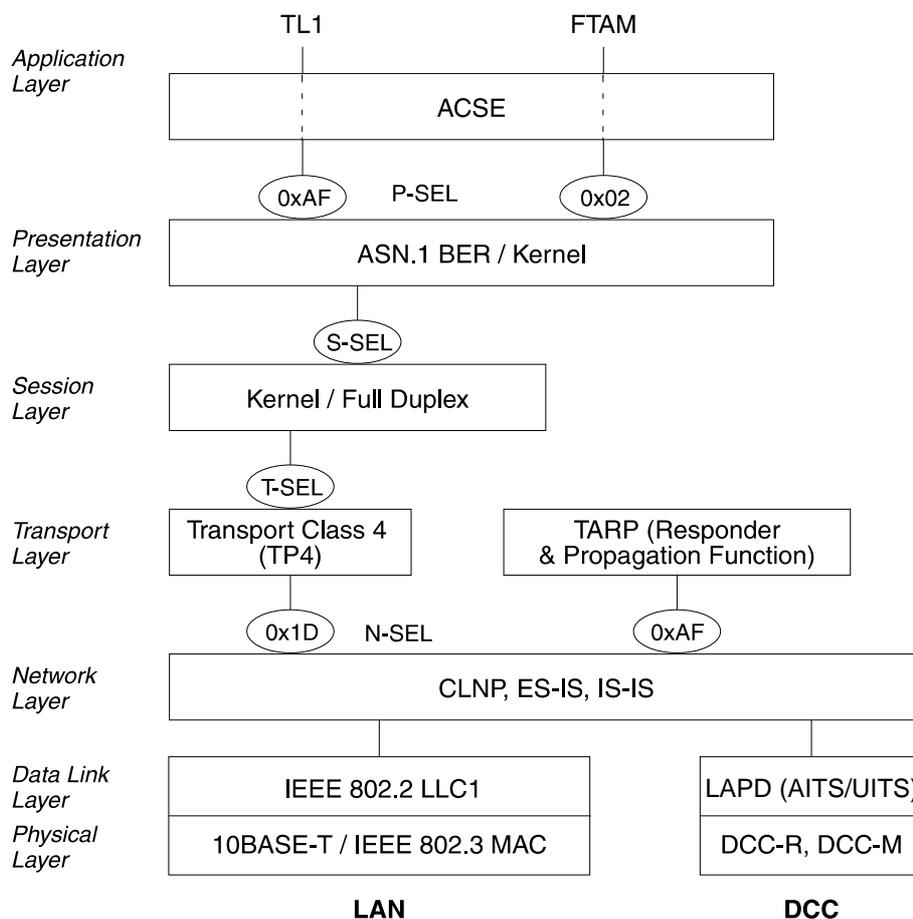
FTAM   File Transfer, Access and Management (FTAM), defined by ISO 8571, is an Application Service Element (ASE). FTAM facilitates file transfer and allows file manipulation across a network. The FTAM protocol is used for *WaveStar* TDM 10G (STM-64) software management purposes, such as software download, backup or restoration.

IAO LAN access   The IAO LAN serves two main purposes:

*   It provides a standard means of connecting a network element into a central office (CO) data communications network (DCN) to provide OS access

*   It provides an alternate path for data communications channel (DCC) communications to travel within a subnetwork.

The *WaveStar* TDM 10G (STM-64) IAO LAN is internally connected to the DCC subnetwork so that operations messages on the IAO LAN

can be seamlessly delivered to a remote network element by the DCC and vice-versa (DCC to IAO LAN).

Internal IAO LAN hub

The system supports an internal 4-port 10BaseT Ethernet IAO LAN hub (located on the ADJCTL/DCCEI circuit pack in each shelf). The *WaveStar* TDM 10G (STM-64) 10BaseT Ethernet IAO LAN backplane connectors and the *WaveStar* CIT port on the user panel are all connected to this internal hub. The internal LAN hub supports direct connection of the *WaveStar* CIT (or NCC or SNMS) without requiring an external LAN hub.

Daisy chain

The internal IAO LAN hub also supports daisy-chaining of multiple *WaveStar* TDM 10G (STM-64) shelves, for example, in the same bay. A daisy-chain connection is similar to a null-modem connection. Reference is made to a 10BaseT connection where there is no hub. In this connection, the receive pair on one end of the cable is connected to the transmit pair on the opposite end. Conversely, the transmit pair on one end is connected to the receive pair on the opposite end.

Important! A daisy-chain connection can only be repeated five times. A preferred connection would go through an external office LAN hub.

TL1 over TCP/IP   A TL1 TCP/IP gateway may be used to connect multiple collocated *WaveStar* TDM 10G (STM-64) systems to a remote OS equipped to communicate through a TCP/IP WAN. Since the OS communicates through TCP/IP, a gateway is required to provide a mapping between TCP/IP and OSI. That gateway function is included as a feature of the *WaveStar* TDM 10G (STM-64) system.

The gateway is provisioned to provide a TL1 TCP/IP gateway between TCP/IP and OSI. This process is bidirectional, mapping messages originating in the OS to the proper NE NSAP, as well as mapping messages originating in the NE to the proper OS IP address and returning then to the OS.

This interface supports TL1 messages only.

IP tunneling   The IP tunneling feature provides a way to

- manage IP managed devices (e.g. SNMP) through the OSI based DCN network (called ″IP fringe″),

- manage NEs in an OSI based DCN via an IP based access network, using IP based protocols like FTP and SNMP (called ″IP access″).

In both cases it is necessary to transport IP messages through an OSI based network.

The figure below shows the ″IP fringe″ and ″IP access″ topologies:
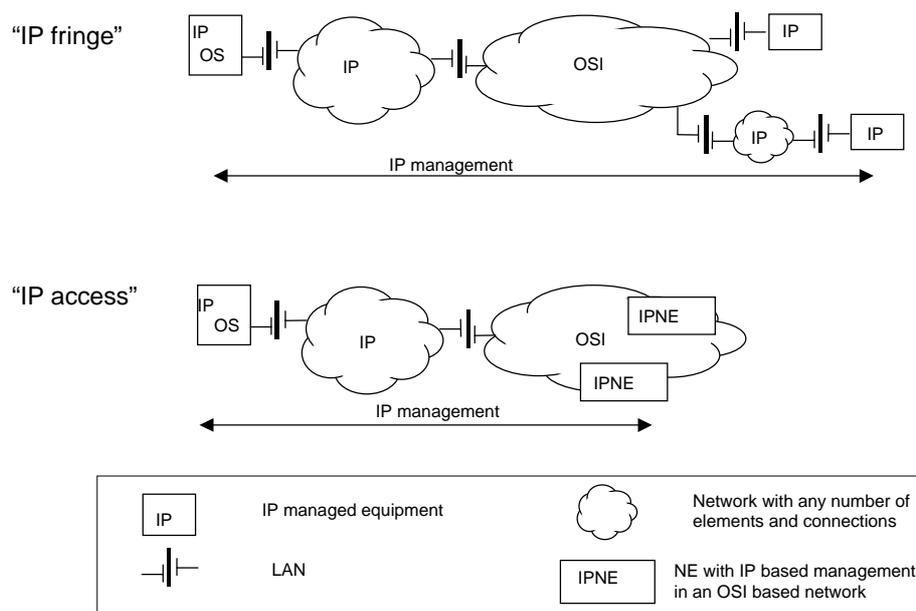
A (bidirectional) tunnel can be seen as a set of two static routing entries in nodes of the OSI network. The term tunnel may be misleading because it is often associated with connections which must be set up in advance. In this case, only some routing information needs to be provisioned and no communication between two systems is needed to set up the ″tunnel″ between them. To avoid confusion, it is better to speak of encapsulation and to think of the OSI network as a NBMA (non broadcast multiple access) subnetwork within the IP network. The NEs need to be configured with one IP address on the LAN side, connected to the IP subnet with the IP NE or the IP NEs.The LAN can be used for both OSI and IP traffic. The same ethernet address will be used for both protocols.

In the figure below, a simple example of an ″IP access″ network is given. OS is the operations system (IP based), R is an IP router, GNE

is a Gateway Network Element (any NE supporting IP tunneling can fulfill this role)

220.20.3.17/28

OS

220.20.1.1
220.20.1.2

NE 1

220.20.2.2/24

R

GNE

NE 2

220.20.2.1/24

220.20.3.33/28

NE 3

220.20.3.49/28
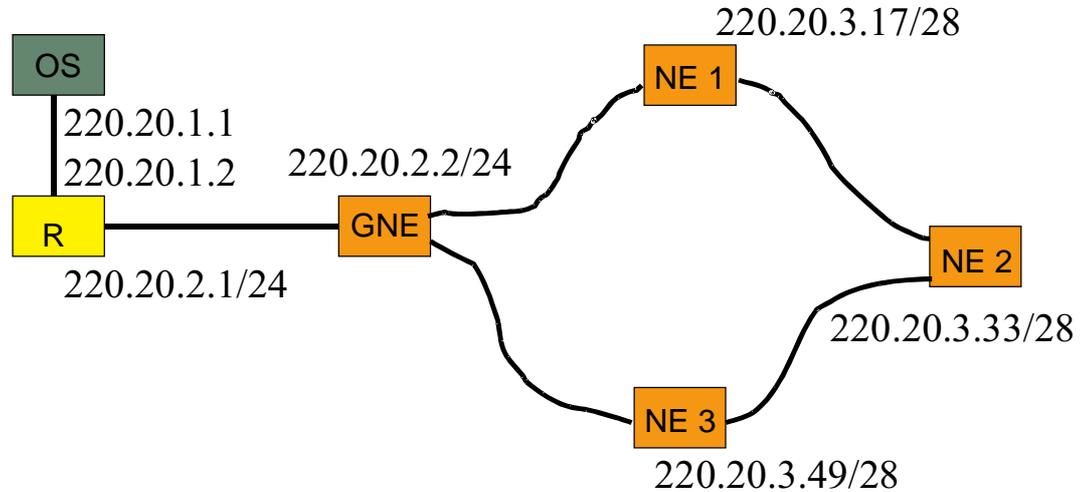
IP tunneling for FTP access

WaveStar TDM 10G (STM-64) supports IP Tunneling as a means of enabling file transfers from TCP/IP networks across the OSI network to terminating NEs. The tunneling encapsulates the TCP/IP message and protocol in an OSI envelope. The receiving unit can then regain the TCP/IP protocol as well as the message.

File transfer between manager and NE is used for two purposes:

- Software download, to upgrade the software of a network element.

- Configuration backup and restore, to make copies of the configuration of an NE so that the status can be restored after a crash.

Please note that for FTP access the NE, which is used to be the FTP client, must have TCP/IP enabled.

The following figure illustrates theIP tunneling for FTP access.

IP

FTP

OSI

SNMS
FTP Server

GNE

NE

IP tunnelling

FTP through
IP tunnel

FTP client

CIT
FTP Server

IP tunnelling
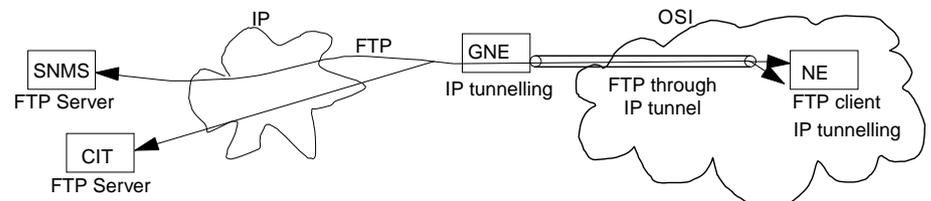
NSAP address format

....

Related information   Please refer to "Basic DCN principles" (14-2) and to "DCN configurations" (14-6). These two sections provide theoretical background information on Data Communication Networks.

For related task-oriented procedures, please refer to Chapter 3, "Management communication setup".

NSAP address   The Network Service Access Point (NSAP) address is used by the network protocol for location information. The NSAP address of a node is its DCN-wide identifier which uniquely identifies the node in the network.

ISO-DCC NSAP address format   Although different NSAP formats exist, preferably all nodes in a network should use the same address structure. The *WaveStar*® TDM 10G (STM-64) supports the 20-byte ISO Data Country Code (DCC) NSAP address format in accordance with ISO 8348.

The structure of the ISO-DCC NSAP address format is shown in the following figure.
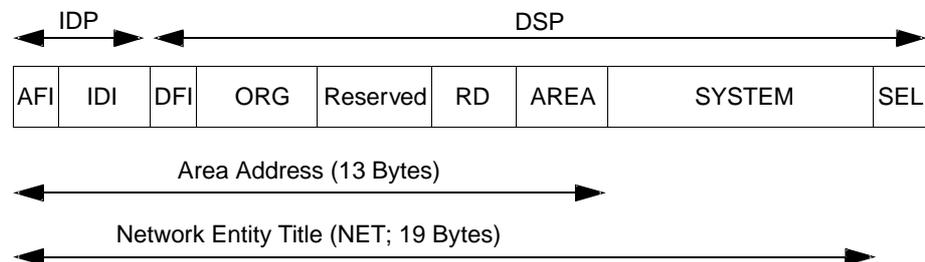
The NSAP address consists of the Initial Domain Part (IDP) and the Domain Specific Part (DSP).

The first 13 bytes ("AFI" to "AREA" fields) of the NSAP address make up the area address.

The meaning of the individual fields of the ISO-DCC NSAP address is explained in "NSAP address fields" (14-17).

Flexible NSAP address format   Alternatively to the ISO-DCC NSAP address format the flexible NSAP address format can be used.

....

Lucent Technologies

The structure of the flexible NSAP address format is shown in the following figure.
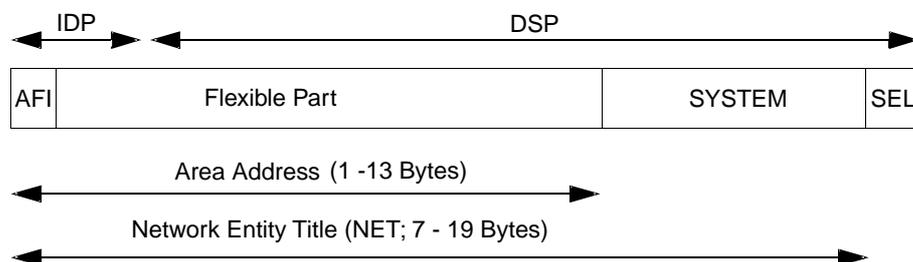
The flexible NSAP address format has an Area Address part consisting of the AFI part and a flexible part of 12 bytes length (the contents of this part can cary). Notice that the flexible NSAP address format can be used to derive the other formats.

NSAP address fields

The following table lists the NSAP address fields and describes their meaning.

Field	Meaning	Description
Initial Domain Part (IDP):		
AFI	Authority and Format Identifier specifying the NSAP address format.	The predefined value is 0x39 (hex.), indicating that the ISO Data Country Code (ISO-DCC) is the address format. This field is configurable.
IDI	Initial Domain Identifier specifying the country code.	The predefined value is 0x840F (hex.). This field is configurable.
Domain Specific Part (DSP):		
DFI	DSP Format Identifier specifying the DSP format.	The predefined value is 0x80 (hex.). This field is configurable.
ORG	Organization identifier (or Operator identifier) representing the Network Service Provider (NSP).	The predefined value is 0x000000 (hex.). This field is configurable.

Field	Meaning	Description
Reserved	Reserved portion of the NSAP.	The predefined value is 0x0000 (hex.). This field is configurable.
RD	Routing Domain	The predefined value is 0x0000 (hex.). This field is configurable.
AREA	Area identifier indicating the routing area to which a node belongs (cf. "Hierarchical routing" (14-6)).	The predefined value is 0x0000 (hex.). This field is configurable.
SYSTEM	System identifier representing the node. The IEEE 802.3 MAC address, stored on the DCC controller (ADJCTL/DCCEI circuit pack) during the manufacturing process, is used as the system identifier.	The system identifier is the field that makes the NSAP address unique throughout the DCN. This field is *not configurable*. When a new DCC controller is inserted, then the system identifier, and thus the NSAP address, automatically changes.
SEL	The selector field is used to direct the Protocol Data Units (PDUs) to the correct destination making use of the CLNP network layer service.	The predefined value is: • 0x1D (hex.) for PDUs to be processed via the OSI stack • 0xAF (hex.) for PDUs to be processed via the TID Address Resolution Protocol (TARP; cf. "Name-to-address translation" (14-27)). This field is *not configurable*.

Network entity title   The area address together with the system identifier (SYSTEM field) of the NSAP address is also called the Network Entity Title (NET; cf. "ISO-DCC NSAP address format" (14-16)).

DCC controller reset   All parameters related to DCC communication including all fields of the NSAP address are retained over a DCC controller reset. All parameters are kept in non-volatile memory.

Configuring the NSAP address   You can configure the NSAP address on each active DCC controller individually.

Important! Changing the NSAP address causes the DCC controller to be restarted, thus causing momentary loss of communication with the system via that circuit pack.

Additional information   For information on how to change the configurable fields of the network element's NSAP address, please refer to "Configuring the basic DCN parameters for an NE" (3-31).

Data communication channels

....

Exchange of network management information

Network management information can be exchanged between SDH network elements via Data Communication Channels (DCCs) using the D1-D12 Section Overhead (SOH) bytes of the first STM-1 frame within an STM transmission signal.

This makes it possible to set up a Data Communication Network (DCN; cf. "Basic DCN principles" (14-2)) which uses SDH connections for exchanging network management data.

Please note that all nodes in an area must have DCC connectivity *within the area* to all other nodes in the same area (cf. "DCN configuration guidelines" (14-10)).

The DCC uses OSI protocols. IP traffic is carried on the DCC by encapsulating it in CLNP PDUs.

DCC-R (Section DCC)

The Regenerator Section Data Communication Channel (DCC-R or Section DCC) makes use of the RSOH bytes D1-D3 thus providing a transmission channel with a capacity of 192 kbit/s. The DCC-R is automatically set as the default DCC for provisioned (configured) or pre-provisioned optical interface ports.

DCC-M (Line DCC)

The Multiplex Section Data Communication Channel (DCC-M or Line DCC) uses the MSOH bytes D4-D12 thus providing a transmission channel with a capacity of 576 kbit/s.

Supported data communication channels

The Data Communication Channels are supported for the following optical interfaces:

- STM-1
- STM-4
- STM-16
- STM-64

Termination of Data Communication Channels

The *WaveStar*® TDM 10G (STM-64) system supports the 7-layer OSI protocol stack over the DCC links which terminate on the DCC controller (ADJCTL/DCC32EI). The ADJCTL/DCC32EI circuit pack provides the source and sink of the DCC bytes to and from the active DCC links via LAPD devices. The LAPD protocol acc. to ITU-T Rec. Q.921 is used. You can define DCC links by assigning DCC terminations to optical interface ports.

....

The following figure illustrates the functional principle.
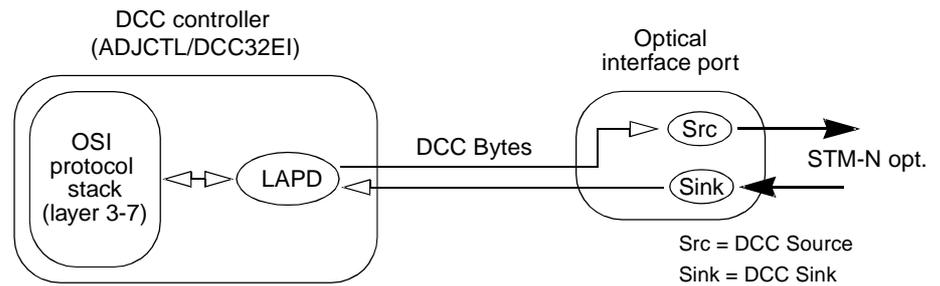
DCC controller
(ADJCTL/DCC32EI)

Optical
interface port

OSI
protocol
stack
(layer 3-7)

LAPD

DCC Bytes

Src

Sink

STM-N opt.

Src = DCC Source
Sink = DCC Sink

Max. number of active DCC links

The maximum number of simultaneously supported LAPD channels per DCC controller is 32. Each DCC controller thus can support up to 32 active DCC links. Upon circuit pack insertion, DCCs will automatically be enabled and a LAPD channel assigned as long as LAPD channels are available.

DCC provisioned state

A Data Communication Channel (either DCC-R or DCC-M) can be in one of the following provisioned states:

- *Enabled*

  - The corresponding DCC bytes are allocated to an optical interface port.

  - The DCC is assigned a LAPD channel.

- *Disabled*

  - The corresponding DCC bytes are no longer allocated to an optical interface port.

  - The DCC is no longer accessed by a LAPD channel.

  The provisioned state of a DCC as well as the LAPD channel assignments are persistent over a DCC controller or NE reset.

No DCC protection switching!

The *WaveStar* TDM 10G (STM-64) system does not support DCC protection switching. However, the system allows for protection switching of the DCC overhead bytes with the optical interfaces on which they reside. If no protection of the optical interface is provisioned, then the DCC bytes are unprotected as well.

Mandatory DCC access for MS-SPRing

When an MS-SPRing protection group is created and the MS-SPRing management mode is "automatic discovery", then two DCCs must be *enabled* (one for the east and one for the west port), and each of the DCCs must be assigned a LAPD channel; otherwise the creation of the MS-SPRing protection group will fail due to insufficient resources (LAPD channels).

Important! The following has to be observed:

1. Data Communication Channels used for MS-SPRing management cannot be disabled as long as the MS-SPRing protection group exists and the MS-SPRing management mode is "automatic discovery".

2. If the neighboring node in an SDH MS-SPRing is an ADM-16/1, then you must enable the DCC-M on the side connected to the ADM-16/1.

Enabling of DCCs   A Data Communication Channel can be enabled in either of the following ways, always provided that the required number of LAPD channels is available:

*   Automatically upon circuit pack initialization
    When a port unit is initialized (e.g. after circuit pack insertion) the DCC-R will be enabled for each port provided that the required number of LAPD channels is available.

*   Automatically upon creation of a protection group

*   Manually by user provisioning
    Please refer to "Configuring data communication channels" (3-39).

A DCC will be successfully enabled if an LAPD channel exists that

*   can be assigned to this DCC in the unprotected mode, or

*   can be shared with this DCC in a protected mode.
    A DCC channel with its own LAPD channel when in the unprotected mode, can share its LAPD channel when in the 1+1, 1:1 or 1:N protection mode.

DCC pre-provisioning   A DCC can be pre-provisioned to be enabled for a provisioned or pre-provisioned optical interface port even if the DCC controller or port is not physically equipped.

Disabling of DCCs   A Data Communication Channel can be disabled in either of the following ways:

*   Automatically when an optical interface port is de-provisioned.
    When an optical interface port is provisioned to be removed (de-provisioned), then all enabled DCCs will be disabled, and the corresponding LAPD channels will be released.

*   Manually by user provisioning.
    Please refer to "Configuring data communication channels" (3-39).

....

Important! Disabling a previously enabled DCC at a local NE needs to be coordinated with disabling the same DCC at the opposite end of the DCC link (remote NE) to avoid persistent communication alarms from the remote NE.

LAPD mode

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

- *Network Side*
  The LAPD is assigned as Network. This mode complies with the standards and interoperates successfully with other LAPDs operating in user_side mode.

- *User Side*
  The LAPD is assigned as User. This mode complies with the standards and interoperates successfully with other LAPDs operating in network_side mode.

Please note that the DCCs work according to the master/slave principle, i.e. the LAPD modes of two interconnected SDH ports must be set differently. A corresponding "User-Network Side Failure" alarm will be generated if the LAPD mode is the same at both ends of a DCC.

AITS and UITS supported

WaveStar TDM 10G (STM-64) network elements support the Acknowledged Information Transfer Service (AITS) and the Unacknowldeged Information Transfer Service (UITS) as the basis for the LAPD protocol with the AITS mode being the default mode of operation.

AITS and UITS functional principles

In the LAPD protocol, all PDUs are sent with a checksum to verify that the data has not been corrupted during the transmission over the DCC link. If a PDU is received with a bad checksum, it is not acknowledged and will be resent:

- In the *Unacknowldeged Information Transfer Service* (UITS), corrupted PDUs are ignored and no further actions taken. Upper layers of the OSI stack are responsible for recovery actions.

- In the *Acknowldeged Information Transfer Service* (AITS), PDUs are numbered and transmitted sequentially, and acknowledgement PDUs are sent back from the receiver to the sender. If a PDU is lost, that is, if the sender gets no acknowledgement, the PDU is retransmitted.

....

365-371-522
Issue b, October 2001

Lucent Technologies

1 4 - 2 3

**Functional principle of the
AITS**
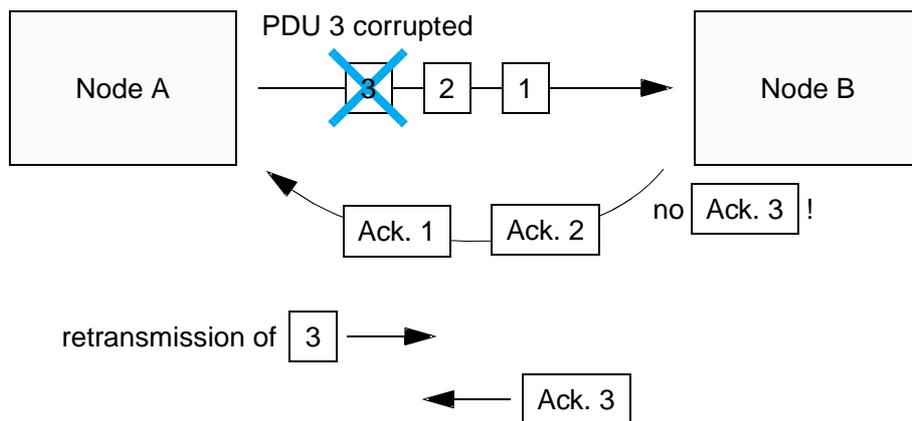
Routing metric   The shortest-path-first (SPF) algorithm calculates the preferred route between two nodes based on the cost of a route. The cost of a route is described by a single dimensionless routing metric.

The *WaveStar* TDM 10G (STM-64) system makes use of the default routing metric as defined in ISO 10589.

LAN access

Internal LAN   Individual parts of a *WaveStar*® TDM 10G (STM-64) network element are interconnected via an internal LAN, the so-called Operations Network (ON), for the purpose of exchanging management information.

External LAN access   Both the low-speed part and the high-speed part of the main shelf facilitate the access to an external LAN, the so-called Intraoffice LAN (IAO-LAN), by means of three 10-BaseT Ethernet interfaces on 4-wire RJ-45 connectors.

The following figure illustrates the *WaveStar* TDM 10G (STM-64) LAN connections.
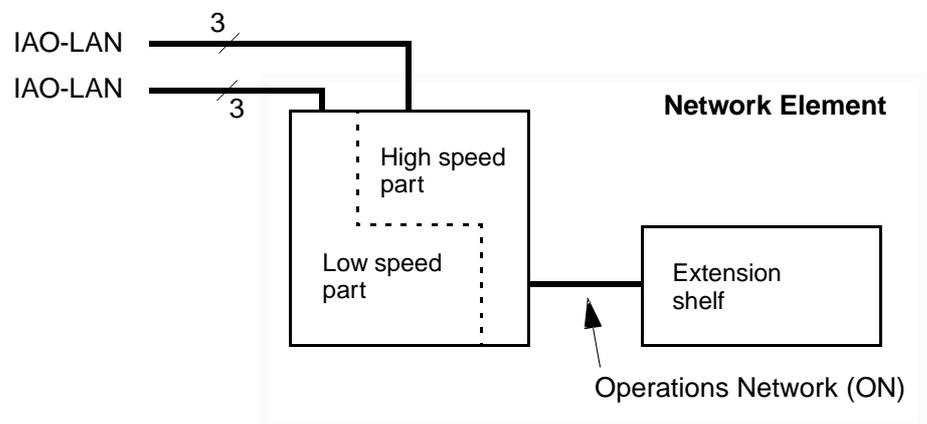
Intraoffice LAN   The Intraoffice LAN (IAO LAN) is an IEEE 802.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detection) type LAN at a data rate of 10 Mbit/s and a baseband signalling type. It is used to connect other NEs in the same office which do not have optical connectivity to the *WaveStar* TDM 10G (STM-64) network, or to connect management systems.

LAN connectors   The RJ-45 LAN connectors are located on the User Panel (connector labelled "CIT"; this is the LAN 1 interface of the low speed part of the main shelf) and on the LAN I/O-Panel at the rear.

The following figure illustrates the LAN I/O-panel.

(1-1) DCC **(1-2) DCC**

LAN 2 **LAN 3** **LAN 1** **LAN 2** **LAN 3**

Low speed part... High speed part... ... of the main shelf
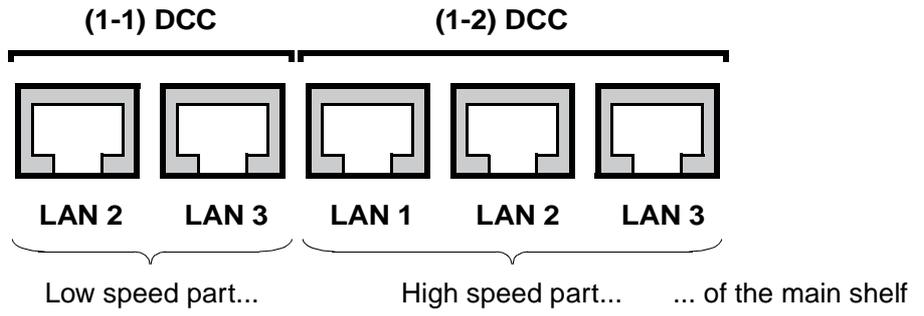
Name-to-address translation

Overview The communication between *WaveStar*® TDM 10G (STM-64) network elements and their management systems, such as the *WaveStar* CIT, is established by using TL1 command messages.

A TL1 message addresses a network element by its "name", also referred to as its target identifier (TID), whereas nodes within an OSI network are identified by their NSAP address. Hence a name-to-address translation becomes necessary.

Naming conventions "NE name" and "TID" are used synonymously throughout this User Operations Guide.

TID to NSAP-address translation *WaveStar* TDM 10G (STM-64) offers two possible ways to accomplish the TID to NSAP-address translation:

1. A static routing table; please refer to "Static routing" (14-27) (starting below).

2. The TID Address Resolution Protocol (TARP); please refer to "TARP" (14-28).

To establish a management association to a remote NE, the *WaveStar* CIT first evaluates the static routing table. If the corresponding name/address pair cannot be found in the table, the TARP will automatically be used.

Static routing The complete area address part of the NE's NSAP address is configurable (cf. "NSAP address format" (14-16)). Therefore, the *WaveStar* CIT allows static routing, i.e. the TID-to-NSAP-address translation is realized by using a static routing table (Name/Address List) stored in the *WaveStar* CIT.

Static routing table The static routing table

*   must be constructed and maintained manually by a system administrator and

*   must be synchronized in ***all*** *WaveStar* CITs managing the network elements.

Important! Each DCC controller exchange needs to be reflected in the static routing tables of all *WaveStar* CITs managing the NEs. The IEEE 802.3 MAC address, stored on the DCC controller (ADJCTL/DCCEI) circuit pack during the manufacturing process, is used as the system identifier in the NE's NSAP address (cf. "NSAP address fields" (14-17)). Hence, when a new DCC controller is inserted, then the system identifier, and so the NSAP address,

automatically changes. After a DCC controller exchange, the static routing tables in all *WaveStar* CITs managing the NEs need to be adapted; please refer to "Administering the address list at the *WaveStar* CIT" (3-19).

TARP

The TID Address Resolution Protocol (TARP) acc. to Telcordia Technologies (formerly Bellcore) GR-253 standard provides a means to perform the TID to NSAP address translation dynamically by means of TARP Protocol Data Units (TARP PDUs), originating from an end system such as the *WaveStar* CIT.

Three basic TARP functionalities can be distinguished:

- TARP originator functionality
- TARP propagation functionality
- TARP responder functionality

TARP originator functionality

The TARP originator functionality means the ability to spontaneously originate a TARP PDU type 1, 2 or 5 query (cf. "Types of TARP PDUs" (14-28)) and broadcast it over the OSI network.

TARP propagation functionality

The TARP propagation functionality means the ability to evaluate a received TARP PDU type 1, 2 or 5 query and to further broadcast it over the OSI network if the requested TID or NSAP address does not match the NE's TID or NSAP address, and if the requested TID or NSAP address could not be found in the TARP Data Cache (TDC; cf. "TARP data cache" (14-30)).

A TARP propagator decrements the lifetime of a received TARP PDU by one and broadcasts the modified PDU to all of its network neighbors (with the exeption of the previous PDU sender). When the TARP PDU lifetime becomes zero, then no further propagation takes place.

TARP responder functionality.

The TARP responder functionality means the ability to respond to a TARP PDU type 1, 2 or 5 query via a type 3 response (cf. "Types of TARP PDUs" (14-28)).

Types of TARP PDUs

The following table shows the five defined types of TARP PDUs.

Type	Characteristic	Description
1	Query	Given an NE name (TID), the corresponding NSAP address is requested (restricted to IS-IS level-1 area).

Type	Characteristic	Description
2	Query	Given an NE name (TID), the corresponding NSAP address is requested (IS-IS level-1 and 2 areas).
3	Response	Response to a TARP Query.
4	Autonomous notification	Autonomous notification of a TID or NSAP address change, or a reset indication.
5	Query	Given an NSAP address, the corresponding NE name (TID) is requested.

Supported TARP functionality

The *WaveStar* CIT supports the TARP originator functionality which is permanently enabled. *WaveStar* TDM 10G (STM-64) network elements support the TARP propagation and TARP responder functionalities. These functionalities can be either enabled or disabled.

TARP example

The following figure shows an example to illustrate the TARP functional principle.
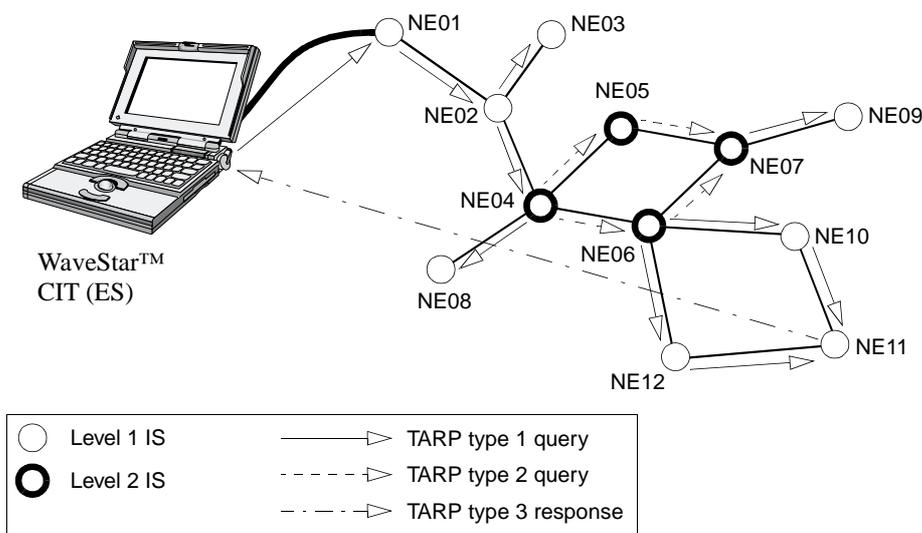
When a user requests to establish a management association to NE11 and the corresponding NSAP address cannot be found in the static routing table, then the *WaveStar* CIT originates a TARP type 1 query. This query will be propagated over the network until it reaches NE11. NE11 then sends a TARP-type-3 response directly back to the *WaveStar* CIT.

Please note that the TARP Data Cache (TDC; cf. "TARP data cache" (14-30)) was not taken into consideration for this example.

Network services/protocols

TARP depends on the network layer services and protocols provided by the Connectionless Network Service/Connectionless Network Protocol (CLNS/CLNP) and the ES-IS and IS-IS routing protocols (cf. "ISO-OSI network protocols" (14-4)) to obtain information about the network neighbors of an NE.

TARP data cache

A local database, the TARP Data Cache (TDC), is used in each NE to store information on the NE's adjacencies, i.e. its direct neighbors in the network. Hence an NE may be able to respond to a TARP query, even if the requested TID or NSAP address does not match the NE's own TID or NSAP address. Thus, the network performance can be enhanced.

TARP manual adjacencies

By using TARP manual adjacencies it is possible to route TARP PDUs over subnetworks which do not support the TARP functionality. However, a precondition is that the nodes within the non-TARP subnetwork are "generic routers". A TARP manual adjacency is simply the Network Entity Title (NET; cf. "Network entity title" (14-18)) of a node that supports TARP.
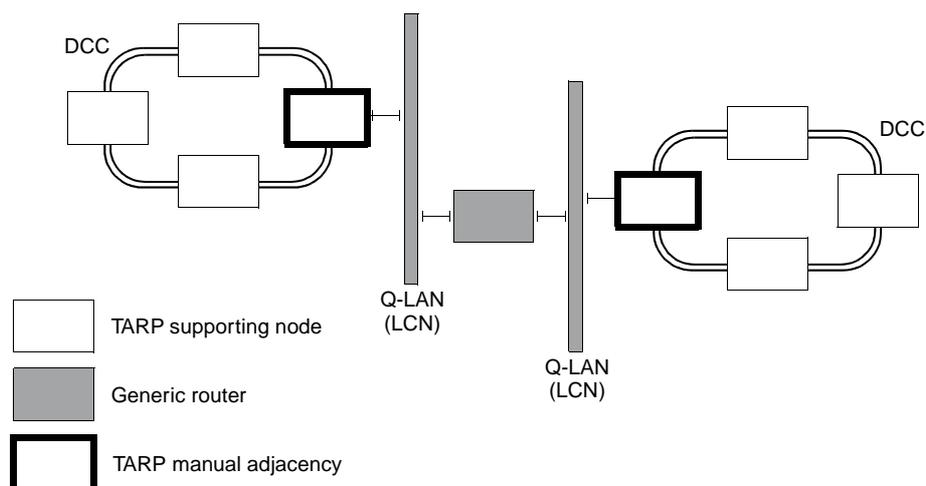
Loop detection

WaveStar TDM 10G (STM-64) nodes provide a loop detection mechanism to prevent a repeated processing of previously processed TARP PDUs. A loop detection buffer (LDB) in conjunction with an LDB entry timer and an LDB flush timer is used for this purpose. A previously processed and again received TARP PDU is discarded.

Configuration of TARP parameters

For information on the configuration of TARP parameters, please refer to the following procedures:

- "Configuring the TARP parameters for an NE" (3-47),
- "Assigning TARP manual adjacencies" (3-52),
- "Configuring the LDB timers for the *WaveStar* CIT" (3-16).

⌐

NE name administration

Definition **NE Name (TID)** The NE name, also referred to as the NE's target identifier (TID), is an alphanumeric string of up to 20 characters, used to uniquely identify a network element within the network. "NE name" and "TID" are used synonymously throughout this User Operations Guide.

Configuration rules The following NE name configuration rules must be observed:

- Each NE name must be unique within the network.
- The following characters are allowed in an NE name:
    - Upper-case letters ("A" .. "Z"),
    - Lower-case letters ("a" .. "z"),
    - Special characters("-", "+", "_", ".", "/"),
    - Digits ("0" .. "9").
- An NE name must must not end and begin with an special character.
- Each NE name must be maximally 20 characters in length.
- The NE name may contain segments separated by hyphens ("-") or slashes ("/"), but each segment must begin with a letter.

Please note that NE names are case insensitive.

Examples:

The following are examples for valid and invalid NE names.

- "NE-A1", "CHICAGO7" or "NY-B3/C5" are valid NE names.
- "NE-01", "CHICAGO-7" or "NY-3/5" are invalid NE names.

Changing the NE name For information on how to change the NE name, please refer to "Changing the NE name (TID)" (3-2).

System provisioning

....

Overview   System provisioning allows you to configure parameters associated with the entire system.

Parameters   The following parameters can be set:

- ***Date***
  Selection of year, month and day.

- ***Time***
  The time can be displayed in a format specific to the country in which the *WaveStar*® CIT is being used.

⌐

....
System provisioning

365-371-522   **Lucent Technologies**   1 4 - 3 3
Issue b, October 2001

15 Equipment provisioning concepts

Overview

Purpose   This chapter gives you an overview of the hardware components of the *WaveStar*® TDM 10G (STM-64) network elements which have to be configured.

Contents

⌐|

Equipment provisioning and autoprovisioning

What does equipment provisioning mean?

Equipment provisioning is the pre-configuration of network element components before protection groups and cross-connections can be defined.

Provisioning can take place for the first time after the installation of the equipment (initial provisioning) or when re-configuration of the *WaveStar*® TDM 10G (STM-64) in an existing SDH network is necessary.

The following components have to be provisioned initially:

- System (optional)
- Shelves
- Slots/circuit packs
- Optical and electrical ports
- Tributaries

Equipment provisioning can be carried out with the *WaveStar* CIT. The configuration data is placed in the NE and stored in a non-volatile memory (NVM) on the PCMCIA card.

Autoprovisioning

Some of the components are autoprovisioned. This means some system parameters are assigned automatically after installation and system start. These are:

- Bay 1
- The low-speed shelf
- System control circuit packs
- Synchronization circuit packs
- Switch circuit packs
- Synchronization default mode (free running)
- Synchronization equipment protection (if two timing circuit packs are available)
- DCC default modes: LAPD role is User-Side for all ports, DCC_R (Section DCC) is enabled, DCC_M (Line DCC) is disabled
- All mandatory circuit packs in a shelf and all circuit packs which are already plugged-in during system start.

A modification of the autoprovisioned parameters is possible.

WaveStar® CIT methods to perform provisioning

Overview The *WaveStar* CIT supports two different methods, graphical and windows-style explorer, to perform provisioning tasks. You may choose to use only one of the methods or a combination of the two. Generally, you can switch from one method to the other at any time.

Graphical The following steps demonstrate the graphical method.

1 From the *WaveStar* CIT System View window, either:

- Double-click on the desired shelf, or

- Right-click on the desired shelf (for example, Shelf 1 and Bay 1). In the displayed menu, select (highlight and left-click) **View Shelf #.**
  A graphic drawing of the selected shelf is displayed. Note that each port unit has a light-emitting diode (LED) associated with each port. Each LED displays the alarm status of the associated port. "*WaveStar* CIT visual alarm indicators" (16-7) and "Alarm severities" (16-26)

2 Place the cursor anywhere on a circuit pack and right-click to select the circuit pack.

3 Place the cursor on a port-unit LED and right-click to select a port on the circuit pack.

4 Select **Provision Circuit Pack** or **Provision Port #** in the pop-up menu to provision the selected circuit pack or port.

All provisionable parameters for the selected circuit pack or port are displayed in the pop-up dialogue box. You can select each parameter and display or change the parameter for a specific application.

E N D   O F   S T E P S

Windows-style explorer   The following steps demonstrate the windows-style method:

....

1   Select **Configuration** → **Provision** in the *WaveStar* CIT System View
window.

>   **Result:**

>   A Windows-style explorer window opens.

....

2   Do one of the following:

- Enter the AID (for example, 1-1-#-#-1-1) of the desired
  component in the **Enter AID:** field, or

- In the left side of the window, click the "+" symbol left to the
  desired bay to expand bay information.

  1.   Select the desired shelf in the bay to expand shelf
       information.

  2.   Select the desired circuit pack or slot location.

  3.   Select the desired port.

....

3   Select the **Provision** button at the bottom of the window.

The provisionable parameters of the selected port are displayed in the
right portion of the window. You can select each parameter and
display or change the parameter for a specific application.

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

Provisioning of new components

Overview   You can add new components to an existing system. This can be necessary during reconfiguration or after installation. The following components can be added:

- Bays (additionally to Bay 1; Bay 1 is autoprovisioned)
- Shelves
- Circuit packs
- Protection groups

Invocation   Select in the main menu **Configuration** → **Create New**. In the pop-up menu you can select the desired component.

Parameters   Already while creating a component you can define some parameters of the respective component:

- Bay
  A new Bay with a selectable *AID* (*1*...*99*) can be created.

- Shelf
  A new Shelf (Extension shelf) can be created. The following parameters can be provisioned:

  - *Shelf AID*: *1-3*

  - *ON Cable Identifier*: *1*...*4*
    The ON Cable Identifier is the controller address of a shelf for the connection to the low-speed shelf which contains the main controller for the whole network element. For the high-speed shelf it is always *1*. For the extension shelf it should be *2*.

  - shelf type (2.5or 10G)

  - ASAP (only default)

- Circuit Pack
  New circuit packs can be established. The circuit pack types can be selected. In the following chapter "Main shelf configuration" (15-9) and "Extension shelf configuration" (15-15), the slot distribution for the main shelves and the extension shelf is described. In the selection window for new circuit packs only the circuit packs, which are suitable for the respective slot can be selected.

- Protection Group

All entities which are necessary for the creation of a new protection group can be selected. They can be part of the following protection types:

- 1+1 MSP

- 2-Fiber MS-SPRing

For further information on the protections please refer to "Protection mechanisms" (18-10).

⌐

Exchangeability of circuit packs

....

Overview   You can physically exchange the line and tributary circuit packs with different application codes (LEY), if they are functionally compatible, as far as the feature sets are concerned (transmission rate, FEC-Type).

The provisioned connections will be restored without deprovisioning or reprovisioning of the circuit pack and all its traffic. Thus service interruptions are minimized.

Full exchangeability   Full exchangeability allows exchanging port units with different port attributes (but same line rate and same number of ports).

It includes exchanging direct-optics and non-direct-optics of the same (line) rate.

Exchangeability table   The following table gives an overview over the exchangeable circuit packs. Only the packs of the same Exchangeability Group can be exchanged.

Circuit Pack		Application Code	Exch. Group	Comments
Name	Qualifier			
OC192/STM64	1.5SR1	LEY67	1	40km (SH)=DA!
(10 Gbit/s)	1.5IR1	LEY69	1	60km (SH) 1.5u EIR (with ADP)
	1.5IRS1	LEY97	1	60km (SH) 1.5u IR (with PIN)
	WDM [nnnn]	LEY201-240	1	OLS400G-40 colors
	POU [nnnn]	LEY284-299	1	16×OLS_passive optics
OC48/STM16	1.3LR1	LEY7	2	51km (LH); +LEY307=CR(M)
(2.5 Gbit/s)	1.3SR1	LEY182	2	VSR; 2km (intra-office)
	1.5LR1	LEY8	2	80km (LH); +LEY308=CR(M)
	DWDM [01-16]	LEY50-65	2	OLS40/80G-16 colors
	WDM [nnnn]	LEY101-180	2	OLS400G-80 colors 1.5u
	POU [nnnn]	LEY80-95	2	16× OLS_passive optics
OC12/STM4	1.3SR2	LEY14	3	IR/SR-2 port 15km (SH)
(622 Mbit/s)	1.3LR2	LEY13	3	2 port, 51km (LH)
	1.5LR2	LEY190	3	2 port, 80km (LH)

....

OC3/STM1	1.3SR4	LEY16	4	4 port; 15km (SH)
(155Mbit/s)	1.3LR4	LEY15	4	4 port; 51km (LH)
	1.3SR8	LEY23	8	IR/SR-8 port 15km (SH)
	4	LEY44	5	STM1E (4 ports, electrical)
	4	LEY40	5	STM1EE4 (never E4)
OBA-10G Booster	1.5LR1	SEN3	6	25mm; 80km (LH)
OBPA-10G Booster + Amplifier	1.5VR1	SEN4	9	25mm; 120km (VLH)

SH/LH = Short/long Haul

DA = Discontinued Availability

Main shelf configuration

Overview   This chapter describes the configuration of the main shelf of the
WaveStar® TDM 10G (STM-64).

Layout (front view)   The following figure depicts the *WaveStar* TDM 10G (STM-64) Main Shelf plug-in units and circuit pack slots (front view), including the 16 slots used for STM-1(o), STM-1(e), STM-4 or STM-16 tributary port units. The minimum required circuit packs are highlighted. The circuit pack designations used here also appear in the drop-down list box of the creation window for new circuit packs.

High-Speed Part

Low-Speed Part

(1-2) fan1

SWITCH/STS576 (M0)	CTL/SYS50DM (M0)	ADJCTL/DCC32EI (M0)	reserved	TMG/STRAT3 (M1) (1-1) tmg1	SWITCH/STS576 (M1)	OBA/OBPA (West)	OBA/OBPA (East)	PPROC/STS192(West)	SWITCH/STS576 (0)	PPROC/STS192(DM0)	ADJCTL/DCC32EI (0)	CTL/SYS50DM (0)	reserved	TMG/STRAT3 (1) (1-2) tmg1	PPROC/STS192(DM1)	SWITCH/STS576 (1)	PPROC/STS192(East)

(1-1) switch0 · (1-1) ctlmem0 · (1-1) dccei · (1-1) ctlmem1 · TMG/STRAT3 (M0) (1-1) tmg0 · (1-1) switch1 · (1-2) oaw · (1-2) oae · (1-2) pprocw · (1-2) switch0 · (1-2) ppls0 · (1-2) dccei · (1-2) ctlmem0 · (1-2) ctlmem1 · TMG/STRAT3 (0) (1-2) tmg0 · (1-2) ppls1 · (1-2) switch1 · (1-2) pproce

LEY4 LEY10B LEY1   LLY2 LEY4 SEN3/SEN4 SEN3/SEN4 LEY3 LEY4 LEY3 LEY1/LEY301 LEY10B   LLY2 LEY3 LEY4 LEY3

User Panel

STM-64
STM-16, GE1/SX
STM-4
STM-1o
STM-1e

Port Unit slots: (1-1) 01 · 02 · 03 · 04 · 05 · 06 · 07 · 08 — Port Unit (Protection) (1-1) eprn · EPS-64 (1-1) eprotnsw — (1-1) 09 · 10 · 11 · 12 · 13 · 14 · 15 · 16

(West) (1-2) trw   (East) (1-2) tre

LEY44   LEY42

(1-1) fan1

Explanation of the switching and PPROC circuit pack designation extensions:

(DM0): Delay Management, main
(DM1): Delay Management, protection
(0): Second stage switch (high speed part), main
(1): Second stage switch (high speed part), protection
(M0): First stage switch (low speed part), main
(M1): First stage switch (low speed part), protection

The following table lists all possible tributary port units.

Port unit with	Apparatus Code	Description
STM-64	LEY67	OC192/STM64/1.5SR1
	LEY69	OC192/STM64/1.5IR1
	LEY97	OC192/STM64/1.5IRS1
	LEY201–240	OC192/STM64/WDM9580–9190
	LEY284–299	OC192/STM64/POU9590–9210
STM-16	LEY7	OC48/STM16/1.3LR1
	LEY307	OC48/STM16/1.3LR1
	LEY8	OC48/STM16/1.5LR1
	LEY308	OC48/STM16/1.5LR1
	LEY50–65	OC48/STM16/DWDM01–16
	LEY101–180	OC48/STM16/WDM9585–9190
	LEY182	OC48/STM16/1.3SR1
GE1/SX	LEY309	1 Gigabit Ethernet
STM-4	LEY13	OC12/STM4/1.3LR2
	LEY14	OC12/STM4/1.3SR2
	LEY190	OC12/STM4/1.5LR2
STM-1o	LEY15	OC3/STM1/1.3LR4
	LEY16	OC3/STM1/1.3SR4
	LEY23	OC3/STM1/1.3SR8
STM-1e	LEY40	STM1EE4/4

Designation and equipage of slot

The following table shows the relation between slot designations and required circuit packs used in the Main Shelf of the *WaveStar* TDM 10G (STM-64). The slots designations in the low-speed part of the shelf begin with the string "(1-1)", the high-speed part of the shelf is referred to as "(1-2)".

Slot designation	Slot equipage
(1-1) 01 to (1-1) 16 STM1e: LEY40 STM1o: LEY16, 23 STM4: LEY13, 14, 190 STM16: LEY7, 8, 101-180, 182, 307, 308 GE1/SX: LEY309	Any mix of transmission interface circuit packs (optical and electrical): • STM-1(e) port units (STM1E/4, STM1EE4/4) • STM-1(o) port units (STM1) • STM-4 port units (STM4) • STM-16 port units (STM16), incl. 16 colours DWDM interfaces. • 1 Gigabit Ethernet interface (GE1/SX). Each of the STM-16 port units as well as the 1 Gigabit Ethernet circuit pack GE1/SX (LEY 309) requires two slots. Allowed slots are: 02, 04, 06, 08, 10, 12, 14, 16. If the slot (1-1)16 is configured for an optical port unit (STM-1(o), STM-4 or STM-16), no 1:N equipment protection of the STM-1(e) port units is possible. If 1:N equipment protection of the STM-1(e) port units is configured, slot (1-1)16 must be left empty.
(1-2) trw **(1–2) tre** LEY67, 69, 97, 201-240, 284-299	STM-64 port units (STM64), incl. 56 colours DWDM interfaces. Depending on the distance, different STM-64 port units are required (see table above).
(1-1) eprn LEY44	Electrical protection. Equipped with an STM1E/4 circuit pack to protect STM1E/4 port units. This slot can also be left empty if no protection is required.
(1-1) eprotnsw LEY42	Electrical protection switch. Equipped with an EPS-64 protection switching circuit pack to provide the 1:N switching function for protected STM1E/4 port units. This slot can also be left empty, if no protection is required.
(1–1) switch0 LEY4	Fabric switch 0. The SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. This switch is paired with fabric (1-1) switch 1 in a 1+1 non-revertive protection mode configuration.
(1-1) ctlmem0 LEY10B	Controller for the system including non-volatile memory. The CTL/SYS50DM circuit pack in this slot is the working controller for the low speed part of the shelf and additionally the system controller for the whole shelf.
(1-1) dccei LEY1	Adjunct controller, DCC and external interface. The ADJCTL/DCC32EI circuit pack in this slot terminates up to 32 data communications channels and interfaces them to the shelf 10Base-T LAN.
(1-1) ctlmem1	The slot is left empty for the current release of *WaveStar* TDM 10G.
(1-1) switch1 LEY4	Fabric switch 1. The SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. This switch is paired with fabric (1-1) switch 0 in a 1+1 non-revertive protection mode configuration.

Slot designation	Slot equipage
(1-1) tmg1 *(1-1) tmg0* LLY2	Two half-height Stratum 3 timing generator circuit packs are located one above the other in this slot. They are the master TMGs in the shelf (and also for the Expansion Shelf). When *WaveStar* TDM 10G is initially powered on after shipment from the factory, the lower TMG/STRAT3 is the active circuit pack and the upper TMG/STRAT3 is the standby circuit pack. However, both circuit packs are of equal level and protection switching is non-revertive, so there is no default configuration.
(1-2) oaw *(1-2) oae* SEN3 or SEN4	OBAs or OBPAs (depending on the optical distance, see table above).
(1-2) pprocw LEY3	The PPROC/STS192 circuit pack in this slot supports the STM64 port unit function assigned to the western aggregate port. The CP is responsible for pointer processing and synchronisation to the system clock and for POH monitoring.
(1-2) switch0 LEY4 LEY73	Fabric switch 0. A SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. A SWITCH/STS768 circuit pack (LEY73) in this slot can make cross-connections for 384 STM-1 equivalent circuits. This switch is paired with fabric (1-2) switch 1 in a 1+1 non-revertive protection mode configuration.
(1-2) ppls0 LEY3	The PPROC/STS192 or PPROC/STS384 circuit pack in this slot provides frame delay management between the switch functions of the low speed part of the shelf and the high speed part ((1-1) sw. 0).
(1-2) ctlmem0 LEY10B	The CTL/SYS50DM circuit pack in this slot is the working shelf controller for the high speed part. The system controller for the whole shelf is located in slot (1-1) ctlmem0.
(1-2) dccei LEY1	Adjunct controller, DCC and external interface. The ADJCTL/DCC32EI circuit pack in this slot terminates up to 32 data communications channels and interfaces them to the shelf 10Base-T LAN. If Orderwire support is required, use LEY301 instead.
(1-2) ctlmem1	The slot is left empty for the current release of *WaveStar* TDM 10G.
(1-2) switch1 LEY4 LEY73	Fabric switch 1. A SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. A SWITCH/STS768 (LEY73) circuit pack in this slot can make cross-connections for 384 STM-1 equivalent circuits. This switch is paired with fabric (1-2) switch 0 in a 1+1 non-revertive protection mode configuration.

Slot designation	Slot equipage
(1-2) tmg1 *(1-2) tmg0* LLY2	Two half-height Stratum 3 timing generator circuit packs are located one above the other in this slot. They are slave TMGs. Their function is to distribute the system clock from the active master TMG to the circuit packs in the high speed part of the shelf or to the Expansion Shelf. When *WaveStar* TDM 10G is initially powered on after shipment from the factory, the lower TMG/STRAT3 is the active circuit pack and the upper TMG/STRAT3 is the standby circuit pack. However, both circuit packs are of equal level and protection switching is non-revertive, so there is no default configuration.
(1-2) ppls1 LEY3 LEY47	The PPROC/STS192 (LEY3) or PPROC/STS384 (LEY47) circuit pack in this slot provides frame delay management between the switch functions of the low speed part of the shelf and the high speed part ((1-2) sw. 1).
(1-2) pproce LEY3	The PPROC/STS192 circuit pack in this slot supports the STM64 port unit function assigned to the eastern aggregate port. The CP is responsible for pointer processing and synchronisation to the system clock and for POH monitoring.

Extension shelf configuration

Layout (front view) The following figure depicts the *WaveStar*® TDM 10G (STM-64) Extension Shelf plug-in units and circuit pack slots (front view), including the 16 slots used for STM-1(o), STM-1(e), STM-4 or STM-16 tributary port units. The circuit packs required for a minimum configuration are highlighted.
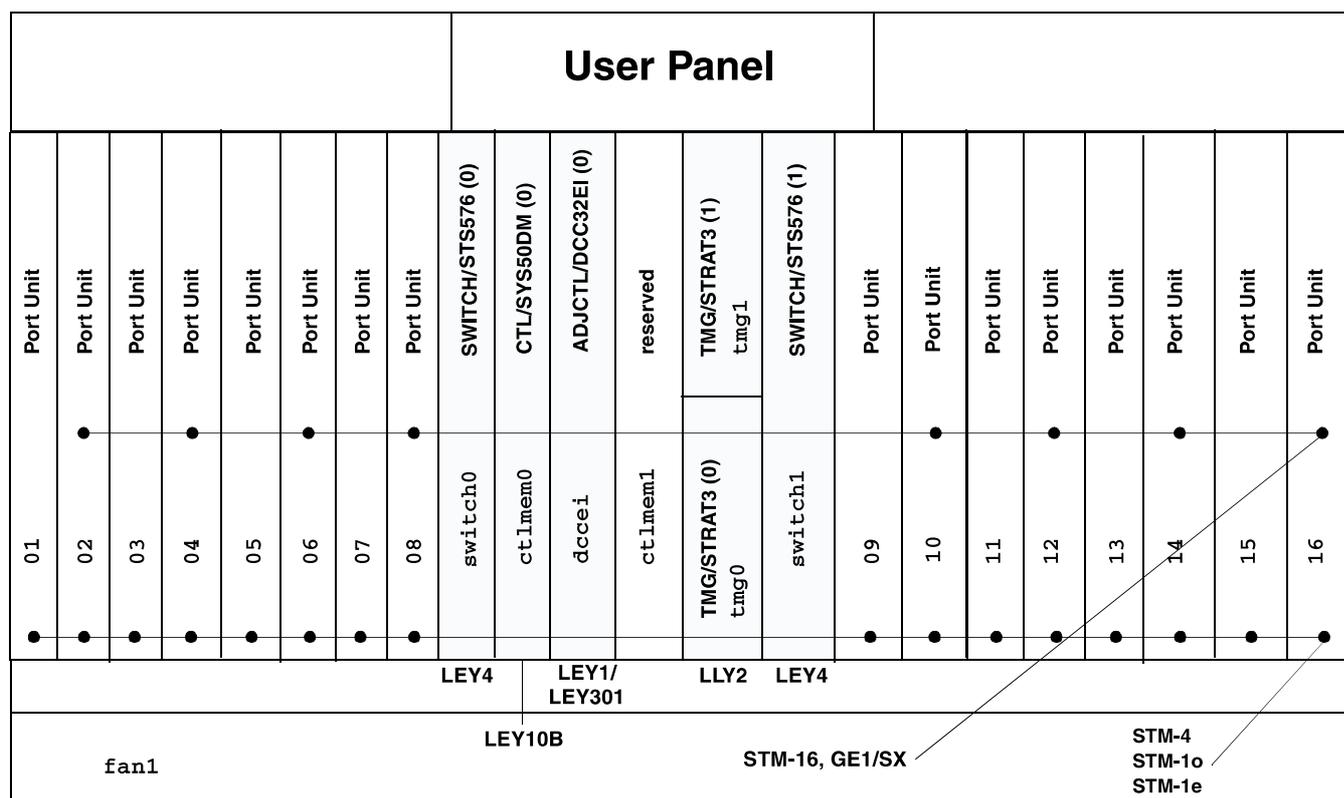
The following table lists all possible tributary port units.

Port unit with	Apparatus Code	Description
STM-16	LEY7	OC48/STM16/1.3LR1
	LEY307	OC48/STM16/1.3LR1
	LEY8	OC48/STM16/1.5LR1
	LEY308	OC48/STM16/1.5LR1
	LEY50–65	OC48/STM16/DWDM01–16
	LEY101–180	OC48/STM16/WDM9585–9190
	LEY182	OC48/STM16/1.3SR1
GE1/SX	LEY309	1 Gigabit Ethernet

Port unit with	Apparatus Code	Description
STM-4	LEY13	OC12/STM4/1.3LR2
	LEY14	OC12/STM4/1.3SR2
	LEY190	OC12/STM4/1.5LR2
STM-1o	LEY15	OC3/STM1/1.3LR4
	LEY16	OC3/STM1/1.3SR4
	LEY23	OC3/STM1/1.3SR8
STM-1e	LEY40	STM1EE4/4

Circuit pack slot equipment The following table identifies the circuit packs used in the *WaveStar* TDM 10G. Refer to the port unit descriptions in the *WaveStar* TDM 10G (STM-64) Application, Planning and Ordering Guide for additional information about the transmission interface circuit packs.

Slot designation	Slot equipage
01 to 16 STM1e: LEY40 STM1o: LEY16 STM4: LEY13, 14, 190 STM16: LEY7, 8, 101–180, 182, 307, 308	Any mix of transmission interface circuit packs: • STM-1(e) port units (STM1EE4/4) • STM-1(o) port units (STM1) • STM-4 port units (STM4) • STM-16 port units (STM16). Each of the STM-16 port units as well as the 1 Gigabit Ethernet circuit pack GE1/SX (LEY309) requires two slots. Allowed slots are: 02, 04, 06, 08, 10, 12, 14, 16.
switch0 LEY4	Fabric switch 0. A SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. This switch is paired with fabric switch 1 in a 1+1 non-revertive protection mode configuration.
ctlmem0 LEY10B	The CTL/SYS50DM circuit pack in this slot is the working controller for the shelf. It can be used for CIT and EMS connections. Furthermore it collects all alarms and signals them on the User Panel and the office alarm interface.
dccei LEY1	Adjunct controller, DCC and external interface. The ADJCTL/DCC32EI circuit pack in this slot terminates up to 32 data communications channels and interfaces them to the shelf 10Base-T LAN. If Orderwire support is required, use LEY301 instead.
ctlmem1	The slot is left empty for the current release of *WaveStar* TDM 10G.

Slot designation	Slot equipage
tmg1, tmg0 LLY2	Two half-height Stratum 3 timing generator circuit packs are located one above the other in this slot. They are slave TMGs. Their function is to distribute the system clock from the active master TMG (Main Shelf) to the circuit packs in the Expansion Shelf. When *WaveStar* TDM 10G is initially powered on after shipment from the factory, the lower TMG/STRAT3 is the active circuit pack and the upper TMG/STRAT3 is the standby circuit pack. However, both circuit packs are of equal level and protection switching is non-revertive, so there is no default configuration.
switch1 LEY4	Fabric switch 1. A SWITCH/STS576 circuit pack in this slot can make cross-connections for 192 STM-1 equivalent circuits. This switch is paired with fabric switch 0 in a 1+1 non-revertive protection mode configuration.

Overview of access identifiers

Overview   Access identifiers (AIDs) are used for addressing particular components within a *WaveStar*® TDM 10G (STM-64) system, like a shelf, circuit pack, slot or port, for example. An AID is case-insensitive, but AID values are usually given in lower case.

Hierarchical structur   AIDs are hierarchically structured. The following table provides an overview of the general AID structure by presenting some examples.

Entity	Format	Example
Net-work element	bay	1
Shelf	bay-shelf	1-1
Protec-tion group	bay-shelf-protection group	1-1-t01
Slot	bay-shelf-#-#-slot	1-1-#-#-01
Circuit pack	bay-shelf-#-#-slot-CP	1-1-#-#-01-cp
Port	bay-shelf-#-#-slot-port	1-1-#-#-01-1
Tribu-tary	bay-shelf-#-#-slot-port-trib	1-1-#-#-01-1-1

The entity network element refers to a logical unit which can be composed of up to three shelves, high-speed shelf, low-speed shelf and optional extension shelf. The extension shelf is physically located in a different rack.

The "#" character serves as a wildcard if a particular AID field cannot be specified, instead of leaving the field empty.

General AID structure   The general AID structure is based on the assumption that there is a hierarchy associated with the system entities in the order of bay, shelf, protection group, line/side, slot, port/circuit pack and tributary. Therefore, the general structure consists of these entities separated by "-":

- ***bay-shelf-protection group-line/side-slot-port/circuit pack-tributary***

Some entities such as the system itself fall out of this hierarchy and are handled separately.

An AID may not exceed 20 characters in length (including "-").

Lucent Technologies

Simple and compound AIDs

Access identifiers can be distinguished into simple and compound AIDs. For example, "system", "extref1", "line1" or "exttmg0_out" are simple AIDs. Compound AIDs follow the general AID structure given in the previous paragraph.

Please refer to "Overview of AIDs" (15-19) for an overview of *WaveStar* TDM 10G (STM-64) AIDs.

The "all" AID entry

Access identifiers allow for the specification of a range of entities by using the term **all**. The **all** AID entry may be used in the bay, shelf, slot, port, and tributary fields. It can neither be used in the protection group field nor in the side/line field.

If **all** is used in the bay and/or shelf AID fields, it cannot be used in any other AID fields.

Overview of AIDs

The following table gives an overview of the access identifiers defined for *WaveStar* TDM 10G (STM-64). If there are several values possible for an entry, they are given in curly braces ({ }).

Entity	Access Identifier
System	
system	system
system switch group	esysswitchgrp
Bay	
Bay with Main Shelf and optionally one Extension Shelf	1
I/O Bay	2
Shelf	
Main Shelf (low-speed part)	1-1
Main Shelf (high-speed part)	1-2
Extension Shelf	{1..2}-{1..3}
Protection Group	
1+1 Facility Protection Group	{1..2}-{1..3}-o{01..99, all}
1:N Facility Protection Group	{1..2}-{1..3}-n{01..99, all}
2-fiber MS-SPRing Facility Protection Group	{1..2}-{1..3}-t{01..99, all}
1+1 Timing Equipment Protection Group	{1..2}-{1..3}-etmggrp
1+1 DCC Equipment Protection Group (DCC and DCCEI)	{1..2}-{1..3}-edccgrp

Entity	Access Identifier
1:N Equipment Protection Group (STM1E/4)	{1..2}-{1..3}-stm1ee4grp
1+1 ctlmem Group	{1..2}-{1..3}-esysctlgrp
Side/Line	
2-fiber MS-SPRing Facility Protection Group East/West Side	{1..2}-{1..3}-t{01..99}-{e,w}
	Note: {e,w} stands for east or west side.

Slot (please refer to "Circuit pack slot equipment " (15-16))

All slots of a specified shelf	{1..2}-{1..3}-#-#-all
Main Shelf - low-speed part port card slot	1-1-#-#-{01..16}
Main Shelf - low-speed part stm1(e) slot	1-1-#-#-{01..16}
Main Shelf - low-speed part OC-3/STM-1 slot	1-1-#-#-{01..16}
Main Shelf - low-speed part OC-12/STM-4 slot	1-1-#-#-{01..16}
Main Shelf - low-speed part OC-48/STM-16 slot	1-1-#-#-{02, 04, 06, 08, ..14, 16}
Main Shelf - low-speed part electrical protection pack slot	1-1-#-#-eprn
Main Shelf - low-speed part electrical protection switch pack slot	1-1-#-#-eprotsw
Main Shelf - low-speed part (576) switch0 slot	1-1-#-#-switch0
Main Shelf - low-speed part ctlmem0 slot (for shelf controller)	1-1-#-#-ctlmem0
Main Shelf - low-speed part dccei slot	1-1-#-#-dccei
Main Shelf - low-speed part ctlmem1 slot (for shelf controller)	1-1-#-#-ctlmem1
Main Shelf - low-speed part tmg0 slot	1-1-#-#-tmg0
Main Shelf - low-speed part tmg1 slot	1-1-#-#-tmg1

Entity	Access Identifier
Main Shelf - low-speed part (576) switch1 slot	1-1-#-#-switch1
Main Shelf - low speed part Gigabit Ethernet slot	1-1-#-#-{02,04,06,08,...14,16}
Main Shelf - high-speed part trw slot	1-2-#-#-trw
Main Shelf - high-speed part tre slot	1-2-#-#-tre
Main Shelf - high-speed part oaw slot	1-2-#-#-oaw
Main Shelf - high-speed part oae slot	1-2-#-#-oae
Main Shelf - high-speed part pprocw slot	1-2-#-#-pprocw
Main Shelf - high-speed part switch 0 slot	1-2-#-#-switch0
Main Shelf - high-speed part pproc 0 slot	1-2-#-#-pproc0
Main Shelf - high-speed part dccei slot	1-2-#-#-dccei
Main Shelf - high-speed part ctlmem 0 slot	1-2-#-#-ctlmem0
Main Shelf - high-speed part ctlmem 1 slot	1-2-#-#-ctlmem1
Main Shelf - high-speed part tmg0 slot	1-2-#-#-tmg0
Main Shelf - high-speed part tmg1 slot	1-2-#-#-tmg1
Main Shelf - high-speed part pproc 1 slot	1-2-#-#-pproc1
Main Shelf - high-speed part switch 1 slot	1-2-#-#-switch1
Main Shelf - high-speed part pproce slot	1-2-#-#-pproce

Entity	Access Identifier
Extension Shelf Port unit slot	{1..2}-{1..3}-#-#-{01-16}
Extension Shelf stm1(e) slot	{1..2}-{1..3}-#-#-{01..06, 11-16}
Extension Shelf OC-3/STM-1 slot	{1..2}-{1..3}-#-#-{01..8}
Extension Shelf OC-48/STM-16 slot	{1..2}-{1..3}-#-#-{02, 04, 06, 08, ..14, 16}
Extension Shelf (576) switch0 slot	{1..2}-{1..3}-#-#-switch0
Extension Shelf ctlmem0 slot (for shelf controller)	{1..2}-{1..3}-#-#-ctlmem0
Extension Shelf dccei slot	{1..2}-{1..3}-#-#-dccei
Extension Shelf ctlmem1 slot (for shelf controller)	{1..2}-{1..3}-#-#-ctlmem1
Extension Shelf tmg0 slot	{1..2}-{1..3}-#-#-tmg0
Extension Shelf tmg1 slot	{1..2}-{1..3}-#-#-tmg1
Extension Shelf (576) switch1 slot	{1..2}-{1..3}-#-#-switch1
Extension Shelf	1-3-#-#-{01-16}
Gigabit Ethernet	{2-4}-{1-3}-#-#-{02,04,06,08,...14,16}
Port	
All the ports on a shelf	{1..2}-{1..3}-#-#-all-all
STM1(e) port	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}
OC-3/STM-1(o) port	{1..2}-{1..3}-#-#-{01..8}-{1..4,all}
OC-12/STM-4 port	{1..2}-{1..3}-#-#-{01..16}-{1..2,all}
OC-48/STM-16 port	{1..2}-{1..3}-#-#-{02, 04, 06, 08, ..14, 16}-{1,all}
OC-192/STM-64 port	{1..2}-{1..3}-#-#-{tre,trw}-{1,all}
Electrical Port (unprotected)	{1..2}-{1..3}-#-#-{01..16}-{1..4, all}
Optical Port (unprotected)	{1..2}-{1..3}-u-#-{01..16}-{1..4, all}

Entity	Access Identifier
1+1 Port	{1..2}-{1..3}-o{01..99}-{w,p}-{01..16}-{1..4,all}
(Port in a 1+1 facility protection group)	{1..2}-{1..3}-o{01..99}-{w,p}-#-#
	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}
	Note: {w,p} stands for working or protection side.
1:N Port	{1..2}-{1..3}-n{01..99}-{1-n,p}-{01..16}-{1..4,all}
(Port in a 1:N facility protection group)	{1..2}-{1..3}-n{01..99}-{1-n,p}-#-#
	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}
	Note: The 'n' in '1-n' is the number of lines in the 1:N protection group. When a port is added to a protection group, it is assigned a line number. 'p' stands for protection.
STM-16 2-fiber MS-SPRing port	{1..2}-{1..3}-t{01..99}-{e,w}-{02, 04, 06, 08, ..14, 16}-{1,all}
(Port in a 2-fiber MS-SPRing facility protection group)	{1..2}-{1..3}-t{01..99}-{e,w}-#-#
	{1..2}-{1..3}-#-#-{02, 04, 06, 08,...14, 16}-{1,all}
	Note: {e,w} stands for east or west side.
STM-64 2-fiber MS-SPRing port	{1..2}-{1..3}-t{01..99}-{e,w}-{tre,trw}-{1,all}
(Port in a 2-fiber MS-SPRing facility protection group)	{1..2}-{1..3}-t{01..99}-{e,w}-#-#
	{1..2}-{1..3}-#-#-{tre,trw}-{1,all}
	Note: {e,w} stands for east or west side.
Generic Gigabit Ethernet port	1-{1,3}-#-#-{02,04,06,08,...14,16}-{1-2,all}
	{2-4}-{1-3}-#-#-{02,04,06,08,...14,16}-{1-2,all}
Generic Gigabit Ethernet port (VCG group)	1-{1,3}-#-#-{02,04,06,08,...14,16}-v{1-2,all}
	{2-4}-{1-3}-#-#-{02,04,06,08,...14,16}-v{1-2,all}
Tributary	
All the tributaries on all the ports on all the slots	{1..2}-{1..3}-#-#-all-all-all
STM1(e) tributary	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}-{1..3,all}
OC-3/STM-1(o) tributary	{1..2}-{1..3}-#-#-{01..8}-{1..4,all}-{1..3,all}
OC-12/STM-4 tributary	{1..2}-{1..3}-#-#-{01..16}-{1..2,all}-{1..12,all}
OC-48/STM-16 tributary	{1..2}-{1..3}-#-#-{02, 04, 06, 08,...14, 16}-{1,all}-{1..48,all}
OC-192/STM-64 tributary	{1..2}-{1..3}-#-#-{tre,trw}-{1,all}-{1..192,all}
Electrical tributary	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}-{1..3,all}
Unprotected optical tributary	{1..2}-{1..3}-u-#-{01..16}-{1..4,all}-{1..192,all}
1+1 Optical tributary	{1..2}-{1..3}-o{01..99}-{w,p}-{01..16}-{1..4,all}-{1..48,all}
	{1..2}-{1..3}-o{01..99}-{w,p}-#-#-{1..48,all}
	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}-{1..48,all}
	Note: {w,p} stands for working or protection side.

Entity	Access Identifier
1:N Electrical and optical tributary	{1..2}-{1..3}-n{01..99}-{1..n, p}-{01..16}-{1..4,all}-{1..48,all}
	{1..2}-{1..3}-n{01..99}-{1..n, p}-#-#-{1..48,all}
	{1..2}-{1..3}-#-#-{01..16}-{1..4,all}-{1..48,all}
	Note: The 'n' in '1-n' is the number of lines in the 1:N protection group. When a port is added to a protection group, it is assigned a line number. 'p' stands for protection.
Generic Gigabit Ethernet port VCG tributary	1-{1,3}-#-#-{02,04,06,08,...14,16}-v{1-2,all}-{1-24,all}
	{2-4}-{1-3}-#-#-{02,04,06,08,...14,16}-v{1-2,all}-{1-24,all}
STM-16 2-fiber MS-SPRing tributary	{1..2}-{1..3}-t{01..99}-{e,w}-{02, 04, 06, 08,...14, 16}-{1,all}-{1..48,all}
	{1..2}-{1..3}-t{01..99}-{e,w}-#-#-{1..48,all}
	{1..2}-{1..3}-#-#-{02, 04, 06, 08,...14, 16}-{1,all}-{1..48,all}
	Note: {e,w} stands for east or west side.
STM-64 2-fiber MS-SPRing tributary	{1..2}-{1..3}-t{01..99}-{e,w}-{tre,trw}-{1,all}-{1..192,all}
	{1..2}-{1..3}-t{01..99}-{e,w}-#-#-{1..192,all}
	{1..2}-{1..3}-#-#-{tre,trw}-{1,all}-{1..192,all}
	Note: {e,w} stands for east or west side.
Fans	
Main Shelf Fan (low-speed part)	1-1-fan1
Main Shelf Fan (high-speed part)	1-2-fan1
Extension Shelf Fan	{1..2}-{1..3}-fan1
External Timing References	
External Timing reference 1	extref1
External Timing reference 2	extref2
External Line Timing reference 1	line1
External Line Timing reference 2	line2
External Line Timing reference 3	line3
External Line Timing reference 4	line4
External Line Timing reference 5	line5
External Line Timing reference 6	line6
Timing Ports	
External Timing Input Port 0	exttmg0
External Timing Input Port 1	exttmg1
External Timing Output Port 0	exttmg0_out
External Timing Output Port 1	exttmg1_out

Entity	**Access Identifier**
Miscellaneous Discrete Inputs and Outputs	
Miscellaneous Discrete Input	misc_in{1..8},
	misc_inall
Miscellaneous Discrete Output	misc_out{1..8},
	misc_outall

Shelf provisioning

....

Overview   Shelf provisioning allows the user to configure parameters associated with a specific shelf.

Parameters   The following parameters can be viewed:

- *Shelf AID*

- *ON Cable Identifier*
  The ON Cable Identifier is the Controller Address of a shelf for the connection to the low-speed shelf which contains the main controller for the whole network element. For the high-speed shelf it is always *1*. For the extension shelf it should be *2*.

The following parameter can be set:

- *Alarm Severity Assignment Profile* (cf. "Alarm severity assignment profiles" (16-28))
  An Alarm Severity Assignment Profile (ASAP) is a list of alarms that can occur in an NE and which have each an alarm severity assigned. Several ASAPs for different functional categories are predefined for the WaveStar™ TDM 10G system.

For the current release only the default Alarm Severity Assignment Profile is available.

Additionally SS bit override can be enabled or disabled for a shelf. When SS bit override is enabled, the SS bits are set to 00 for all ports on a shelf. This overrides normal SS bit provisioning when interworking with non-compliant SONET network elements. When SS bit override is disabled, the SS bits are set to 10 for all ports on a shelf .

⌐

....

1 5 - 2 6   **Lucent Technologies**   365-371-522
Issue b, October 2001

Slot/circuit pack provisioning

Slot provisioning Slot provisioning allows the user to configure parameters associated with a specific slot. This is a pre-provisioning measure for a future upgrade of the system.

Parameter The *Alarm Severity Assignment Profile* (cf. "Alarm severity assignment profiles" (16-28)) can be selected.

For the current release only the default Alarm Severity Assignment Profile is available.

Circuit pack provisioning Currently, no parameters concerning circuit pack provisioning can be set. For future releases, Alarm Severity Assignment Profile (ASAP) settings will be possible.

Parameters The following parameters can be set (cf. Chapter 5, "Alarm management"):

- *Equipment Alarm Severity Assignment Profile*
- *System Event Alarm Severity Assignment Profile*

ASAPs An Alarm Severity Assignment Profile (ASAP) is a list of alarms that can occur in an NE and which have each an alarm severity assigned. Several ASAPs for different functional categories are predefined for the *WaveStar*® TDM 10G system.

❒

Port and tributary provisioning

Optical SDH ports — Optical port provisioning allows the user to configure parameters associated with a specific optical port (cf. "Configuring an optical port" (4-23)).

Electrical SDH ports — Electrical port provisioning allows the user to configure parameters associated with a specific electrical (STM-1) port (cf. "Configuring an electrical port" (4-38)).

Tributary provisioning — Tributary provisioning allows the user to configure parameters associated with a specific tributary belonging to an SDH port (cf. "Configuring a tributary" (4-43)).

Gigabit Ethernet (GE1/SX2) Interface

Overview   *WaveStar*® TDM 10G supports a Gigabit Ethernet (GE1/SX2) interface. The GE1/SX2 interface conforms to the standards outlined in IEEE 802.3, and supports the 1000BASE-SX protocol.

Capabilities   The GE1/SX2 interface supported by the *WaveStar* TDM 10G allows you to transport GE1/SX2 signals over SDH networks by encapsulating ethernet packets in virtually concatenated VCs. The GE1/SX2 interface supports point-to-point connectivity. Each GE1/SX2 port unit offers two 1000BASE-SX Ethernet LAN ports. Each port supports two bidirectional, Ethernet lines (one transmit and one receive). Each line can be associated with a WAN link. The capacity per Gigabit Ethernet line is user provisionable to a maximum of 7 VC-4s. All connections to the 1000BASE-SX ethernet interface on the GE1/SX2 port unit require Dual SC Connectors.

Virtual Concatenation   VC-4 concatenation can be used for the transport of payloads that do not fit efficiently into the standard set of virtual containers. Two methods for concatenation are defined, contiguous and virtual concatenation. Both methods provide concatenated bandwith of X times Container-N at the path termination. The difference is the transport between the path termination. Contiguous concatenation maintains the contiguous bandwidth throughout the whole transport. It requires concatenation functionality at each network element. Virtual concatenation breaks the contiguous bandwidth into individual VCs, transports these VCs and recombines them to a contiguous functionality only at the path termination equipment i.e. the GE1/SX2 Gigabit Ethernet port unit.
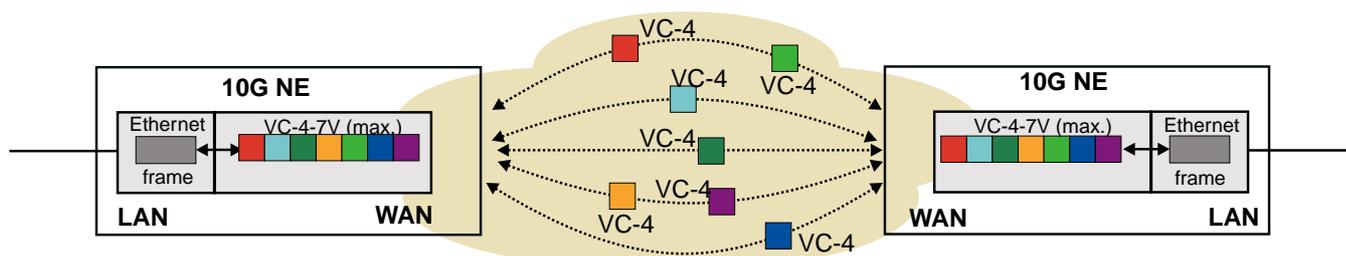
The H4 POH byte is used for the sequence and multiframe indication specific for virtual concatenation.

Due to different propagation delay of the VC-4s a differential delay will occur between the individual VC-4s. This differential delay has to be compensated and the individual VC-4s have to be realigned for access to the contiguous payload area. The realignment process covers at least a differential delay of 125 μs.

Point-to-point connectivity   The following figure shows a point-to-point Gigabit Ethernet (GbE) network application. Protection of the VC-4-Xv traffic is possible via SNCP and MS-SPRing protection schemes.
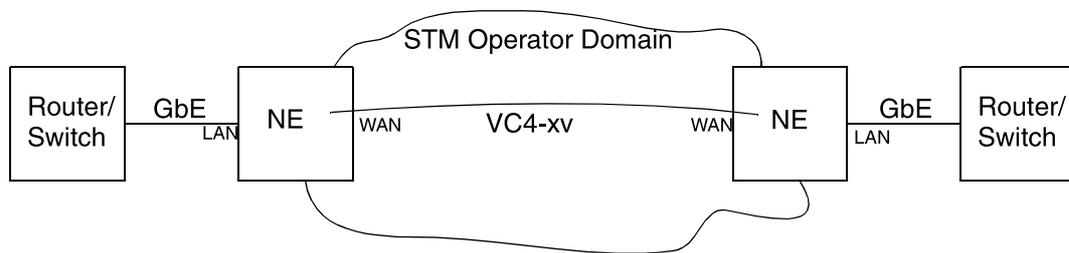
Equipment protection

Principle
An equipment protection always involves one or more plug-in units which carry traffic (*working* plug-in unit) and one plug-in unit which will assume the function of a plug-in unit that has failed (*protection* plug-in unit). Together they form a *protection group*.

Types
For the following circuit packs, equipment protection is supported:

- Timing Generator circuit pack (TMG): 1+1

- Cross-connect circuit pack (SWITCH/STS576 or SWITCH/STS768 and PPROC/STS192 or PPROC/STS384): 1+1

- Electrical STM-1 port unit (STM1E/4): 1:N

- Power feed is maintained duplicated throughout the system

Cross-connect unit protection
The cross-connect in the Main Shelf is implemented as a two-stage, higher-order switch, and consists of two switching circuit-packs (SWITCH/STS576 or SWITCH/STS768) and one delay management unit (PPROC/STS192 or PPROC/STS384). The complete cross-connect is 1+1 equipment protected, that means in detail:

- The SWITCH/STS576 circuit pack in slot (1-1) switch0 in the Main Shelf is paired with the circuit pack in slot (1-1) switch1 in a 1+1 non-revertive protection mode configuration.

- The SWITCH/STS576 or SWITCH/STS768 circuit pack in slot (1-2) switch0 in the High Speed Shelf is paired with the circuit pack in slot (1-2) switch1 in a 1+1 non-revertive protection mode configuration.

- The PPROC/STS192 or PPROC/STS384 circuit pack in slot (1-2) ppls0 is assigned to the switching circuit pack in slot (1-2) switch0 and the PPROC/STS192 or PPROC/STS384 circuit pack in slot (1-2) ppls1 is assigned to the switching circuit pack in slot (1-2) switch1. Thus, a protection switch of the switching circuit pack also means that another PPROC/STS192 or PPROC/STS384 circuit pack will be used.

The cross-connect in the Extension Shelf consists of the SWITCH/STS576 circuit pack in slot switch0 and is paired with the circuit pack in slot switch1 in a 1+1 non-revertive protection mode configuration.

Equipment protection of the STM-1 (e) interface circuit pack
The 1:N equipment protection of the STM1E/4 circuit packs can be configured in the Main Shelf.

The desired number of working circuit packs can be plugged in slots (1-1) 01 to (1-1) 16. The standby circuit pack has to be plugged in

---

slot (1-1) eprn. Furthermore the Electrical Protection Switch circuit pack (EPS-64) is necessary for the equipment protection and has to be plugged in slot (1-1) eprotnsw.

All inserted STM1E/4 circuit packs belong to the protection group. A modification can be done by disabling single circuit packs via the switch command Lockout (cf. "Switching a 1:N equipment protection" (4-70)).

Please note that 1:N equipment protection for **STM1EE4/4** circuit packs is ***not possible***.

Creation   The equipment protection groups are created automatically if the required circuit packs are plugged in the shelves.

Operation   The equipment protections operate in non-revertive mode.

⌐

....

1 5 - 3 2   **Lucent Technologies**   365-371-522
                                                            Issue b, October 2001

Miscellaneous Discrete Inputs and Outputs

Overview   The *WaveStar*® TDM 10G provides 8 input and 8 outputs which can be used for the supervision and control of external devices.

Description   The miscellaneous discrete inputs (MDIs) and outputs (MDOs) allow the user to control and monitor equipment co-located with the *WaveStar* TDM 10G through a set of input and output relay contact closures. There are 8 miscellaneous inputs that can monitor conditions such as open doors or high temperature, and 8 miscellaneous discrete outputs to control equipment such as fans and generators. These can be set by the user.

The status of the miscellaneous discrete inputs can be configured and queried from the WaveStar™ CIT. The *WaveStar* TDM 10G collects miscellaneous discrete alarms and automatically sends them to the OS.

⌐

16 Alarm management concepts

Overview

Purpose   This chapter provides information about alarm management concepts.

Contents

⌐

Fault management

Overview

Purpose   Fault management deals with the detection and reporting of particular degraded conditions by the NE and the NE's corresponding actions.

Fault management process

....

Overview   Occurrences of degraded conditions are detected by an NE as defects, derived from anomalies. Faults may be generated as a consequence of evaluating existing defects. When a fault persists for a configurable observation period (or "validation time"; cf. "Alarm configuration" (16-5)), a corresponding failure is declared and the NE reports the failure to the management systems and to the local alarm interfaces by means of an alarm notification. When the defect is absent for a configurable observation period, the NE clears the failure and generates an appropriate alarm clear notification.

Fault management process diagram   The following figure illustrates the fault management process in conjunction with the main influencing factors (visualized by means of dotted lines), such as the port monitoring mode, the alarm configuration etc.
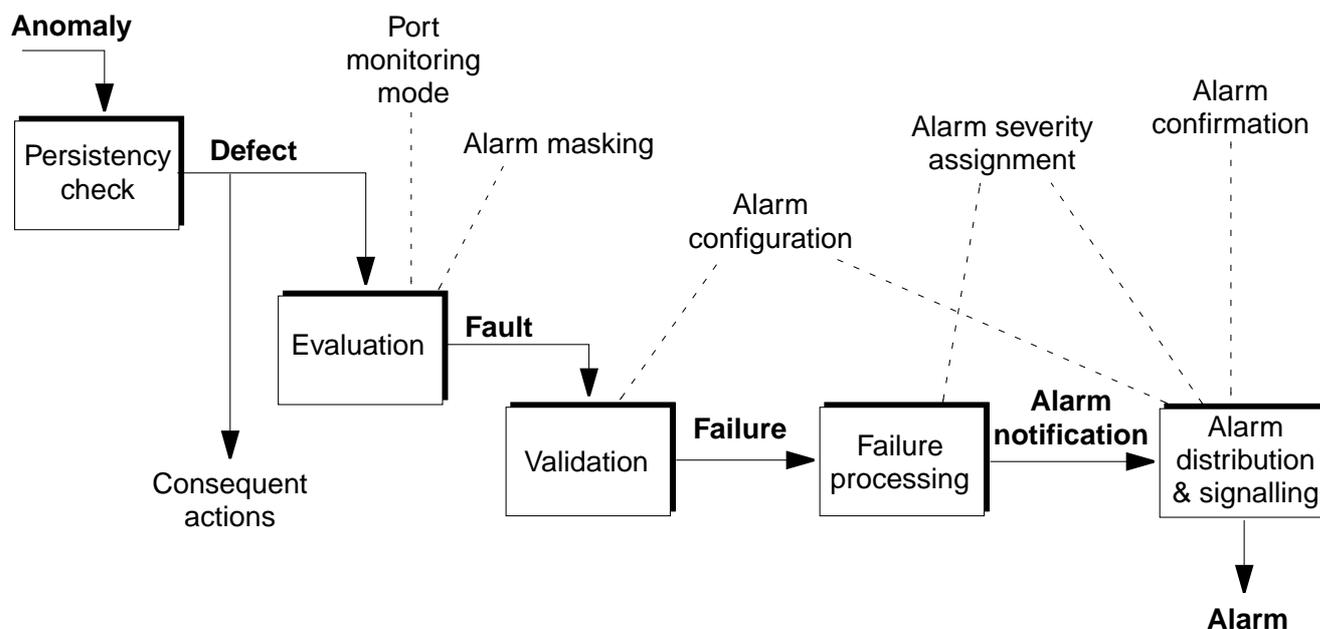
On the following pages, the fault management process will be described in more detail.

Definitions   **Anomaly** An anomaly is the smallest observable discrepancy between the actual and the desired characteristic of a system component. The occurrence of a single anomaly does not interrupt the ability to perform a required function.

Defect A defect is a limited interruption of a system component's

....

ability to perform a required function. An anomaly becomes a defect when it persists for a significant amount of time. For transmission defects this can be three STM frames in sequence for example (persistency check). Consequent actions (for example insertion of AIS or RDI) are initiated due to the existence of defects.

Fault A fault is the inability of a system component to perform a required function. Faults may be declared dependent on the evaluation of defects.

Failure A failure is the termination of a system component's ability to perform a required function. If a fault is present for at least its configured observation period (or "validation time") it becomes a failure. There is a 1:1 relation between faults and failures.

Alarm notification An alarm notification is a system message containing information on an alarm condition, such as the probable cause, the alarm category, the time of occurrence, the alarm severity, the affect on service a.s.o. Alarm notifications are used to inform management systems and local alarm interfaces on the presence or absence of alarms.

Alarm An alarm is a human observable alerting indication (e.g. visually or acoustically) to a condition that may have immediate or potential negative impact on the state of the monitoring network element.

Evaluation Evaluation is done by masking and correlation.

Masking The masking for *WaveStar*® TDM 10G (STM-64) is described on "Masking" (16-22).

Correlation The relation between defects and faults can be either

- 1:1, i.e. one defect corresponds exactly to one fault, or

- n:1, i.e. several defects are mapped to the same fault. Correlation means the calculation of faults where the relation is n:1.

Validation Validation is the mechanism that prevents alarming of faults whose presence (or absence in the case of alarm clearing) is shorter than the relevant observation period (or "validation time"). The validation time is configurable, its default setting is 0 seconds (cf. "Alarm configuration" (16-5)).

Alarm configuration   The observation period (or "validation time") for which a fault must be present before a failure will be declared can be configured individually for both equipment and communication (facility) faults. The same is true for the observation period for which a fault must be absent before the corresponding failure will be cleared. Furthermore, the signalling of office alarms can be enabled or disabled.

Please refer to "Configuring validation times and office alarm signalling" (5-14).

Port monitoring mode   Please refer to "Port monitoring mode" (16-39).

Alarm confirmation   Please refer to "Alarm confirmation" (16-43).

Signalling of alarms

Overview

....

Purpose   This section provides information about signalling of alarms.

Alarm interfaces   *WaveStar*® TDM 10G (STM-64) systems provide the following interfaces for alarm signalling:

- Management systems:
  - *WaveStar* SNMS subnetwork management system
  - *WaveStar* CIT customer interface terminal
  Please notice that administration, maintenance and provisioning activities via *WaveStar* SNMS are described in the separate *WaveStar* SNMS documentation set.

- Alarm LEDs on the user panel

- Fault LED on the circuit pack faceplate

- Office alarms

Control of alarm signalling   Alarm signalling is influenced and controlled by the following factors:

- Alarm severity
  Signalling via the management systems, the alarm LEDs on the user panel and the office alarm LEDs correspond to the currently assigned alarm severity.

- Alarm configuration
  Office alarms can be enabled or disabled by means of the *WaveStar* CIT.

- Alarm confirmation
  Please refer to "Alarm confirmation" (16-43).

Contents

⌐

....

WaveStar® CIT visual alarm indicators

....

Kinds of alarm indicators   The *WaveStar* CIT provides the following visual alarm indicators to
display the current NE alarm status:

- **External Timing Reference Alarm** indication,

- Alarm status display,

- **System View** alarm indicators,

- **Shelf View** alarm indicators.

External Timing Reference   The field left of the **Alarm List button displays the message **Ext
Alarm indication**   Timing Ref Failure** if such an alarm is reported. Otherwise this field
is left blank.

Alarm status display   The alarm status display, permanently displayed in the lower left
corner of the **System View** or **Shelf View** window, reflects the current
alarm status of the entire NE. It shows a count of all alarms currently
present on the NE, sorted by alarm severity (alarm level), for the
Prompt (**PR**) and Deferred (**DF**) alarm severities.

**Update of the alarm status   The alarm status display is automatically updated as soon as the NE
display**   alarm status varies. The date and time of the last update is indicated
on the right hand side of the alarm status display.

The **Update Alarms** button beside the **Alarm List** button can be used
to manually refresh the alarm status display.

System view alarm   In the **System View, each shelf is functionally depicted with a shelf
indicators**   level alarm LED which serves to indicate the highest level of alarm
for that shelf.

Shelf view alarm   In the **Shelf View, each circuit pack may have two different types of
indicators**   alarm indicators:

- Circuit pack alarm indicators

....

Each circuit pack has a bell symbol to indicate the circuit pack's current alarm status. Notice that a bell symbol will only be visible if at least one deferred alarm is present for the circuit pack.

- Port unit LEDs
  Furthermore, each port unit has an LED associated with each port which serves to indicate the alarm status for the associated port.

Circuit pack alarm indicators

Port unit LEDs
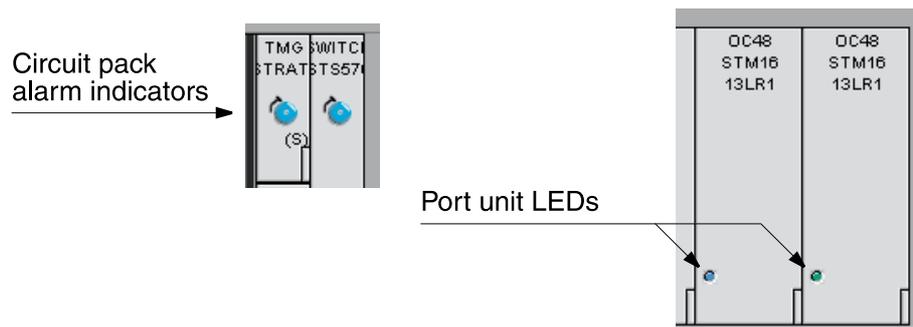
Color scheme   Indication of alarms is according to the following color scheme:

- Red
  Prompt alarm (Critical)

- Yellow
  Prompt alarm (Major)

- Cyan
  Deferred alarm

- Green
  Info alarm

The "NE Alarm List"

The *NE Alarm List* window   The *WaveStar*® CIT provides a list of current alarms, the **NE Alarm List**, to retrieve detailed information about the current alarm status of a *WaveStar* TDM 10G (STM-64) NE.

Structure of the *NE Alarm List*   The following table explains the structure of the **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**).
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.
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 formats depend on the country in which the *WaveStar* CIT is being used.
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 (**-**).

Column	Meaning
Probable Cause	This column indicates the alarm short designation. A more detailed description of the alarm's probable cause can be found in the **Description** column.
Signal Level Affected	This column indicates the affected signal level for communication alarms or the alarm category otherwise. Possible values are:

- **EQPT**
  Equipment (alarm category)
- **T1**
  STM port timing input
- **STM1E**
  electrical STM-1 transport signal (155 Mbit/s)
- **STM16**
  optical STM-16 transport signal (2.5 Gbit/s)
- **STM64**
  optical STM-64 transport signal (10 Gbit/s)
- **STM1**
  optical STM-1 transport signal (155 Mbit/s)
- **VC3**
  VC-3 payload signal
- **VC4**
  VC-4 payload signal
- **VC4-4C**
  VC-4-4C payload signal
- **VC4-16C**
  VC-4-16C payload signal

Alarm Type	This column indicates the alarm category. Possible values are:

- **Communications**,
- **Equipment**,
- **Processing**.

Description	This column describes the alarm's probable cause in more detail.

Pushbuttons The **NE Alarm List** window provides the following buttons:

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 (cf. "Update of the alarm status
   display" (16-7)) beside the **Alarm List** button. The **Update
   Alarms** button can only be used to manually refresh the alarm
   status display, not the alarm list.

NE local indications

....

<table>
<tr><td style="width:25%">Alarm LEDs on the user panel</td><td>Alarms are signalled via the alarm LEDs on the user panel is according to the currently assigned alarm severity:</td></tr>
</table>

Assigned alarm severity	Alarm LED
Prompt, Critical	Red LED (CR)
Prompt, Major	Red LED (MJ)
Deferred	Yellow LED (MN)
Info	No indication via the user panel
Not Reported	allarm LEDs

Please also refer to "User panel" (16-43).

Fault LED on circuit packs   A red "Fault" LED is located on all *WaveStar*® TDM 10G (STM-64) circuit packs to indicate failures attributable to the circuit pack. Please also refer to "Circuit pack status indicators" (16-49).

The possible Fault LED states are shown in the following table.

Fault LED State	Meaning
On	indicates a circuit pack failure
Off	indicates no failures
Flashing	indicates an incoming signal failure, an external timing failure or a memory corruption

Office alarms   The rack alarm lamps located at the rack top are used for visual office alarm signalling. The red lamp indicates prompt alarms having a severity of CR or MJ. The yellow lamp indicates deferred alarms having a severity of MN.

The office alarms interface is a set of discrete relays controlling audible and visible office alarms. Separate relays handle critical, major, and minor alarms. If desired, critical and major alarm outputs can be wired so that either, neither, or both of the outputs control the prompt office alarm.

Please also refer to "Office alarms interface" (16-52).

⌐

....

Network element alarms overview

Overview	This section provides an overview of the network element alarms defined for *WaveStar*® TDM 10G (STM-64) systems. The alarms are arranged in alphabetical order according to their alarm identifier (probable cause).
Signalling of alarms	Signalling of alarms via the management systems, the alarm LEDs on the user panel and the office alarm LEDs is according to the currently assigned alarm severity.
	Please also refer to "Signalling of alarms" (16-6).
Legend to the alarms overview	The structure of the tables and the abbreviations used are explained in the following:

- Category
  This column indicates the alarm category. Possible alarm categories are:
  - C Communication
  - E Equipment
  - P Processing
- Probable cause
  This column indicates the alarm identifier displayed on the *WaveStar* CIT graphical user interface in the **Probable Cause** column of the alarm list.
- Alarm text
  This column indicates the alarm text displayed on the *WaveStar* CIT graphical user interface in the **Description** column of the alarm list.
- Predefined alarm severity
  This column indicates the alarm severity in the predefined alarm severity assignment profiles (cf. "Alarm severity assignment profiles" (16-28)). For a service-independent ASAP associated to the respective alarm, there is only one alarm severity given. In the case of a service-dependent ASAP, there are two severities (NSA/SA) given dependent on the value of the alarm's affect-on-service attribute.
  Please refer to "Alarm severities" (16-26) for an overview of possible alarm severities. The alarm severities according to the Telcordia Technologies standards are used in the following table.
- Alarm source

This column indicates the system function originating the alarm. The following abbreviations are used:

- 1xN opt prot grp
  1:N optical protection group

- 1+1 opt prot grp
  1+1 optical protection group

- Assgn Tmg Ref
  Assigned timing reference

- BLSR prot grp
  BLSR/MS-SPring protection group

- Sys Ctlr Ck Pk
  System controller circuit pack

- VC-N CS
  VC-N constituent signal

- VC-N XC
  VC-N cross connection

- ASAP
  This column indicates the alarm severity assignment profile to which the respective alarm belongs (please refer to "Alarm severities" (16-26)).

Network element alarms

Important! The APSB, APSCM, APSMM and FEPRLF alarms are not supported for *WaveStar* TDM 10G (STM-64) systems. Since these alarms indicate a K1/K2 byte failure and thus constitute a failure of protocol they lead to the alarm "APS Failure of Protocol" (APSFOP). Any changes you may make concerning its alarm severity assignment will have no effect.

The following table lists all network element alarms

Category	Probable cause (alarm identifier)	Alarm text	Predefined alarm severity	Alarm source	ASAP
E	ALS	Automatic Laser Shutdown	MN/CR	Circuit Pack	Equipment
C	APSB	APS Prot Switch Byte Failure	MJ	1xN opt prot grp	Autom. Prot. Switch
C	APSC	BLSR Inconsistent APS Codes	MJ	BLSR prot grp	BLSR/MS-SPring
C	APSCM	APS Channel Mismatch	MJ	1xN opt prot grp	Autom. Prot. Switch

Category	Probable cause (alarm identifier)	Alarm text	Predefined alarm severity	Alarm source	ASAP
C	APSFOP	APS Failure of Protocol	MJ	1+1 opt prot grp	Autom. Prot. Switch
C	APSMM	APS Mode Mismatch	MJ	1xN opt prot grp	Autom. Prot. Switch
C	APSPAI	APS 1xN Port Assignment Invalid	MJ	1xN opt prot grp	Autom. Prot. Switch
C	APSPROV	BLSR Improper APS Codes	MJ	BLSR prot grp	BLSR/MS-SPring
C	AUAIS	AU Alarm Indication Signal	NR/NR	VC-N CS	VC-N(c) Trib.
C	AULOP	AU Loss of Pointer	NR/CR	VC-N CS	VC-N(c) Trib.
P	AUTORESET	Autonomous Reset	NA	Circuit Pack	System Events
E	BKUPMEMO	Non-Volatile Memory Usage	MN/MJ	Sys Ctlr Ck Pk	Equipment
E	BKUPMEMP	Non-Volatile Memory Wearout	MN/MN	Circuit Pack	Equipment
C	BLSR-DKB	BLSR Default K-bytes	MJ	BLSR prot grp	BLSR/MS-SPring
C	CLKOUTQF	ClkOut Quality Failure	MN	System	System Timing
C	CKTAUDSNP	Ring Circuit Validation Suspended	MN	BLSR prot grp	BLSR/MS-SPring
C	CKTAUDUD	Ring Circuit Alarm Suppressed	NA	BLSR prot grp	BLSR/MS-SPring
C	CRSMAP-UPD	Auto Disconnected Cross-Connect	NA	VC-N CS	System Events
E	DATAFLT	Memory Mismatch	MN/MJ	Circuit Pack	Equipment
E	DBMEMTRF	Auto Database Backup Failure	NA	System	System Events
C	DCCMSF	DCC MSect Failure	MN/MN	STM-N port	STM-N Port
E	DCCPR	DCC Partition Repair	MN	System	Equipment
C	DCCRSF	DCC RSect Failure	MN/MN	STM-N port	STM-N Port
E	DCCTO	DCC Tunnel Overflow	MN	System	Equipment
C	DUPL-RNG	Duplicate Ring Node	MJ	BLSR prot grp	BLSR/MS-SPring

Category	Probable cause (alarm identifier)	Alarm text	Predefined alarm severity	Alarm source	ASAP
C	EOC	DCC Type Mismatch	NA	STM-N port	System Events
E	EQPT	Circuit Pack Failure, Initialization	MN/CR	Circuit Pack	Equipment
		Circuit Pack Failure, Interface			
		Circuit Pack Failure, Internal			
C	FAILTOSW	Path Switch Failure	NA	Path prot grp	Path Prot. Switch
C	FEPRLF	APS Far-End Prot Line Failure	MJ	1xN opt prot grp	Autom. Prot. Switch
C	HLDOVRSYNC	System Clock Holdover	MN	System Timing	System Timing
C	HPDEG	HP Signal Degrade	NR/NR	VC-N CS	VC-N(c) Trib.
C	HPEXC	HP Excessive Error	NR/NR	VC-N CS	VC-N(c) Trib.
C	HPRDI	HP Remote Defect Indication	NR/NR	VC-N CS	VC-N(c) Trib.
C	HPTIM	(HP Trace Identifier Mismatch)	NR/CR	VC-N CS	VC-N(c) Trib.
C	HPUNEQ	HP Unequip	NR/CR	VC-N CS	VC-N(c) Trib.
E	INIT-1	Startup/Initialization Complete	NA	System	–
E	INT	Fan Failure	MN/CR	Shelf	Equipment
C	MSAIS	MSect Alarm Indication Signal	NR/NR	STM-N port	STM-N Port
C	MSDEG	MSect Signal Degrade	MN/MJ	STM-N port	STM-N Port
C	MSEXC	MSect Excessive Error	MN/CR	STM-N port	STM-N Port
C	MSRDI	MSect Remote Failure Indication	NR/NR	STM-N port	STM-N Port
C	MSSSF	MSect Server Signal Failure	NR/NR	STM-N port	STM-N Port
C	NID-CONFL	Node ID Mismatch	MJ	BLSR prot grp	BLSR/MS-SPring

Category	Probable cause (alarm identifier)	Alarm text	Predefined alarm severity	Alarm source	ASAP
C	OVRDSW	Ring Prot Switching Suspended	MJ	BLSR prot grp	BLSR/MS-SPring
C	PAINTGRT	Path Integrity Failure	MJ	VC-N CS	BLSR/MS-SPring
C	PAPRVERR	Circuit Provisioning Error	MN	VC-N CS	BLSR/MS-SPring
E	PRCDRERR	Circuit Pack Invalid, Illegal	MN/MN	Slot	Equipment
		Circuit Pack Invalid, Unexpected			
		Circuit Pack Invalid, Unknown			
E	PROCROVLD1	Resource Usage	MN/MJ	Circuit Pack	Equipment
P	PROGFLT	File Error	NA	Sys Ctlr Ck Pk	System Events
C	PSA	Path Switch Active	MN	Path prot grp	Path Prot. Switch
C	PSI	Path Switch Inhibited	NA	Path prot grp	Path Prot. Switch
E	PWR	Power/Fuse Failure	MN/CR	Shelf	Equipment
E	RCVRY	System in Restoration Condition	NA	System	–
E	REPLUNITMISS	Circuit Pack Unequipped/Missing	MN/CR	Circuit Pack	Equipment
E	REPLUNITMISS	Mate Circuit Pack Unequipped	MN/MN	Circuit Pack	Equipment
C	RNG-CERR	E/W Cable Error	MJ	BLSR prot grp	BLSR/MS-SPring
C	RNG-DSCVY	Ring Discovery in Progress	NA	BLSR prot grp	BLSR/MS-SPring
C	RNG-INC	Ring Incomplete	MJ	BLSR prot grp	BLSR/MS-SPring
C	RNG-INITC	Ring Startup in Progress	MJ	BLSR prot grp	BLSR/MS-SPring
C	RNG-IRPM	Inconsistent Ring Prot Mode	MJ	BLSR prot grp	BLSR/MS-SPring
C	RNG-OPEN	Ring Open	MJ	BLSR prot grp	BLSR/MS-SPring

Category	Probable cause (alarm identifier)	Alarm text	Predefined alarm severity	Alarm source	ASAP
C	RNG-PREEMPT	Extra Traffic Preempted	NA	BLSR prot grp	BLSR/MS-SPring
C	RNG-SQUELCH	BLSR Traffic Squelched	MJ	BLSR prot grp	BLSR/MS-SPring
C	RNG-URT	Unknown Ring Type	NA	BLSR prot grp	BLSR/MS-SPring
C	RSTIM	(RSECT Trace Identifier Mismatch)	MN/CR	STM-N port	STM-N Port
E	SCMMA	System in Maintenance Condition	NA	System	–
P	SFT	Software Error, non-fatal	NA	Circuit Pack	System Events
		Software Error, fatal			
C	SQMAP-CONFL	Local Squelch Map Conflict	MN	BLSR prot grp	BLSR/MS-SPring
C	SQMAP-INCST	Local Squelch Map Inconsistent	MN	BLSR prot grp	BLSR/MS-SPring
C	STMLOF	STM Loss of Frame	MN/CR	STM-N port	STM-N Port
C	STMLOS	STM Loss of Signal	MN/CR	STM-N port	STM-N Port
C	SYNC	Line Sync Reference Failure	MJ	Assgn Tmg Ref	System Timing
C	SYNC	Sync Reference Failure	MJ	Assgn Tmg Ref	System Timing
C	SYNCSTATCHNG	System Timing Quality Level Chg	NA	System Timing	System Events
E	SYSBOOT	System Restart	NA	System	–
E	TSA	Alarm Test	NR	System	System Events
C	UNSMSF	User-Network Side MSect Failure	MN/MN	STM-N port	STM-N Port
C	UNSRSF	User-Network Side RSect Failure	MN/MN	STM-N port	STM-N Port
P	WKGMEM	Out of Memory Error	NA	Circuit Pack	System Events

Signal level affected   The following table lists the affected signal level displayed on the *WaveStar* CIT graphical user interface in the **Signal Level Affected** column of the alarm list.

Probable cause (alarm identifier)	Signal level affected						
	STM-1 electr.	STM-1 opt.	STM-4 opt.	STM-16 opt.	STM-64 opt.	VC-3	VC-4
ALS	–	–	–	X	X	–	–
APSB	–	X	–	–	–	–	–
APSC	–	–	–	X	X	–	–
APSCM	–	X	–	–	–	–	–
APSFOP	–	X	–	–	–	–	–
APSMM	–	X	–	–	–	–	–
APSPROV	–	–	–	X	X	–	–
AUAIS	–	–	–	–	–	X	X
AULOP	–	–	–	–	–	X	X
AUTORESET	–	–	–	–	–	–	–
BKUPMEMO	–	–	–	–	–	–	–
BKUPMEMP	–	–	–	–	–	–	–
BLSR-DKB	–	–	–	X	X	–	–
CKTAUDSNP	–	–	–	X	X	–	–
CKTAUDUD	–	–	–	X	X	–	–
CRSMAP-UPD	–	–	–	–	–	X	X
DATAFLT	–	–	–	–	–	–	–
DBMEMTRF	–	–	–	–	–	–	–
DCCMSF	–	–	–	X	–	–	–
DCCRSF	–	X	X	X	X	–	–
DUPL-RNG	–	–	–	X	X	–	–
EOC	–	X	X	X	X	–	–
EQPT	–	–	–	–	–	–	–
FAILTOSW	–	–	–	–	–	X	X
FEPRLF	–	X	–	–	–	–	–
HLDOVRSYNC	–	–	–	–	–	–	–
HPDEG	–	–	–	–	–	X	X
HPEXC	–	–	–	–	–	X	X
HPRDI	–	–	–	–	–	X	X
HPUNEQ	–	–	–	–	–	X	X
INIT-1	–	–	–	–	–	–	–
INT	–	–	–	–	–	–	–

Probable cause (alarm identifier)	Signal level affected						
	STM-1 electr.	STM-1 opt.	STM-4 opt.	STM-16 opt.	STM-64 opt.	VC-3	VC-4
MSAIS	–	–	–	X	–	–	–
MSDEG	X	X	X	X	X	–	–
MSEXC	X	X	X	X	X	–	–
MSRDI	X	X	X	X	X	–	–
MSSSF	X	X	X	X	X	–	–
NID-CONFL	–	–	X	X	X	–	–
OVRDSW	–	–	X	X	X	–	–
PAINTGRT	–	–	–	–	–	X	X
PAPRVERR	–	–	–	–	–	X	X
PRCDRERR	–	–	–	–	–	–	–
PROCROVLD1	–	–	–	–	–	–	–
PROGFLT	–	–	–	–	–	–	–
PSA	–	–	–	–	–	X	X
PSI	–	–	–	–	–	X	X
PWR	–	–	–	–	–	–	–
RCVRY	–	–	–	–	–	–	–
REPLUNITMISS	–	–	–	–	–	–	–
RNG-CERR	–	–	–	X	X	–	–
RNG-DSCVY	–	–	–	X	X	–	–
RNG-INC	–	–	–	X	X	–	–
RNG-INITC	–	–	–	X	X	–	–
RNG-IRPM	–	–	–	X	X	–	–
RNG-OPEN	–	–	–	X	X	–	–
RNG-PREEMPT	–	–	–	X	X	–	–
RNG-SQUELCH	–	–	–	X	X	–	–
RNG-URT	–	–	X	X	X	–	–
SCMMA	–	–	–	–	–	–	–
SFT	–	–	–	–	–	–	–
SQMAP-CONFL	–	–	–	X	X	–	–
SQMAP-INCST	–	–	–	X	X	–	–
STMLOF	X	X	X	X	X	–	–
STMLOS	X	X	X	X	X	–	–

Probable cause (alarm identifier)	Signal level affected						
	STM-1 electr.	STM-1 opt.	STM-4 opt.	STM-16 opt.	STM-64 opt.	VC-3	VC-4
SYNC	–	–	–	–	–	–	–
SYNCSTATCHNG	–	–	–	–	–	–	–
SYSBOOT	–	–	–	–	–	–	–
TSA	–	–	–	–	–	–	–
UNSMSF	–	–	–	X	–	–	–
UNSRSF	–	X	X	X	X	–	–
WKGMEM	–	–	–	–	–	–	–

Masking

Overview Many alarms inevitably cause follow-up alarms, e.g. loss of signal
(LOS), which always means a loss of frame (LOF) as well. To avoid
increasing the message traffic unnecessarily, it is advisable to only
report LOS and suppress the display of LOF. This is called ″masking″
the follow-up alarms.

Masking hierarchy Therefore, a masking hierarchy is defined and implemented for *WaveStar*® TDM 10G (STM-64) alarms.

SDH Physical Interface/
Regenerator Section/
Multiplex Section

LOS: STM Loss of Signal
LOF: STM Loss of Frame
RS-TIM: RS Trace Identifier Mismatch
MS-RDI: MS Remote Defect (Failure) Indication
MS-AIS: MS Alarm Indication Signal
MS-EXC: MS Excessive Bit Error Ratio
MS-DEG: MS Signal Degrade
MS-SSF: MS Server Signal Fail
RS: Regenerator Section
MS: Multiplex Section

```
SDH Physical Interface/Regenerator Section/Multiplex Section:

    LOS
     |
    LOF
     |
   RS-TIM ──────────────────────────────> MS-SSF[1]
     |   \                                     |
  MS-AIS  MS-RDI                               |
     |                                         |
  MS-EXC                                       |
     \                                         |
    MS-DEG                                     |
- - - - - - - - - - - - - - - - - - - - - - - -|- -
Higher Order Path                              |
      AU-SRM      AU-LOP       AU-AIS <─────────
         \          |          /
              HP-UNEQ
                 |
              HP-TIM
              /     \
        HP-RDI     HP-EXC
                      |
                   HP-DEG
```

Higher Order Path

AU-SRM: AU Signal Rate Mismatch
AU-LOP: AU Loss of Pointer
AU-AIS: AU Alarm Indication Signal
HP-UNEQ: HP Unequipped
HP-TIM: HP Trace Identifier Mismatch
HP-RDI: HP Remote Defect (Failure) Indication
HP-EXC: HP Excessive Bit Error Ratio
HP-DEG: HP Signal Degrade
AU: Administrative Unit
HP: Higher (order) Path

1   MS-SSF is generated as a consequent action if either of the following alarms is present:LOS, LOF, RS-TIM, MS-AIS or MS-EXC.

Communication alarms The communication alarms shown in the above figure with an arrow pointing downwards mask all the alarms below them in the direction of the arrow.

If a certain alarm is already displayed and an alarm with a higher severity in the masking hierarchy occurs, the display for the lower severity alarm is cancelled and only the higher severity alarm is

displayed. If a higher-severity alarm is cleared, a lower-severity alarm present at the same time but suppressed until now due to the masking hierarchy is now displayed.

Equipment alarms   An equipment alarm of a circuit pack will clear any currently present communication alarms directly associated with the same pack, i.e. an equipment alarm has a higher priority than a communication alarm.

Any currently present alarm associated to a circuit pack will be cleared when the circuit pack is removed. A circuit pack unequipped alarm will then be displayed instead.

Alarm provisioning

Overview

Purpose   This section on alarm provisioning deals with the provisioning activities related to the generation and display of alarms.

Alarm provisioning includes:

- assigning alarm severities,
- setting the port monitoring mode,
- enabling or disabling office alarm signalling,
- configuring thresholds for bit error monitoring, and
- enabling or disabling consequent actions in case of an excessive bit error ratio.

....
Alarm provisioning

365-371-522   **Lucent Technologies**   1 6 - 2 5
Issue b, October 2001

Alarm severities

Overview   An alarm can be assigned one of the alarm severities listed in the following table.

Network Elements		SDH Mapping (Management Systems)
Telcordia Technologies Standards (formerly Bellcore)	ITU-T Rec. M.3100	ITU-T Rec. M.20
Critical (CR)	Critical	Prompt (PR)
Major (MJ)	Major	Prompt (PR)
Minor (MN)	Minor	Deferred (DF)
Not-alarmed (NA)	Warning	Info (INF)
Not-reported (NR)	Non-alarmed	–

Please note that you can select the alarm format, i.e. how alarm severities will be displayed on the *WaveStar*® CIT graphical user interface, by means of the **System View** tab in the **Preferences** window. Possible alarm formats are:

- Critical/Major/Minor (***CR/MJ/MN***),

- Prompt/Deferred/Info (***PR/DF/INF***).

In the latter case, "Prompt" comprises "Prompt, Critical" and "Prompt, Major".

Meaning of the alarm severities   The alarm severities listed in the following table have the following meaning:

Alarm Severity	Meaning
Critical Major	"Critical" and "Major" represent prompt maintenance conditions. Immediate action is required by maintenance personnel to remove defective equipment from service for the purpose of restoring good service and effecting repair of the failed equipment.

Alarm Severity	Meaning
Minor	"Minor" represents a deferred maintenance condition.
	No immediate action is required by maintenance personnel, for example, when performance falls below standard but the effect does not warrant removal from service, or generally, if automatic changeover to standby equipment has been used to restore service.
Not-alarmed	Alarm conditions having the "Not-alarmed" alarm severity assigned will neither be signalled by the management systems nor by the user panel LEDs or the office alarm grid. However, in principle alarm signalling is possible since an alarm notification will be generated.
Not-reported	No alarm notification will be generated for alarm conditions having the "Not-reported" alarm severity assigned. Therefore no alarm signalling is possible.

Assigning alarm severities The alarm severity assignment is accomplished by means of alarm severity assignment profiles (ASAPs); please refer to "Alarm severity assignment profiles" (16-28).

⌐

Alarm severity assignment profiles

Overview   An alarm severity assignment profile (ASAP) is a list of alarms that can occur in a network element and which each have an alarm severity assigned.

ASAPs can be assigned to *WaveStar*® TDM 10G (STM-64) functional system components (a circuit pack or a specific port for example) during provisioning.

Basic ASAP variants   **Important!** In the present *WaveStar* TDM 10G (STM-64) release, apart from the "STMn Port" and "VC-N(c) Tributary" ASAP types only the default ASAP of each ASAP type can be assigned to a functional system component.

Depending on their affect-on-service attribute (Non-Service Affecting (NSA) or Service Affecting (SA)), two types of alarms can be distinguished, service-dependent and service-independent alarms. Accordingly, the following variants of ASAPs can be distinguished:

- Service-independent (SI)
  The ASAP consists of assigning an alarm severity to each alarm.

- Service-dependent (SD)
  The ASAP consists of assigning an alarm severity to each alarm dependent on the value of its corresponding affect-on-service attribute (NSA or SA).

Important! In the case of a service-dependent ASAP, the SA alarm severity cannot be less than the NSA alarm severity.

Alarm severities   Please refer to "Alarm Severities" for information about possible alarm severities.

Available ASAP types   Several ASAP types for different functional categories are available for the *WaveStar* TDM 10G (STM-64) system.

ASAP Type	SI	SD	Functional Category	Default Settings
STMn Port		X	SDH transmission alarms (RS- or MS-related)	cf. "STMn port ASAP" (16-31)
Path Termination SDH	X		Path Termination SDH alarms	cf. "Path Termination SDH ASAP" (16-31)

ASAP Type	SI	SD	Functional Category	Default Settings
VC-N(c) Tributary		X	SDH transmission alarms (path-related)	cf. "VC-N(c) tributary ASAP" (16-32)
Equipment		X	Circuit pack and other equipment alarms	cf. ""Equipment" ASAP" (16-32)
System Timing	X		Synchronization system alarms	cf. ""System Timing" ASAP" (16-33)
Automatic Protection Switch	X		APS alarms for 1+1 and 1:N (1xN) Multiplex Section protection switching	cf. "Automatic protection switch" (16-33)
Path Protection Switch	X		DNI/Path alarms	cf. "Path protection switch" (16-34)
BLSR/MS SPRing Protection Switch	X		BLSR/MS SPRing alarms	cf. "BLSR/MS SPRing protection switch" (16-34)
System Events	X		Event alarms for any of the alarm categories	cf. "System events" (16-35)
Ethernet		X	Ethernet alarms	cf. ""Ethernet" ASAP" (16-35)
Environment		X	Environmental alarms	cf. ""Environmental" ASAP" (16-35)

Default ASAPs   For each of the available ASAP types, there exists a default ASAP containing meaningful factory settings. The composition and the alarm severity assignments of these default ASAPs are given in "STMn port ASAP" (16-31) to "System events" (16-35) (please also refer to the "Default Settings" column in "Available ASAP types" (16-28)).

Customizing ASAPs   New ASAPs with customized alarm severity assignments can be created in addition to the default ASAP for these types of ASAPs:

ASAP type	Max. number of new ASAPs
STMn Port	10
VC-N(c) Tributary	6
Equipment	6
System Timing	2
Automatic Protection Switch	3
BLSR/MS-SPRing Protection Switch	3
Path Protection Switch	3
Ethernet	3
Environment	5
System Events	6

ASAPs can be customized in the following way:

- The maximum number of new ASAPs also includes possible non-reporting ASAPs; please also refer to "Non-reporting ASAPs" (16-30).

- All ASAPs but the default ASAPs can be renamed.

- All alarm severity assignments, including those in the default ASAPs, can be modified individually.

For information on how to customize ASAPs, please refer to the following provisioning tasks:

- "Creating a new alarm severity assignment profile" (5-2),

- "Creating a non-reporting alarm severity assignment profile" (5-6),

- "Modifying an existing alarm severity assignment profile" (5-10).

Non-reporting ASAPs   Non-reporting ASAPs can be created for the "STMn Port" and "VC-N(c) Tributary" ASAP types. They have an alarm severity of Not-reported (NR) assigned to each alarm.

....

1 6 - 3 0   **Lucent Technologies**   365-371-522
Issue b, October 2001

A non-reporting ASAP can be assigned to an STM-N port or a tributary channel and may be useful to supress undesired alarm messages during provisioning activities for example.

STMn port ASAP   The following table shows the default alarm severity assignments of the "STMn Port" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA

Note: <SL> indicates the "signal level" affected. Possible values are: STM1, STM1E, STM4, STM16, STM64 (representing STM-1, STM-1E, STM-4, STM-16 and STM-64)

Probable Cause	Alarm Text	NSA	SA
STMLOS	<SL> port, STM Loss of Signal	DF	PR, CR
STMLOF	<SL> port, STM Loss of Frame	DF	PR, CR
MSAIS	<SL> port, MSect Alarm Indication Signal	–	–
MSRDI	<SL> port, MSect Remote Failure Indication	–	–
RSTIM	<SL> port, RSect Trace Identifier Mismatch	DF	PR, CR
MSEXC	<SL> port, MSect Excessive Error	DF	PR, CR
MSDEG	<SL> port, MSect Signal Degrade	DF	PR, MJ
MSSSF	<SL> port, MSect Server Signal Failure	–	–
DCCRSF	<SL> port, DCC RSect Failure	DF	DF
DCCMSF	<SL> port, DCC MSect Failure	DF	DF
UNSRSF	<SL> port, User-Network Side RSect Failure	DF	DF
UNSMSF	<SL> port, User-Network Side MSect Failure	DF	DF

Path Termination SDH ASAP   The following table shows the default alarm severity assignments of the "Path Termination SDH" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA

Note: <SL> indicates the "signal level" affected. Possible values are: VC3, VC4, (representing VC-3, VC-4)

Probable Cause	Alarm Text	NSA	SA
HPLOP	<SL> CS, HP Loss of Pointer	—	PR, CR
SSF	<SL> CS, HP Server Signal Failure	—	PR, CR
PLM-P	<SL> CS, HP Payload Label Mismatch	—	PR, CR
RFI-P	<SL> CS, HP Remote Defect Indication	—	—
HPDEG	<SL> CS, HP Signal Degrade	—	—
TIMM	<SL> CS, HP Trace Identifier Mismatch	—	PR, CR
UNEQ-P	<SL> CS, HP Unequip	—	PR, CR

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA
LOM	<SL> CS, Loss of Multiframe	—	PR, CR
SQM	<SL> CS, Sequence Number Mismatch	—	PR, CR

VC-N(c) tributary ASAP The following table shows the default alarm severity assignments of the "VC-N(c) Tributary" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA

Note: <SL> indicates the "signal level" affected. Possible values are: VC3, VC4, VC44C, VC416C (representing VC-3, VC-4, VC-4-4C and VC-4-16C)

Probable Cause	Alarm Text	NSA	SA
AULOP	<SL> CS, AU Loss of Pointer	–	PR, CR
AUAIS	<SL> CS, AU Alarm Indication Signal	–	–
AUSRM	<SL> CS, AU Signal Rate Mismatch	–	PR, MJ
HPRDI	<SL> CS, HP Remote Defect Indication	–	–
HPTIM	<SL> CS, HP Trace Identifier Mismatch	–	PR, CR
HPUNEQ	<SL> CS, HP Unequip	–	PR, CR
HPEXC	<SL> CS, HP Excessive Error	–	–
HPDEG	<SL> CS, HP Signal Degrade	–	–

Important! The "VC-N(c) Tributary" ASAP represents the default for point-to-point cross-connection topologies, and as such, the "NSA" column is not applicable because for these cross-connections the affect-on-service attribute is always "SA".

"Equipment" ASAP The following table shows the default alarm-severity assignments of the "Equipment" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA
EQPT	<circuit pack>, Circuit Pack Failure, Initialization	DF	PR, CR
	<circuit pack>, Circuit Pack Failure, Interface		
	<circuit pack>, Circuit Pack Failure, Internal		
REPLUNITMISS	<circuit pack>, Circuit Pack Unequipped/Missing	DF	PR, CR
	<circuit pack>, Mate Circuit Pack Unequipped	DF	DF
BKUPMEMP	<circuit pack>, Non-Volatile Memory Wearout	DF	DF
ALS	<circuit pack>, Automatic Laser Shutdown	DF	PR, CR

Probable Cause	Alarm Text	Alarm Severity	
		NSA	**SA**
PRCDRERR	Slot, Circuit Pack Invalid, Illegal	DF	DF
	Slot, Circuit Pack Invalid, Unexpected		
	Slot, Circuit Pack Invalid, Unknown		
INT	Shelf, Fan Failure	DF	PR, CR
PWR	Shelf, Power/Fuse Failure, Feeder A	DF	PR, CR
	Shelf, Power/Fuse Failure, Feeder B		
PROCROVLD1	<circuit pack>, Resource Usage, <resource type>	DF	PR, MJ
DATAFLT	<circuit pack>, Memory Mismatch	DF	PR, MJ
BKUPMEMO	Sys Ctlr Ck Pk, Non-Volatile Memory Usage	DF	PR, MJ
DCCPR	<circuit pack>, DCC Partition Repair	DF	DF
DCCTO	<circuit pack>, DCC Tunnel Overflow	DF	DF

"System Timing" ASAP   The following table shows the default alarm severity assignments of the "System Timing" ASAP.

Probable Cause	Alarm Text	Alarm Severity
SYNC	Assgn Tmg Ref, Sync Reference Failure	PR, MJ
	Assgn Tmg Ref, Line Sync Reference Failure	PR, MJ
HLDOVRSYNC	System Clock Holdover	DF
CLKOUTQF	ClkOUt Quality Failure	DF

Automatic protection switch   The following table shows the default alarm severity assignments of the "Automatic Protection Switch" ASAP.

Probable Cause	Alarm Text	Alarm Severity
APSB	1xN opt prot grp, APS Prot Switch Byte Failure	PR, MJ
APSCM	1xN opt prot grp, APS Channel Mismatch	PR, MJ
APSMM	1xN opt prot grp, APS Mode Mismatch	PR, MJ
FEPRLF	1xN opt prot grp, APS Far-End Prot Line Failure	PR, MJ
APSFOP	1+1 opt prot grp, APS Failure of Protocol	PR, MJ

Important! The alarms *APSB*, *APSCM*, *APSMM* and *FEPRLF* are not supported for *WaveStar* TDM 10G (STM-64) systems. Since these alarms indicate a K1/K2 byte failure and thus constitute a failure of protocol they lead to the alarm "APS Failure of Protocol" (APSFOP).

Any changes you may make concerning its alarm severity assignment will have no effect.

Path protection switch   The following table shows the default alarm severity assignments of the "Path Protection Switch" ASAP.

Probable Cause	Alarm Text	Alarm Severity
PSA	Path prot grp, Path Switch Active	DF
FAILTOSW	Path prot grp, Path Switch Failure	INF
PSI	Path prot grp, Path Switch Inhibited	INF

BLSR/MS SPRing protection switch   The following table shows the default alarm severity assignments of the "BLSR/MS SPRing Protection Switch" ASAP.

Probable Cause	Alarm Text	Alarm Severity

Note: <SL> indicates the "signal level" affected. Possible values are: STM16, STM64, VC3, VC4, VC44C, VC416C (representing STM-16, STM-64, VC-3, VC-4, VC-4-4C and VC-4-16C)

Probable Cause	Alarm Text	Alarm Severity
APSC	BLSR prot grp, BLSR Inconsistent APS Codes	PR, MJ
APSPROV	BLSR prot grp, BLSR Improper APS Codes	PR, MJ
BLSR-DKB	BLSR prot grp, BLSR Default K-bytes	PR, MJ
RNG-SQUELCH	<SL> port, BLSR Traffic Squelched	PR, MJ
SQMAP-INCST	BLSR prot grp, Local Squelch Map Inconsistent	DF
SQMAP-CONFL	BLSR prot grp, Local Squelch Map Conflict	DF
RNG-INC	BLSR prot grp, Ring Incomplete	PR, MJ
RNG-OPEN	BLSR prot grp, Ring Open	PR, MJ
NID-CONFL	BLSR prot grp, Node ID Mismatch	PR, MJ
DUPL-RNG	BLSR prot grp, Duplicate Ring Node	PR, MJ
RNG-URT	BLSR prot grp, Unknown Ring Type	INF
RNG-IRPM	BLSR prot grp, Inconsistent Ring Prot Mode	PR, MJ
RNG-CERR	BLSR prot grp, E/W Cable Error	PR, MJ
RNG-DSCVY	BLSR prot grp, Ring Discovery in Progress	INF
RNG-INITC	BLSR prot grp, Ring Startup in Progress	PR, MJ
CKTAUDSNP	BLSR prot grp, Ring Circuit Validation Suspended	DF
CKTAUDUD	BLSR prot grp, Ring Circuit Alarm Suppressed	INF
RNG-PREEMPT	BLSR prot grp, Extra Traffic Preempted	INF
OVRDSW	BLSR prot grp, Ring Prot Switching Suspended	PR, MJ
PAPRVERR	<SL> CS, Circuit Provisioning Error	DF

Probable Cause	Alarm Text	Alarm Severity
PAINTGRT	<SL> CS, Path Integrity Failure	PR, MJ

System events The following table shows the default alarm severity assignments of the "System Events" ASAP.

Probable Cause	Alarm Text	Alarm Severity

Note: <SL> indicates the "signal level" affected. Possible values are: STM1, STM4, STM16, STM64, VC3, VC4, VC44C, VC416C (representing STM-1, STM-4, STM-16, STM-64, VC-3, VC-4, VC-4-4C and VC-4-16C)

Probable Cause	Alarm Text	Alarm Severity
AUTORESET	<circuit pack>, Autonomous Reset	INF
SFT	<circuit pack>, Software Error, fatal	INF
	<circuit pack>, Software Error, non-fatal	
WKGMEM	<circuit pack>, Out of Memory Error	INF
PROGFLT	Sys Ctlr Ck Pk, File Error, <affected NVM/error type>	INF
SYNCSTATCHNG	System Timing, System Timing Quality Level Chg	INF
DBMEMTRF	System, Auto Database Backup Failure	INF
TSA	System, Alarm Test	–
CRSMAP-UPD	<SL> CS, Auto Disconnected Cross-Connect	INF
EOC	<SL> port, DCC Type Mismatch	INF

"Ethernet" ASAP The following table shows the default alarm-severity assignments of the "Ethernet" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA
LOS	Ethernet port, Loss of Signal	—	PR, CR
ANM	Ethernet port, Auto Negotiation Mismatch	—	PR, MJ
LOA	VCG, Loss of Alignment	—	PR, CR
GFPLOF	VCG, Loss of Frame Delineation	—	PR, CR
VCGSF	VCG, VCG Signal Fail	—	—

"Environmental" ASAP The following table shows the default alarm-severity assignments of the "Environmental" ASAP.

Probable Cause	Alarm Text	Alarm Severity	
		NSA	SA
MISC	Misc Discrete	—	—

Independent alarms   **Important!** The predefined alarm severity of the alarms listed in the following table cannot be changed.

The alarms listed in the following table do not belong to any of the ASAPs listed on the previous pages.

Probable Cause	Alarm Text	Alarm Severity
Note: <SL> indicates the "signal level" affected. Possible values are: STM1, STM1E, STM4, STM16, STM64, VC3, VC4, VC44C, VC416C (representing STM-1, STM-1E, STM-4, STM-16, STM-64, VC-3, VC-4, VC-4-4C and VC-4-16C); {Monitored parameter} specifies the respective performance monitoring parameter; please refer to Chapter 20, "Performance monitoring concepts".		
SYSBOOT	System, System Restart	INF
INIT-1	System, Startup/Initialization Complete	INF
SCMMA	System, System in Maintenance Condition	INF
UPGRDF	System, Upgrade Failed	INF
RCVRY	System, System in Restoration Condition	INF
T-{Monitored parameter}	<SL> port, Threshold Crossing Alert	INF
	<SL> CS, Threshold Crossing Alert	

⌐

Automatic laser shutdown

Overview In the event of Loss Of Signal (LOS) caused by a cable break or loose connectors, the ALS has the task of switching off the powered laser sources. The operating personnel are thus in no danger of being exposed to laser radiation emitted at unterminated ends of fibre-optic cables.

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/WDM9310… (LEY228)

The following figure illustrates a bidirectional transmission route comprising units with an implemented ALS.
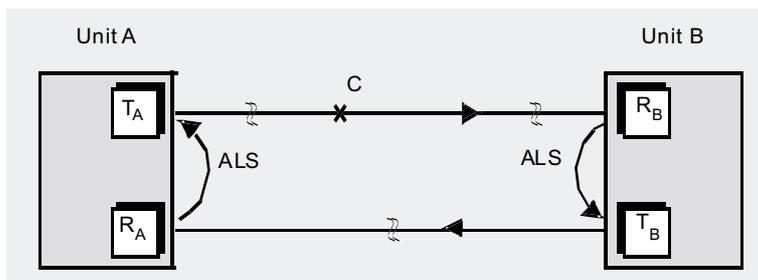
Principle Transmitter TA of unit A transmits to receiver RB of unit B. If a cable break occurs along this route, e.g. at point C, RB receives an LOS (Loss of Signal). If the LOS continues for more than 500 ms, RB shuts down the transmitter TB in the same unit. In consequence receiver RA in unit A also receives LOS. After another 500 ms transmitter TA is also shut down. Both directions of the bidirectional transmission route are thus shut down within about 1 s.

Automatic restart After 100 s an automatic restart of both lasers is initiated and a valid signal is transmitted for 2 s. If receivers RA and RB still receive LOS, the lasers are shut down once again and restarted again after 100 s. If the fault was eliminated, no LOS is detected and transmission can be continued. As soon as the receiver receives a valid signal, the laser in the same unit transmitting in the opposite direction is switched on within 0.85 s.

Manual laser start   Each unit is also provided with a manual laser start facility (refer to "Performing a laser restart" (5-40)). As in the case of the automatic laser restart, a valid signal is sent for 2 s. If LOS is signalled, the laser is shut down again.

Laser test start   A manual laser test start facility is also available which is intended mainly for calibration work. The laser can be switched on for an unlimited time or for 90 s only.

The ALS complies with ITU-T Rec. G.958.

The following figure illustrates the principle of the automatic laser shutdown and the laser restart.
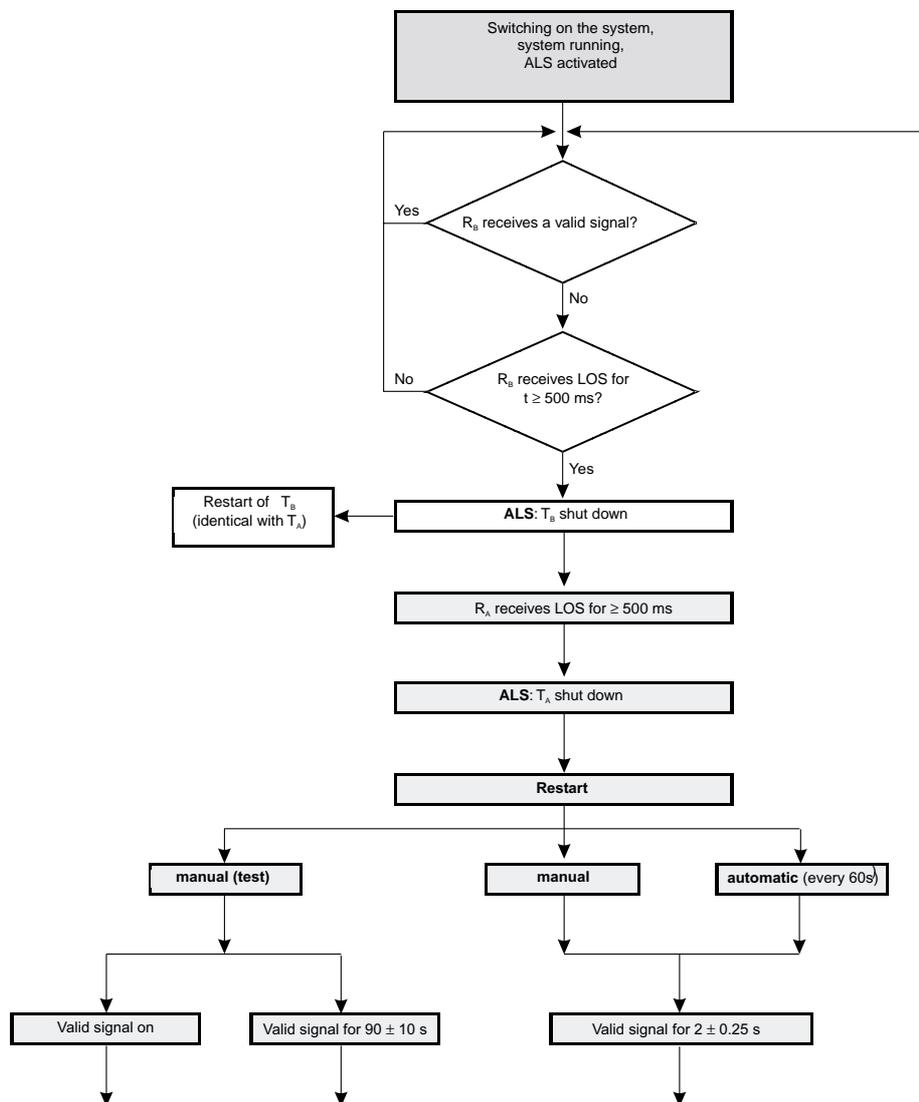
Port monitoring mode

Overview   The setting of the port monitoring mode determines whether an incoming port signal will be monitored for defects. By means of the *WaveStar*® CIT, you can configure the port monitoring mode of each incoming port to "automatic" (***Auto***), ***Monitored*** or ***Not Monitored***.

Meaning of the port monitoring modes   The meaning of the different port monitoring modes is as follows:

- ***Auto***
  Port monitoring is disabled. However, as soon as a valid input signal is detected, the port monitoring mode is automatically switched to ***Monitored***. ***Auto*** is the default setting.

- ***Monitored***
  The incoming port signal is monitored for defects.

- ***Not Monitored***
  Port monitoring is disabled, the incoming port signal is not monitored for defects.

Setting the port monitoring mode   For information on how to set the port monitoring mode for a particular port, please refer to "Setting the port monitoring mode" (5-19).

Forward error correction

Overview   Forward Error Correction (FEC) makes it possible to improve the optical signal-to-noise ratio (OSNR), and thus to lower the bit error ratio, of an optical line signal by adding redundant information. This redundant information can then be used to correct bit errors that unavoidably occur when an optical line signal is transmitted over longer distances over an optical fiber.

Two types of forward error correction   *WaveStar*® TDM 10G (STM-64) systems support two types of Forward Error Correction:

- *In-band FEC (also referred to as "multibit F*EC")
  The redundant information is stored and transported in previously unused overhead bytes, the framing structure as well as the bit rate remain unchanged.

- *Out-of-band FEC (also referred to as "strong F*EC")
  The redundant information is appended to the original signal resulting in an optical signal with a modified framing structure and extended bit rate. The bit rate is increased by approx. 7%. The new signal format is referred to as "Optical Channel" at the corresponding bit rate.

Functional principle   The following figure depicts the functional principle of the Forward Error Correction.
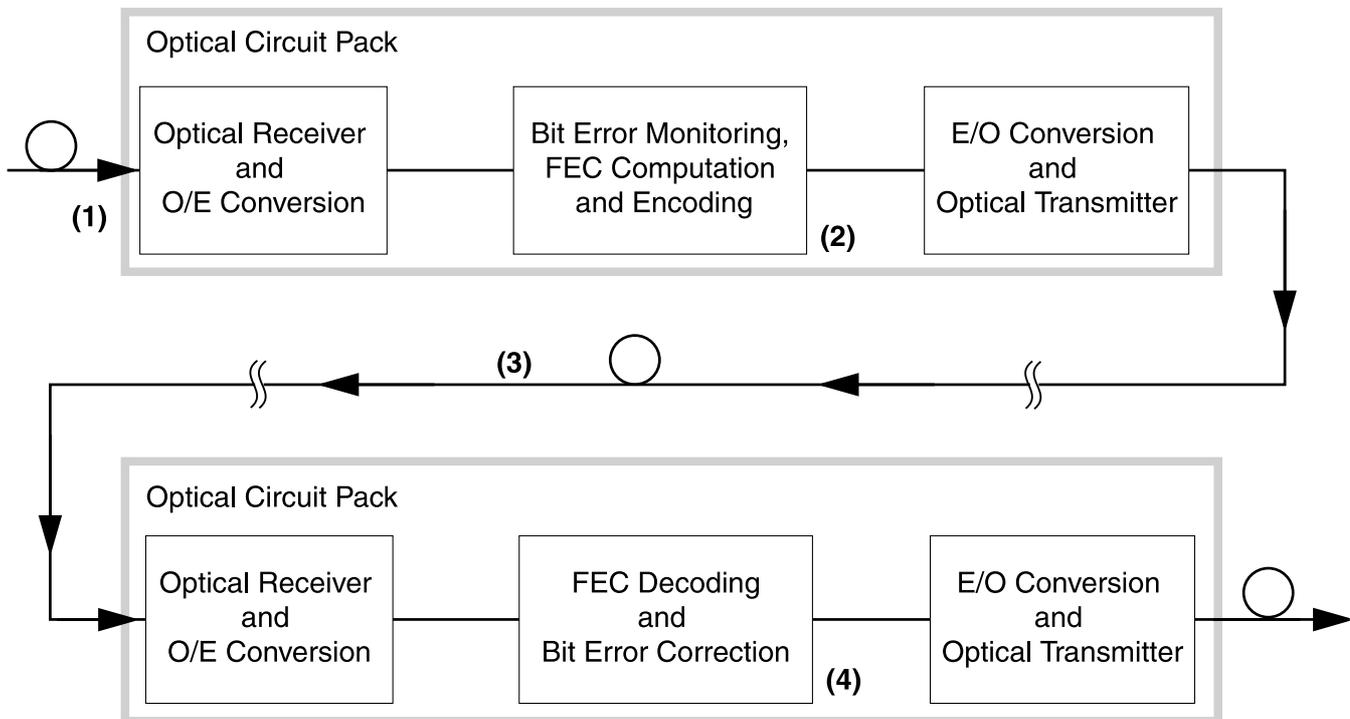
Following an opto-electrical conversion, the bit error ratio in the incoming optical signal (1) is calculated. The FEC algoritm is computed and the redundant information added to the signal (2).

The modified transmit signal is then transported over a transmission line (3) after an electro-optical conversion. The quality of the optical transmit signal is usually decreased by interfering noise, caused among others by chromatical dispersion for instance.

The again opto-electrically converted receive signal is evaluated in the receiver circuit pack, and the FEC information is extracted. Bit errors can now be corrected by using this information (4).

The resulting signal is characterized by a significantly improved BER.

FEC support in STM-64 systems

WaveStar TDM 10G (STM-64) systems support Forward Error Correction for STM-64 signals:

- **In-band FEC**
  WaveStar TDM 10G (STM-64) systems make use of a proprietary BCH-2 algorithm for in-band FEC. The BCH-2 algorithm is a 4-times bit-interleaved 2-bit error correcting BCH algorithm on a row-by-row basis using a block size of 2^{16}. In-band FEC yields an OSNR improvment of approx. 3 dB at a BER of 10^{-12}. It is primarily used to compensate insufficiencies of optical components.

- **Out-of-band FEC**
  WaveStar TDM 10G (STM-64) systems make use of an RS(255,239) Reed-Solomon code for out-of-band FEC in acc. with ITU-T Rec. G.975. The RS(255,239) Reed-Solomon code is a 16-times byte-interleaved systematic linear cyclic block code. Out-of-band FEC yields an OSNR improvment of approx. 5 dB at a BER of 10^{-12}. It enables high-speed transmission more reliably and for longer distances.

Please refer to the following table for information which OC192/STM64 circuit pack variants support which type of FEC.

Circuit Pack	In-band FEC (Prop. BCH-2)	Out-of-band FEC (RS(255,239))
OC192/STM64 1.5SR1 (LEY67)	X	–
OC192/STM64 1.5IRS1 (LEY97)	X	X
OC192/STM64 WDM... (LEY201 .. LEY240)	X	X

Operations interfaces

Overview

Purpose   This chapter provides information about the operations interfaces

Contents

User panel

....

Overview Each shelf is handled separately. Therefore alarms and status indications of the extension shelf are not displayed on the user panel of the main shelf. The main shelf has a single user panel and is therefore handled as one shelf in user panel view although it consists of a high speed and a low speed part.

Alarm LEDs Each alarm signalled at the user panel or via the office alarm interface (cf. "Office alarms interface" (16-52)) is assigned one of the following alarm severities:

- Critical (CR),

- Major (MJ), or

- Minor (MN).

An alarm LED (CR, MJ or MN) is lit, if at least one alarm of the corresponding severity is present.

Alarm confirmation

Alarms can be confirmed by pushing the ACO button (see "Alarm cut-off" (16-43)). The alarm LEDs currently lit are switched off when the ACO button is pushed. Simultaneously the ACO LED is lit as a reminder of the alarms confirmed. If a new alarm is detected afterwards, then the ACO LED is switched off, and the alarm LEDs are lit according to the current alarm status.

Alarm cut-off A local control button (ACO button) is provided on the user panel for local office alarm cut-off for both visual and audible office alarm outputs and the CR, MJ and MN LEDs on the user panel.

Pushing the ACO button on the user panel simultaneously cuts off all existing system alarms indications. The green ACO LED is lit on all user panels with active alarms that have been cut off. When a new alarm is detected all ACO LEDs in the system are turned off until the ACO button is pressed again.

Abnormal conditions The purpose of the ABN LED is to indicate any manually caused potentially service affecting abnormal condition, but not to report failures. The alarm LEDs (CR, MJ, MN) and the PWR ON LED are used for the latter purpose.

The ABN LED is lit when the control system detects manually initiated maintenance activity that could affect service or potentially mask the reporting of service affecting failures.

....

These maintenance activities include the following:

- Any protection lock-out (including low speed, line, and internal timing packs),

- Any forced switch (including low speed, line, and clock mode),

- Any manual switch (including line, low speed, and internal timing packs), except a manual line switch when the Terminal is provisioned for a 1+1 protection switching algorithm (Terminals only, both linear and ring configu-rations),

- timing reference, forced or manual switch (Terminals only, both linear and ring configurations),

- Protection line accessed (non-preemptable linear protection access),

- Protection line accessed (preemptable linear protection access),

- Electronic Loopbacks.

The ABN LED is not lighted for tests or "diagnostics".

Near-end Activity (NE ACTY)

The near-end activity (NE ACTY) LED on the user panel indicates exceptional events and conditions at the local WaveStar™ TDM 10G (STM-64) network element not resulting in an alarm, such as:

- when a Wait-To-Restore (WTR) condition is present,

- during software download is ongoing, or

- when a revertive switch condition is present.

The NE ACTY LED extinguishes when all events are cleared.

Far-end Activity (FE ACTY)

The far-end activity (FE ACTY) LED on the user panel reflects the state of the ring activities within the same SDH maintenance subnetwork using received K bytes for Automatic Protection Switching (APS).

The purpose of this LED is to indicate that a failure has occurred or some activity has taken place at a far-end NE, and that the cause is not located within the local NE.

The FE ACTY LED is lit if one of the following conditions is present:

- The received K1 byte indicates an Automatic Protection Switching (APS) request, i.e. the composition of the K1 byte (bits 1-4) is any value other than '0000'.

- Any of the following three ring protection switch commands was initiated at the far-end NE:

  - Lockout of Service - Ring Switch,

  - Lockout of Service - Span Switch (BLSR only),

  - Lockout of Protection - All Spans.

LED test You can test the user panel and circuit pack LEDs by pushing the
LED TEST button on the user panel.

During a test cycle the LEDs are activated for 2 seconds and then
deactivated for 2 seconds three times in sequence. The LEDs return to
their actual state after the test.

Important! The PWR ON LED on the user panel and the fan unit
LEDs are not affected by the LED test. After an LED test, the
restoration of the LED state before the test may be delayed for some
seconds on single circuit packs.

User panel indicators and controls

Overview   The user panel of the *WaveStar*® TDM 10G (STM-64) system provides visual status indicators as well as various control buttons and connectors.

Structure   The following diagram illustrates the User Panel.
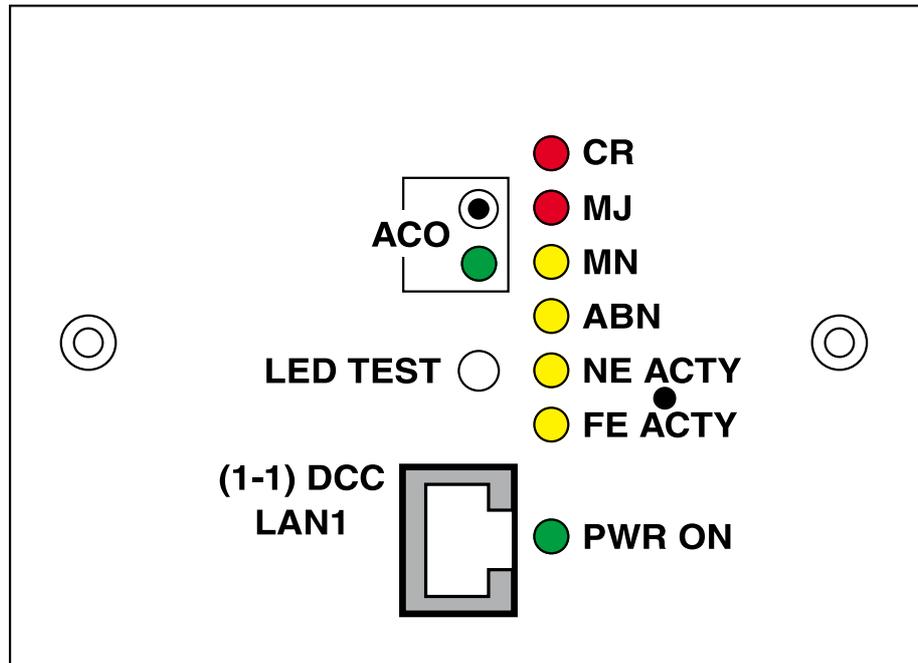
Visual indicators   Each user panel is equipped with the following LEDs:

LED	Function
CR (red)	Indicates that at least one critical alarm is present.
MJ (red)	Indicates that at least one major alarm is present
MN (yellow)	Indicates that at least one minor alarm is present.
ABN (yellow)	Indicates abnormal conditions – temporary conditions that may potentially be service affecting. Please refer to "Abnormal conditions" (16-43).
NE ACTY (yellow)	Indicates near-end activity – status condition at the local terminal, such as a software download. Please refer to "Near-end Activity (NE ACTY)" (16-44).

LED	Function
FE ACTY (yellow)	Indicates far-end activity – status condition indicating a failure which is not located within the local terminal. Please refer to "Far-end Activity (FE ACTY)" (16-44).
PWR ON (green)	Indicates that power is applied to the shelf. The LED is on if either 48V feeder is on.
ACO (green)	Indicates that the ACO button (see "Controls and connectors" (16-47)) was pressed. Please refer to "Alarm cut-off" (16-43).

Controls and connectors   In addition to the LEDs, each user panel is equipped with the following controls and connectors:

Control/ connector	Function
LED TEST	An LED test button for testing all shelf LEDs (except PWR ON on the user panel and the fan unit LEDs). Please refer to "LED test" (16-45).
ACO	An alarm cut-off button to suppress both visual and audible alarm indications. Please refer to "Alarm cut-off" (16-43).
CIT	An RJ-45 connector for connecting a *WaveStar* TDM 10G Customer Interface Terminal (CIT) to the system LAN.

ACO interaction with an alarm test

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

Alarm test sequence   When an alarm test is being performed (Please refer to "Performing an office alarm test" (5-36)), the following sequence of indications occurs:

1   All alarm indicators mentioned above are switched off for five seconds.

If the ACO LED was lit before the test, it goes off. Pushing the ACO button has no effect.

2   The CR and MJ LEDs on the user panel and the rack alarm lamp for prompt alarms are switched on for five seconds.

The indicators can be switched off and the ACO LED be switched on by pushing the ACO button. The indicators as well as the ACO LED are switched off automatically when the five-seconds interval has elapsed.

3   The MN LED on the user panel and the rack alarm lamp for deferred alarms are switched on for five seconds.

The indicators can be switched off and the ACO LED be switched on by pushing the ACO button. The indicators as well as the ACO LED are switched off automatically when the five seconds interval has elapsed.

4   Stage 2 to Stage 3 are repeated according to the specified number of iterations.

5   All alarm indicators as well as the ACO LED (if previously lit) are switched off for five seconds.

Pushing the ACO button has no effect.

6   The control of the alarm indicators is returned to the control system to reflect the actual system status.

Circuit pack status indicators

Overview   All circuit packs are equipped with a red fault LED ("FAULT") and a green activity LED ("ACTIVE") located on the circuit pack faceplate.

LED placement   The following figure illustrates the placement of these LEDs on the circuit pack faceplates of two exemplary circuit packs.

ACTIVE LED   The green ACTIVE LED is used to indicate the activity state of an operational circuit pack. An operational circuit pack can be either in service (LED on) or in the standby mode (LED off). A flashing ACTIVE LED indicates that a circuit pack is in the initialization or self-test phase or that a software download is ongoing.

FAULT LED   The red Fault LED is used to indicate failures attributable to the relevant circuit pack. Please refer to "Circuit pack status indications" (16-50) or "Fault LED on circuit packs" (16-12).

Indications on insertion of circuit packs   The following sequence of indications will occur when you insert a circuit pack into its slot:

1. The red FAULT LED is lit.

2. The FAULT LED goes off, and the green ACTIVE LED flashes as the circuit pack is initialized, self-tests are performed and software is downloaded.

3. The ACTIVE LED stops flashing and

    a. is lit after the circuit pack or at least one port on a multi-port circuit pack becomes active.
    or

    b. goes off if the circuit pack is in the standby mode.

The green ACTIVE LED will be switched off and the red FAULT LED switched on if a failure is detected during initialization, self-test or software download.

The reason why the red FAULT LED is lit immediately after circuit pack insertion is that if you insert a circuit pack with a defective controller the red LED remains lit.

Circuit pack status indications The following table provides an overview of the *WaveStar*® TDM 10G (STM-64) circuit pack status indications.

Operational State	Status	FAULT LED	ACTIVE LED
Circuit pack not yet operational	Powering-up (immediately after circuit pack insertion) (This circuit pack state may not be clearly recognizable depending on the duration of the power-up cycle and the time needed to start initialization.)	X	–
	Initialization	–	¤
	Self-test		
	Software download		
	Failure detected during initialization, self-test or software download	X	–
Active	No failure	–	X
	Failure of the circuit pack hardware	X	X
	Failure of an input signal	¤	X
Standby	No failure	–	–
	Failure of the circuit pack hardware	X	–
	Failure of an input signal	¤	–

Explanation:

X LED is continously lit; – LED is off; ¤ LED flashes (0.5 s on, 0.5 s off)

Important! A failure of an input signal is a failure detected at the input of at least one of the input ports of the circuit pack. A circuit pack input port may be a power supply, timing, control or transmission port.

References For more information on *WaveStar* TDM 10G (STM-64) circuit packs, please refer to the *WaveStar* TDM 10G (STM-64) Applications, Planning, and Ordering Guide.

Fan unit LEDs and controls

....

LEDs   **Important!** The FAIL LED indicates both service-affecting and non-service-affecting alarms. The FILTER ALM LED indicates only non-service-affecting alarms.

The fan unit provides the following and indicators:

LED	Function
PWR ON (green)	Lights when the fan is supplied with -48 V power.
FAIL LED (red)	Lights when there is an alarm of any type associated with the fan unit (for example, a fan in the unit fails).
FILTER ALM (red)	Lights when the fan filter needs attention (for example, the filter is dirty and must be replaced).

Controls   The fan unit provides the following controls:

Control	Function
Filter alarm reset button	Resets the FILTER ALM LED after the alarm condition is resolved.
Two flush-mounted -48 V circuit breakers (A, B)	Protection against current overload.

....

365-371-522   **Lucent Technologies**   16 - 5 1
Issue b, October 2001

Office alarms interface

....

Overview   The office alarms interface is a set of discrete relays controlling audible and visible office alarms. Separate relays handle critical, major, and minor alarms. If desired, CR and MJ alarm outputs can be wired so that either, neither, or both of the outputs control the prompt office alarm. The latter is the recommended configuration for *WaveStar*® TDM 10G (STM-64) systems, i.e. both the CR and MJ alarm outputs control the prompt office alarm.

Rack alarm lamps   The rack alarm lamps located at the rack top are used for visual office alarm signalling. The red lamp indicates prompt alarms having a severity of CR or MJ. The yellow lamp indicates deferred alarms having a severity of MN.

The following figure illustrates the rack alarm lamps at the rack top.
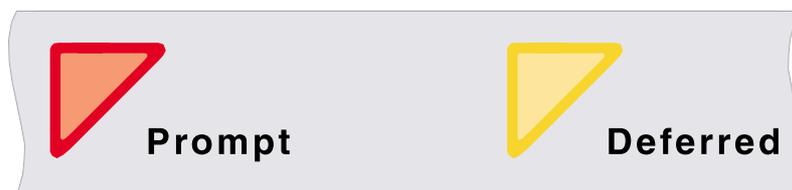
Intermittent failures   To prevent intermittent failures from causing unnecessary maintenance activity, a provisionable incoming signal alarm delay is provided. The office alarms will not be activated unless an incoming signal condition of greater duration than the alarm delay occurs. When a failure clears, an alarm clear delay prevents premature clearing of the alarm.

Multiple alarms   When multiple alarm conditions occur, the highest level office alarm (audible and visible) is activated. When the highest level alarm condition clears, the office alarm "bumps down" to the next highest level alarm condition.

⌐

....

17 Timing provisioning concepts

Overview

Purpose
This chapter describes the timing features *WaveStar*® TDM 10G (STM-64) provides.

WaveStar TDM 10G synchronizes all incoming and outgoing signals to one timing source which is normally locked to an external reference signal. This reference signal is configurable. Various signals can be used as a timing reference signal. Furthermore *WaveStar* TDM 10G provides different clock modes (see "Clock modes" (17-2). Clock protection can also be established by using two timing generator circuit packs within one shelf.

More detailed information on the timing concept is given in the section *"Synchronization"* in the *WaveStar* TDM 10G (STM-64) *Applications, Planning, and Ordering Guide, chapter 4, "Product Description"*.

Contents

⌐

Timing generator

Function of the timing generator

WaveStar® TDM 10G synchronizes all add, drop and through signals by using one timing source. The timing is ensured by the TMG/STRAT 3 circuit packs which generate one common internal clock. The master timing generator for all configurations is located in the low-speed part of the Main Shelf. The output clock signals of the slave timing generators in the high-speed part of the Main Shelf and, if any, in the Extension Shelf, are coupled to the output clock of the master.

The timing generator and the clock distribution within the network elements is described in more detail in the section *"Synchronization"* in the *WaveStar* TDM 10G (STM-64) *Applications, Planning, and Ordering Guide, chapter 4, "Product Description"*.

Clock modes

The *WaveStar* TDM 10G timing generator circuit packs can run in the following clock modes:

- Free-running operation
  The active timing generator circuit pack is not locked to an external timing reference, but the standby timing generator is locked to the active one.

- Holdover mode
  The active timing generator circuit pack enters the holdover mode if all timing reference signals fail. The active timing generator keeps its internal oscillator at the point at which it was synchronized to the last known good reference signal. The standby timing generator remains locked to the active one.

- Locked mode, internal SDH Equipment Clock (SEC) locked to:

  - One of the two external netclock inputs (2048 kHz or 2048 kbit/s)

  - One STM-64 line input (choice of input is provisionable)

  - Up to six line inputs STM1, STM4, STM16 or STM64 are possible, if they are only even slots, only on first port, max. 4 lines in HS and max 4 lines in LS, not referenced from expansion shelfs and only worker port of 1+1 MSP group.

Timing configuration

....

Querying timing configuration The *WaveStar*® CIT allows you to query the timing configuration of the *WaveStar* TDM 10G (STM-64). Please refer to "Viewing the timing configuration" (6-2).

Timing configuration In the menu **Configuration** → **Timing/Sync...** it is possible to change the timing configuration.

This includes:

- the configuration of the external timing input ports (cf. "Configuring the external timing input ports" (6-12))

- the configuration of the external output port (cf. "Configuring the external timing output ports" (6-14))

- the selection and configuration of the timing references (cf. "Configuring the timing references" (6-17))

- the configuration of the system timing, this means the configuration of the master timing generator (cf. "Configuring the system timing" (6-21))

⌐

....

365-371-522   **Lucent Technologies**   1 7 - 3
Issue b, October 2001

Timing quality

Timing marker The timing quality of all SDH data signals is coded in the timing marker (Synchronization Status Marker, SSM) as per ITU-T Rec. G.783 and G.707. The timing marker is located in the lower four bits of the S1 byte of the STM-N signal SOH.

The bit combinations are listed in the following table. The remaining combinations are interpreted as "invalid".

S1 Bits	Quality level
0010	Primary Reference Clock
0100	SSU Transit Node Traceable
1000	SSU Local Node Traceable
1011	SDH Equipment Clock Traceable
1111	Do not use for Synchronization (DUS)

The quality level "DUS" is inserted if AIS, LOS or LOF is detected in the incoming signal. Insertion of "DUS" in an outgoing timing signal can also be configured by the operator in order to avoid timing loops in the network.

SSM of lower quality than the internal system clock If the SSM of a reference clock source indicates a lower quality than the internal clock (SEC), this reference is considered to be failed and the system switches to the reference with the highest quality (above SEC), if SSM is enabled.

The selection criteria are:

- signals which are not locked out and have their priority not disabled
- signals with highest quality
- if there is more than one signal with highest quality the one with the priority is selected
- if there is more than one signal with highest priority one of those is chossen randomly.

When all assigned references are considered to be failed, the system enters the holdover mode.

No SSM available As long as no SSM value has been accepted and evaluated at STM-N interfaces, DUS is assumed. This also applies at the initial system start-up.

SSM for 2048 kbit/s synchronization signals   *WaveStar*® TDM 10G supports the interpretation and generation of SSM values for framed 2048 kbit/s timing input and output ports ("G.703.9 ports"). The coding conforms to ITU-T Rec. G.704. One set of the S_{a4} to S_{a8} bits can be allocated for the Synchronization Status Marker (SSM). The message set is similar to the SSM messages defined for bits 5 to 8 of the byte S1 belonging to an SDH signal.

User operation   You can provision the SSM mode for the selection of the timing reference from which the system timing is derived. The possible values are **enabled** or **disabled**. Furthermore, you can define the quality level of the outgoing timing signal for SDH timing signals.

⌐

Timing protection

**Timing reference
protection switching**

During configuration of the timing references, a priority list is created for the configured timing reference signals. The signal with the highest priority is initially used as the timing reference signal. If it fails, the system switches to the signal with the next lower priority. If all possible timing reference signals fail, the timing generator enters the holdover mode.

The following signals can be used as a timing reference:

- 2 external netclock input signals (2048 kHz or 2048 kbit/s acc. to G.703)

- Up to six line inputs STM1, STM4, STM16 or STM64 are possible, if they are only even slots, only on first port, max. 4 lines in HS and max 4 lines in LS, not referenced from expansion shelfs and only worker port of 1+1 MSP group.

The following alarms cause a protection switch from a G.703 2048 kbit/s signal to another timing reference signal (acc. to the priority list):

- SSF (Server Signal Fail)
    - LOS (Loss of Signal)
    - AIS (Alarm Indication Signal)
    - LOF (Loss of Frame)
    - LOM (Loss of Multiframe)
- DFF (Defect Frequency Fail)

The following alarm causes a protection switch from a G.703 2048 kHz signal to another timing reference signal (acc. to the priority list):

- Loss of Signal

The following alarms and fault criteria cause a protections switch from an SDH signal to another timing reference signal (acc. to the priority list):

- LOS
- AIS
- LOF
- LOM
- EXC (Excessive Bit Error Ratio)

Lucent Technologies

Timing equipment protection switching

There are two timing circuit packs TMG 0 and TMG 1 in the high-speed part and two in the low-speed part of each network element. Thus there are four timing circuit packs in each main shelf. Furthermore, there are two timing circuit packs in each extension shelf.

When two timing circuit packs are present the timing is derived from one circuit pack, called the *active* timing circuit pack. The other timing circuit pack is standby. It is locked to the active clock and produces a timing signal, which is not used, unless the active timing circuit pack fails.

For the initial start-up of the system and initial provisioning of the 1+1 protection group, the default state of operation is TMG 0 as the active timing circuit pack. For the system reset after the 1+1 protection was in operation, the system restores the timing circuit pack as the active one which was active before the system reset operation.

Wait-to-restore time

The timing reference protection is working in a revertive mode (only if the signal after the WTR is selected highest quality and highest priority). If a timing reference is restored the system has to make a wait for a defined time (wait-to-restore time, WTR) to see whether the signal is stable, before the system switches back to it. There is no protection switch if the system clock already was on reference with the same qualification.

18   Traffic provisioning concepts

Overview

Purpose
This chapter gives important background information on the cross-connection management and the Cross-Connection Wizard of the *WaveStar*® TDM 10G (STM-64).

Contents

⌐

Cross-connection management

....

Overview The *WaveStar*® TDM 10G (STM-64) add/drop multiplexer in its basic configuration is a single shelf that interfaces electrical STM-1, optical STM-1, optical STM-4 and optical STM-16 lines to an SDH-standard 2-fiber MS-SPRing protected ring. It has 16 tributary slots that support flexible optical and electrical port unit mixing. If additional capacity for tributary port units is required, the system can be expanded with one or more extension shelfs.

Definitions **Port** A physical transmission interface, consisting of both an input and an output, which may be used to carry traffic between network elements. Operational differences between ports determined by port provisioning include pointer processing, fault and performance monitoring, path maintenance (e.g. Unequipped, AIS, RDI), cross-connections (supported rates), and protection switching.

Port protection group A user-provisioned association of optical interface ports which is used for protection in a particular type of network configuration. Three types of port protection groups are defined:

- 2-fiber MS-SPRing port protection group used for SDH 1+1 MS-SPRing

- 1+1 port protection group used for SDH 1+1 Multiplex Section Protection (MSP)

- 1:1 port protection group used for STM-64 1:1 Multiplex Section Protection (MSP) The operations on a port protection group include the provisioning, control, and status of the protection switching.

Tributary A path-level unit of bandwidth within a port, or the signal(s) being carried in this unit of bandwidth, e.g. a VC-3 or VC-4 within an STM-N port.

Cross-connection A reconfigurable SDH path-level interconnection within a network element between input and output tributaries of specific ports.

Cross-connection leg A one-way connection provisioned from one input tributary to one output tributary. Each leg is identified as an entity by its input and output tributaries, its cross-connection rate, and the type of cross-connection it is part of. A leg pair is a pair of cross-connection legs which are reported as a two-way connection between two tributaries.

Cross-connection types   All meaningful cross-connection types can be reduced to three basic types:

- 1way point-to-point connection

Source	Sink
Sink	Source
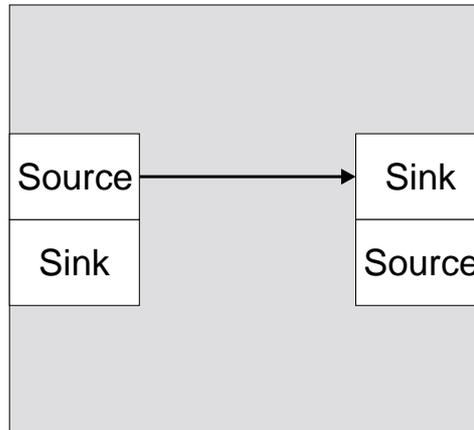
- 1way point-to-multipoint connection (broadcasting/multi-casting)

Source	Sink
Sink	Source
Source Sink	

- 2way connection

Source	Sink
Sink	Source
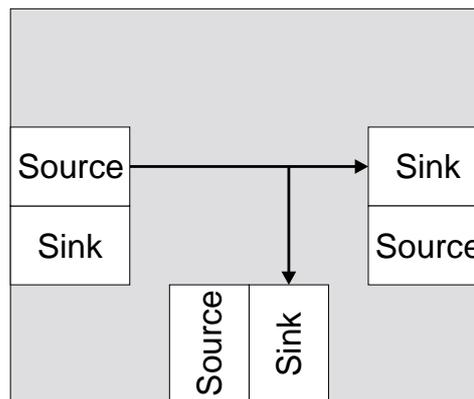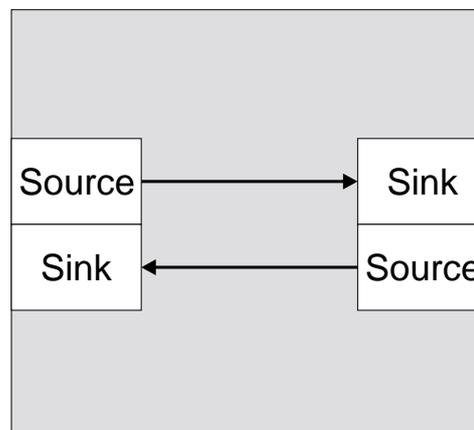
You can provision and reconfigure cross-connections. *WaveStar* TDM 10G provides an STM-1 rate time-slot-assignment capability that supports the following types of cross-connections, which are derived from the three basic types introduced above:

- 1-way point-to-point

- 2-way point-to-point

- 1-way path protected (for Dual Node Ring Interworking (DNI) applications only)

- 1-way adjunct path protected (for DNI applications only)

- Dual Node Ring Interworking (bidirectional) with four nodes

- Dual Node Ring Interworking (bidirectional) with collapsed nodes

- Bidirectional Sub-Network Connection Protection (SNCP)

- Ring-to-ring SNCP

Transmission interfaces *WaveStar* TDM 10G (STM-64) includes the following optical and electrical port units:

Interface type	Transmission rate	Wavelength
Optical	STM-1	1.3 μm (long reach)
	STM-4	1.3 μm (short reach)
	STM-16	1.3 μm (long reach)
		1.5 μm (long reach)
	STM-64	1.5 μm (intermediate reach)
Electrical	STM-1 (Each unit contains four independent bidirectional ports.)	—

Switch capacity The 192 x 192 switch fabric of the *WaveStar* TDM 10G supports simultaneous cross-connections from each of up to 128 source STM-1 equivalents to all of the up to 128 sink STM-1 equivalents. The cross-connections are fully non-blocking.

Cross-connection levels The following cross-connection levels are supported in *WaveStar* TDM 10G (STM-64):

- VC-3

- VC-4

- VC-4-4c (Concatenated VC-4)

- VC-4-16c (Concatenated VC-4)

Inter-MS-SPRing connection

Normally, through-connections between the west and east aggregate interfaces in an ADM are handled by timeslot assignments (TSA), which means that e.g. STM-1 #27 in the incoming STM-64 signal (west) is assigned to STM-1 #27 in the outgoing STM-64 signal (east). The complete STM-64 traffic can be MS-SPRing protected. However, there might be cases where a timeslot interchange (TSI) is required for such through connections (e.g. interchanging timeslots STM-1 #27 from the incoming STM-64 signal (west) with timeslot STM-1 #14 in the outgoing STM-64 signal (east)). TSI is possible as well, but please note that the resulting connection will not be covered by MS-SPRing protection.

The same applies to STM-16 MS-SPRing protected rings attached to the *WaveStar* TDM 10G (STM-64).

Output mode

The cross-connection output mode is a provisionable parameter

- for the destination-to-source direction, and/or

- for the source-to-destination direction.

If some of the facilities are not in place whenever the cross-connection is being established, then you can provision this field as AIS or IDLE/UNEQ and an AIS or an unequipped signal will be inserted to function as a keep-alive signal.

If all of the involved facilities are in place when the cross-connection is established, the field should be provisioned as NORMAL. The end-to-end signal path is then established and the signal can be passed.

Cross-connection wizard

Overview Cross-connections may be configured using the *WaveStar*® CIT Cross-Connection Wizard. The Cross-Connection wizard is opened by selecting the menu sequence **Configuration → Cross Connection** from the system view of the CIT. The wizard will lead you through a series of windows in which you can identify all the attributes of the cross-connection.

Cross-connection sequence Creating or modifying a cross-connection involves the following sequence:

1. Complete all port provisioning and protection provisioning (not needed for 1:1 cross-connections) before creating a cross-connection.

2. Some of the steps involved in setting up a cross-connection will have already been made if a reservation has been made on one or more of the tributaries involved in the cross-connection.

3. Select the rate, cross-connection type, and ports involved in the cross-connection.

4. Identify the tributaries for the cross-connection from a display of tributaries corresponding to the selected ports.

5. Complete the cross-connection by selecting cross-connection parameters and the source and destination TIDs needed for a ring squelch map.

Cross-connection wizard action window The cross-connection action selection window appears when the Cross-Connection Wizard is opened. The cross-connection action selection window allows you to select whether you want to create, modify, or delete a cross-connection. The window options include:

- **Create New** - The Create New option causes the Create New Cross Connection windows to open where you can make the choices necessary to create a new cross-connection.

- **Modify Parameters** - The Modify Parameters option causes the Modify Cross Connection Parameters windows to open where you make the choices necessary to modify a cross-connection.

- **Delete** - The Delete option causes the Delete Cross Connection windows to open where you make the choices necessary to delete a cross-connection or one leg of a protected cross-connection.

- **Roll** - The Roll option causes the Roll Cross Connection Leg windows to open where you can change the source of an existing cross connection.

Access Identifiers For any action on cross-connections you need the Access Identifiers (AID) of the source and destination port of the cross-connection. Please refer to "Overview of access identifiers" (15-18) for the structure of the AIDs.

***Create new cross* connection windows** The following Cross-Connection Wizard window flow allows you to create new cross-connections:

1. The **Rate/Type** window - The **Rate/Type** window allows you to select the cross-connection rate and the cross-connection type.

2. **Source Tributary** window - The **Source Tributary** window allows you to select the source port and tributary for a cross-connection.

3. **Destination Tributary** window - The **Destination Tributary** window allows you to select the destination port and tributary for a cross-connection.

4. **Cross Connection Parameter** window - The **Cross Connection Parameter** window allows you to establish or modify the provisionable parameters for an existing or new cross-connection.

***Rate/Type* window** The **Rate/Type** window allows you to select the cross-connection rate and the cross-connection type. The selection of cross-connection rates may include rates such as VC-3, VC-4, VC-4–4c or VC-4-16c. The cross-connection types are described in "Cross-connection types" (18-3).

***Source Tributary* window** The Source Tributary window allows you to select the source port and tributary for a cross-connection. Port selection is confined to the ports which support the previously chosen cross-connection rate. Protection ports of a 1+1 protection group or ports on the protection unit of a 1:N electrical protection group are not selectable. Protection ports or tributaries of an MS-SPRing or 1:1 protection group may be selected.

Tributaries associated with the selected port are displayed according to the selected cross-connection rate. The following is also displayed for each tributary:

•   AIDs of the tributaries belonging to the selected port are displayed.

•   Availability of the tributaries to be used for the cross-connection source is displayed. Availability (**Avbl**) is **Yes** or **No**.

•   An indication of whether the tributary is a protection tributary is displayed. The indication is working (**Wkg**) or protecting (**Prot**).

Destination Tributary **window**

The **Destination Tributary** window allows you to select the destination tributary for a cross-connection. The Destination Tributary window is the same as the Source Tributary window.

Cross Connection ***Parameter*** **window**

The **Cross Connection Parameter** window allows you to modify provisionable parameters for an existing or new cross-connection. The window may already be populated with defaults or current settings are displayed.

The Parameter window includes the following parameters. Some parameters may not apply to the cross-connection selection and will be greyed out on the window.

- **Src Ring ID** - The Source Ring ID displays the Ring ID associated with the source tributary on a port which is part of an MS-SPRing.

- **Dest. Ring ID** - The Destination Ring ID field lists the Ring ID of a Destination tributary on a port which is part of an MS-SPRing.

- **Src TID** - The Source TID applies to a cross-connection leg which is part of an MS-SPRing. This field displays or lists TIDs you may select to assign as the Source TID.

- **Dest. TID** - The Destination TID applies to a cross-connection leg which is part of an MS-SPRing.

- **Source to Destination Output Mode** - This field allows you to set or display the provisioned output mode for the Source to Destination leg and has the values of **Normal**, **AIS** and **IDLE/UNEQ**.

  - **Normal** refers to a cross-connection which is carrying "normal" traffic.

  - **AIS** is a test and maintenance setting. AIS is transmitted via the respective cross-connection.

  - **IDLE/UNEQ** is a test and maintenance setting. An unequipped signal is transmitted via the respective cross-connection.

- **Destination to Source Output Mode** - This field allows you to set or display the provisioned output mode for the Destination to Source leg and has the values of **Normal**, **AIS** and **IDLE/UNEQ**.

- **XC Type** - This field displays the selected cross-connection type such as 1-way point to point.

- **Action** - This field displays the action you chose to perform, e.g. create or delete.

- **Range** - This field always displays "1".

TID   The Target Identifier (TID) of a network element is its name which can be assigned by the user during the configuration of a network element.

Schematic view   The **Cross Connection Parameter** window provides a schematic view of the selected cross-connections. It displays the cross-connection rate, such as VC-3, VC-4, VC-4–4c and VC-4-16c. Furthermore, it displays the source and destination AIDs of the cross-connection within a schematic diagram which represents the cross connection type by one (1-way) or two (2-way) arrows.

Modify Cross Connection Parameters   The **Modify Cross Connection Parameters** selection invokes the following sequence of wizard windows:

1. Existing Cross Connection Selection window

2. Leg Selection window for any point-to-point or path-protection cross-connection.

3. Cross Connection Parameter window.

Delete Cross Connection   The **Delete Cross Connection** selection invokes the following sequence of wizard windows:

1. Existing Cross Connection Selection window

2. Cross Connection Leg Selection window to allow you to select one or more cross-connection legs for deletion, if applicable.

3. Cross Connection Parameter window.

Roll Cross Connection   The **Roll Cross Connection** selection invokes the following sequence of wizard windows:

1. Existing Cross Connection Selection window

2. Leg Selection window for any point-to-point or path-protection cross-connection.

3. Roll to Tributary Selection window to allow you to select a new source for an existing cross-connection.

4. Cross Connection Parameter window.

Protection mechanisms

....

Overview   The reliability of a transmission system can be considerably increased by means of redundant transmission routes. In the event of a transmission error, e.g. if LOS (Loss of Signal) is signalled due to a cable break, or in the event of an excessive bit error ratio, the signals can be switched to a protection line.

Types   The following types of network protection switching can be realized:

- Path protection (in Dual Node Ring Interworking applications)

- STM-64 and STM-16 2-fiber MS-SPRing

- Sub-Network Connection Protection (SNCP)

- STM-16, STM-4 and STM-1 1+1 Multiplex Section Protection (MSP)

- STM-64 1+1 and 1:1 MSP in Terminal Multiplexer configurations

....

Lucent Technologies

Multiplex Section Protection

Overview In multiplex protection switching, the complete (physical) transmission path between two multiplexers is duplicated. This means that a separate Optical Interface Unit is connected in each multiplexer for the main (working) and standby (protection) section.

1+1 MSP In case of a 1+1 MSP each main line is assigned to one standby line. As for other types of protection switching the signals are duplicated in the transmit direction. In the receive direction, this type of switching either selects, depending on the signal quality, the input signals of the main section or that of the standby section for transmission. The network elements are equipped with an MSP function which carries out the selection and changeover processes. The switching activities are monitored by the K1-K2 byte protocol according to ITU-T Rec. G.783. This takes place in the receive direction on the circuit pack, which is connected to the standby section.

The following figure illustrates the schematic diagram of a 1+1 Multiplex Section Protection.
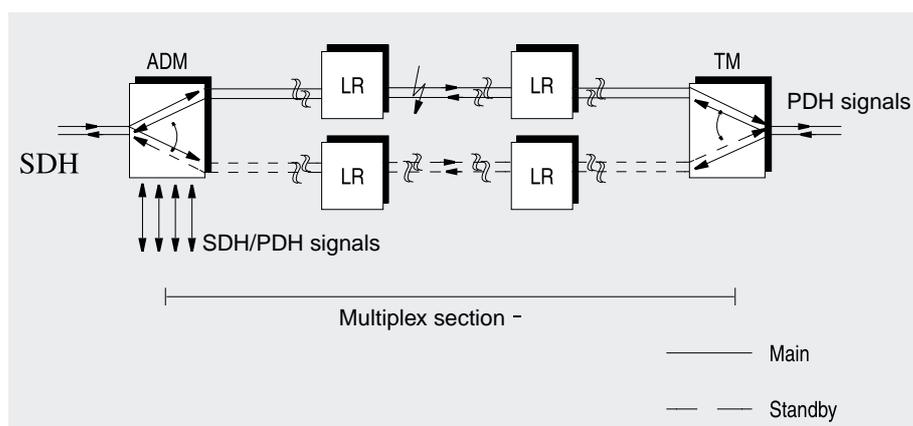
1+1 MSP is implemented in compliance with ITU-T G.841 and ETSI 300 417.

Switching criteria The switchover is triggered by the following switching criteria, which are generated by the MST functional block after evaluation of the SOH:

- *Signal Degrade*(SD)
  Bit error ratio (BER) in the range 10^{-3} ... 10^{-9}

- *Loss of Signal (LOS)*

- *Loss of Frame (LOF)*

- *Multiplex Section Excessive Bit Error Ratio (MS-EXC)*

Bit error ratio $\geq 10^{-3}$

- ***Multiplex Section Alarm Indication Signal (MS-AIS)***

Mode of operation In the *WaveStar*® TDM 10G (STM-64) systems the MSP can be operated in unidirectional or bidirectional and revertive or non-revertive mode each.

DCC protection Together with the creation of an MSP protection group a DCC 1+1 protection can be established. In a unidirectional MSP the DCC protection is operated in non-revertive mode. It is applied to the DCC_R only. In a bidirectional MSP the DCC protection adopts all settings of the MSP group. Thus the DCC protection can be operated in revertive or non-revertive mode. Additionally it is applied to both DCC_M and DCC_R.

1:1 MSP with preemptible protection access For STM-64 optical ports also a 1:1 MSP is possible. In a 1:1 MSP configuration low-priority traffic can be transmitted via the protection port as long as no protection switch occurs. If the traffic of the working section has to be switched to the protection section, the low-priority traffic is lost (1:1 MSP with preemptible protection access).

The 1:1 MSP is working in revertive mode. It can be established as unidirectional or bidirectional protection.

The K1 and K2 bytes of the SOH within the protection section define the Automatic Protection Switch (APS) protocol as defined in ITU-T G.841.

2-fiber MS-SPRing

Overview   A 2-fiber Multiplex Section - Shared Protection Ring (MS-SPRing) is a self-healing ring configuration in which traffic is bidirectional between each pair of adjacent nodes and is protected by redundant bandwidth on the bidirectional lines that interconnect the nodes in the ring. Since traffic flow is bidirectional between nodes, traffic can be added at one node and dropped at the next without traveling around the entire ring. This leaves the spans between other nodes available for additional traffic. Therefore, with many traffic patterns a bidirectional ring can carry much more traffic than the same facilities could carry if configured for a unidirectional ring. Additionally, the protection capacity can be used to provide unprotected transport for extra traffic when no failures are present.

MS-SPRing in *WaveStar*®
TDM 10G (STM-64)   *WaveStar* TDM 10G (STM-64) provides the possibility to configure MS-SPRing for one STM-64 ring and for up to four STM-16 rings per shelf.

The STM-16 and STM-64 2-fiber MS-SPRing is compliant with ETS 300 417 and ITU-T G.841.

Traffic capacity   The following figure shows working and protection traffic capacities in a *WaveStar* TDM 10G (STM-64) 2-fiber MS-SPRing.
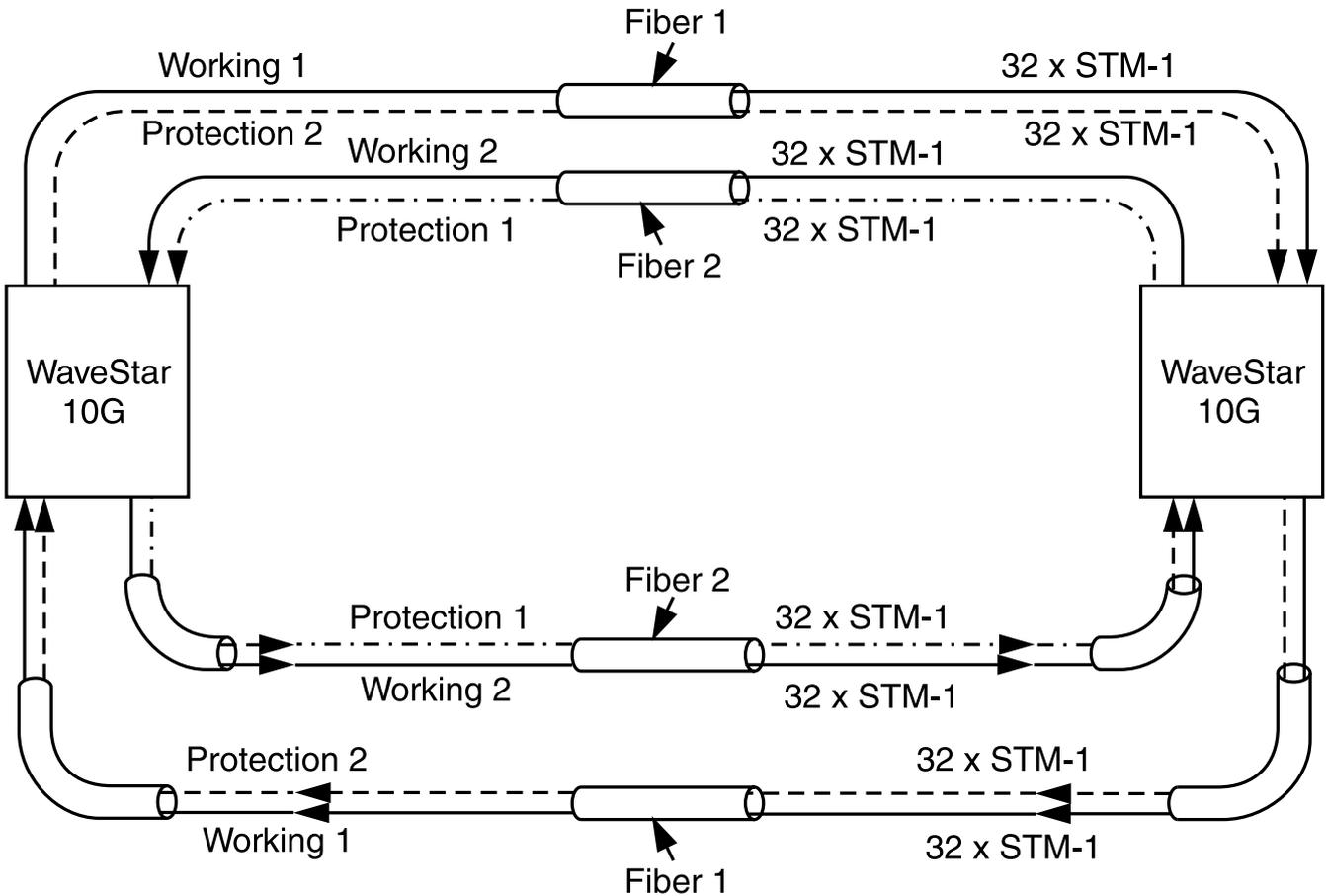
NC-2.5GAPOG-067

Self-healing rings   *WaveStar* TDM 10G (STM-64) 2-fiber MS-SPRings are self healing in that transport is automatically restored after node or fiber failures. In case of STM-64 MS-SPRing, each line carries 32 STM-1 equivalent timeslots of working capacity plus 32 STM-1 equivalent timeslots of protection capacity. For STM-16 MS-SPRing, the working capacity is 8 STM-1 equivalents, the protection capacity 8 STM-1. In the event of a fiber or node failure, service is restored by switching traffic from the working capacity of the failed line to the protection capacity in the opposite direction around the ring. (See "2-fiber MS-SPRing traffic flow" (18-15) and "Fiber cut example" (18-16).)

Low-priority traffic   Unprotected traffic can be established on the protection channels (low-priority traffic). This traffic is preempted in case of a protection switch.

2-fiber MS-SPRing traffic flow The following figure shows normal (non-protection-switched) traffic flow in a *WaveStar* TDM 10G (STM-64) 2-fiber MS-SPRing.
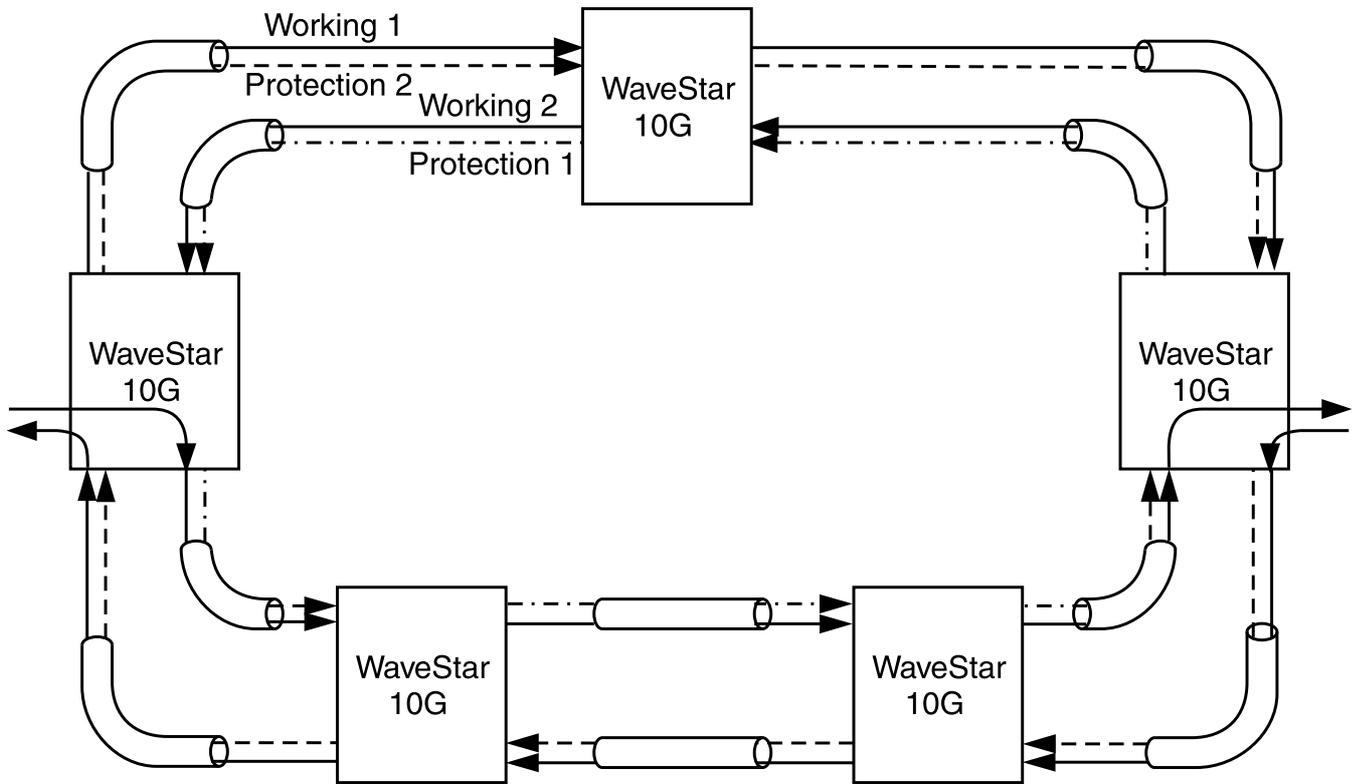
Sdh-10gapog-051

Protection switching When a line-level event triggers a protection switch, the affected nodes switch traffic on to protection capacity and transport it to its destination by looping it back the long way around the ring. (See "Fiber cut example" (18-16).) Service is reestablished on the protection capacity in less than 50 milliseconds after detection of the failure (for catastrophic failures in rings without existing protection switches or extra traffic).

Fiber cut example   The following figure illustrates a 2-fiber MS-SPRing protection switch that results from a fiber cut.
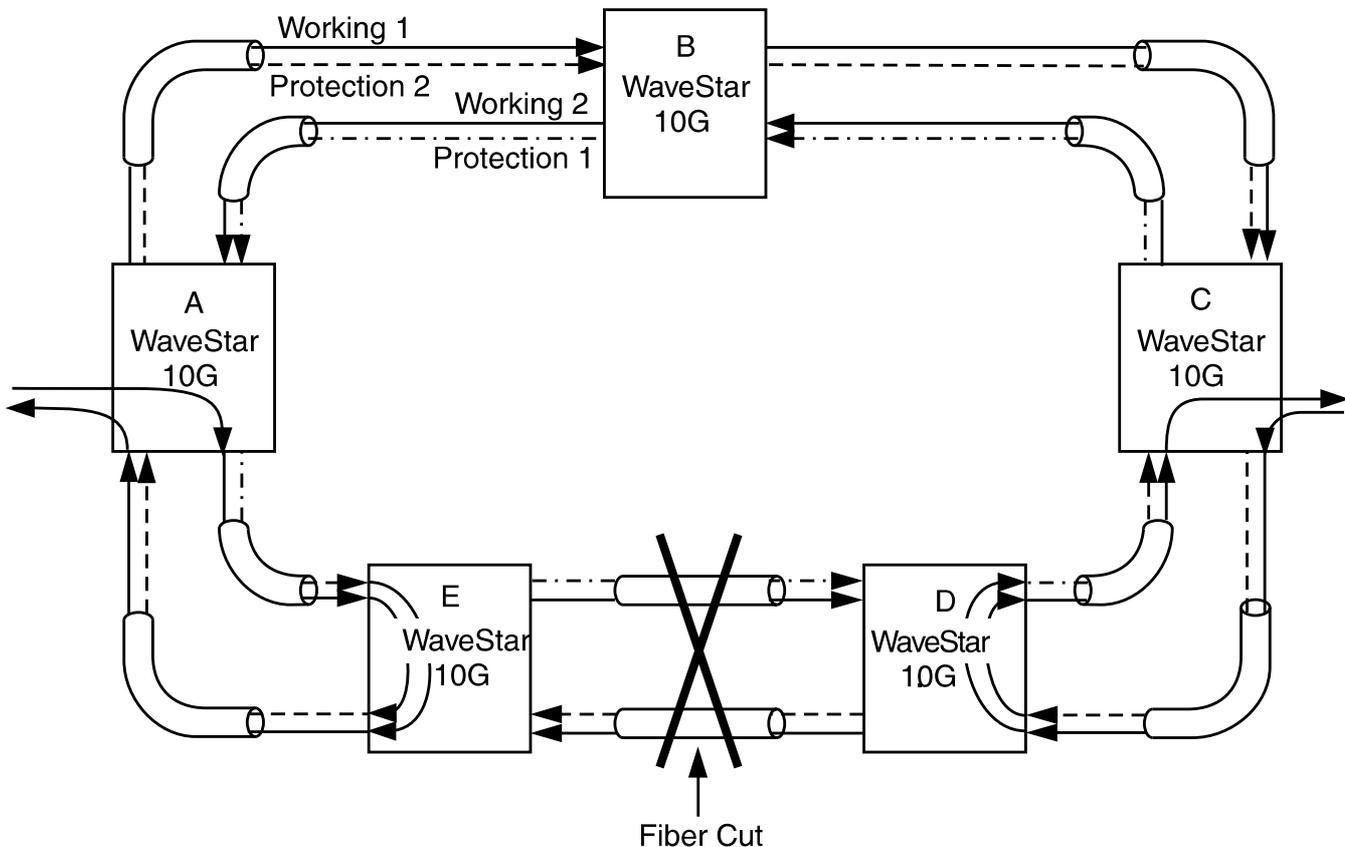
Sdh-10gapog-050

Protection traffic flow   In "Fiber cut example" (18-16), traffic going from Node A to Node C that normally passed through Node E and Node D on "working 2" capacity, is switched onto the "protection 2" capacity of the line leaving Node E in the opposite direction. The traffic loops back around the ring via Node A, B, C, and D (where the loopback switch is active) to Node C. Similarly, traffic going from Node C to Node A that normally passed through Node D and Node E on "working 1" capacity is switched on to the "protection 1" capacity of the line leaving Node D in the opposite direction.

The same approach is used for a node failure. For example, if Node D were to fail, Nodes C and E would perform loopback protection switches to provide an alternate route for ring traffic.

2-fiber MS-SPRing with Non-preemptible Unprotected Traffic (NUT)

Overview Non-preemptible Unprotected Traffic (NUT) offers the possibility to exclude timeslots from the MS-SPRing protection.

NUT allows the operator to selectively exclude individual HO-VCs from the MS-SPRing in a flexible way. This feature extends the traffic availablity and optimizes the utilization of the bandwidth.

Low priority traffic In a normal MS-SPRing the protection bandwidth can be used for low priority traffic, but this traffic is lost, if a protection switch is carried out. In this case the whole working bandwidth is switched to the protection bandwidth.

Non-preemptible Unprotected Traffic A better availability can be achieved by deciding not to access a portion of the protection bandwidth (temporary or definitely), i.e. making some of the protection timeslots unaccessible for protection purposes. The traffic in these timeslots is called ***non-preemptible***. As there is a 1:1 relationship between the working and the protection timeslots, the corresponding working timeslots are thus unprotected. Traffic contained in such working timeslots is called ***Non-preemptible Unprotected Traffic (NUT)***.

The following graphic illustrates the switch behaviour in an MS-SPRing protected network element.
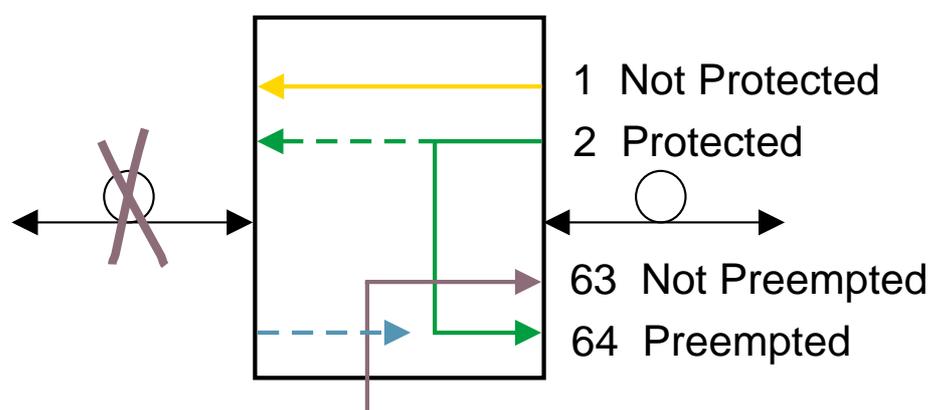
Protection attribute and Local NUT configuration Each timeslot of an MS-SPRing protected optical signal gets an attribute, the ***Protection Attribute***, which indicates whether a working timeslot is protected or not or whether a protected timeslot may be preempted by the MS-SPRing or not.

For working timeslots the following values are possible:

- **Protected**

- **Not Protected**

- **Temporarily Not Protected**

If a timeslot is set to **Temporarily Not Protected**, an alarm is generated in the local NE.

For protection timeslots the following values are possible:

- **Preemptible**

- **Non-Preemptible**

- **Temporarily Non-Preemptible**

As working and protection timeslots are always paired, the value of the Protection Attribute of a working timeslot determines the value of the corresponding protection timeslot.

Local NUT configuration
The *Local NUT configuration* is a table with all timeslot and their corresponding **Protection Attribute** value. It represents the provisioning made by the user *in the local node*.

Operational NUT configuration
The *Operational NUT configuration* provides the real NUT configuration *of the ring*. It contains a unique and identical set of Protection Attributes as they have to be used by the nodes. It must be identical in all nodes.

The Operational NUT configuration is created according to the following rules:

- It is autpoprovisiond out of the Local NUT configurations

- It contains up to 96 entries, one per timeslot

- all default values are set to protected/preemptible

- If in any node the **Protection Attribute** of a certain timeslot is set to **Not Protected/Non-preemptible**, this will be indicated in the Operational NUT configuration and is valid for the whole ring.

- If two or more nodes have the same setting for a specific time slot (**Not Protected** or **Temporarily Not Protected**), this will only be indicated once for the node with the highest Node ID.

Modifications of the Local NUT configuration in any node are broadcasted to all other nodes in the ring via DCC. Settings which have been carried out in a ceratin node can only be modified from the same node. Duplicate settings from two nodes have to be changed in both nodes.

Sub-Network Connection Protection (SNCP)

Overview The principle of a Sub-Network Connection Protection (SNCP) is based on the duplication of the signals to be transmitted and the selection of the best signal available at the sub-network connection termination. The two (identical) signals are routed over two different path segments (Sub-Network Connections, SNCs), one of which is defined as the main SNC and the other as standby SNC. The same applies to the opposite direction (bidirectional SNCP). The system only switches to the standby SNC if the main SNC is faulty.

Sub-Network Connection Protection (SNCP) provides path-level protection for VC-3, VC-4, VC-4-4c, and VC-4-16c signal rates in STM-64, STM,16, STM-4 or STM-1 optical rings. It is possible to add/drop SNCP protected traffic from/to all ports in the NE.

The type of SNCP implemented in this release is an inherent SNCP (SNC/I).

Benefits This feature allows you to provide additional end-to-end survivability for selected circuits in a network comprising any mix of topologies (e.g. ring, mesh, unprotected, multiplex section protection and MS-SPRing).

Topologies The *WaveStar*® CIT Cross-Connection Wizard supports the creation of SNCP protected paths in single rings and in connected rings (ring-to-ring configuration, i.e., one NE connects to two rings). Please note that in the ring-to-ring configuration the full SNCP is available within each ring. The connection between the rings, this means the connection within the network element, is unprotected, because there is no dual node ring interworking.

The following figure shows a single ring SNCP application. SNC 1 is the working (main) SNC, SNC 2 is the protection (standby) SNC in this example. The path termination is always outside the *WaveStar*

TDM 10G (STM-64). For simplification, the SNCP switch is only shown for a unidirectional connection.
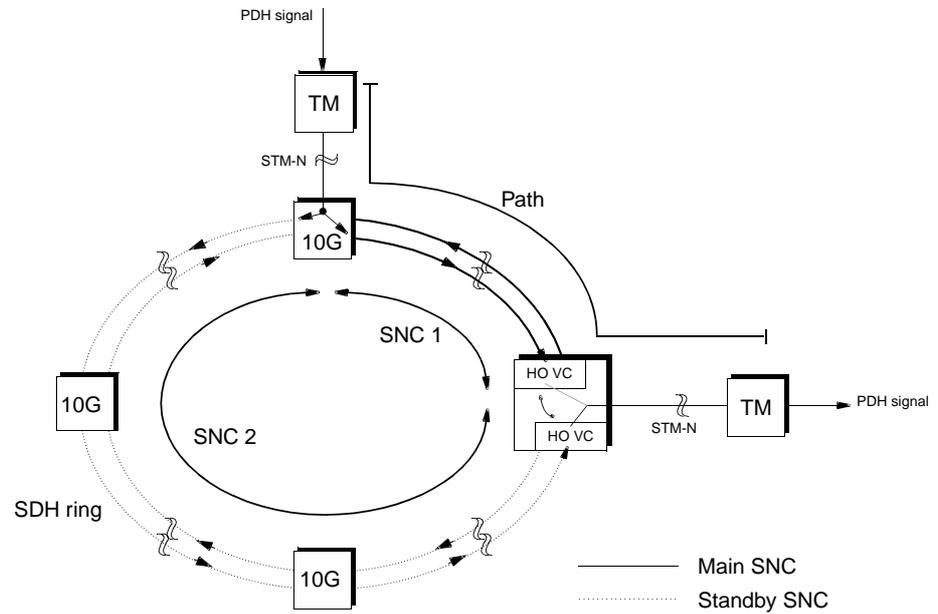
The following figure shows a ring-to-ring SNCP configuration. Here, the SNCP also consists of a broadcast in transmit direction. The signal then moves through the first ring via SNC 1 (working) and SNC 2 (protection). The ring is connected to another ring via one single NE.

For simplification, the SNCP switch is only shown for an unidirectional connection.
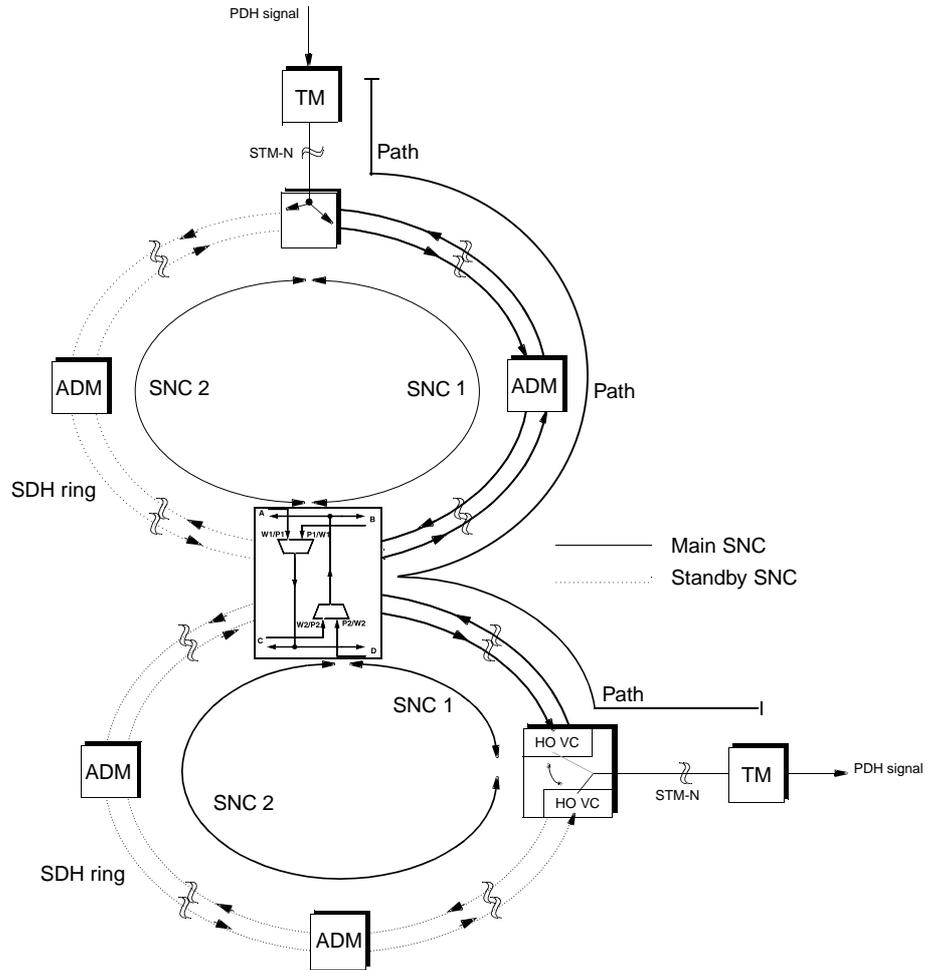
Switching criteria   The following switching criteria trigger an automatic SNCP protection switch

- Signal failure (AUdAIS, AUdLOP, Unequipped)

- Signal degrade

- Circuit pack failure

Controller failures in the NE do not affect the capability of automatic SNCP protection switching.

SNCP protection switching can be configured revertive or non-revertive with *WaveStar* CIT. When revertive switching is configured, a wait-to-restore time can be defined. The default configuration is non-revertive.

Switching time   For automatic SNCP protection switching, the total time to complete the protection switch does not exceed 50 ms. It is possible to provision a hold-off time, i.e. a time period before initiating a switch.

Manual switch   The following manual switching actions are possible with *WaveStar* CIT:

- manual to working: switches the traffic to the main SNC if it is not faulty

- manual to protection: switches the traffic to the standby SNC if it is not faulty

- forced to working: causes switchover to the main (working) SNC (even if this SNC is faulty)

- forced to protection: causes forced switchover to the standby (protection) SNC (even if this SNC is faulty)

The "Clear" request clears any active manual switch request. Clear will also release the wait-to-restore timer when provided for revertive switching.

Dual Node Ring Interworking

Overview   Dual node ring interworking (DNI) is a configuration that provides path-level protection for selected STM-N circuits that are being carried through two rings. Protection for the route between the two rings is provided by interconnecting the rings at two places.

Each circuit that is provisioned with DNI protection is dual-homed, meaning it is duplicated and subsequently terminated at two different nodes on a ring. The two interconnecting nodes in each ring do not need to be adjacent.

DNI protection   The self-healing mechanisms of the two rings remain independent and together protect against simultaneous single failures on both rings (not affecting the interconnections). The DNI configuration additionally protects against failures in either of the interconnections between the rings, whether the failure is in a facility or an interconnection node.

Interworking   All *WaveStar*® TDM 10G (STM-64) tributary interfaces (STM-16, STM-4 and STM-1) can support dual node ring interworking.

A *WaveStar* TDM 10G (STM-64) STM-64 ring can interwork with 2-fiber MS-SPRing, including rings using

- *WaveStar* BandWidth Manager

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

- *WaveStar* ADM16/1 STM-16 interfaces

Additionally, there can be intermediate network elements in the interconnection routes between the two rings.

Primary and secondary nodes   In the MS-SPRing, a bidirectional DNI-protected circuit to and from the terminating node is added and dropped at both a primary node and a secondary node, both of which interconnect with the other network. The primary and secondary nodes are defined and provisioned on a per-circuit basis.

Drop and continue

WaveStar™ TDM 10G supports the drop and continue method of DNI, in which the primary node is located between the terminating node and the secondary node and performs the drop-and-continue and path-selection functions. The primary node drops the circuit in the direction of the other network and also continues (bridges) the circuit to the secondary node. The secondary node drops the circuit in the direction of the other network and adds the circuit from the other network in the direction of the terminating node. The primary node either adds the circuit received on its tributary interface from the other network, or else passes through the duplicate signal received on the line from the secondary node, depending on standards-compliant path selection criteria.

Protection switching example

The following graphic illustrates a failure of the interconnection to a primary node at the point labeled "X" in the figure. The failure results in a DNI switch at the primary node in the top ring. A DNI protection switch in a *WaveStar* TDM 10G (STM-64) occurs in ≤ 50 milliseconds (not counting the detection time) plus a provisionable hold-off time nominally of 100 milliseconds. The graphic shows a DNI configuration transporting traffic between nodes A and Z.

1. DNI configurations: two rings interconnected by two nodes

2. Circuit originating and terminating in Nodes A and Z

3. Failure (depicted by x) triggers a DNI switch at top ring primary node, which automatically selects traffic from secondary node
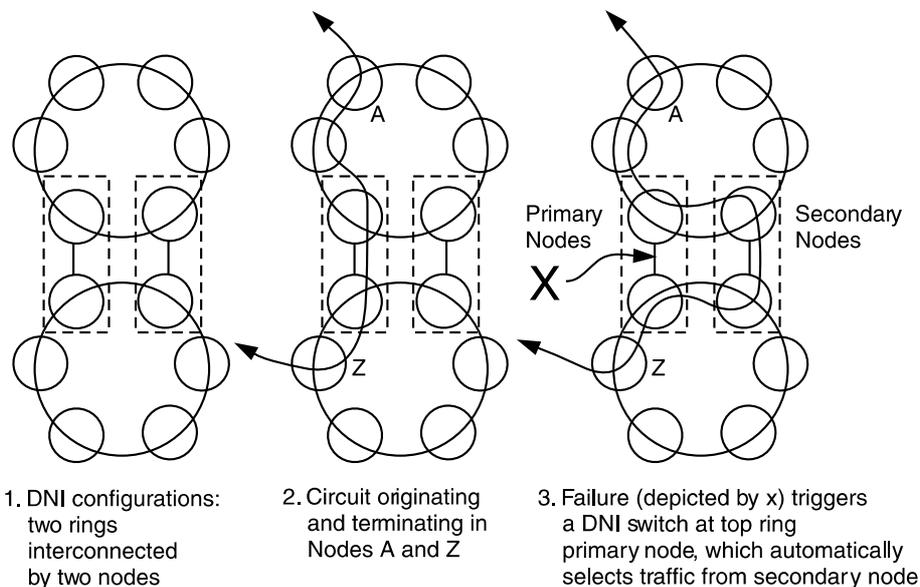
Sdh-10gapog-006

Types of connection

The following graphic illustrates a DNI configuration that uses STM-1 interfaces between a *WaveStar* TDM 10G (STM-64) ring and a

WaveStar ADM16/1 STM-16 ring. Two types of connection are shown. These are:

- A direct intraoffice connection between the primary nodes, Node 1 and Node 2, at the first central office (CO 1).

- An optically extended, direct secondary connection between the secondary nodes (Node 3 at the second central office (CO 2) and Node 4 of the *WaveStar* ADM16/1 STM-16 ring). This type of connection is achieved through the STM-1 low-speed interfaces at the interconnected nodes and can go through other equipment.

Both types of connection can be used in either primary or secondary nodes.
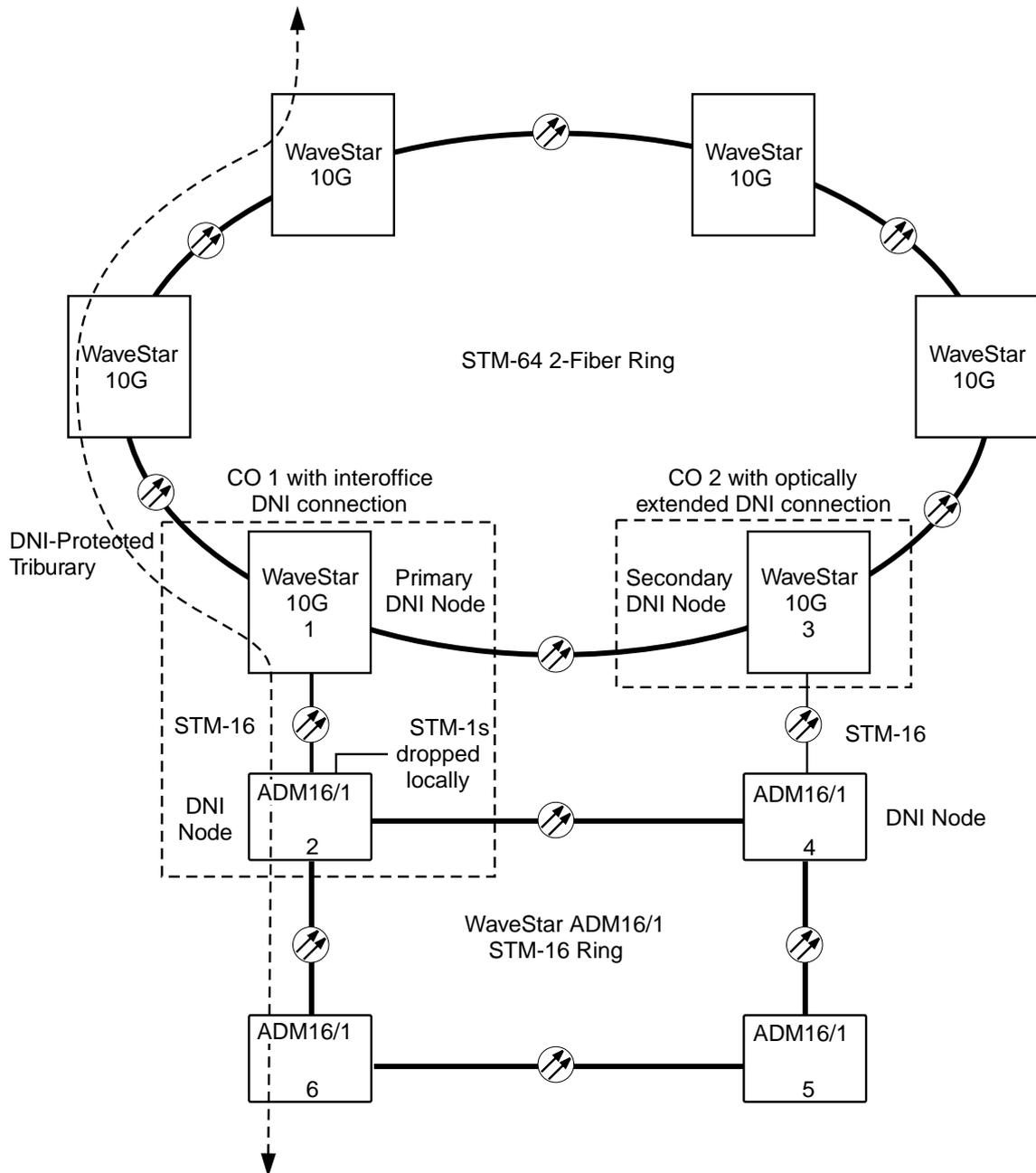
Sdh-10gapog-009

Failure conditions   In the illustrated configuration *WaveStar* TDM 10G (STM-64) protection switching results from the following failure conditions (grouped by priority, from highest to lowest):

- LOP, P-AIS, or Unequipped

- Excessive Bit Error Ratio (EXC)

- Signal Degrade (DEG)

Implementation of the switch

The following figure shows in more detail the implementation of the protection switch in the previous example in NE 1 and NE 2.
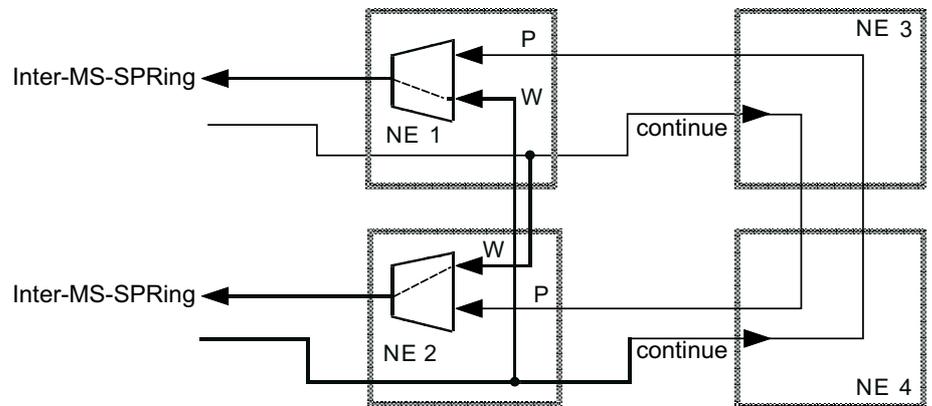
Collapsed nodes   A further, more sophisticated, possibility is to use the *WaveStar* TDM
10G (STM-64) itself as the DNI node. By means of the STM-16
interfaces, the STM-16 ring can be directly connected to the
WaveStar™ TDM 10G (STM-64), as depicted in the following graphic.
So, the complete DNI node is included in one network element.
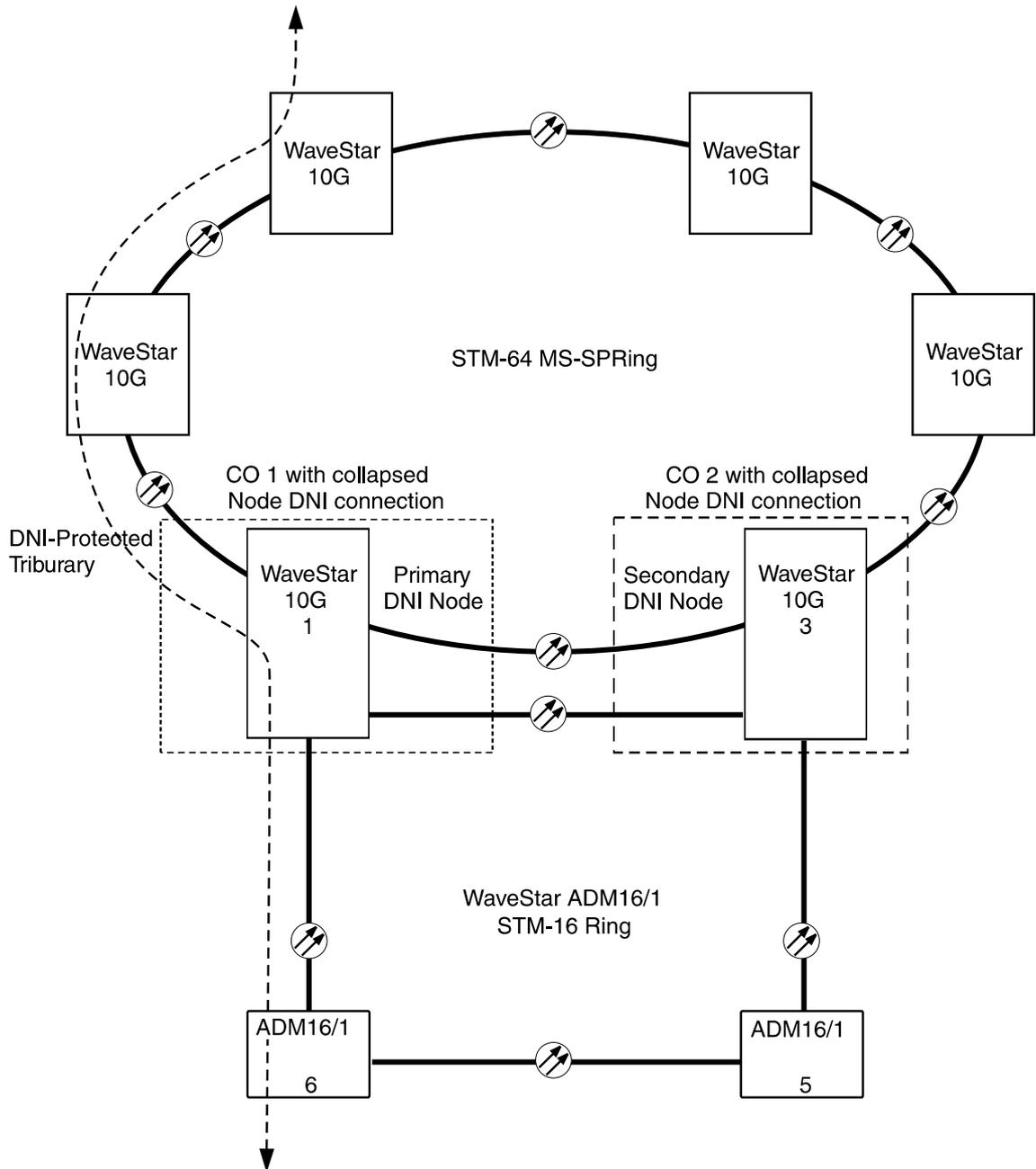
Sdh-10gapog-X09

Dual Node Ring Interworking between MS-SPRing and SNCP ring

Overview   WaveStar™ TDM 10G (STM-64) supports Dual Node Ring Interworking (DNI) with the Drop-and-Continue method between a MS-SPRing and a SNCP ring.

Benefits   This feature allows for

- highly survivable services where circuits are carried through interconnected rings with different protection schemes

- advanced networking capabilities with a single network element that supports OC-48/STM-16 and OC-192/STM-64 rings and interconnects traffic directly from one ring to another.

Concept   The ring interworking between a MS-SPRing and a SNCP ring provides a high degree of protection of the traffic crossing from one ring to the other.

It is capable of protecting against the failure of

- one interconnecting node

- two interconnecting nodes (each on different rings, but on the same interconnect)

- the connection between two interconnecting nodes.

Note that, within the MS-SPRing, any line or node failure (including interconnecting node) will be protected at Multiplex Section level by the standard MS-SPRing scheme, as described in ITU-T Recommendation G.842.

There are two variants of interconnection between rings. The two interconnected rings being in

- the same network element or

- in different network elements.

The SNCP and MS-SPRing behaves as described in ITU-T Recommendation G.841. The MS-SPRing is either a STM-64 or a STM-16 2-Fiber MS-SPRing The SNCP ring is either a STM-64, a STM-16, a STM-4 or an optical STM-1 SNCP ring.

The following combinations of ring interworking between a
MS-SPRing and a SNCP ring are supported:

- STM-64 MS-SPRing with either STM-16 or STM-4 or optical
  STM-1 SNCP ring.

- STM-16 MS-SPRing with either STM-64 or STM-16 or STM-4
  or optical STM-1 SNCP ring.

- STM-64 MS-SPRing with STM-64 SNCP ring, with both rings in
  separate nodes.

Both MS-SPRing and SNCP ring support VC-3, VC-4, VC-4-4c and
VC-4-16c signal rates. The interconnection between rings can be done
at any of these rates. The ring interworking does not require inter-ring
signalling. Ring interconnection may occur among multiple rings.

The following figure shows the two variants of interconnection
between the rings.
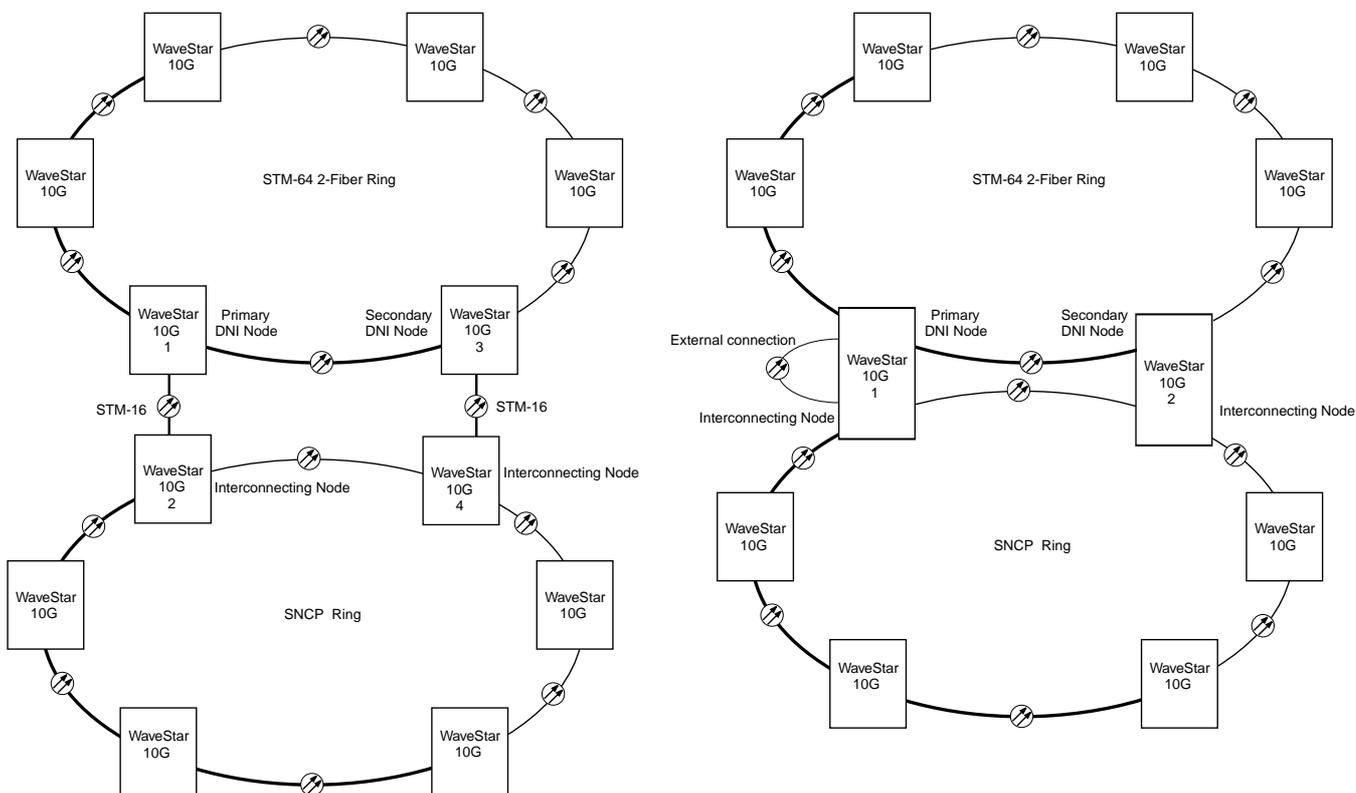
Functional Details   The following figure shows in more detail the interworking between
the two rings (one MS-SPRing and one SNCP ring) in different
network elements.
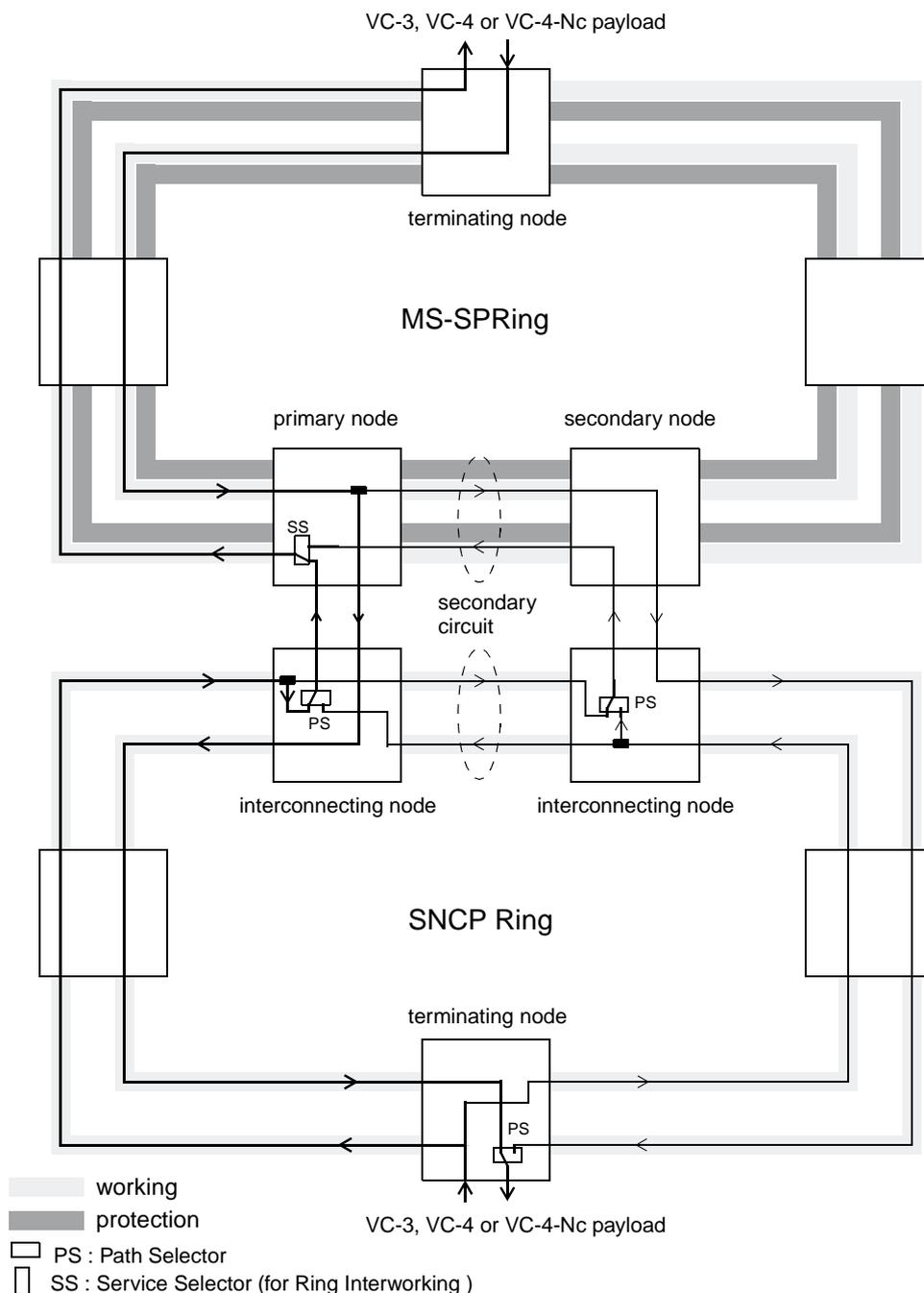
MS-SPRing Nodes   The MS-SPRing nodes support the Drop-and-Continue method, i.e.

- in one direction, the traffic is extracted from a working channel on the ring (Drop), and transmitted towards the opposite side on the ring (Continue);

- in the other direction, the signal is selected from either a traffic entering the ring (Add), or a channel from one side on the ring (Continue), and it is transmitted towards the opposite side on the ring.

The selector is called ring interworking service selector. The interconnecting node providing the Drop-and-Continue function for a tributary is called the primary node for this tributary.

The Continue traffic is only carried over the working bandwidth between the primary and secondary nodes, i.e. the channel assignment (timeslot) on the multiplex section used between the primary and secondary nodes is the same as that used between the primary and terminating nodes. The Drop-and-Continue on the protection bandwidth is not supported in this release.

The ring interworking service selector in the primary node is used to protect against ring interconnection failures. It protects at path level, based on path defects detection. It supports the SNC/N protection type only, and operates in either the revertive or the non-revertive mode. By default, it operates in the revertive mode, with a Wait-to-Restore time of 5 minutes. In other words, the ring interworking service selector shall behaves just like any other path selector.

The service selector in the primary node can be operated by the user.

The ring interworking service selector in the primary node behaves independently of the MS-SPRing scheme. Though these two protection mechanisms (i.e. path protection and MS-SPRing) are cascaded back-to-front in a primary node, they do not interfere since they do not protect at the same level. Therefore it is required to support a hold-off time for the service selector in order to avoid a double protection (hence a double transmission hit) in some failure scenarios (like a line failure between the primary and secondary nodes). The default hold-off time is 100 ms.

The hold-off time to the ring interworking service selector is also required to avoid propagation of switching from one ring to the other (e.g. a path protection switch in the SNCP ring leading to a service selector switch at the primary node in the other ring).

An interconnecting node failure is protected at Multiplex Section level by the standard MS-SPRing scheme.

The two interconnecting nodes (i.e. the primary and secondary nodes) within the MS-SPRing do not need to be adjacent.

SNCP Ring Nodes   The SNCP Ring nodes support the Drop-and-Continue method. Note that the connections for this Drop-and-Continue method differ from that used in a MS-SPRing interconnecting node (primary node). For each direction of transmission in the SNCP ring, the signal is dual-fed from the terminating (source) node around both sides of the ring. When each of the dual-fed signals hits an interconnection node, it is dropped at that node and continued onto the other interconnection node using drop-and-continue. Thus, each interconnection node can select from two signals sent on a different way around the ring. The output of the selector in each interconnection node is then transmitted to the other ring (MS-SPRing). In the other direction, the signal coming from the other ring (MS-SPRing) is transmitted towards the terminating (sink) node, away from the other interconnection node. Finally, the terminating (sink) node makes the selection between the two signals from the two directions around the ring. Due to the symmetry of this scheme, the two interconnecting nodes are completely equivalent.

The path selector in the interconnecting node supports the SNC/N protection type only, and operates in either the revertive or the non-revertive mode. By default, it operates in the revertive mode, with a Wait-to-Restore time of 5 minutes. In other words, the ring interworking service selector behaves just like any other path selector.

The path selector in the interconnecting node can be operated by the user.

A hold-off time to the path selector avoids propagation of switching (i.e. one protection switch leading to another). The default hold-off time is 100 ms.

The two interconnecting nodes within the SNCP ring do not need to be adjacent.

Both rings in the same NE   The ring interworking between a MS-SPRing and a SNCP ring is supported with both rings in different NEs or with both rings in the same NE.

For this latter case, the recommended method is to connect the circuits in this limited category through an additional pair of optical ports and fibers, as if between separate NEs. One pair of unprotected optical ports could be used for all such circuits in the NE unless the number of these circuits requires additional capacity.

A bidirectional VC-3/VC-4/VC-4-Nc circuit, which is interconnected between a MS-SPRing and a SNCP Ring, is depicted in the following figure, according to this feature restriction.

VC-3, VC-4 or VC-4-Nc payload

terminating node

MS-SPRing

primary node   secondary node

SS

secondary
circuit

Must be
external
connections !

PS

PS

interconnecting node   interconnecting node

SNCP Ring

terminating node

working

protection

PS : Path Selector

SS : Service Selector (for Ring Interworking)

VC-3, VC-4 or VC-4-Nc payload
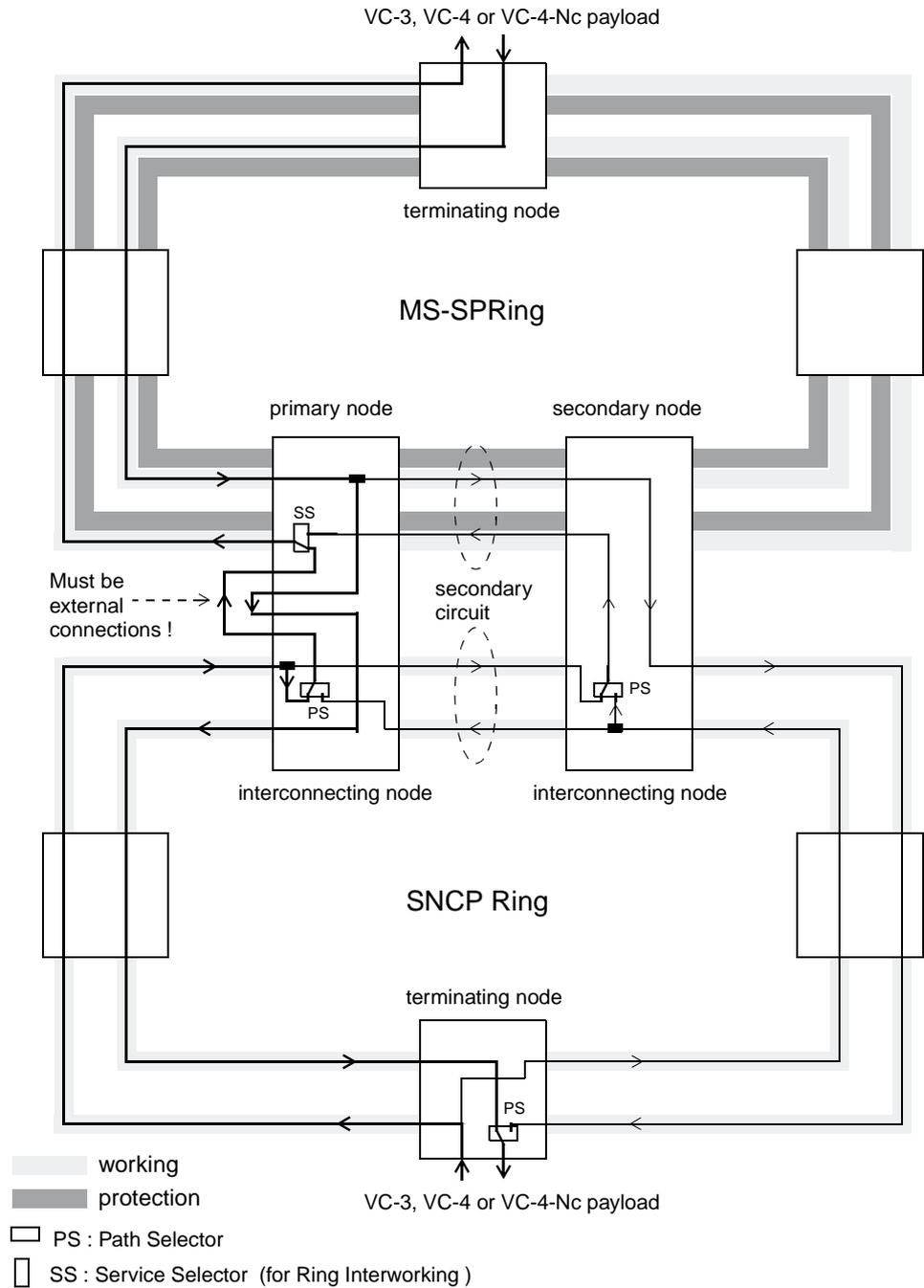
Protection configurations

Overview   This section describes the shelf configuration guidelines that have to be observed for the following protection mechanisms:

- 2-fiber MS-SPRing

- 1+1 MSP.

All protection mechanisms are only supported within one shelf, so it is not possible to have a circuit pack in the Main Shelf be protected by a circuit pack in the Extension Shelf.

MS-SPRing   The MS-SPRing related STM-16 circuit pack pairs have to be plugged into the following dedicated port unit slot pairs: 02-04, 06-08, 10-12, 14-16, 02-16, 04-14, 06-12, 08-10.

MSP   MSP can only be established between two separate circuit packs (which are of the same type), i.e. it is not allowed to establish MSP between 2 ports on the same circuit pack. MSP between different ports on different circuit packs can be configured independently, e.g. one port of circuit pack 1 can be protected with one port of circuit pack 2 while the second port on circuit pack 1 is protected by circuit pack 3. The MSP-related circuit packs are not restricted to specific slots.

For STM-16 port units, any pair combination of allowed slot positions can be applied: 02, 04, 06, 08, 10, 12, 14, 16.

For optical STM-1 and STM-4 port units, any pair combination of allowed slot positions can be applied: 01...16.

19   Traffic maintenance concepts

Overview

Purpose
This chapter gives background information on the traffic maintenance. This includes provisioning of traffic monitoring and manual protection switching.

Related information
The background information on traffic monitoring, that means regenerator section trace and path trace, are inlcuded in this chapter.

Although the task belonging to manual protection switching and intershelf bandwith utilization are traffic maintenance tasks, the background information on this features are described in Chapter 18, "Traffic provisioning concepts".

Contents

⌐

Regenerator section trace

....

Trace identifier   The Trace Identifier TI is used to verify regenerator section set-up completion and to make sure the traffic is not delivered to the wrong destination. An arbitrary identifier can be assigned to each regenerator section termination point by the *WaveStar*® CIT to trace a section from source to sink.

Three basic components are necessary for the Trace Identifier functionality:

- Transmit Section Trace Identifier: identifier which is sent by the source TP.

- Expected Section Trace Identifier: identifier which is expected by the sink TP to be received from the remote source TP.

- Received Section Trace Identifier: identifier which is received by the sink TP from the actually connected remote source TP.

Trace identifier TI format   Two modes for the Trace Identifier format can be selected by the *WaveStar* CIT for transmit (TI transmit mode) and receive direction (TI receive mode):

- Non-Specific-byte:
  The Received Trace Identifier matches, if it is any constant byte value within the range 00..FFhex. Otherwise Trace Identifier Mismatch is assumed. The Transmit Trace Identifier is one byte set by the NE to the value "01" (cannot be changed). No check with Expected Trace Identifier will be performed during this mode.

- Single-byte:
  The Transmit Trace Identifier and Expected Trace Identifier are a "constantly repeating single byte". The value of the byte is provisionable within the range 00..FFhex.

- 16–byte
  The Transmit Trace Identifier and Expected Trace Identifier are 16 byte ASCII strings which can be set by the user.

TI mismatch   If the Received Trace Identifier does not match the Expected Trace Identifier a mismatch alarm is reported and consequent actions are performed. Consequent actions are not affected by suppression of alarm reporting.

⌐

....

Path trace

Path trace identifier
The Path Trace Identifier (TI) is used to verify path set-up completion and to make sure the traffic is not delivered to the wrong destination. *In the* WaveStar® TDM 10G *system the Path Trace Identifier can only be monitored.*

Two basic components are necessary for the Trace Identifier functionality:

- Expected Path Trace Identifier: identifier which is expected by the sink TP to be received from the remote source TP.

- Received Path Trace Identifier: identifier which is received by the sink TP from the actually connected remote source TP.

Path trace identifier format
Three modes for the Trace Identifier format can be monitored by the *WaveStar* CIT:

- Non-Specific-byte:
  The Received Path Trace Identifier matches, if it is any constant byte value within the range 00..FF hex. Otherwise Trace Identifier Mismatch is assumed. The Transmit Trace Identifier is one byte set by the NE to the value "01" (cannot be changed). No check with Expected Trace Identifier will be performed during this mode.

- Single-byte:
  The Expected Trace Identifier is a ″constantly repeating single byte″. The value of the byte is provisionable within the range 00..FF hex.

- 16-byte
  The Expected Trace Identifier is a 16 byte ASCII string.

- 64-byte
  The Expected Trace Identifier is an ASCII string consisting of up to 64 byte, with the last two bytes being carriage return and line feed.

Path trace identifier mismatch
If the Received Path Trace Identifier does not match the Expected Path Trace Identifier a mismatch alarm is reported and consequent actions are performed. Consequent actions are not affected by suppression of alarm reporting.

20 Performance monitoring concepts

Overview

Purpose   Performance Monitoring allows you to systematically track the quality of a particular transport entity. This is done by means of continuous collection and analysis of the data derived from defined measurement points.

Contents

Background

....

Definitions The following definitions explain expressions which are important for the performance monitoring.

Anomaly An anomaly is a discrepancy between the actual and the desired characteristic of a system component.

Defect A defect is the limited interruption of the ability of a system component to perform a required function.

Block A block is a set of consecutive bits associated with the path/section. Each bit belongs to one and only one block. Consecutive bits may not be contiguous in time.

Errored block An errored block is a block in which one or more bits are in error.

Errored second An errored second (for in-service measurements) is a one-second interval with one or more errored blocks or at least one anomaly.

Severely errored second A severely errored second (for in-service measurements) is a one-second interval which contains a configurable amount of errored blocks (default: 30 %) or at least one defect

Background block error An errored block not occurring as part of a severely errored second is a background block error.

Unavailable seconds Unavailable seconds determine the period of time during which a path is in the unavailable state. A period of unavailable time begins at the onset of ten consecutive severely errored second events. These ten seconds are considered to be part of unavailable time. A new period of available time begins at the onset of ten consecutive non severely errored second events. These ten seconds are considered to be part of available time.

⌐┐

....

Performance Measurements

....

Basic SDH measurement parameters

The following definitions explain expressions which are important for the performance monitoring.

Near-end parameters, related to the receive direction:

- Near-End Errored Seconds (N-ES)
- Near-End Severely Errored Seconds (N-SES)
- Near-End Unavailable Seconds (N-UAS)
- Near-End Background Block Errors (N-BBE)

Far-end parameters, related to the transmit direction:

- Far-End Errored Seconds (F-ES)
- Far-End Severely Errored Seconds (F-SES)
- Far-End Unavailable Seconds (F-UAS)
- Far-End Background Block Errors (F-BBE)

Ethernet performance monitoring

Ethernet Performance Monitoring in SDH network elements is kept as closely related to SDH performance monitoring as possible. This means that the concepts of binning and thresholding are completely reused. This also implies a deviation from SNMP MIB counter like behaviour where counters are continuously updated and not stored into bins. One of the differences with SDH performance monitoring is the fact that higher values for counters not always imply worse behaviour.

There are four levels of Ethernet Performance Monitoring possible:

- Monitoring per port
- Monitoring per port per traffic class. This option monitors all packets of all customers that belong to a specific traffic class
- Monitoring per port per (top-level) VLAN-id. This option monitors all packets, irrespective of the traffic class, of a specific VLAN-id.
- Monitoring per port per traffic class per (top-level) VLAN-id. This option monitors all packets of a specific VLAN-id and a specific traffic class

The following gives an overview of the Ethernet Performance Parameters. These parameters are presented in 15 minute and 24 hour reports and thresholding is applicableEthernet parameters, related to the transmit direction:

- Outgoing number of Mbytes (EONB)
- Outgoing number of Mframes (EONF)

....

- Dropped frames - congestion (EDFC)
- Dropped frames - errors (EDFE)
- Incoming number of Mbytes (EINB)
- Incoming number of Mframes (EINF)

Enabling performance measurement points

Performance measurement points can be enabled via the *WaveStar*® SNMS Element Manager and via the *WaveStar* CIT.

Supported counter types

The following table gives an overview which performance monitoring counter type can be configured for certain termination points. As no path termination is done within the *WaveStar* TDM 10G (STM-64) network element, an intermediate higher-order path performance monitoring is implemented on VC-3, VC-4, VC-4-4c and VC-4-16c level.

Counter Type	Multiplex Section	Regenerator Section	HO VC Intermediate Path
N-ES	X	X	X
N-SES	X	X	X
N-UAS	X	X	X
N-BBE	X	X	X
F-ES	X	–	X
F-SES	X	–	X
F-UAS	X	–	X
F-BBE	X	–	X

Data storage

All the data is stored in the current bin. The managed NE has a current data register (current bin) for 15 minutes and 24 hours. Once a termination point for measurements has been configured, you are able to get a snapshot view of the data gathered at any time (default).

Data retrieval

Performance Data can be polled via the *WaveStar* SNMS and via the *WaveStar* CIT.

Historic bins

The network element keeps a store of the historic 15-minute and 24-hour bins.

Interval	Number of historic bins	Total storage time
15 minute	32	8 hours

Interval	Number of historic bins	Total storage time
24 hours	1	1 day

Reports

The *WaveStar* SNMS allows you to create reports from history data stored in the database of the network management system.

Zero suppression

Performance data records with counter value zero, i.e. no errors occured, will not be stored in the perfomance data log.

Thresholds and alarms

Threshold values for the performance parameters can be defined. If the counter value of a performance parameter exceeds the threshold, an alarm can be generated and displayed on *WaveStar* SNMS and CIT.

Threshold profiles

Threshold profiles store the threshold values of PM parameters that require thresholding. One threshold profile of each parameter group type may be associated with each port. PM values stored in threshold profiles determine the threshold crossing alerts of a monitored value for a port. The **Performance** menu in the **System View** window of the *WaveStar* CIT allows you to create, modify, or delete profiles, view profile information, and assign profiles to ports.

Maximum number of threshold profiles

The maximum number of threshold profiles is limited to the NVM space. The system supports the following maximum number of default and user created profiles:

- 30 regenerator multiplex-section port-level profiles

Threshold profiles TCA reporting

The system supports enabling or disabling a threshold-crossing alert (TCA) reporting, on a parameter basis using threshold profiles. When the threshold value of a parameter is set to zero, no quality of service (QOS) alarm message is generated. Enabling/disabling the TCA reporting of an individual parameter is independent of any other parameter. The system does not provide disabling TCA reporting on a parameter grouping such as line. You can disable reporting on a parameter group by setting zeros to a parameter group in the threshold profile. For example, you can set the threshold values of all line PM parameters to zero to disable the TCA reporting on the line level.

All TCAs are retrievable either locally or remotely via the *WaveStar* CIT. If provisioned for autonomous TCA reporting, the message-based operations system interface can communicate TCA reports to the operations centers.

Provisioning TCA parameter thresholds

The current 15-minute and current 24-hour thresholds for each performance-monitoring parameter are provisionable according to a profile using the *WaveStar* CIT. Whenever the current 15-minute or the current 24-hour threshold for a performance-monitoring parameter is either reached or exceeded, the system generates a TCA in the form of a quality-of-service (QOS) alarm. The alarm condition is then entered into the appropriate performance-monitoring report.

Fault localization

Performance alarms only give a hint that the signal quality at a certain measurement point is degraded. They can be used as a help for the fault location. The severity of such an alarm is strongly dependent on the application of your network. Often it can be helpful to define a very low threshold value in order to realize a not alarmed signal degradation at a very early stage.

Clearing

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

Physical Layer PM

What is monitored? Physical layer Performance Monitoring applies to service and protection STM-16 and STM-64 optical laser port units.

Prerequisite: The STM-16 or STM-64 optical laser circuit pack must be physically installed to activate the physical layer PM.

Threshold values: Physical layer PM is not measured in time intervals but as a snap-shot in time. The threshold values of the physical layer PM parameters are set and cannot be changed by provisioning.

Parameters monitored: PM monitors the following parameters to detect degrading performance of the laser.

Normalized Laser Bias Current (LBCN)	This parameter monitors the laser bias current of each active laser transmitter. This parameter does not vary among the optical circuit packs and is stored in the system non-volatile memory (NVM). The upper limit is 150% of the initial factory value. There is no lower limit.

Optical Transmit Power (OPT)	This parameter monitors the average optical output power of each active laser transmitter. This parameter varies among the different optical circuit packs and is therefore not stored in the system NVM but is stored in the inventory NVM of each circuit pack. This parameter has two values, high and low. The high value is +1 dBm above the initial factory value and the low value is -1 dBm below the initial factory value.
Optical Power Received (OPR)	This parameter monitors the average optical power received. This parameter varies among the different optical circuit packs and is therefore stored in the inventory NVM of each circuit pack instead of the system NVM. This parameter has two values, high and low. The high value is -10 dBm nominal and the low value is -29 dBm nominal.

21 Engineering orderwire concepts

Overview

Purpose   The purpose of this section is to describe the Engineering orderwire concepts of the *WaveStar*® TDM 10G (STM-64) and to provide information about the User Byte I/O-Panel.

Contents

Engineering Orderwire

....

User Byte I/O-Panel

By means of a codirectional G.703 interface (9–pin Sub-D socket) on the User Byte I/O-Panel, (cf. "User Byte I/O Panel" (21-4)) an external orderwire system, e.g. *WaveStar*® EOW can be connected which uses this orderwire channel for transparent data transmission via the *WaveStar* TDM 10G (STM-64) transmission network.

E1 and E2 bytes

For this functionality the bytes E1 and E2 are used as orderwire channels. The RSOH byte E1 is accessible in all network element types, the MSOH byte E2 is only accessible in the multiplexers. The E1 and E2 bytes of both STM-64 interfaces are permanently assigned to User Byte ports. The permanent assignment is done at initialization; i.e. this functionality is not manageable via *WaveStar* CIT.

PCM signals

The data received or transmitted via the G.703 interface represents pulse code modulated signals of voice frequency according to ITU-T Rec. G.711. As encoding rule the A-law is used.

Please note that feedback paths must not occur within an orderwire network. An external orderwire system can therefore only be connected in networks which have no feedback paths. This functionality is only available in meshed networks or networks with a ring structure, if these network structures are interrupted between two NEs for the orderwire traffic.

Number of orderwire branches per NE

There are two orderwire branches per network element, one for the east STM-64 interface and one for the west STM-64 interface. Each one gives access to the E1 byte and to the E2 byte.

Call occupies the entire channel

A call always occupies the entire channel, i.e. only one call can be made at any given time via this orderwire channel.

Channel control

The channel control and call signalling are taken over by the connected external orderwire system, and the *WaveStar* TDM 10G (STM-64) transmission network serves only as a transmission medium. *WaveStar* CIT does not provide any setting options.

⌐

....

User channel

....

User channel   The *WaveStar*® TDM 10G (STM-64) offers two user-channel interfaces (F1 byte) in accordance with ITU-T Recommendation V.11. The (15–pin Sub-D socket) interfaces are located on the User Byte I/O-Panel (cf. "User Byte I/O Panel" (21-4)).

F1 byte   The F1 byte of both STM-64 interfaces are permanently assigned to the User Byte I/O-Panel ports. The permanent assignment is done at initialization; i.e. functionality is not manageable via *WaveStar* CIT.

⌐

....

User Byte I/O Panel

Front view

CIT

E2 byte
STM-64
East side

UB 5

E1 byte
STM-64
East side

UB 4

E2 byte
STM-64
West side

UB 3

E1 byte
STM-64
West side

UB 2

F1 byte
STM-64
East side

UB 1

F1 byte
STM-64
West side

UB 0
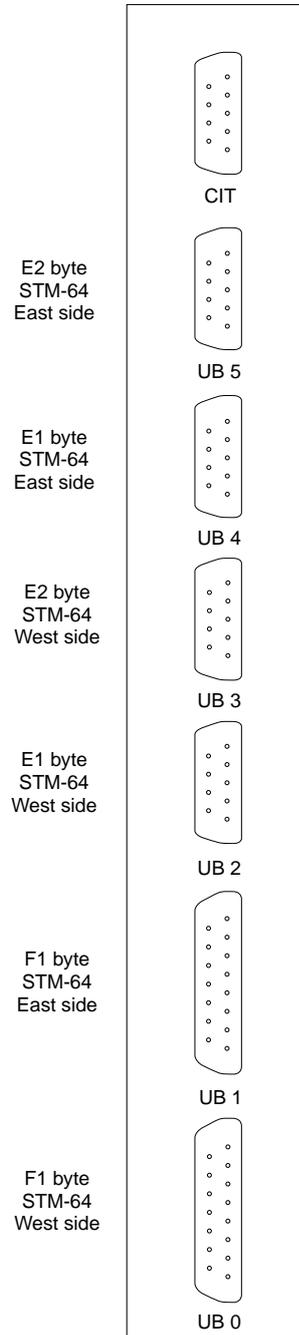
CIT:
Connector for CIT PC,
female Sub-D9 connector for RS-232 interface.

UB #0...1:
User byte #0...1 (used for F1 byte),
female Sub-D15 connector for V.11 interface.

UB #2...5:
User byte #2...5 (used for E1 and E2 bytes),
female Sub-D9 connector for G.703 interface.

22 Software upgrade concepts

Overview

....

Purpose
This section provides information on features relating to the NE Software Management, including

- *WaveStar*® TDM 10G (STM-64) memory concept
- Downloading new software
- Activating new software

Related information
For stepwise operating instructions on these items, please refer to the task oriented procedures part Chapter 10, "Software upgrade") of this manual.

Contents

⌐

....

NE memory concept

Overview The *WaveStar*® TDM 10G (STM-64) system is equipped with volatile working memory and non-volatile memory (NVM). *WaveStar* TDM 10G (STM-64) systems make use of a PCMCIA (Personal Computer Manufacturer's Card Interface Adapter) card, a so called "flash disk" as a non-volatile memory.

PCMCIA flash disk The PCMCIA flash disk is used to store the currently active and a previous version of the executable NE software and configuration data. The PCMCIA flash disk is inserted into the PCMCIA slot of the CTL/SYS50DM system controller. The "previous" store area is the one into which data can be downloaded using the SNMS network management system or the *WaveStar* CIT. Activating ("installing") a newly downloaded software version changes the current/previous assignment automatically.

The following figure illustrates the partitioning of the PCMCIA flash disk.
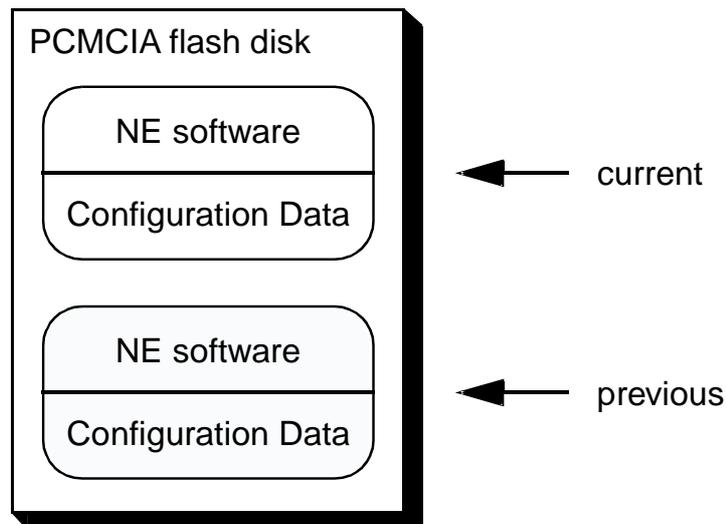
Preparing a PCMCIA flash disk When initially delivered, the PCMCIA card is empty. *WaveStar* CIT can be used to copy the initial software generic from the CD-ROM to the PCMCIA card.

Software download

....

Definition   **Software download**   is the process of transferring a software generic from a remote entity to a target NE's memory. The remote entity may be a network management system or a CIT. The download process is responsible for establishing the association between the source of the software generic and the target NE and ensuring the integrity of the data during the transfer. The download procedure uses bulk transfer to move an uninterpreted binary file into an NE.

Types of software download   Depending on the state of the network element, there are two possible types of software download:

- Initial software download

- Software download for upgrade purposes.

For each type, an individual procedure has to be applied.

There are *WaveStar*® CIT screens to support the user initiated steps and to indicate progress during download, software application, and test.

Initial software download   Typically, when a software generic is installed for the first time, it is necessary for a craft person to be present on site to monitor the installation. The on-site installation is supported via removable storage media (PCMCIA card) associated with *WaveStar* CIT.

The software is initially delivered to the customer on a CD-ROM. The PCMCIA card is initially empty. The software generic has to be copied from the CD-ROM to the empty PCMCIA card via *WaveStar* CIT. Afterwards, the PCMCIA card is inserted into the NE.

Software download for upgrade purposes   After a software generic is initially installed on-site, it can be downloaded remotely from a centralized location supported by a configuration management application. Remote downloading of software generics not only minimizes dispatching of technicians, but also provides tighter coordination and synchronization among the activation of these software generics across multiple NEs.

Upgrading a software generic in the NE

- causes no disruption to customer services

- causes no disruption to operations support, such as performance monitoring and protection switching

....

- does not alter any of its existing option settings, e.g., performance monitoring parameters

- requires no re-entry of site-dependent data (e.g., provisioned parameters) into the service database of the NE.

Before accepting the loading of a software generic, the NE verifies a match between its type and the type specified in the software generic control information.

The download time for a software generic to the non-volatile memory (NVM) of the NE from a *WaveStar* CIT or a Management System connected indirectly via a LAN network is approx. 1 hour, via DCC approx. 2 hours.

After completion of the software download, there are now two versions of the software on the NE, the currently active version and the newly downloaded version which has replaced the former backup version.

After a software generic has successfully been loaded onto the NE, the NE waits for an activation or apply command.

23   Database backup concepts

Overview

Purpose   This section provides information on features relating to NE database backup and restore.

Related information   For stepwise operating instructions on these items, please refer to the task oriented procedures part Chapter 11, "Database backup") of this manual.

Contents

⌐

Configuration backup and restoration

Background To recover from loss of NE data because of human error, power failure, NE design flaws, software bugs etc., the system provides a backup and restoration capability.

Restore In the restoration process the backup data is copied back into the working memory. After the binary image is loaded, the OS sends the incremental changes to the NE. The NE verifies a match between the destination of the binary image against its TID before accepting a restoration file. All command processing is suspended during restoration.

No impact on service The backup and restore operation does not interfere with or interrupt the service.

⌐

24 *WaveStar*® CIT Tutorial

Overview

Purpose The purpose of this chapter is to describe the installation procedures of the *WaveStar* CIT application software on a PC and to give basic operating instructions.

This chapter provides information you should know before performing specific tasks, e.g.:

- how to log into and log out from the *WaveStar* CIT

- how to log into and log out from network elements

- the layout and the structure of the three different series of windows

    - *WaveStar* CIT main window and its menus and sub-menus

    - *WaveStar* System View window and its menus and submenus

    - *WaveStar* Cut-Through window and its menus

- the elements of the *WaveStar* CIT user interface

- the bay and shelf display

- how to get help-information on items that are displayed on the *WaveStar* CIT main window

- how to display the system defaults for a particular component

Menu structure overviews Also, this chapter presents menu structure overviews of the *WaveStar* CIT application with references to the parts of this manual where the respective descriptions and tasks can be found.

Intended audience

This subject is intended for personnel responsible for installation of the *WaveStar* CIT software on a PC, for administrators, and for first-time users of the *WaveStar* CIT application. Experienced users may benefit from the menu structure overviews.

Contents

Lucent Technologies

⌐

Installation procedures

Overview

Purpose The purpose of this section is to describe the installation procedures of the *WaveStar®* CIT application software on a PC and to give basic operating instructions.

This chapter provides information you should know before performing specific tasks, e.g.:

- how to log into and log out from the *WaveStar* CIT

- how to log into and log out from network elements
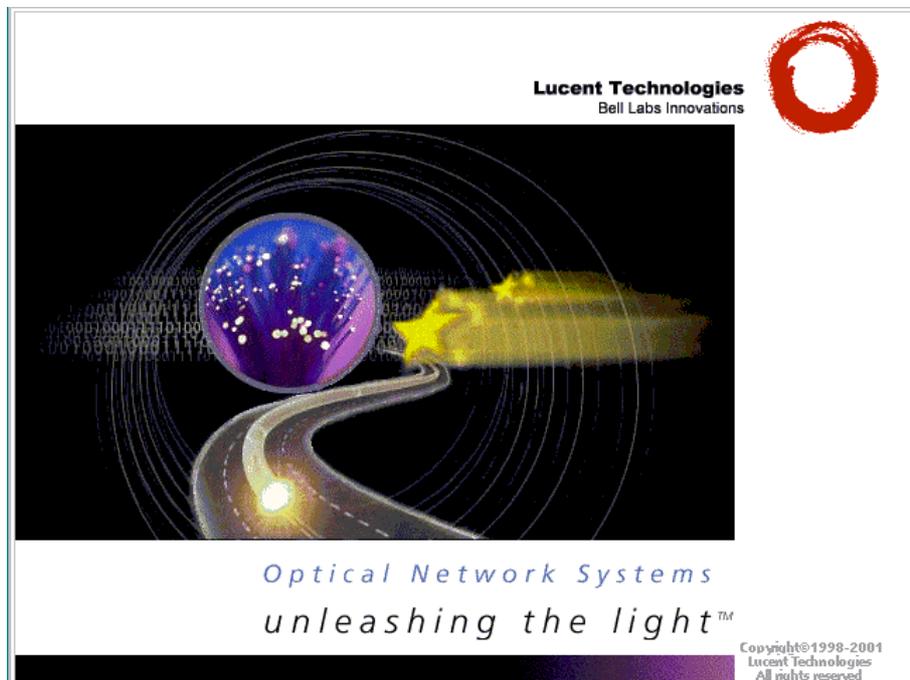
Contents

Installing the *WaveStar*® CIT

Purpose   Use this procedure to:

- Install the *WaveStar* CIT software onto a new system.

- Upgrade/change an existing *WaveStar* CIT to a new software version.

Required equipment   The minimum requirements for a *WaveStar* CIT are a personal computer with

- Pentium® 266 MHz processor (Pentium® III 500 MHz or higher recommended) with 128 MB of RAM (256 MB of RAM or higher recommended)

- 139 MB (and more) of Virtual Memory

- Standard floppy-disk drive for 1.44 MB 3.5" floppy disks

- 150 MB of free hard-disk drive space

- CD-ROM drive (16X recommended)

- PCMCIA (Personal Computer Manufacturer's Card Interface Adapter) slot type II

- SVGA monitor set to 800x600 resolution or greater, with 256 colors (1024x768 recommended)

- 10BaseT LAN interface built-in or supplied with a PCMCIA card, installed and working

- Microsoft Windows® NT 4.0 operating system with Service Pack 5 or Microsoft Windows® 2000

- Adobe Acrobat Reader for Windows (version 3.01 or later)

- Removable hard-disk drive (optional; required only for system backup).

The performance of the user interface can be enhanced by using a higher performance personal computer.

NOTE: The minimum requirements are sufficient to run the *WaveStar* CIT on a single NE while the recommended requirements should be used to optimize the *WaveStar* CIT performance. As the *WaveStar* CIT is used with multiple NE connections and multiple NE types, the processor type and speed and the memory size will all factor into *WaveStar* CIT performance.

Before you begin   A user who has Windows NT / Windows 2000 System Administration privileges must install the software. That same user, then, becomes the *WaveStar* CIT System Administrator. The *WaveStar* CIT System

Administrator sets up the operating environment for other users. Some of these administration functions include:

- Assigning login IDs

- Assigning an initial password for each login ID

- Customizing the access privileges and security attributes for each login ID, and so forth.

The installation program cannot install system files or update shared files if they are in use by other programs. For this reason you should stop as many Windows® NT / Windows 2000 applications as possible, before starting with the installation procedure.

Installation   Complete the following steps to install the *WaveStar* CIT software on your PC:

....

1   Insert the *WaveStar* CIT CD-ROM (ComCode: 109074641) into the appropriate drive of your PC.

> **Result:**
>
> Autorun will start the install process.

....

2

IF	THEN
autorun does not start	manually start the program by clicking **Start** → **Run**, click on **Browse**, select the CD-ROM drive, and select **setup.exe**, click **Open** and click **ok**.
	Result: The **WaveStar CIT CD Browser** appears.
autorun starts	no action is required.
	Result: The **WaveStar CIT CD Browser** appears.

....

3   Click on **continue.**

....

4   Choose the entry **CIT Software.**

....

5   Select the **WaveStar CIT** area on the right.

....

....

6   Follow the on-screen instructions. Select **Full Install** when prompted.

....

7   If there are 2 or more LAN cards on the PC, select the LAN card
with the IP Address that corresponds to the OSI LAN, otherwise if
there is only 1 LAN card, *WaveStar* CIT will select it automatically.

....

8   If not yet available on your PC, install the **Acrobat Reader** by
selecting the respective area below the entry **CIT Software**.

....

9   The PC will have to be rebooted if the OSILLC driver is installed.
This is installed on the initial *WaveStar* CIT installation. Subsequent
upgrades do not require OSILLC driver installation.

E N D   O F   S T E P S

....

365-371-522   **Lucent Technologies**   2 4 - 7
Issue b, October 2001

Connecting the *WaveStar*® CIT to the NE

....

Overview   The *WaveStar* CIT can be connected to a network element in three
different ways:

- Direct LAN Access (point-to-point)

- LAN Access (network)

- Remote Access via DCC.

- Remote Access via TCP/IP

Direct LAN access   The *WaveStar* CIT (LAN card) is connected to the *WaveStar* TDM
(point-to-point)   10G (STM-64) via the "CIT" port of the user panel or through a
backplane connector (LAN I/O Panel). An Ethernet LAN cable
(10BaseT) with 4-wire RJ-45 connectors is used for this connection.

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*.

For wiring details, refer to the *WaveStar* TDM 10G (STM-64)
Installation Manual.

The following figure illustrates the Direct LAN Access
(Point-to-Point).

User Panel
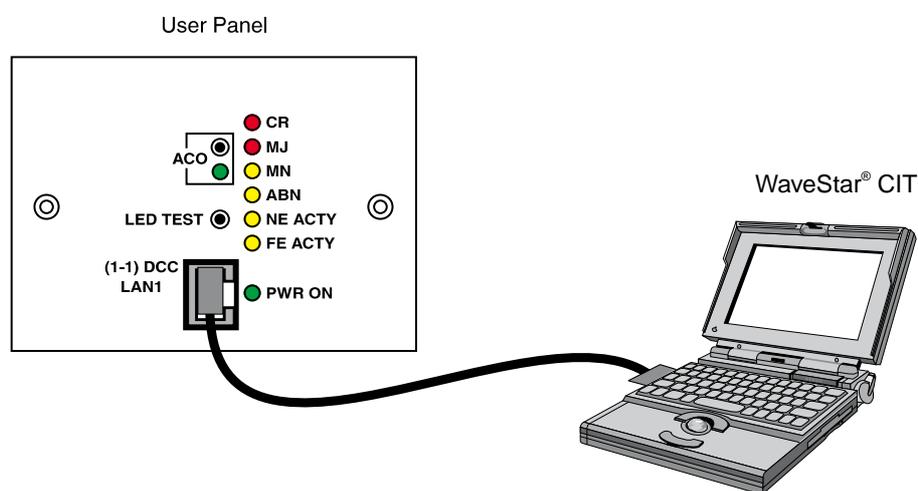
WaveStar CIT LAN access   *WaveStar* CIT access to more than one NE, e.g. within one site, can
(network)   be done via a Local Area Network (LAN). The LAN is connected to
the NEs by means of 10-BaseT Ethernet interfaces on 4-wire RJ-45
connectors.

....

The following figure illustrates the *WaveStar* CIT LAN Access (Network).
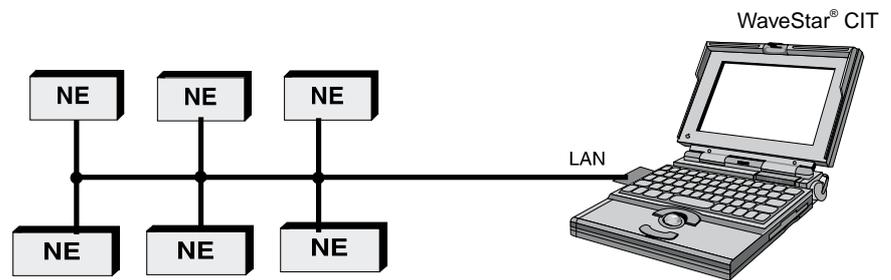
LAN Local Area Network

Important! 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**.

***WaveStar* access via Data Communications Channel (DCC)**

WaveStar CIT access to remote NEs can easily be done via the Data Communications Channel (DCC) which are part of the SDH aggregate or tributary signals. The CIT is connected via a point-to-point connection to one NE of the network (cf. "Direct Access"), which is then called the Gateway NE. All other NEs can be reached by the DCC. Thus, no additional management network is needed to connect the CIT to each individual NE.

The following figure shows an example of the access via the Data Communications Channel.
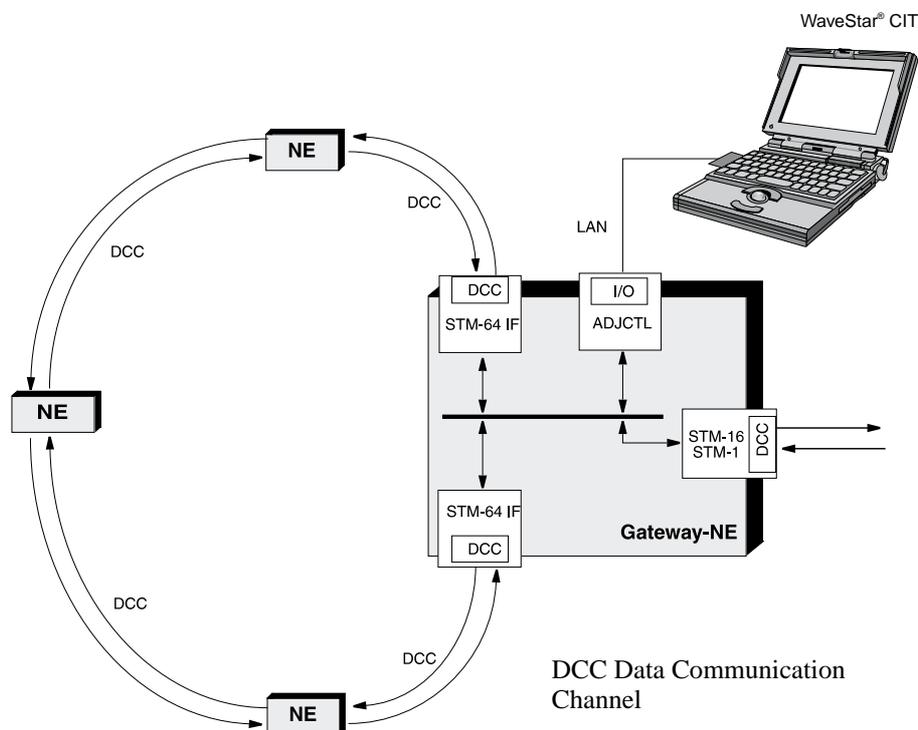
WaveStar CIT access via TCP/IP

The *WaveStar* CIT can be directly connected to remote NEs via TCP/IP.

In the absence of a directory server and/or a DNS, NEs that are linked to the CIT via TCP/IP will not appear in the Network Map in the Network View screen "Network element selection and login" (24-31)).

To establish a connection with a TCP/IP linked NE, the following procedure is performed by the CIT:

1. To connect to an NE, either via the normal CIT GUI or via TL1 cut-through, the user enters the TID of the NE and indicates **Graphical** or **TL1**.

2. The CIT assumes that this NE is linked via OSI and uses TARP to find the NE's NSAP. TARP searches the Data Cache (TDC) for the TID. If it is not already in the TDC, it will send out a broadcast query on the network.

3. If TARP fails to find the TID and NSAP, the CIT assumes that the connection is to be made via TCP/IP and searches its local Address file for the TID (refer to "Administering the address list at the *WaveStar* CIT" (3-19)). If the TID exists in the file, the CIT uses the associated IP Address and Port Number to connect to the NE via TCP/IP.

4. If the TID is not in the CIT Address list, the regular connection failure message is displayed..

More Information   Information on how to set up the Data Communications Network (DCN) are given in Chapter 14, "Management communication setup concepts" and "Configuring the data communication network" (3-6).

WaveStar® CIT login/logout procedure

Purpose   Many procedures throughout this document require the user to log into and log out of the *WaveStar* CIT GUI. The following procedure describes how this is accomplished. This procedure requires the *WaveStar* CIT to already be loaded on the PC and the PC connected to an NE.

Login procedure   Complete the following steps to log into the *WaveStar* CIT GUI:

1   Start the *WaveStar* CIT software by double clicking on the *WaveStar* icon.

2

IF ...	THEN ...
it is the first *WaveStar* CIT installation on the respective PC,	log into *WaveStar* CIT with **User Id**: "LUC01" or "LUC02" and **Password**: "LUC+01" or "LUC+02".
a previous *WaveStar* CIT version has already been installed on the respective PC,	log into *WaveStar* CIT with **User Id**: "LUC01" or "LUC02" and the last used **Password**.

3   Click **OK** to connect. *WaveStar* CIT will be "initializing views" for about 3 minutes. Click **OK** and read the legal notice.

4

IF ...	THEN ...
it is the first *WaveStar* CIT session,	proceed to Step 5.
it is not the first *WaveStar* CIT session,	**Stop! End of Task.**

5   In the *WaveStar* CIT Main Window, choose the option **Administration → Data Communications...** .

6   Make sure that the **Auto-Learn NSAP** box is not checked.

7   After initial login, it is recommended to change the passwords for the Super user logins immediately and to set up the logins for the other users.

Reference:

Please refer to "Administering user logins" (2-2).

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

Logout from *WaveStar* CIT   Complete the following steps to log out from *WaveStar* CIT:
....

1   In the *WaveStar* CIT main window, click **File → Exit**.

Result:

If there are still connections to NEs established from this CIT session, an alert window appears which shows the currently established connections.

....

2

IF	THEN
you are sure you want to exit	click **Yes** in the alert window.
you do not want to exit,	press the **No** pushbutton.

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

....

365-371-522
Issue b, October 2001

Lucent Technologies

2 4 - 1 3

General *WaveStar*® CIT concept

Overview
After login, *WaveStar* CIT comes up with the main window. This window allows you to perform general (NE independent) actions, e.g. administrative tasks, setting of preferences and options, etc. Furthermore, the main window serves as an entry screen for the log into the individual network element.

Interaction with network elements
WaveStar CIT provides two possibilities to interact with a network element:

- *WaveStar* System View: This is the graphical bay and shelf view of the network element.

- *WaveStar* Cut-Through: here, you can execute TL1 commands on a one-at-a-time basis or in a series/script.

The following figure illustrates the general *WaveStar* CIT concept.

```
                    ┌─────────────────────┐
                    │   WaveStar® CIT     │
                    │    Main Window      │
                    │   Network View      │
                    └─────────────────────┘
                      /                  \
          ┌─────────────────────┐   ┌─────────────────────┐
          │   WaveStar® CIT     │   │   WaveStar® CIT     │
          │    System View      │   │  Cut Through View   │
          └─────────────────────┘   └─────────────────────┘
                     │
          ┌─────────────────────┐
          │   WaveStar® CIT     │
          │     Shelf View      │
          └─────────────────────┘
```
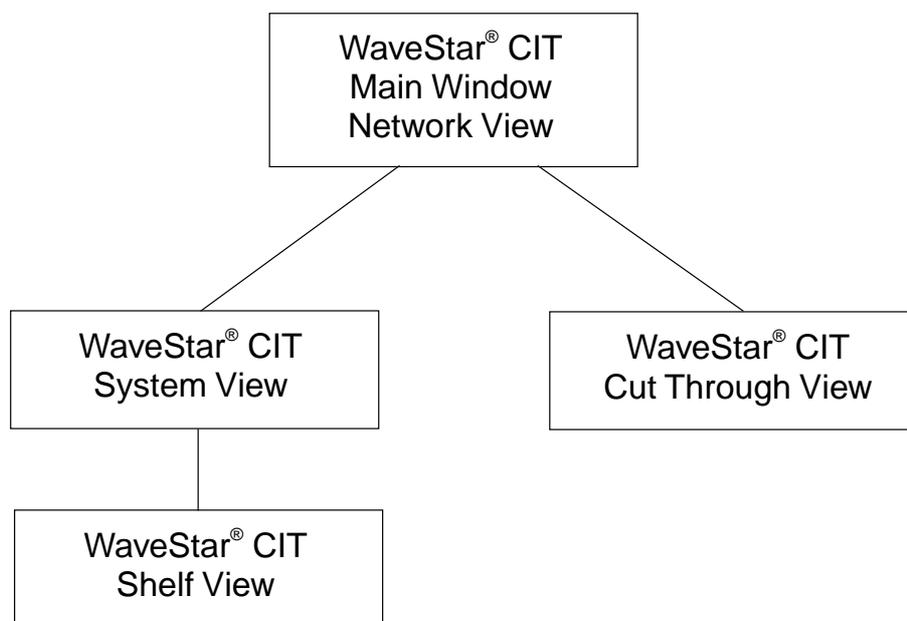
The structure of this chapter follows the *WaveStar* CIT concept.

⌐

WaveStar® main window

Overview

....

Purpose This chapter provides information you should know before performing specific tasks, e.g.:

- how to log into and log out from network elements

- the layout and the structure of the *WaveStar* CIT main window and its menus and sub-menus

- the elements of the *WaveStar* CIT user interface

- how to get help/information on items that are displayed on the *WaveStar* CIT main window

- how to display the system defaults for a particular component.

Menu structure overviews Also, this chapter presents menu structure overviews of the *WaveStar* CIT application with references to the parts of this manual where the respective descriptions and tasks can be found.

Contents

⌐

....

Elements of the *WaveStar*® CIT user interface

Overview   The graphical user interface of *WaveStar* CIT consists of:

- The main window for accessing all functions of *WaveStar* CIT

- *WaveStar* System View window

- *WaveStar* Cut-Through window

- Input and output windows for displaying and entering data

- Notification windows that are displayed to inform you, for example, about the termination of a function or to have entries confirmed.

Elements of the main window   The main window contains the following window bars:

- The title bar: shows the *WaveStar* CIT version.

- The menu bar: contains the main menu of *WaveStar* CIT.

- The status bar: displays information relevant in the current situation:

  - NE type, TID and, if available NE comment.

  - ID of currently logged in user

  - computer time settings, correlated to the local time

- The tool bar: provides push-button access to common menu options.

WaveStar® main window
Elements of the *WaveStar*® CIT user
interface

WaveStar® *CIT Tutorial*

The following figure illustrates the *WaveStar* CIT main window.

Title bar   Tool bar   Menu bar

User Local Environment

TID Entry Field

Graphical System View

Cut-Through View

Currently Logged into NE(s)   Status bar
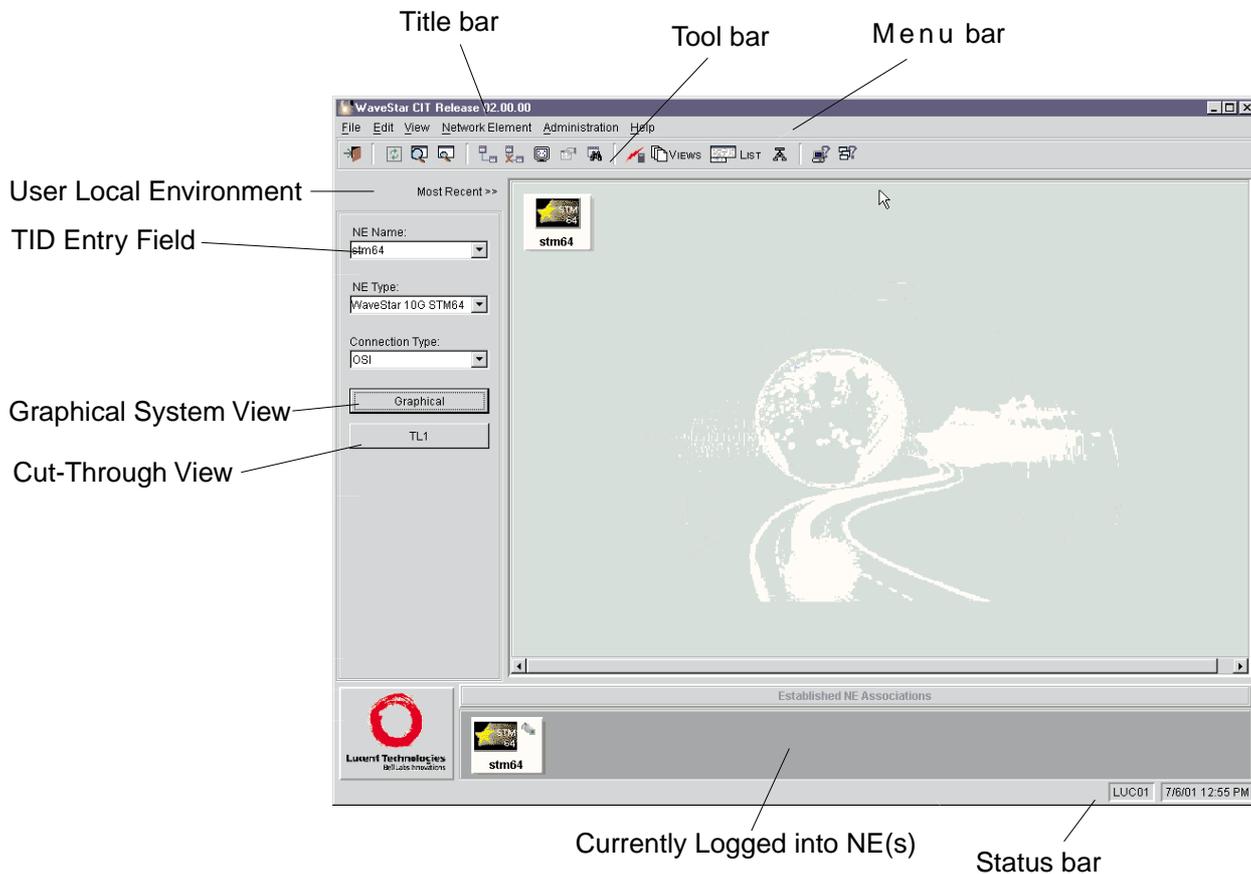
Tool bar of the *WaveStar*® CIT

Overview   The tool bar: provides push-button access to common menu options. The *WaveStar* CIT applications software supports tool-tips.

CIT toolbar   The following figure shows the toolbar of the *WaveStar* CIT application and its push-buttons.

Functions of the toolbar icons   To determine the meaning of a particular toolbar icon, place the cursor over that icon, hold for two seconds, and its name/function will be displayed.

The following table describes the push-buttons of the *WaveStar* CIT toolbar.

No.	Meaning	Equivalent Menu
1	**Exit CIT**	**File/Exit**
2	**Refresh Directory**	**View/Refresh View**
3	**Large icon view**	**View/Large Icons**
4	**Small icon view**	**View/Small Icons**
5	**Connect to NE**	**Network Element/Connect to NE**
6	**Disconnect from NE**	**Network Element/Disconnect from NE**
7	**Cut-Through view**	**Network Element/Cut Through**
8	**NE Properties** (not accessible)	**Network Element/Properties**
9	**Find**	**Network Element/Find**
10	**Prepare PCMCIA**	**Administration/Prepare PCMCIA Disks**
11	**Administer Views**	**Administration/Administer Views...**
12	**Address list**	**Administration/Adress List...**
13	**SONET Directory Service**	**Administration/SDS Administration**
14	**CIT About**	**Help/About WaveStar CIT**
15	**NE support**	**Help/Supported NEs**

User-defined toolbar settings

You can decide whether you want to have the tool bar displayed in the main window. Select the **View** → **Preferences** menu item. In the **Preferences** window select the **Network View** tab where in the **Misc.** group box you can either check or uncheck the **Hide Toolbar** check box.

Moreover, the **Toolbar** tab in the **Preferences** window allows you to change the above described standard setting of the toolbar icons. Also, the toolbar can be re-arranged to another location on the screen by using the **ToolBar Location** group box.

⌐

Standard window components

Overview   For the creation of input and output windows as well as the notification windows standard window components were used.

Diagram   The following diagram illustrates the standard window components. Please note that the following screens are just examples and are not exactly according to the current release.
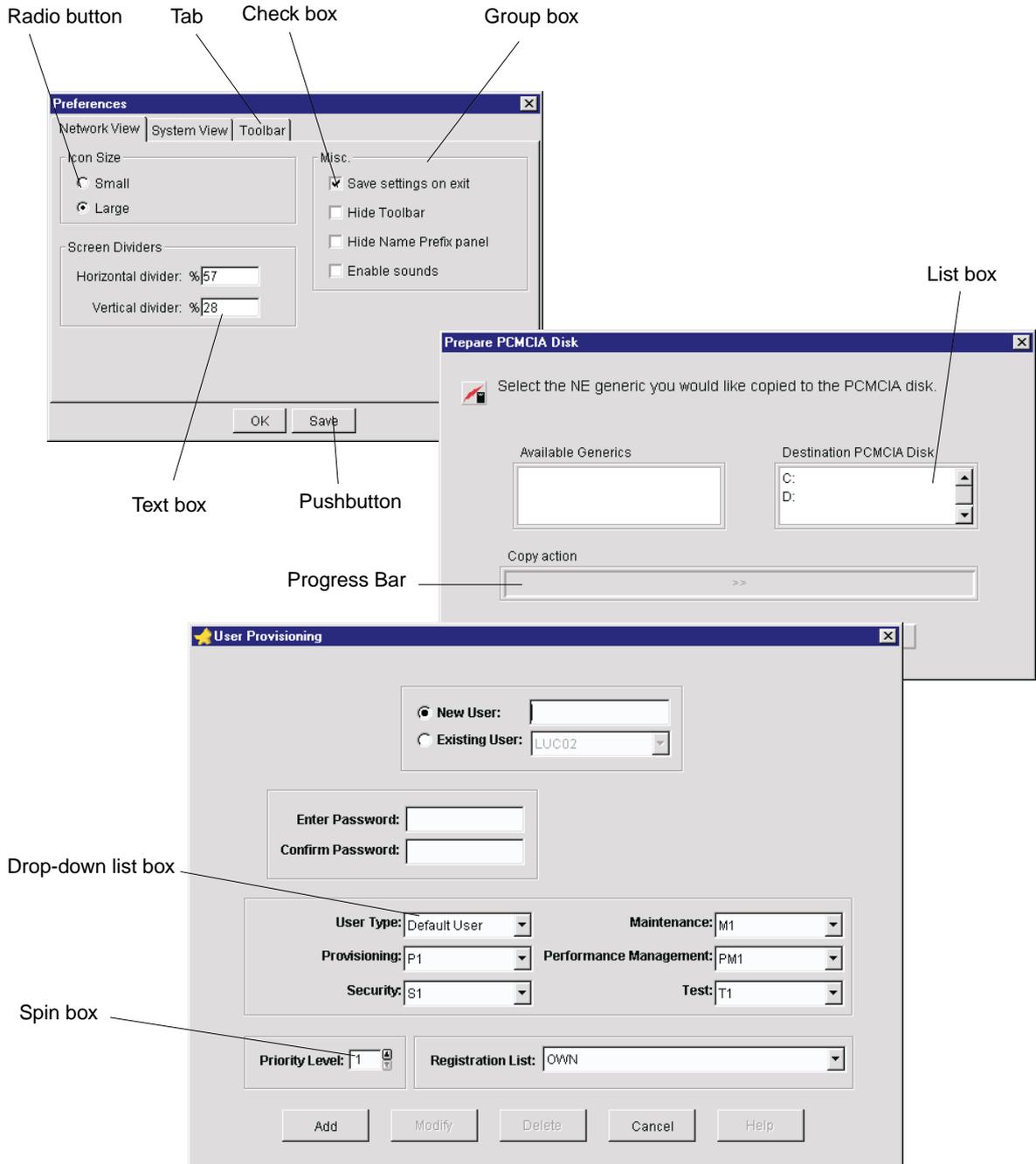
Functions of the window elements

The functions of the window elements are as follows:

Window element	Function
Text box	A text box allows you to enter a text via the keyboard.
Information field	An information field is read-only. It only displays data.
List box	A list box contains read-only data in list form. To scroll through a list you have to use the scroll bar at the right of the list box.
Radio button	A radio button functions as an on/off switch. If the radio button is pressed (on) the option next to it is selected. If it is not pressed (off), the option next to it has no meaning. Only one of the several radio buttons in a group box can be pressed at any one time.
Group box	A group box is used to indicate that a set of radio buttons or check buttons inside this box are logically related or to assign an additional title to the elements that are inside the group box.
Drop-down list box	A drop-down list box allows you to enter data by selecting an entry from a list that drops down after clicking on the triangle on the right of the box.
Pushbutton	The text of the pushbutton explains which function will be initiated when clicking on it. Pushbuttons like **OK**, **Cancel** and **Apply** are available in most of the windows. These general pushbuttons and their functions are explained below.
Check box	A check box functions as an on/off switch. If the check box is checked (on) the option next to it is selected. If it is not checked (off), the option next to it has no meaning. There is no limitation on how many check boxes in a group box can be pressed at the same time.
Spin box	A spin box only allows a limited set of discrete ordered input values. You have to use the up and down arrows to increment or decrement the value.
Tab	A window can contain several tabs. Clicking on a tab displays the corresponding contents in the window.

Window element	Function
Progress Bar	A progress bar shows the percentage of completion of a lengthy operation, e.g. when loading software.
Table	The table element is often used for reports, alarm lists, etc. The table element provides you with several possibilities to configure the contained data according to your individual needs:

• re-sizing of columns
  This is done by positioning the cursor on the right border of the column heading cell, pressing the left mouse button and dragging the cell border to the desired position.

• re-arrangement of the columns
  This is done by positioning the cursor on the column heading cell, pressing the left mouse button and dragging the cell to the desired position.

• sorting of the whole table depending on the selected column
  This is done by left-clicking on the respective column heading cell. The sort order depends on the column contents. For example, alarm descriptions will be sorted alphabetically (a...z), time and date will be sorted chronologically, alarm severity will be sorted in the order "critical", "major", "minor", "not alarmed".

Example: Table element: The following figure shows an example for the table element: The **NE Alarm List** window.

Selection windows

Overview   The selection windows enable you to select any AID, or in the case of the Ring ID selection screen, any ring, defined for the system. Upon initial invocation, the user is presented with a hierarchical equipment view of the system appears. But there are also other selection views such as a protection group view which can be accessed through tabs on the screen.

Tabs   The tabs appear in the following order:

- Equipment
- Protection Group
- Ring IDs.

Window layout   The following figure shows an example of a selection window.
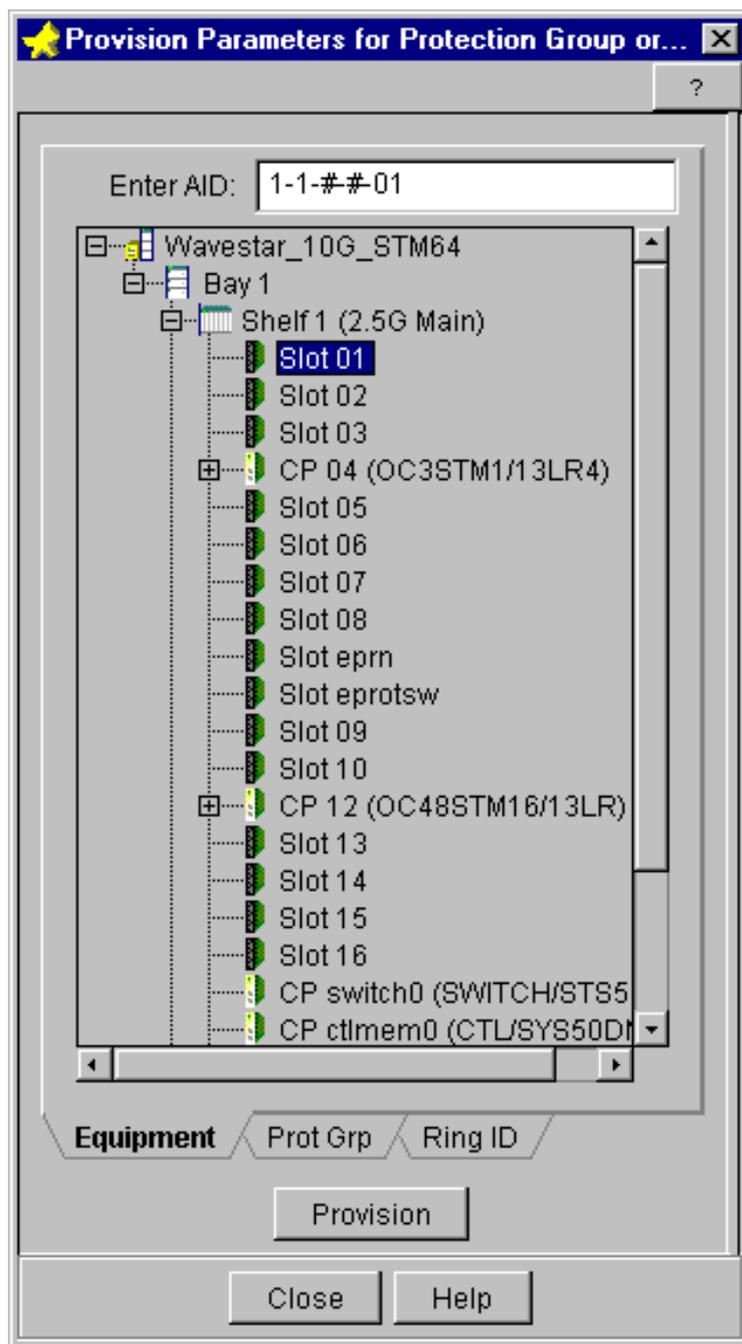
Specifying a component, a signal, etc.

There are two methods to specify/identify a particular component (bay, shelf, slot, circuit pack, port, etc.), signal, termination point, ring ID or protection group:

• by clicking through the directory tree

• by specifying the AID directly (for an overview of all applicable AIDs see "Overview of access identifiers" (15-18)).

Directory tree You can make multiple selections browsing through the directory tree until finally selecting the desired item. The network element components are organised in a tree structure from the system level down to the tributaries. Components of a lower level become visible by clicking on the "**+**" in front of a higher-level component.

Enter AID directly If you know the AID of the circuit pack and the signal identification - then you can enter it directly into the field labeled "Enter AID:". And, as you make each selection the directory tree will highlight that entry.

Select **or** *Provision* **button** It depends on the outer window type which selection in a selection window is valid and which is invalid. A valid selection can be recognized by means of the **Select** or **Provision** pushbutton at the bottom of the selection window. If a selection in the directory tree or in the **Enter AID** field is valid, the pushbutton is active and can be pressed. If a selection is invalid, the button is inactive.

General window handling

Title bar   Each input and output window and the main window of *WaveStar*®
CIT contain a title bar consisting of

- the window title,

- the minimize pushbutton (in the following minimize button),

- the maximize pushbutton (in the following maximize button)

- and the close pushbutton (in the following close button).

The following figure illustrates the title bar.

Window title area   Minimize button

Maximize button

Close button
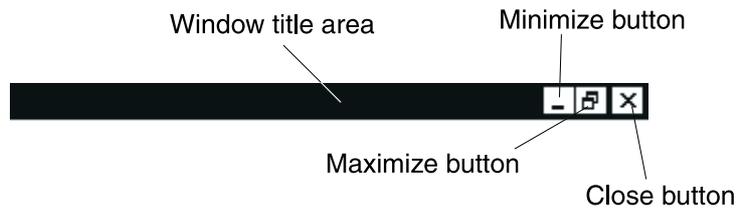
Minimizing a window and   To minimize a window and to open a minimized window proceed as
opening a minimized   follows:
window

IF	THEN
you want to minimize a window,	click with the left button of the mouse on the minimize button in the upper right corner of the window.
	Result:
	After minimizing a window, the window will appear on the Windows NT / Windows 2000 task bar.
you want to open a minimized window,	click with the left button of the mouse on the minimized window on the task bar to open it again.

Maximizing a window   To maximize a window proceed as follows:

1   Click with the left button of the mouse on the maximize button in the
upper right corner of the window.

> **Result:**
>
> After maximizing, the "square" in the maximize button becomes
> "two little squares".

You cannot move or resize a maximized window.

....

2   Click with the left button of the mouse on the maximize button with the "two little squares" in the right corner of the window.

You may also double-click with the left button of the mouse on the window title area to maximize a window or to get the normal size of the window.

E ND OF S TEPS
....

Closing a window   To close a window proceed as follows:
....

1   Click with the left button of the mouse on the close button in the upper right corner of the window to close the window.

> **Result:**
>
> Closing the main window will exit the *WaveStar* CIT application.

E ND OF S TEPS
....

Moving a window   To move a window proceed as follows:
....

1   Press the left button of the mouse on the window title area.

....

2   Keep the left button of the mouse pressed and move the window to the place you wish on the screen.

....

3   Release the left button of the mouse to place the window.

E ND OF S TEPS
....

....

365-371-522
Issue b, October 2001

Lucent Technologies

2 4 - 2 7

Resizing a window   To resize a window proceed as follows:

....

1   Move the mouse pointer to the border of the window.

Result:

The cursor changes from its default shape to a line with arrows.
The arrows indicate in which direction you can move the
window border.

....

2   Press the left button of the mouse.

....

3   Drag the window border to the new size.

....

4   Release the left button of the mouse.

Result:

The window is now changed to the new size.

E ND   OF   S TEPS

General pushbuttons

Overview
In the following some general pushbuttons are explained. They are part of many windows of the *WaveStar*® CIT graphical user interface. Whenever they appear they have the same function and lead to the same reaction.

Description of general pushbuttons
The following table describes the functions of the general pushbuttons.

Designation	Function
Apply	The **Apply** pushbutton allows you to commit changes in a dialog without closing the dialog. This control is useful in situations where a number of separate edit operations are to be invoked. It ensures that you do not have to keep invoking the edit window for each operation. An example is where you have to provision a number of cross connections separately. No changes are applied to a network element until the **Apply** or **OK** pushbutton has been selected.
Cancel	The **Cancel** pushbutton discards any changes to values in fields within an edit dialog and closes the dialog.
Close	The **Close** pushbutton closes an information-only window.
OK	The **OK** pushbutton commits any changes made within a window (if editable) and closes the window.
Refresh	If a window has been open for a while, the data displayed may no longer be up-to-date. The **Refresh** pushbutton allows you to obtain the most recent information.
Save As	Selecting the **Save As** pushbutton prompts you for a file name where *WaveStar* CIT shall store all data retrieved for the current window in ASCII format. The data stored includes visible data and data that is unvisible on the screen such as data accessible via a scroll bar.
Print	The **Print** pushbutton, e.g. in a report window, allows you to send the contents of the report, i.e. the data visible on the screen as well as data that is unvisible such as data accessible via a scroll bar, to the printer.

Basic operations

Overview This section provides hints on several basic operations you can perform using the menus of the *WaveStar*® CIT main window:

- Setting preferences

- Requesting version information

- Viewing the list of supported NE types

Setting preferences The **View-Preferences** menu item provides several possibilities to configure the *WaveStar* CIT to your individual needs:

- Tab **Network View**:

  - specify the size of the icons which represent the network elements in the main window. If a large amount of NEs is to be shown, it is advantageouse to choose **Small**.

  - re-configure the **Screen Dividers** between "User Local Environment" and SDS Listing (**Horizontal Divider**) field and the **Vertical Divider** in the main screen

  - some miscellaneous settings, e.g. hide toolbar, enable sounds.

- Tab **System View**:
  enables you to select the alarm format. Possible is either Critical (CR), Major (MJ), Minor (MN) or Prompt (PR), Deferred (DF), Info (INF). This is used e.g. in the NE Alarm List and in the Shelf View.

- Tab **Toolbar**:
  allows you to change the above described standard setting of the toolbar icons. Also, the toolbar can be re-arranged to another location on the screen by using the **ToolBar Location** group box.

The settings made in this window are retained for the respective user also after logging out.

Requesting version information To request the version information on *WaveStar* CIT select **Help About***WaveStar* **CIT** in the main menu. The Release and Subrelease number is displayed.

Supported NE types The *WaveStar* CIT application software may function with different types of NEs (for example, *WaveStar* Bandwidth Manager, *WaveStar* 2.5G, *WaveStar* TDM 10G and so forth). The full list of supported NE types can be viewed from the *WaveStar* CIT view screen by selecting **Help Supported NE(s)**.

⌐

Network element selection and login

NE selection possibilities

Setting up an association to an NE is facilitated by the NE selection possibilities in the *WaveStar*® CIT main window. You can

- select the NE by specifying its NE Name

- select the NE via the" Graphical System View".

NE Type field

NE Name field

WaveStar® TDM 10G icon
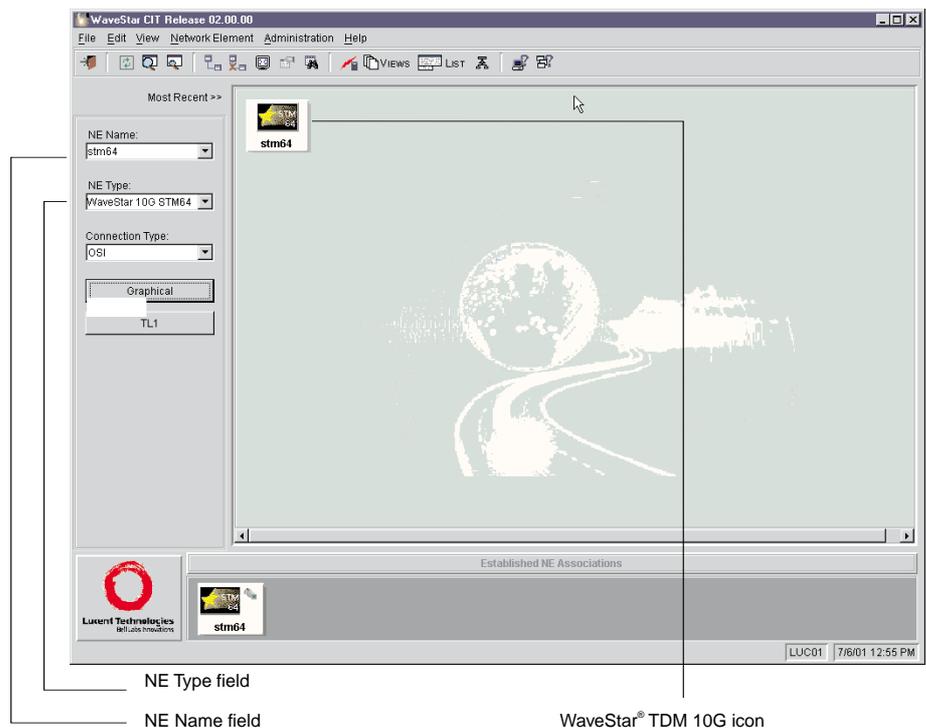
Before you begin

A prerequisite for logging into a network element is to have *WaveStar* CIT connected physically to the desired network element for a local login. For a remote login, connect the *WaveStar* CIT to any network element that is part of the sub-network containing the remote NE.

When you log into an NE for the first time, you have to select the NE by specifying a TID. You can also use this method for other logins.

Important! If an initial load to the non-volatile memory (NVM) of a newly established network element has been performed, the NE comes up with a standard name or Target Identifier (TID). This name is LUCENT-WAVESTAR-NE for all NEs. The first action that should be done is to change the TID. To be able to work in a network properly, each NE has to be given its unique TID. Please refer to "Changing the NE name (TID)" (3-2) for changing the TID.

Logging into an NE   In order to log into the NE, proceed as follows:

....

1   In the *WaveStar* CIT main window, enter the target identifier (TID) of the NE you wish to connect to in the **NE Name** box.

....

2   Select used **NE Type** and the preferred **Connection Type** and click **Graphical**.

  Result:

  The *WaveStar* CIT password is now being used for a login attempt to the NE.

....

3   If this password is accepted, no extra login window for the NE will appear. In this case, continue with Step 6.

....

4   Log in with your User Id and Password for the NE. For initial login after having the software installed the pre-installed Super-user logins "LUC01" and "LUC02" are used. The associated passwords are "LUC+01" and "LUC+02".

....

5   Click **OK** to connect.

....

6   Click **OK** to the legal notice.

  Result:

  The **System View** window appears for the selected NE.

....

7   After initial login, it is recommended to change the passwords for the Super-user logins immediately and to set up the logins for the other users.

  Reference:

  Please refer to "Changing your password" (2-18).

  E ND   OF   S TEPS ....

....

2 4 - 3 2   **Lucent Technologies**   365-371-522
Issue b, October 2001

Selecting and displaying an NE from the "Graphical System View"

If the *WaveStar* CIT has previously been used to display a system view for one or more NEs, then there exists a history of that event and the "User Local Environment" can be used to refer/select the previously displayed NEs.

....

1 In the "Graphical System View" pull down menu, select **Most Recent**.

> **Result:**
>
> The previously displayed NEs are shown in the area on the right of the window.

....

2 Double-click on the NE icon to establish the connection to the respective NE.

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

Saving NE views

Besides the **Most Recent** view, you have the possibility to save each individual NE view, i.e. the icons shown in the area on the right of the window.

....

1 Select from the menu bar **Adminstration** → **Administer Views...** (alternatively press the right mouse button in the "User Local Environment" area and select **Save View As...**).

....

2 Specify a name for the new view.

> **Result:**
>
> This name is now shown in the "User Local Environment" area under the **Saved Views** directory and will be retained also when logging out from the *WaveStar* CIT.

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

Administer NE views
The NE views can be administered by using the **Administration** menu in the menu bar.

IF	THEN
you want to add a NE view,	select from the menu bar: **Administration** → **Administer Views...** → **Add** (alternatively click on the icon Administer Views of the toolbar and then **Add**).
you want to modify a NE view,	select from the menu bar: **Administration** → **Administer Views...** → **Modify** .(alternatively click on the icon Administer Views of the toolbar and then **Modify**).
you want to delete a NE view,	select from the menu bar: **Administration** → **Administer Views...** → **Delete**.(alternatively click on the icon Administer Views of the toolbar and then **Delete**).

Editing the appearance of the icons
The appearance of the NE icons in the area on the right of the window can be tailored to your individual needs.

IF	THEN
you want to change the display from large icons to small icons and vice versa,	select from the menu bar: **View** → **Small Icons**; **View** → **Large Icons**.
you want to sort and arrange the icons by TID,	select from the menu bar: **View** → **Arrange Icons** → **by NE Name**.
you want to sort and arrange the icons by Type,	select from the menu bar: **View** → **Arrange Icons** → **by Type**.
you want to read the directory database and update the view,	select from the menu bar: **View** → **Refresh OSI View**.

Overview of the menu structure

The following table gives an overview where you can find the related description of the *WaveStar*® CIT main window menu structure.

Menu function		Submenu	refer to
File	**Save Settings**		"Network element selection and login" (24-31)
	Login as New User...		"Administering user logins" (2-2)
	Exit		"*WaveStar* CIT login/logout procedure" (24-12)
Edit	**Copy Icon(s) to...**		"Network element selection and login" (24-31)
View	**Refresh View**		"Network element selection and login" (24-31)
	Large Icons		
	Small Icons		
	Arrange Icons	**by TID**	
		by Type	
	Preferences...		"Basic operations" (24-30)
Network Element	**Graphical...**		"Network element selection and login" (24-31)
	TL1...		"Entering the Cut Through view" (24-63)
	Disconnect from NE... (only accessible if connection to NE already established)		"Logout from NE(s)" (24-37)
	Disconnect from All NEs (only accessible if connection to NE already established)		
	Find...		"Network element selection and login" (24-31)
	Properties...(only accessible if connection to NE already established)		

Menu function	Submenu		refer to
Administration	View CIT Administration...		"DCN protocols and services" (14-11)
			"NSAP address format" (14-16)
	Change Password...		"Changing your password" (2-18)
	Security	View User Logins...	"Displaying login information" (2-28)
		User Provisioning...	"The *WaveStar* CIT User Provisioning window" (2-5)
		Change Superuser Login ID	"Changing super user ids on the *WaveStar* CIT" (2-16)
	Prepare PCMCIA Disks...		"Performing an initial software download using the CIT" (10-2)
	Data Communications...		"Configuring the data communication network" (3-6)
	Serial COM Selection		
	Address List...		"Administering the address list at the *WaveStar* CIT" (3-19)
	Administer Views...		"Network element selection and login" (24-31)
	Defaults...		
	SDS Administration...(not accessible)		
Help	About WaveStar CIT...		"Basic operations" (24-30)
	Help Contents, Index & Find... (not accessible)		
	Supported NEs...		"Basic operations" (24-30)
	View Documents (not accessible)		

Logout from NE(s)

Procedure   You have several possibilities to disconnect from an NE. Complete the following steps to disconnect from NE(s) using the *WaveStar*® CIT GUI:

1   Determine if you want to exit *WaveStar* CIT completely or if you want to disconnect from NE(s)

2

IF	THEN
you want to exit *WaveStar* CIT completely,	in the *WaveStar* Main window click **File → Exit**, then **Yes** in the confirmation window.
you want to close all connections to all existing NEs,	in the *WaveStar* CIT Main window click **Network Element → Disconnect from All NEs.**
you want to to disconnect from single NE(s),	continue with Step 3.

3

If you want to disconnect from NE(s) in the	then
System View for the NE	click **File → NE Disconnect**, then **Yes** in the confirmation window.
WaveStar CIT Main window,	continue with Step 4.

4   Choose the menu option **Network Element → Disconnect from NE...**.

> **Result:**
>
> The **NE Disconnect List** window appears.

5   Select the NE you want to disconnect from in the list.

6   Press the **Disconnect** pushbutton.

E N D   O F   S T E P S

System view

Overview

Purpose   This section provides information about the layout and the structure of the *WaveStar®* **System View** window and its menus and submenus.

Contents

Elements of the System View window

Overview   The following figure displays the **System View** of the specified TID (which in this case is "STM64").
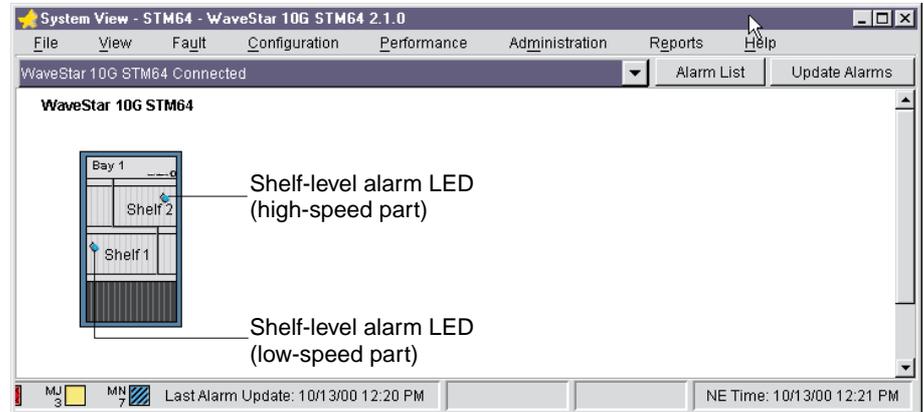
Components   The **System View** consists of a graphical representation of the bays, shelves, and alarms. You can interact with these components by using your cursor. Please note that the representation of the *WaveStar*® TDM 10G (STM-64) main shelf (cf. "How to get to the shelf map" (24-42)) is realized as two separate shelves:

- Shelf 1 (1-1) which is the low-speed part of the main shelf
- Shelf 2 (1-2) which is the high-speed part of the main shelf.

The bay level represents here the complete physical main shelf (shelf 1 + shelf 2).

Alarm list   The NE alarms can be displayed by pressing the **Alarm List** pushbutton.

Update alarms   In order to retrieve the latest alarms from the NE, the **Update Alarms** pushbutton can be used.

Alarm LEDs   In the **System View**, each shelf is functionally depicted with a shelf level alarm LED. This LED serves to indicate the highest level of alarm for that shelf. Also, the **System View** includes (in the lower left corner of the display) two alarm indicators (Prompt and Deferred). When alarms are present in the NE, these alarm indicators serve to indicate the alarm level and number of occurrences.

Command list	The most recently executed command is displayed on a command line near the top of the **System View** screen. Place your cursor on the drop-down arrow for this command line. To display a list of the last attempted commands, both those that were executed successfully and unsuccessfully, left-click on the "drop-down" arrow.
Setting system view preferences	The **View-Preferences** menu item provides several possibilities to configure the *WaveStar* CIT **System View** to your individual needs:

- Tab **WaveStar 10G STM64 Alarm Format**:
  enables you to select the alarm format. Possible is either the **SONET Format** Critical (CR), Major (MJ), Minor (MN) or the **SDH Format** Prompt (PR), Deferred (DF), Info (INF). This is used e.g. in the NE Alarm List and in the Shelf View.

- Tab **Audible Alarm Alerting**:
  allows you to enable or disable audible alarm alerting.

- Tab **System View Resizing**:
  allows you to enable or disable auto resizing of the system view.
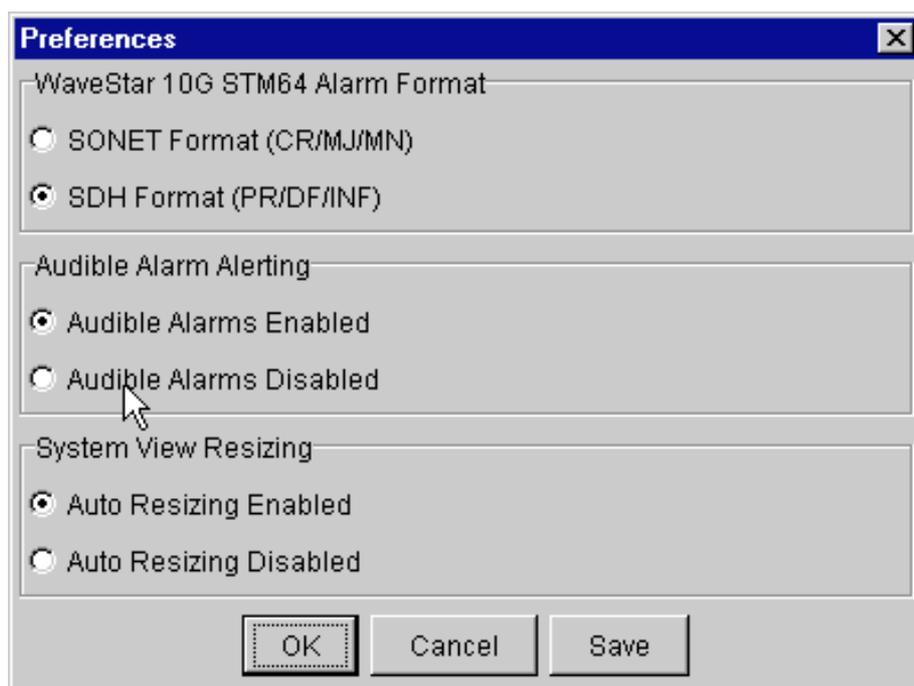
The settings made in this window are retained for the respective user also after logging out.

How to get to the shelf map	The next level of detail below the **System View** is the **Shelf View** where a graphical drawing of the selected shelf and the configured circuit packs is displayed.

From the *WaveStar* CIT **System View** window, either double-click left on the desired shelf, or right-click on the desired shelf (for example, Shelf 1 and Bay 1). In the displayed menu, select (highlight and left-click) **View Shelf #.**

Alternatively, the views can be changed via the menu bar:

1. Select **View** → **Change Equipment Display** in the *WaveStar* CIT System View window. A Windows-style explorer window opens.

2. Do one of the following:

    a. Enter the AID (for example, 1-1 or 1-2) of the desired shelf in the **Enter AID**: field, or

    b. In the left side of the window, click the "+" symbol at the left of the desired bay to expand bay information and select the desired shelf in the bay.

....

365-371-522
Issue b, October 2001

Lucent Technologies

2 4 - 4 1

The following figure illustrates the navigation through the graphical system view and the shelf view:
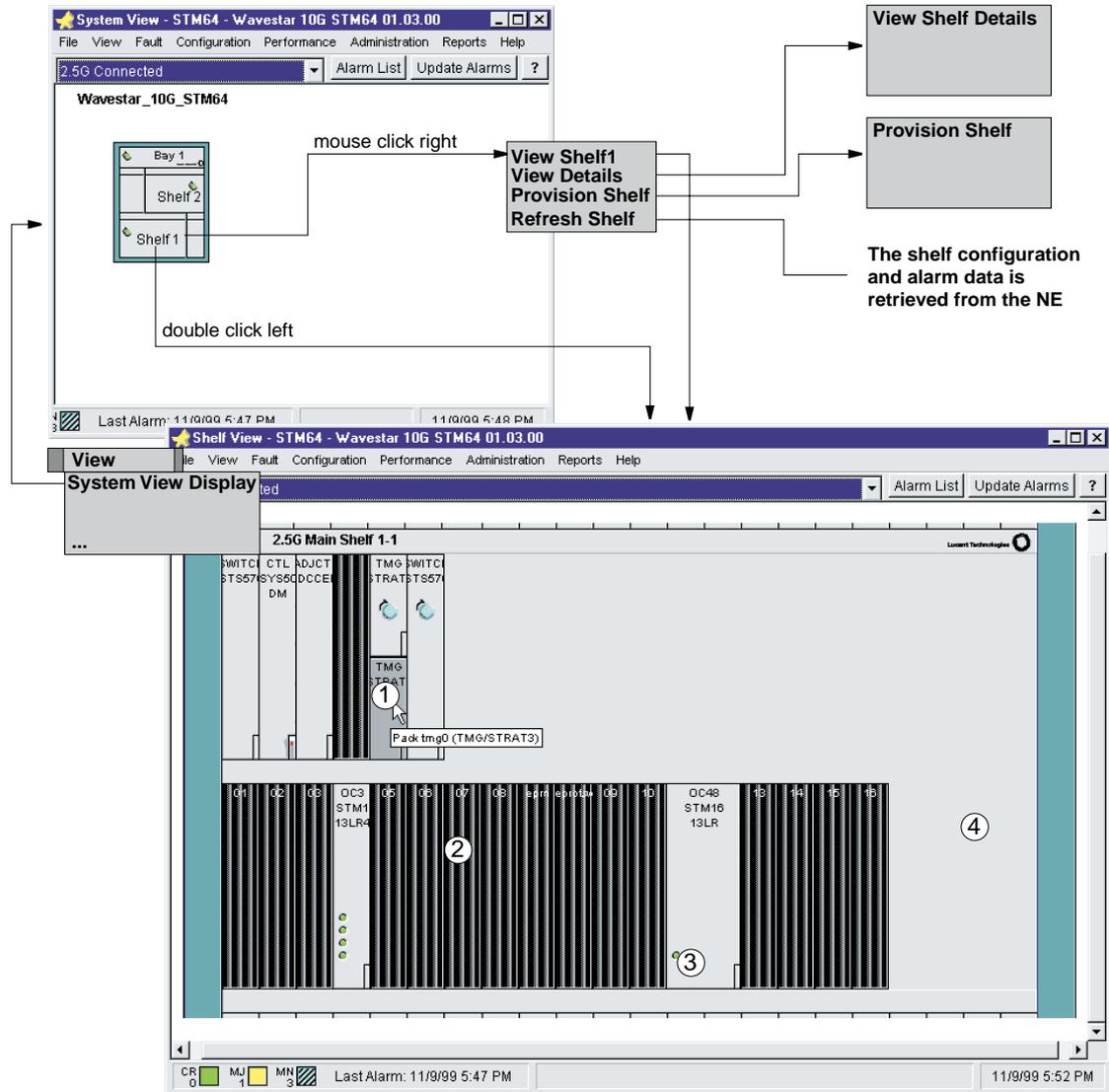
① View CP Details
mouse click right:

View Details
Provision Circuit Pack
Delete Circuit Pack
View Protection
Protection Switch
Refresh Circuit Pack

② View Slot Details
mouse click right:

View Details
Create New Circuit Pack
Delete Circuit Pack
Provision Slot
Refresh Slot

③ View Port Details
mouse click right:

View Details
Tributary Details
Provision Port #
View Protection
Protection Switch
View Cross Connections
Refresh Port #

④ View Shelf Details
mouse click right:

View Details
Provision Shelf
Refresh Shelf

Shelf view

....

The shelf map   The shelf map, a graphical representation of the selected shelf, displays the following:

- The top left corner displays the type of the shelf (Low speed part: ***2.5G Main Shelf 1-1***; High speed part: ***10G I/O Shelf 1-2***)

- Circuit pack slot positions are depicted

- Empty slots which have not been provisioned are depicted with a dark grey color

- Empty slots which have already been provisioned (or pre-provisioned) are depicted with a light grey color with dark grey diagonal stripes. The latch mechanism, which is located in the lower right-hand corner of the slot, is also depicted as being open.

- Equipped slots are shown with the label of the occupying circuit pack (slot 4 = OC3/STM1, slot 11/12 = OC48/STM16, etc.)

- You can hold the cursor on a slot for 2 seconds to display a more detailed label (that is, Pack ctlmem0 (CTLSYS50DM), Pack dccei (ADJCTL/DCCEI), and so forth.)

- A double-click on an ***equipped*** slot brings up the **View Circuit Pack Details** window for the individual circuit pack in this slot (e.g. for TMG/STRAT3 circuit pack, cf. "View Circuit Pack Details window" (24-45).

- A double-click on an ***unequipped*** slot brings up the **View Slot Details** window for this slot. This window shows which circuit packs are allowed for this individual slot and gives status information (cf. "View Slot Details window" (24-46)).

- A right-click on an ***equipped*** slot brings up the pop-up menu which provides several menu options shown in "View Circuit Pack Details window" (24-45), designation "1".

- A right-click on an ***unequipped*** slot brings up the pop-up menu which provides several menu options shown in "How to get to the shelf map" (24-42), designation "2".

- Each port unit has a light-emitting diode (LED) associated with each port. Each LED displays the alarm status (for example, green = no alarm, red = critical alarm, yellow = major alarm, cyan = minor alarm) for the associated port. A double-click on a port LED brings up the **View Port Details** window for this individual port (e.g. for Optical Port, cf. "View Port Details window" (24-49)).

....

- A right-click on a port LED brings up a pop-up menu which provides several menu options shown in "View Port Details window" (24-49), designation "3".

- A double-click on the shelf area (outside the slot area) brings up the **View Shelf Details** window for the complete shelf (e.g. for the high-speed part, cf. "View Port Details window" (24-49)).

- A right-click on the shelf area (outside the slot area) brings up a pop-up menu which provides several menu options shown in "How to get to the shelf map" (24-42), designation "4".

View Circuit Pack Details window   The following figures illustrate the **View Circuit Pack Details** window for TMG/STRAT3.
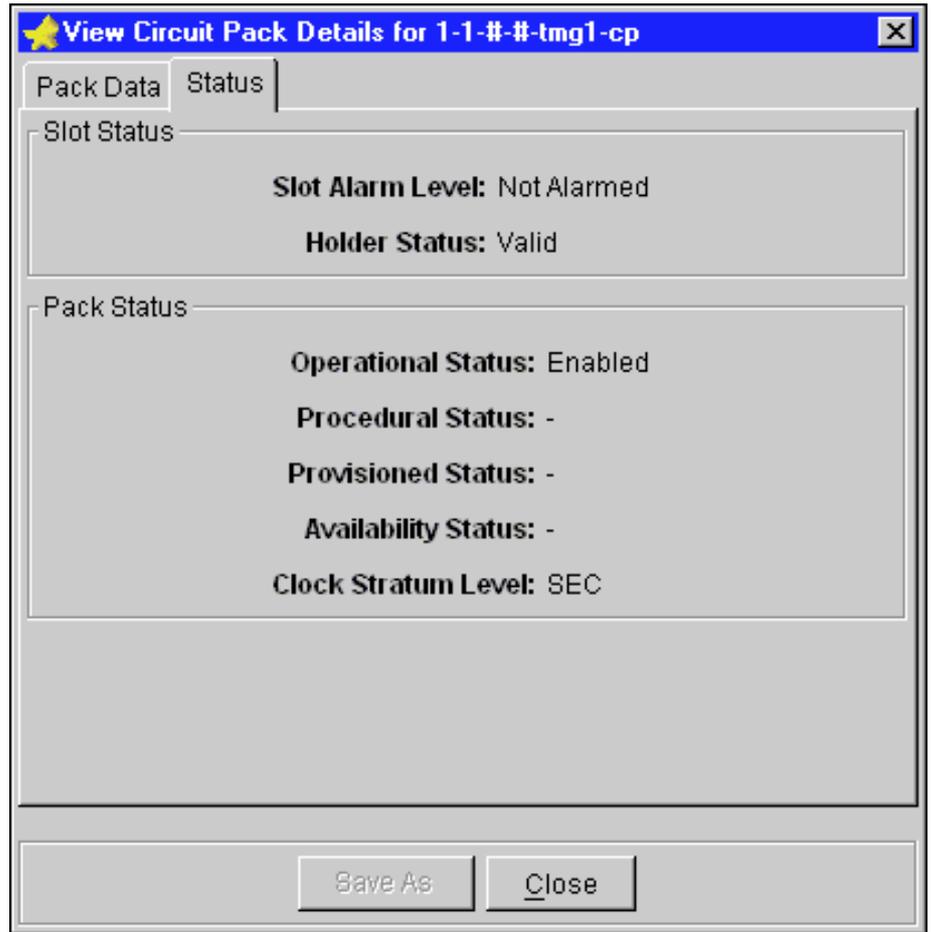
***View Slot Details* window**   The following figure illustrates the **View Slot Details** window.
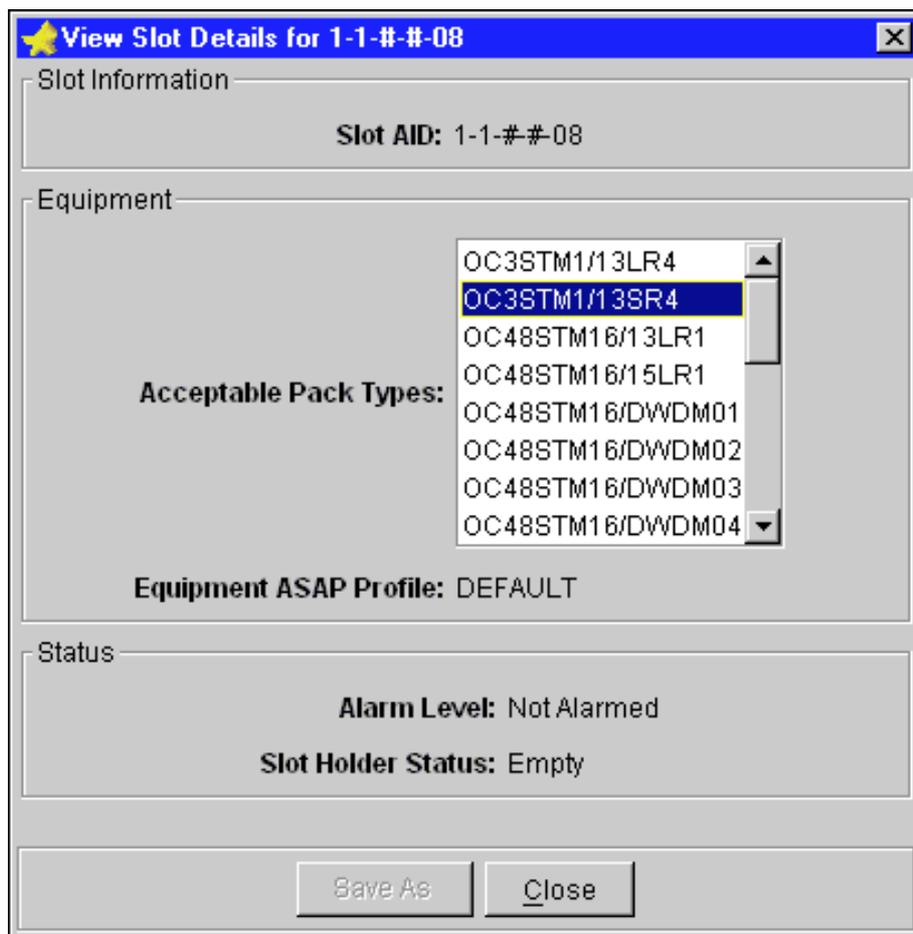
***View Port Details* window**   The following figures illustrate the **View Port Details** window.
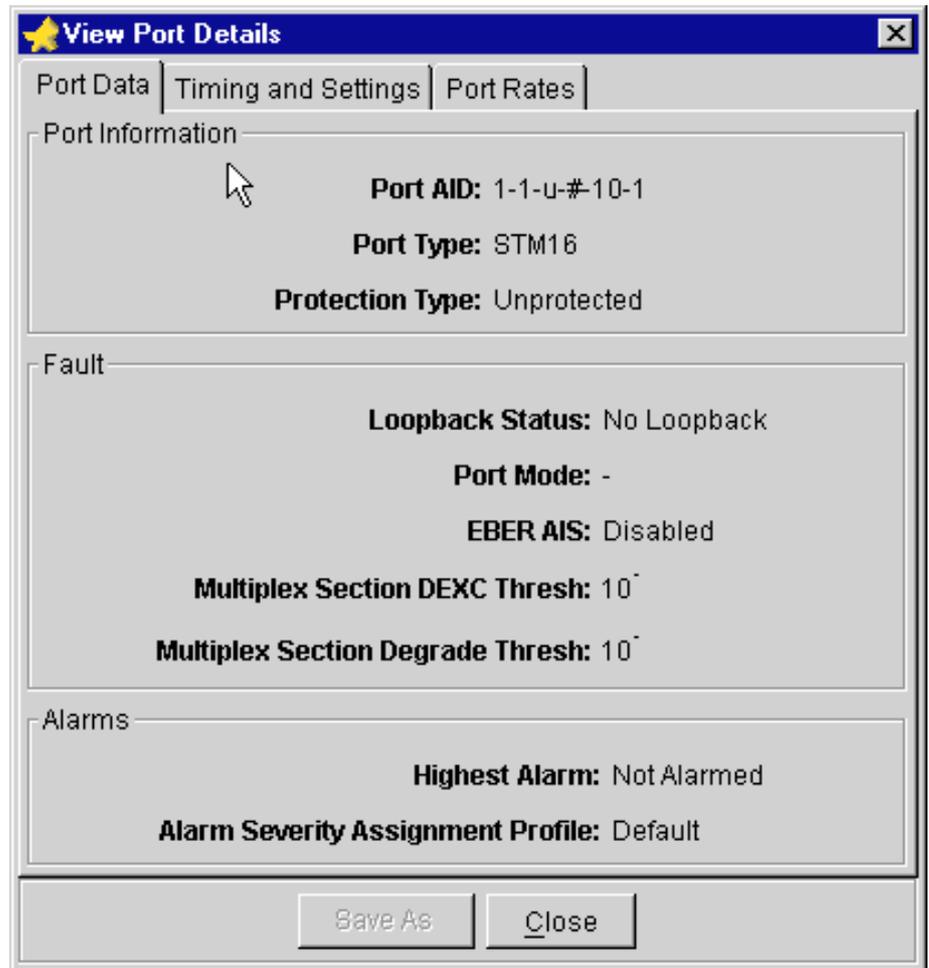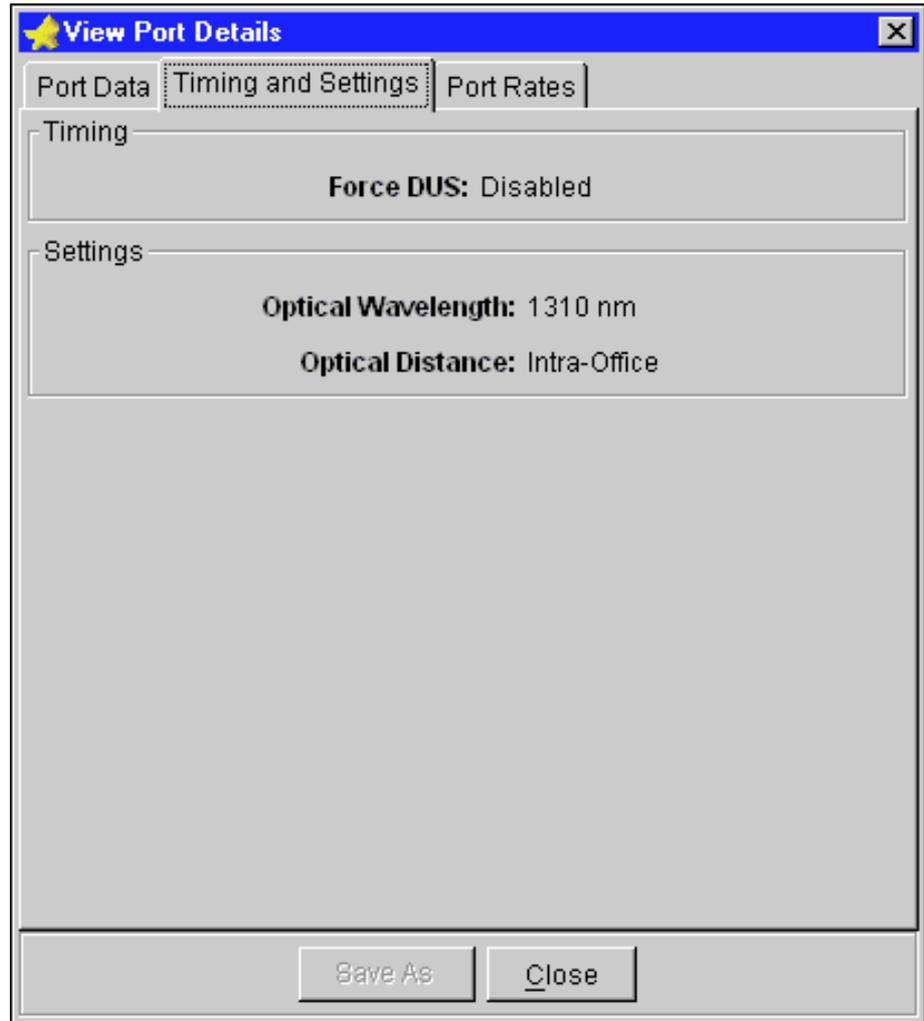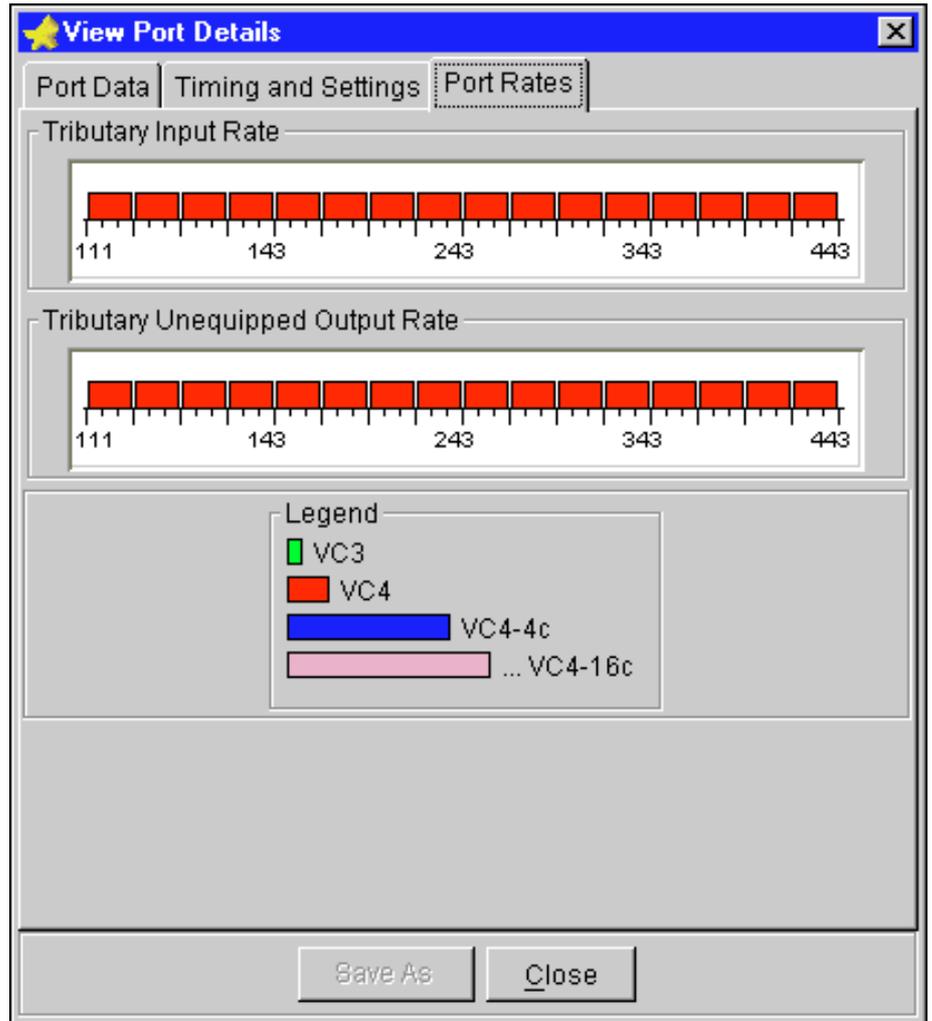
***View Shelf Details* window**   The following figure illustrates the **View Shelf Details** window.
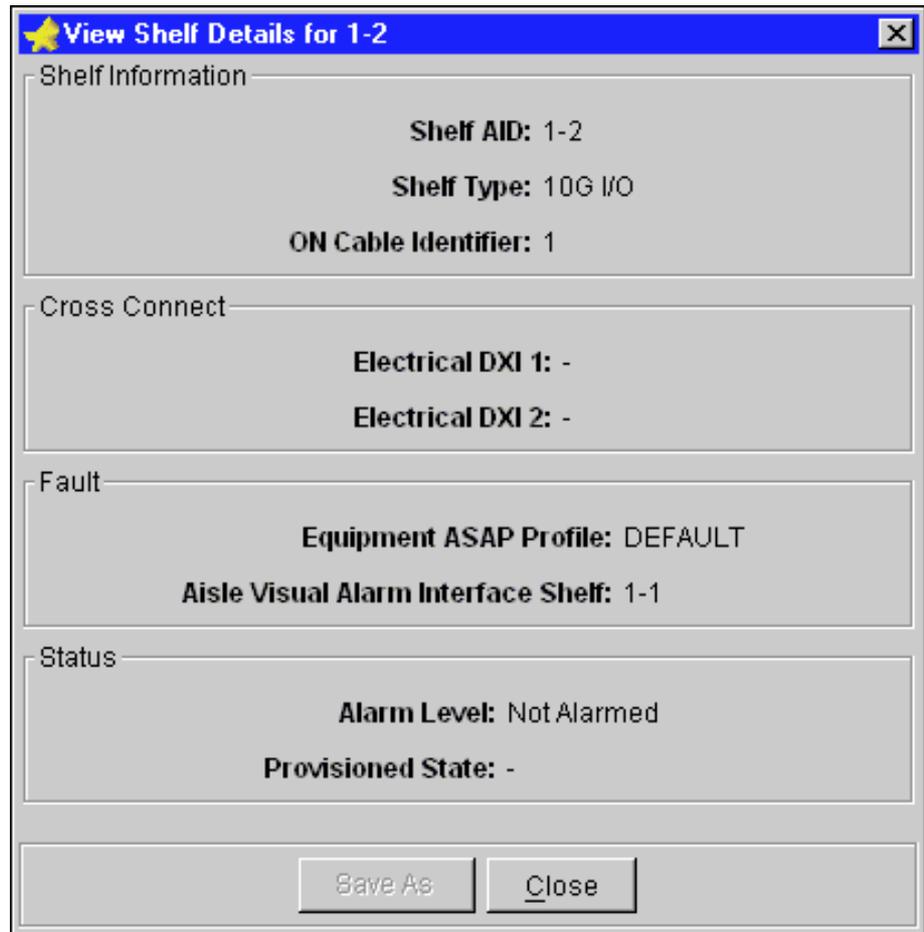
The ring map

Overview   For MS-SPRing protected rings, *WaveStar*® provides textual and
graphical information on the ring configuration, the so-called ring
map. Here, all the nodes in a selected ring are displayed.

How to get there   In order to view a certain ring map, use the menu **View** → **Rings** →
Ring Map.... The **View Ring Map** window appears. The windows type
explorer allows you to select a configured MS-SPRing. This can be
done either via the **PTN Grp** (Protection Group) tab which shows the
established MS-SPRing protection groups or via the **Ring ID** tab
which identifies the rings by use of their 15 character ring
identification.

Contents of the ring map   After pressing the **Select** pushbutton, the ring map is shown in table
format in the right window area and contains the following columns:

Column	Description/Behavior
Node NE Name	Up to 20 character Target Identifier (TID) of this Ring Node NE
Node Port	Port AID on this node. If this is an end node of an open ring, the field is left blank.
Node Port Direction	Values of E(ast) or W(est).
Node Neighbor NE Name	NE Name of the Neighbor NE. If this is an end node of an open ring, the files is left blank. Otherwise, up to 20 ASCII characters can be displayed.
Neighbor Port	Port AID on the Neighbor NE. If this is an end node of an open ring, the field is left blank.
Neighbor Port Direction	Values of E(ast) or W(est).
Node NE Title	First part of the NSAP Address for this Ring Node NE.
Node ID	Ring address of this Ring Node NE. May take the integer values 0 through 15, inclusive.

Graphical view   The graphical view of the ring map is invoked by the **Display Ring
Map Graph** pushbutton.

The individual NEs are shown as boxes with the NE name in them.
The bottom part of the window shows the data of the currently

selected NE. The currently selected NE is displayed as a bold box. You can select an NE by clicking on the respective NE box.

The data displayed at the bottom of the window for the selected NE are:

- NE Name
- NSAP Address of the NE
- Node ID
- Names of west and east neighbor NEs
- West and East NE Ports involved in the MS-SPRing

Graphical ring map display

The figure below is an example of how a ring map is graphically depicted.
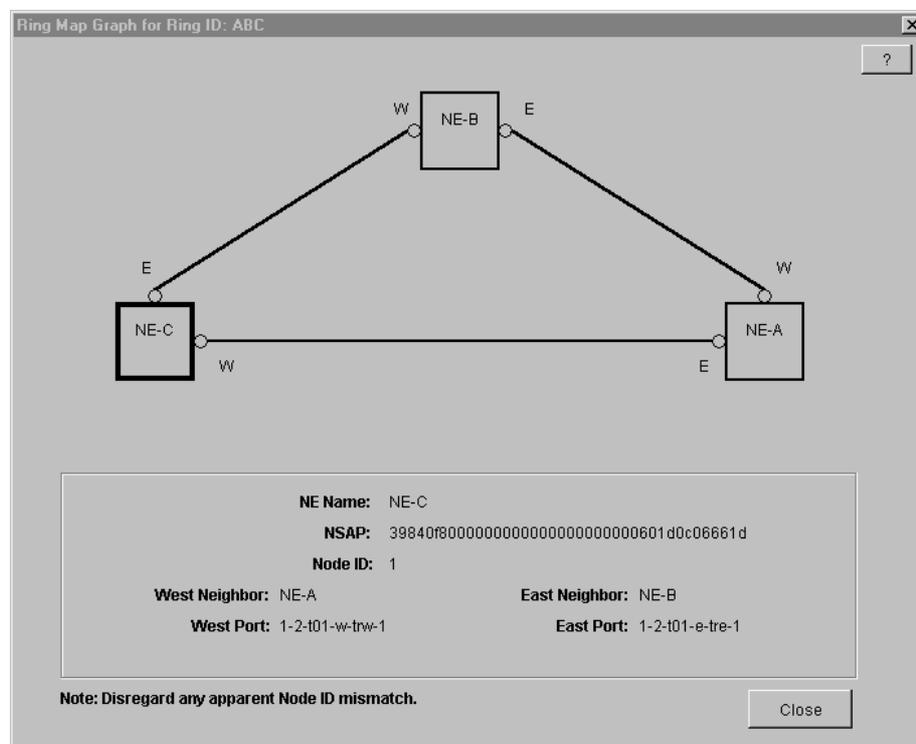
System view and overview of the shelf-view menu structure

Menu structure overview   The next figure gives an overview of the *WaveStar*® CIT system view or shelf view menu structure (after logging into a *WaveStar* TDM 10G (STM-64) network element).

The following table gives an overview where you can can find the related description of the *WaveStar* CIT system view or shelf view menu structure (after logging into a *WaveStar* TDM 10G (STM-64) network element).

Menu function	Submenu	please refer to
File	**Enable TL1 Logging ...**	"Working with logs" (24-70)
	Disable TL1 Logging ...	
	Set/Change TL1 Logging File	
	NE Disconnect	"*WaveStar* CIT login/logout procedure" (24-12)

Menu function	Submenu	please refer to
View	**Preferences…**	"Setting system view preferences" (24-40)
	System View Display	"Elements of the System View window" (24-39)
	Change Equipment Display...	
	View Equipment Details...	
	View Rolling Events	"View rolling events" (24-61)
	Rings **Ring Map...**	"The ring map" (24-51)
	Protection...	"Protection mechanisms" (18-10)
	Path Protection Group Names…	
	View Alarms **View Alarm Severity Assignment Profile...**	Chapter 16, "Alarm management concepts"
	View Alarm Configuration...	
	Cross Connections...	"Parameters of the window "View Cross Connections"" (7-5)
	VLAN Topology **VLAN Details**	Chapter 16, "Alarm management concepts"
	Loopback...	Chapter 16, "Alarm management concepts"
	DCC Terminations...	Chapter 14, "Management communication setup concepts"
	Misc. Discretes...	"Viewing Miscellaneous Discrete Inputs and Outputs" (4-75)
	Intershelf Bandwidth Utilization...	"Viewing the Intershelf Bandwidth Utilization" (8-12)
	Timing/Sync...	"Parameters of the "View Timing/Sync" window" (6-4)
	Software Generic...	Chapter 22, "Software upgrade concepts"
	NE Data...	Chapter 23, "Database backup concepts"
	Refresh Equipment...	"Elements of the System View window" (24-39)
	Refresh System View...	

Menu function	Submenu		please refer to
Fault	**NE Alarm List...**		Chapter 16, "Alarm management concepts"
	View Alarm Severity Assignment Profile		
	NE Alarm Log...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	Protection Switch...		Chapter 15, "Equipment provisioning concepts"
	Enter/Exit Maintenance Condition...	**Enter Maintenance Condition...**	Chapter 16, "Alarm management concepts"
		Exit Maintenance Condition...	
	Operate Output Misc. Discretes...		"Operating Miscellaneous Discrete Outputs" (4-77)
	Test	**LED...**	Chapter 16, "Alarm management concepts"
		Office Alarm...	
	Analysis	**Cross-Connect Loopback...**	Chapter 16, "Alarm management concepts"
		Facility Failure States...	AMTCG (Alarm Messages and Trouble Clearing Guide)
		Equipment Failure States...	
		View Current Optical Trib. Maintenance Signal...	
		View Current Port Optical Maintenance Signal...	
		View Current VCG Tributary Maintenance Signal...	
		View Current VCG Tributary delay within VC Group...	
	Reset	**Circuit Pack...** (not accessible)	
		Controller Group... (not accessible)	
		System...	AMTCG (Alarm Messages and Trouble Clearing Guide)
	Timing/Sync Protection Switch	**Clock Mode Switch...**	Chapter 17, "Timing provisioning concepts"
		Switch Timing Reference Switch...	
		Output Timing Reference Switch...	
	Laser Restart		AMTCG (Alarm Messages and Trouble Clearing Guide)

Menu function	Submenu		please refer to
Configuration	Provision...		"*WaveStar* CIT methods to perform provisioning" (15-3)
	Create New	Bay...	"Provisioning of new components" (15-5)
		Shelf...	
		Circuit Pack...	
		Protection Group...	
	Exchange Circuit Pack...		AMTCG (Alarm Messages and Trouble Clearing Guide)
	Delete...		"Provisioning of new components" (15-5)
	Path Protection Type...		"Creating a bidirectional DNI between one MS-SPRing protected ring and one SNCP protected ring." (7-73)
	Misc. Discretes...		"Configuring Miscellaneous Discrete Inputs and Outputs" (4-72)
	DCC Terminations...		"Configuring data communication channels" (3-39)
	Cross-Connection...		"Cross-connection management" (18-2)
	Timing/Sync		Chapter 17, "Timing provisioning concepts"
	Alarms	Alarm Severity Assignment Profile...	Chapter 16, "Alarm management concepts"
		Create NonReporting ASAPs...	
		Set ASAPs for a Shelf...	
		Alarm Configuration...	
	Software	Remote Backup...	Chapter 23, "Database backup concepts"
		Remote Restore...	AMTCG (Alarm Messages and Trouble Clearing Guide)
		Download Software...	Chapter 22, "Software upgrade concepts"
		Activate Software...	

Menu function		Submenu	please refer to
Performance	**View TCA Profile**	**Physical...**	Chapter 9, "Performance Monitoring"
		SDH Regenerator-Multiplex…	
		SDH HOVC Path...	
		Ethernet…	
	Provision TCA Profile	**Physical...**	
		SDH Regenerator-Multiplex…	
		SDH HOVC Path...	
		Ethernet…	
	Reports	**SDH Physical...**	
		SDH Regenerator Section...	
		SDH Multiplex Section...	
		SDH Path...	
		SDH UAT...	
		(not accessible)	
	Initialize Registers...		
	View PM Ports...		
	Provision Ports...		

Menu function	Submenu		please refer to
Administration	Change Password...		"Changing your password" (2-18)
	Change Notifications...		"Modifying user notification" (2-23)
	Security	View User Logins...	"Displaying login information" (2-28)
		View Logged-In Users...	
		Disable User Login...	"Administering user logins" (2-2)
		Enable User Login...	
		Logout NE User...	"Logging out NE users" (2-26)
		User Provisioning...	"Administering user logins" (2-2)
		Change Super User Id...	"Changing super user IDs on the NE" (2-17)
		Security Provisioning...	"Modifying user security parameters" (2-20)
	View NE Administration...		Chapter 3, "Management communication setup"
	View MAC Addresses...		"NSAP address fields" (14-17)
	Set TID...		"Changing the NE name (TID)" (3-2)
	Data Communications...		"Configuring the data communication network" (3-6)
	OSI Routing Map...		"OSI routing map and OSI neighbor map" (14-5)
	OSI Neighbor Map...		

Menu function		Submenu	please refer to
Reports	**Equipment Lists**	**Shelf...**	"Reports" (24-60)
		Pack...	
		Port...	
		VCG...	
		Trib...	
		Miscellaneous Discretes...	
	Status Lists	**Shelf...**	
		Pack...	
		Port...	
		Trib...	
	Cross-Connection List...		
	NE Alarm List...		
	NE ALarm Log...		
	NE Protection Switch Activity Log...		
	MS-SPRing Protection Switch List...		
	NE User Log...		
	NE Security Log...		
	(not accessible)		
	NE Notification Log...		
Help	**About This Network Element...**		"Basic operations" (24-30)
	Help Contents, Index & Find...		
	View Documents	**Alarm Messages and Trouble Clearing Guide**	
		User Operations Manual	

Reports

....

Overview   *WaveStar®* CIT allows you to generate reports of the NE equipment configuration, switched cross-connections, alarm lists, etc. via the **Reports** menu item.

Report formats   The reports are formatted as tables and can be saved to a specified file (ASCII format) and/or can be sent to a printer as well.

The following reports are provided on demand:

- Equipment lists for shelves, circuit packs or ports or tributaries
- Status lists for shelves, circuit packs, ports or tributaries
- Cross-connection list
- NE alarm list
- NE alarm log
- NE protection switch activity log
- MS-SPRing protection switch list
- NE user log
- NE notification log.

....

2 4 - 6 0   **Lucent Technologies**   365-371-522
                                                                             Issue b, October 2001

View rolling events

Overview There are some events (e.g. protection switch) which do not generate an alarm. Therefore it may be difficult for a user to determine whether such events occur. The "View rolling events" screen is intended to fill that void. The user can invoke it and leave it open, to see at an instant the latest received autonomous event notification.

The *Event View* window The **Event View** window can be invoked via **View → View Rolling Events** from the NE **System View** or **Shelf View** respectively.
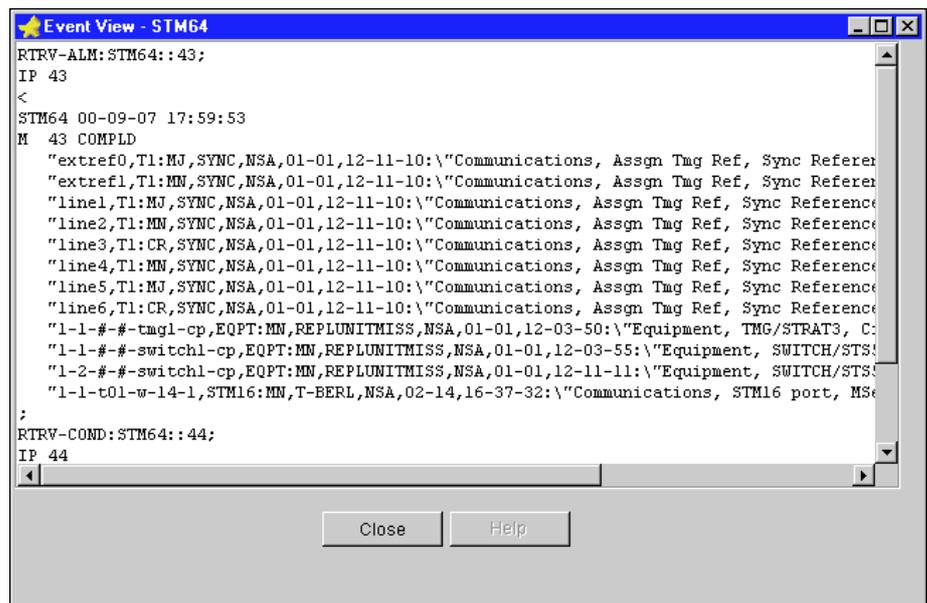
Syntax The syntax of the events shown in this window is the TL1 syntax. For details about TL1, please refer to the *WaveStar®* TDM 10G (STM-64) TL1 Reference Manual.

Log length The log is max. 256 lines long. As additional autonomous notifications are received in excess of 256, they are added to the screen at the bottom and the oldest entry (i.e., at the top) is removed.

⌐

Cut Through view

Overview

....

Purpose   This section provides information about the layout and the structure of
the Cut Through view window and its menus.

Usage of the *WaveStar*®   As an alternative to using the graphical-user-interface based System
***Cut Through* window**   View, the *WaveStar* TDM 10G (STM-64) provides a Cut-Through to
TL1 capability. With Cut-Through you can execute single TL1
commands or commands in a series/script.

Important! While in System View, the user is alerted with a warning
message to inform them that if they follow through with their
command it could be service impacting. As a contrast, Cut-Through
mode does not provide any warning message and thus the user does
not get a second opportunity to review/consider the consequences of
their command.

TL1 commands   For the detailed descriptions of each of the TL1 commands, please
refer to the *WaveStar* TDM 10G (STM-64) ***TL1 Reference Manual***

Contents

⏌

....

Entering the Cut Through view

The following figure is a functional illustration of the **Cut Through** view menus.

File	**Interactive**	Logs	Scripts	Help

File
Exit

Interactive
Select TL1 Listbox File...
Edit TL1 Listbox File...
Add last command to TL1 Listbox & File

Logs
Start...
View...
Time/Date Stamp

Scripts
New...
Edit...
Run...
Stop
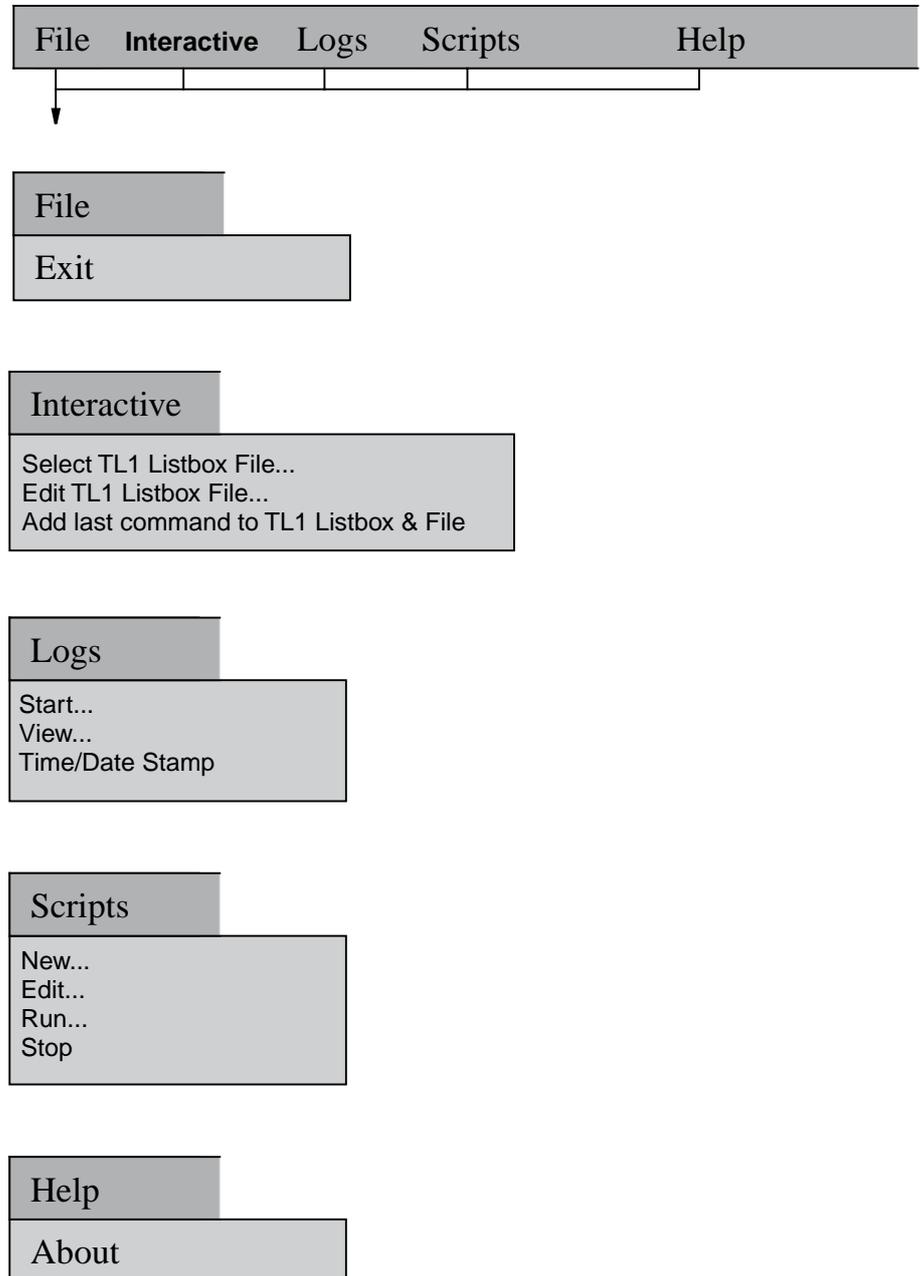
Help
About

Legend:

Interactive	see "Interactive – Manage a listbox file" (24-68)
Logs	see "Working with logs" (24-70)

Scripts   see "Working with script files" (24-69)

Help   see "Basic operations" (24-30)

Procedure   For entering the Cut-Through view, proceed as follows:

....

1   In the *WaveStar*® CIT main window, enter the **NE Name** and select
the **NE Type** and **Connection Type** of the NE for which you wish to
establish a Cut-Through session.

....

2   Select (left-click) the **TL1** option.

Result:

The **Connection Type Selection** window appears.

You can select the following modes:

- **TL1PeerComm (TL1 Command Response Only)**: by default,
this mode should be used if only TL1 command responses should
be displayed.

- **TL1 Maintenace (TL1 Alarms, EventsCommand Responses)**:
by default, this mode should be used to enter TL1 commands.

- **TL1MemoryAdministration (TL1 Database Changes and
Command)**: by default, this mode should be used to enter TL1
Database Change commands.

- **TL1test (TL1 Test and Command)**: by default, this mode should
be used for TL1 test and to enter TL1 commands.

The CIT application verifies commands prior to being sent.

....

3   Left-click on the **OK** button.

Result:

A selection window appears.

You can select the following modes:

- **TL1**: by default, this mode should be used to enter TL1
commands. The CIT application verifies commands prior to being
sent.

- **Command Builder**: This mode should not be used in the current
release.

....

4   Left-click on the **TL1** button.

....

Result:

The **Select Cut-Through Execution Mode** window appears.

You can select the following modes:

- **Filter TL1 Commands/Replies**: by default, this mode should be used to enter TL1 commands. The CIT application verifies commands prior to being sent.

- **Raw TL1 Commands**: In raw mode, any command entered will not be in any way modified or verified by the CIT application prior to being sent.

....

5 Click **OK**.

Result:

The **Cut Through** window appears.

....

6 As an alternative, the Cut-Through window can be accessed via the menu bar. Select **Network Element** → **TL1...**. In the **NE Selection** window, select the TID of the NE for which you wish to establish a Cut-Through session.

E N D   O F   S T E P S

Interactive – Execute TL1 single commands

Two methods   You can execute single TL1 commands on an interactive basis. There are two methods:

- If you know the exact TL1 command, enter the command on the command line

- If you do not know the exact command, left-click on the drop-down arrow, which is located at the end of the command line. A drop-down list appears, called the TL1 listbox file (for default location and editing of the listbox file, please refer to "Interactive – Manage a listbox file" (24-68)):

    - Scroll down the list until you see the command that you want to send to the NE or a command that is similar and which can be easily changed in the command line.

    - Left-click on the command to select/place it on the command line.

    - Left-click on the Send button. Your display should look similar to the following figure.
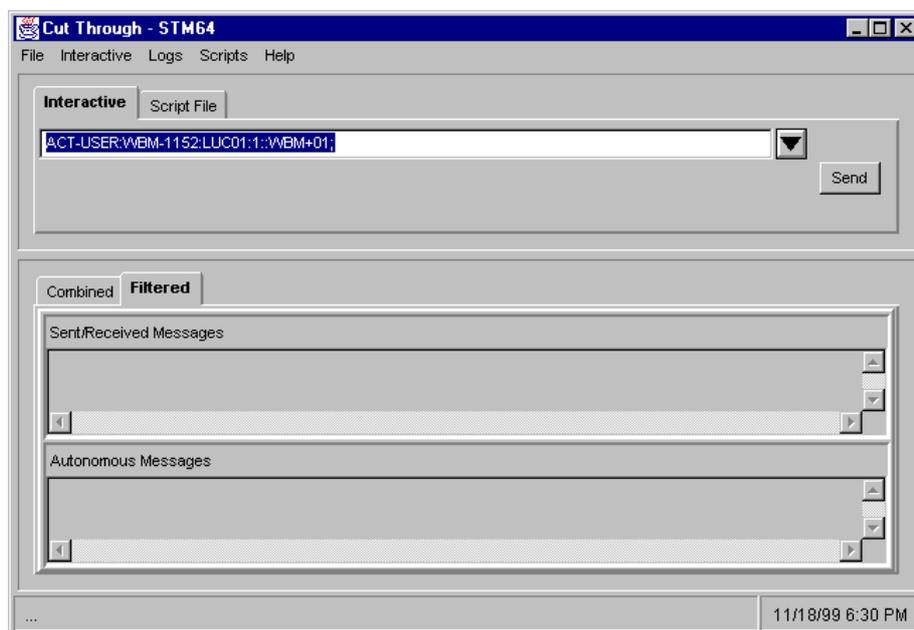
As desired, you can view the system response in a combined format, which is shown in the figure below, or a filtered format. Alternatively,

if **Raw TL1 Commands** has been chosen in the **Select Cut-Through Execution Mode** window, the system response is shown in raw mode.
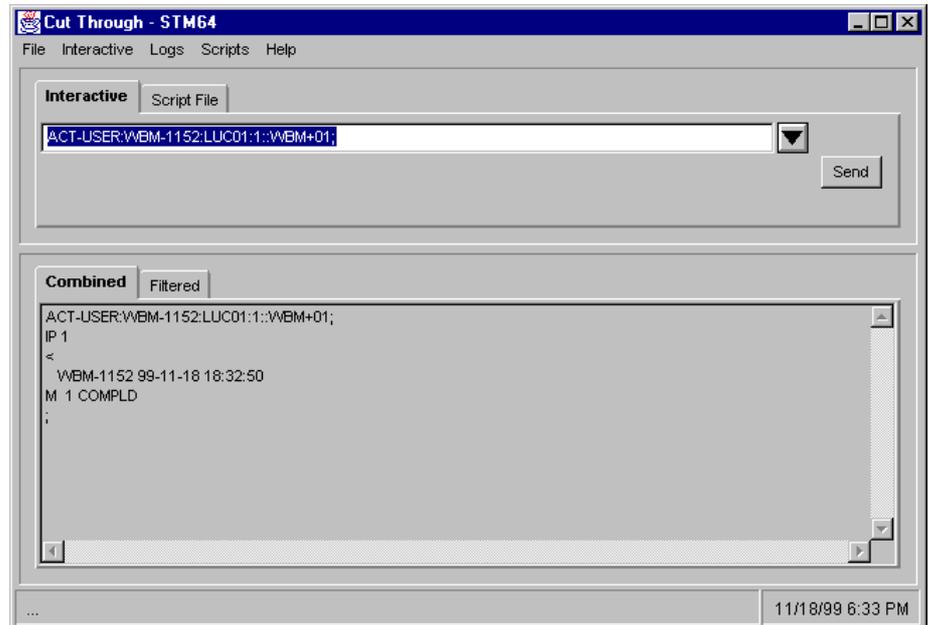
Combined format   The combined format displays commands in the order they are sent along with the received replies. Due to delays a command and its received reply may be separated by other commands and replies from other commands. This is especially true when sending commands from a script file where the commands are separated by a small delay interval.

Filtered format   The filtered format separates autonomous messages from the sent commands and their received replies. A sent command will not be displayed until its corresponding reply is received. Demarcation banners are added to help distinguish between sent/received messages.

Interactive – Manage a listbox file

Overview   *WaveStar*® CIT allows you to create and modify the TL1 listbox files which can be used for easier access to the appropriate TL1 commands in the interactive operating mode of the Cut Through interface.

Options   From the interactive menu, you can choose the following options:

- **Select TL1 Listbox File...** that already exists on the PC hard-disk drive.
  The text contained within the newly selected file will replace the previous text displayed in the interactive TL1 box when the drop-down arrow is clicked.

- **Edit TL1 Listbox File...** opens up the Wordpad application. The Wordpad application will open the file selected from the item above, or will default to the originally displayed TL1 list box found in the default file of[drive:]\Program Files\Lucent Technologies\WaveStar CIT\bin\tl1-listbox.txt. You can also manually overwrite the tl1-listbox.txt file outside of the CIT application so that it becomes the new default.

- **Add last TL1 command to** TL1 Listbox & File. No NE operations are performed in this step.
  The last command sent from the interactive command line will be added to the interactive TL1 listbox.

⌐

Working with script files

Overview   If several network elements have to be provisioned in the same way, it is advantageous to create a script file containing all the TL1 commands required for that provisioning. This script file can then be run on several NEs.

Executing a script file   You can execute a script by selecting **Scripts → Run...** from the menu bar.

In the **Run TL1 Script File** window, an existing script file can be selected by using the **Browse** button. The script file(s) exist(s) on the PC hard disk. The **Browse** button is simply the means to move up and down the directory structure in order to locate the desired script file.

When beginning to execute a script file, you are prompted once to select one of the following execution modes:

- Pause and Prompt each command

- Send all commands.

**Editing a script file /
Creating a new script file**   When editing a script file (**Scripts - Edit**) or creating a new script file (**Scripts - New**) the following should be observed:

- A script file can contain any number of lines of ASCII text.

- Any line not containing a valid command will be displayed in an Invalid TL1 message box.

- Lines beginning with forward-slash forward-slash "//" are ignored.

- A script file may be edited from the script menu, and a script may be stopped at any time by selecting **Stop** from the script menu.

- A log file can be created (automatically) for each script file by inserting *#logfile=on* on any single line. This can be inserted/turned-on at any time during the script file and can be turned on multiple times. Each time that a new *#logfile=on* command is executed, the previous logfile is closed. The generated log file will have a unique name consisting of the current time/date-stamp plus the name of the current script file.

- Between the individual commands, pauses can be inserted (e.g. *#delay=5000* indicates a pause of 5 seconds).

Working with logs

Overview   *WaveStar*® CIT can create log files for all TL1 commands that have been sent/received.

Start logging   To create a log file, proceed as follows:

1   From the menu bar, select **Logs** → **Start**, and you are prompted to:

1.   Enter the name for a new log file (for example, [drive:]\Program Files\Lucent Technologies\WaveStar CIT\bin\new-log-file), or

2.   Enter the full path name of an existing log file

2   Start the TL1 logging process by left-clicking on the **OK** button.

Result:

All TL1 commands sent/received are now logged in a filtered format.

E N D O F S T E P S

Stop logging   To stop logging TL1 commands, proceed as follows:

1   Select **Stop**.

Result:

Once TL1 logging is started, the next time that menu bar item **Logs** is selected, the start menu item will toggle to stop.

2   Close the user's log file.

E N D O F S T E P S

View log file   To view the log file, proceed as follows:

1   From the menu bar, select **Logs → View.**

Result:

You are prompted to enter the name of an existing log file that you wish to view.

2   Enter the name of the log file that you wish to view.

Result:

The selected log file is displayed using Wordpad. You can view and/or print the log file.

E ND OF S TEPS

Activating/deactivating time and data stamp   To activate or deactivate the time and data stamp, proceed as follows:

1   From the menu bar, select menu item **Logs-Time/Date Stamp** to toggle (on/off) the time and date stamp.

Result:

The time and date stamp, when on, is listed at the beginning of the command head for both the filtered view and the log file.

E ND OF S TEPS

Glossary

μ
Microns

NUMERICS

0x1 Line Operation

0x1 means unprotected operation. The connection between network elements has one bidirectional line (no protection line).

1+1 Line Protection

A protection architecture in which the transmitting equipment transmits a valid signal on both the working and protection lines. The receiving equipment monitors both lines. Based on performance criteria and OS control, the receiving equipment chooses one line as the active line and designates the other as the standby line.

1xN Equipment Protection

1xN protection pertains to N number of circuit pack/port units protected by one circuit pack or port unit. When a protection switch occurs, the working signals are routed from the failed pack to the protection pack. When the fault clears, the signals revert to the working port unit.

12NC (12-digit Numerical Code)

Used to uniquely identify an item or product. The first ten digits uniquely identify an item. The eleventh digit is used to specify the particular variant of an item. The twelfth digit is used for the revision issue. Items with the first eleven digits the same, are functionally equal and may be exchanged.

A   ABN

Abnormal (condition)

ABS (Absent)

Used to indicate that a given circuit pack is not installed.

AC

Alternating Current

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.

....

GLOSSARY   **Lucent Technologies**   365-371-522
GL - 2   Issue b, October 2001

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.

BCSR

Bidirectional Circuit Switched Ring

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

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

CPU
Central Processing Unit

CR (Critical (alarm))
Alarm that indicates a severe, service-affecting condition.

CRC
Cyclical Redundancy Check

Cross-Connect Map
Connection map for an SDH Network Element; contains information about how signals are connected between high speed time slots and low speed tributaries.

Crosstalk
An unwanted signal introduced into one transmission line from another.

CSMA/CD
Carrier Sense Multiple Access with Collision Detection

CTIP
Customer Training and Information Products

CTS
Customer Technical Support within Lucent Technologies

Current Value
The value currently assigned to a provisionable parameter.

D   DACS/DCS
Digital Access Cross-Connect System

Data
A collection of system parameters and their associated values.

Database Administrator
A user who administers the database of the application.

dB
Decibels

DC
Direct Current

DCC (Data Communications Channel)
The embedded overhead communications channel in the synchronous line, used for end-to-end communications and maintenance. The DCC carries alarm, control, and status information between network elements in a synchronous network.

DCE (Data Communications Equipment)
The equipment that provides signal conversion and coding between the data terminating equipment (DTE) and the line. The DCE may be separate equipment or an integral part of the DTE or of intermediate equipment. A DCE may perform other functions usually performed at the network end of the line.

DCF
Data Communications Function

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.

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 manag ement 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 6, December 1997.

Folded Rings

Folded (collapsed) rings are rings without fiber diversity. The terminology derives from the image of folding a ring into a linear segment.

Forced

Term used when a circuit pack (either working or protection) has been locked into a service-providing state by user command.

FR (Frame Relay)

A form of packet switching that relies on high-quality phone lines to minimize errors. It is very good at handling high-speed, bursty data over wide area networks. The frames are variable lengths and error checking is done at the end points.

Frame

The smallest block of digital data being transmitted.

Framework

An assembly of equipment units capable of housing shelves, such as a bay framework.

Free Running

An operating condition of a clock in which its local oscillator is not locked to an internal synchronization reference and is using no storage techniques to sustain its accuracy.

G   GB

Gigabytes

Gbit/s

Gigabits per second

GHz

Gigahertz

Global Wait to Restore Time

Corresponds to the time to wait before switching back to the timing reference. It occurs after a timing link failure has cleared. This time applies for all timing sources in a system hence the name global. This can be between 0 and 60 minutes, in increments of one minute.

GNE (Gateway Network Element)

A network element that passes information between other network elements and management systems through a data communication network.

H   Hard Failure

An unrecoverable nonsymptomatic (primary) failure that causes signal impairment or interferes with critical network functions, such as DCC operation.

HDB3 (High Density Bipolar 3 Code)

Line code for 2 Mb/s transmission systems.

HDLC (High Level Data Link Control)

OSI reference model datalink layer protocol.

HMI

Human Machine Interface

HML (Human Machine Language)

A standard language developed by the ITU for describing the interaction between humans and dumb terminals.

HO

High Order

Holdover

An operating condition of a clock in which its local oscillator is not locked to an external reference but is using storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronization reference.

Hot Standby

A circuit pack ready for fast, automatic placement into operation to replace an active circuit pack. It has the same signal as the service going through it, so that choice is all that is required.

HPA (Higher Order Path Adaptation)

Function that adapts a lower order Virtual Container to a higher order Virtual Container by processing the Tributary Unit pointer which indicates the phase of the lower order Virtual Container Path Overhead relative to the higher order Virtual Container Path Overhead and assembling/disassembling the complete higher order Virtual Container.

HPC (Higher Order Path Connection)

Function that provides for flexible assignment of higher order Virtual Containers within an STM-N signal.

HPT (Higher Order Path Termination)

Function that terminates a higher order path by generating and adding the appropriate Virtual Container Path Overhead to the relevant container at the path source and removing the Virtual Container Path Overhead and reading it at the path sink.

HS

High Speed

HW

Hardware

Hz

Hertz

I   I/O

Input/Output

IAO LAN

Intraoffice Local Area Network

ID

Identifier

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.

IS (In-Service)

A memory administrative state for ports. IS refers to a port that is fully monitored and alarmed.

IS-IS Routing

The Network Elements in a management network, route packets (data) between each other using an IS-IS level protocol. The size of a network running IS-IS Level 1 is limited, and therefore certain mechanisms are employed to facilitate the management of larger networks.

For STATIC ROUTING, the capability exists for disabling the protocol over the LAN connections, effectively causing the management network to be partitioned into separate IS-IS Level 1 areas. In order for the network management system to communicate with a specific Network Element in one of these areas, the network management system must identify through which so-called Gateway Network Element this specific Network Element is connected to the LAN. All packets to this specific Network Element are routed directly to the Gateway Network Element by the network management system, before being re-routed (if necessary) within the Level 1 area.

For DYNAMIC ROUTING an IS-IS Level 2 routing protocol is used allowing a number of Level 1 areas to interwork. The Network Elements which connect an IS-IS area to another area are set to run the IS-IS Level 2 protocol within the Network Element and on the connection between other Network Elements. Packets can now be routed between IS-IS areas and the network management system does not have to identify the Gateway Network Elements.

ISDN

Integrated Services Digital Network

ITM

Integrated Transport Management

ITM-NM

Integrated Transport Management Network Module

ITU

International Telecommunications Union

ITU-T

International Telecommunications Union — Telecommunication standardization sector. Formerly known as CCITT: Comité Consultatif International Télégraphique & Téléphonique; International Telegraph and Telephone Consultative Committee.

J   Jitter

Short term variations of amplitude and frequency components of a digital signal from their ideal position in time.

K   kbit/s

Kilobits per second

L   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 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

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 an 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 Channel
A STM-N wavelength within an optical line signal. Multiple channels, differing by 1.5 μm in wavelength, are multiplexed into one signal.

Optical Line Signal

A multiplexed optical signal containing multiple wavelengths or channels.

Original Value Provisioning

Preprogramming of a system's original values at the factory. These values can be overridden using local or remote provisioning.

OS (Operations System)

A central computer-based system used to provide operations, administration, and maintenance functions.

OSF

Open Software Foundation Operations System Function

OSI (Open Systems Interconnection)

Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Outage

A disruption of service that lasts for more than 1 second.

OW (Orderwire)

A dedicated voice-grade line for communications between maintenance and repair personnel.

P   Parameter

A variable that is given a value for a specified application. A constant, variable, or expression that is used to pass values between components.

Parity Check

Tests whether the number of ones (or zeros) in an array of binary bits is odd or even; used to determine that the received signal is the same as the transmitted signal.

Pass-Through

Paths that are cross-connected directly across an intermediate node in a network.

Path

A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Terminating Equipment

Network elements in which the path overhead is terminated.

PCB

Printed Circuit Board

PCM

Pulse Code Modulation

PCMCIA
Personal Computer Manufacturer's Card Interface Adapter

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.

Revertive
A protection switching mode in which, after a protection switch occurs, the equipment returns to the nominal configuration (that is, the working equipment is active, and the protection equipment is standby) after any failure conditions that caused a protection switch to occur, clear, or after any external switch commands are reset. (See "Non-Revertive".)

Revertive Switching
In revertive switching, there is a working and protection high-speed line, circuit pack, etc. When a protection switch occurs, the protection line, circuit pack, etc. is selected. When the fault clears, service "reverts" to the working line.

Ring
A configuration of nodes comprised of network elements connected in a circular fashion. Under normal conditions, each node is interconnected with its neighbor and includes capacity for transmission in either direction between adjacent nodes. Path switched rings use a head-end bridge and tail-end switch. Line switched rings actively reroute traffic over the protection capacity.

Route

A series of contiguous digital sections.

Router

An interface between two networks. While routers are like bridges, they work differently. Routers provide more functionality than bridges. For example, they can find the best route between any two networks, even if there are several different networks in between. Routers also provide network management capabilities such as load balancing, partitioning of the network, and trouble-shooting.

RSOH

Regenerator Section OverHead; part of SOH

RST

Regenerator Section Termination

RT

Remote Terminal

RTRV

Retrieve

RZ (Return to Zero)

A code form having two information states (termed zero and one) and having a third state or an at-rest condition to which the signal returns during each period.

S   SA

Service Affecting

SA

Section Adaptation

SD

Signal Degrade

SDH (Synchronous Digital Hierarchy)

A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

SDS

Standard Directory Service based on ANSI recommendation T1.245

SEC

Secondary

SEC

SDH Equipment Clock

Section

The portion of a transmission facility, including terminating points, between a terminal network element and a line-terminating network element, or two line-terminating network elements.

Section Adaptation

Function that processes the AU-pointer to indicate the phase of the VC-3/4 POH relative to the STM-N SOH and assembles/disassembles the complete STM-N frame.

Self-Healing

A network's ability to automatically recover from the failure of one or more of its components.

SEMF (Synchronous Equipment Management Function)

Function that converts performance data and implementation specific hardware alarms into object-oriented messages for transmission over the DCC and/or Q-interface. It also converts object-oriented messages related to other management functions for passing across the S reference points.

Server

Computer in a computer network that performs dedicated main tasks which generally require sufficient performance.

Service

The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

SES (Severely Errored Seconds)

This performance monitoring parameter is a second in which a signal failure occurs, or more than a preset amount of coding violations (dependent on the type of signal) occurs.

SH

Short Haul

Single-Ended Operations

Provides operations support from a single location to remote Network Elements in the same SDH subnetwork. With this capability you can perform operations, administration, maintenance, and provisioning on a centralized basis. The remote Network Elements can be those that are specified for the current release.

Site Address

The unique address for a Network Element.

Slot

A physical position in a shelf designed for holding a circuit pack and connecting it to the backplane. This term is also used loosely to refer to the collection of ports or tributaries connected to a physical circuit pack placed in a slot.

SM (Single-Mode Fiber)

A low-loss, long-span optical fiber typically operating at either 1310 nm, 1550 nm, or both.

SMN
SDH Management Network

SNC/I
SubNetwork Connection (protection) / Inherent monitoring

SNC/N
SubNetwork Connection (protection) / Non-Intrusive Monitoring

SNR (Signal-to-Noise Ratio)
The relative strength of signal compared to noise.

Software Backup
The process of saving an image of the current network element's databases, which are contained in its NVM, to a remote location. The remote location could be the *WaveStar* CIT or an OS.

Software Download
The process of transferring a generic (full or partial) or provisioned database from a remote entity to the target network element's memory. The remote entity may be the *WaveStar* CIT or an OS. The download procedure uses bulk transfer to move an uninterpreted binary file into the network element.

Software ID
Number that provides the software version information for the system.

SOH (Section Overhead)
Capacity added to either an AU-4 or assembly of AU-3s to create an STM-1. Contains always STM-1 framing and optionally maintenance and operational functions. SOH can be subdivided in MSOH (multiplex section overhead) and RSOH (regenerator section overhead).

SONET (Synchronous Optical Network)
The North American standard for the rates and formats that defines optical signals and their constituents.

Span
An uninterrupted bidirectional fiber section between two network elements.

Span Growth
A type of growth in which one wavelength is added to all lines before the next wavelength is added.

SPE
Synchronous Payload Envelope

SPI
SDH Physical Interface

Squelch Map
This map contains information for each cross-connection in a ring and indicates the source and destination nodes for the low-speed circuit that is part of the cross-connection. This information

is used to prevent traffic misconnection in rings with isolated nodes or segments.

SSM

Synchronization Status 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 Mbit/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

TBD
To Be Determined

TCA (Threshold-Crossing Alert)
A message type sent from a Network Element that indicates that a certain performance monitoring parameter has exceeded a specified threshold.

TDM (Time Division Multiplexing)
A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a portion of each signal one after another.

Through (or Continue) Cross-Connection
A cross-connection within a ring, where the input and output tributaries have the same tributary number but are in lines opposite each other.

Through Timing
Refers to a network element that derives its transmit timing in the east direction from a received line signal in the east direction and its transmit timing in the west direction from a received line signal in the west direction.

THz
Terahertz (10^{12} Hz)

TID (Target Identifier)
A provisionable parameter that is used to identify a particular Network Element within a network. It is a character string of up 20 characters where the characters are letters, digits, or special characters ("-", "+", "_", ".", "/").

TL1 (Transaction Language One)
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 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3, VC4, STM-1 or STM-4) that may be added to or dropped from a line signal.

Tributary
A path-level unit of bandwidth within a port, or the constituent signal(s) being carried in this unit of bandwidth, for example, an STM-1 tributary within an STM-N port.

Tributary Unit Pointer
Indicates the phase alignment of the VC with respect to the TU in which it resides. The pointer position is fixed with respect to the TU frame.

True Wave™ Optical Fiber
Lucent Technologies' fiber generally called non-zero dispersion-shift fiber, with a controlled amount of chromatic dispersion designed for amplified systems in the 1550/1310 nm range.

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 kbit/s to 2 Mbit/s.

Working

Label attached to a physical entity. In case of revertive switching the working line or unit is the entity that is carrying service under normal operation. In case of nonrevertive switching the label has no particular meaning.

Working State

The working unit is currently considered active by the system and that it is carrying traffic.

WRT (Wait to Restore Time)

Corresponds to the time to wait before switching back after a failure has cleared, in a revertive protection scheme. This can be between 0 and 15 minutes, in increments of one minute.

WS

Work Station

WTR (Wait to Restore)

Applies to revertive switching operation. The protection group enters the WTR state when all Equipment Fail (EF) conditions are cleared, but the system has not yet reverted back to its working line. The protection group remains in the WTR state until the Wait-to-Restore timer completes the WTR time interval.

X   X.25

An ITU standard defining the connection between a terminal and a public packet-switched network

X.25 Interface/Protocol

The ITU packet-switched interface standard for terminal access that specifies three protocol layers: physical, link, and packet for connection to a packet-switched data network.

Z   Zero Code Suppression

A technique used to reduce the number of consecutive zeros in a line-coded signal (B3ZS, B8ZS).

Index