Lucent Technologies
Bell Labs Innovations

WaveStar® LambdaRouter 128/256 Release 2.0

User Operations Guide

365-375-001
Issue 2
October 2001

Notice

The information in this document is subject to change without notice. Lucent Technologies assumes no responsibility for any errors that may appear in this document.

Mandatory Customer Information

FCC Compliance

This equipment is designed to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions manual, may cause interference to radio communications.

Trademarks

MicroStar is a trademark, and WaveStar is a registered trademark of Lucent Technologies.
Java is a registered trademark of Sun Microsystems, Inc.
Telcordia and CLEI are trademarks, and COMMON LANGUAGE is a registered trademark of Telcordia Technologies, Inc.
Metral is a trademark of Berg Technologies, Inc.
FIND-R-SCOPE is a trademark of J. W. Industries, Inc.
Pentium is a trademark of Intel Corporation.
PowerPoint, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Limited Warranty

The terms and conditions of sale include a one-year warranty on hardware and 90-days on software.

Ordering Information

To order this document, contact the Lucent Technologies Customer Information Center (CIC) at 1-888-LUCENT8 (1-888-582-3688) or *http://www.lucent8.com*. The document order number is 365-375-001.

Support Telephone Numbers

Information Product Support Telephone Number

Contact the CIC at 1-888-LUCENT8 (1-888-582-3688) or *http://www.lucent8.com*.

Technical Support Telephone Number

The Lucent Technologies Global Technical Support Services (TSS) Contact Center provides a technical assistance telephone number that is monitored 24 hours a day. For technical assistance, in the United States call 1-866-LUCENT8 (1-866-582-3688). International customers call +630-224-4672.

Developed by the Lucent Learning Organization.

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar LambdaRouter 128/256 Release 2.0
User Operations Guide

365-375-001 Issue 2 Date: 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

8 Management Communication Setup Tasks

9 Equipment Configuration Management Tasks

About this information product

Purpose

The *WaveStar LambdaRouter 128/256 Release 2.0 User Operations Guide* provides the information a user needs to operate the Lucent Technologies *WaveStar*® LambdaRouter optical switch.

Reason for reissue

This is the second issue of this User Operations Guide. This issue supports the Generally Available Release 2.0 WaveStar LambdaRouter 128/256.

Safety labels

The following safety labels are used in this User Operations Guide:

WARNING

Indicates the presence of a hazard that can cause death or severe personal injury if the hazard is not avoided.

CAUTION

Indicates the presence of a hazard that will or can cause minor personal injury or property damage if the hazard is not avoided. Caution is also used for property-damage-only accidents, including equipment damage, loss of software, or service interruption.

Intended audience

This user guide is intended for use by all WaveStar LambdaRouter 128/256 operations and maintenance technicians.

How to use this information product

This user guide consists of reference and task chapters. The reference chapters provide detailed information for understanding the security, configuration, alarm monitoring and fault management, cross-connection, and software features of the WaveStar LambdaRouter 128/256.

The task chapters provide detailed procedures for performing operations, administration, and provisioning tasks.

The following table provides a brief description of each chapter in this user guide.

Ch.	Title	Contents
1	Safety	Provides laser safety information, electrostatic discharge considerations, and other important safety information pertaining to the WaveStar LambdaRouter 128/256.
2	Security Management	Describes system security administration for the WaveStar LambdaRouter 128/256, and user login administration and authentication for the WaveStar LambdaRouter 128/256 and interfaces to the WaveStar LambdaRouter 128/256, such as the WaveStar CIT (Craft Interface Terminal) for LambdaRouter.
3	Equipment Configuration Management	Describes the types of provisioning, including pre-provisioning and auto-provisioning, the order in which entities must be provisioned in the database, and the use of access identifiers (AIDs) and other equipment identifiers when performing provisioning tasks.
4	Alarm Monitoring and Fault Management	Describes the WaveStar LambdaRouter 128/256 alarm monitoring features, provisioning, protection switching, and an introduction to fault management.

Ch.	Title	Contents
5	Cross-Connection Management	Describes the WaveStar LambdaRouter 128/256 transmission interfaces, cross-connection configurations, signal maintenance, and the commands used to establish, modify, and remove cross-connections, operate and release cross-connection loopbacks, and retrieve cross-connection lists and reports.
6	Software Management	Describes software and database installation and upgrade, and backup and restore of provisionable data.
7	Security Management Tasks	Provides detailed procedures for performing user administration and system security tasks on the WaveStar LambdaRouter 128/256 and the WaveStar CIT for LambdaRouter.
8	Management Communication Setup Tasks	Provides detailed procedures for configuring the WaveStar LambdaRouter 128/256 and WaveStar CIT to communicate via the management network.
9	Equipment Management Tasks	Provides detailed procedures for performing network element provisioning tasks such as: startup, reset, and shutdown, viewing equipment lists, configuring equipment, and provisioning system-wide parameters.
10	Alarm Monitoring and Fault Management Tasks	Provides detailed procedures for setting alarm reporting states and delay intervals, viewing alarm and status logs, and executing or releasing a forced or manual protection switch.
11	Cross-Connection Management Tasks	Provides detailed procedures for establishing, modifying, and removing cross-connections and loopbacks, viewing existing cross-connections and loopbacks, and provisioning cross-connection parameters.
12	Software Management Tasks	Provides detailed procedures for performing software installation and upgrade, and database backup and restore tasks on the WaveStar LambdaRouter 128/256.
A	WaveStar CIT Tutorial	Provides information on how to navigate and use the WaveStar CIT for LambdaRouter user interface.
B	Operations Interfaces	Describes the operations interfaces that can be used to provision a WaveStar LambdaRouter 128/256.
C	Abbreviations and Acronyms	Defines abbreviations and acronyms used throughout the WaveStar LambdaRouter 128/256 documentation.
GL	Glossary	Defines terms used throughout the WaveStar LambdaRouter 128/256 documentation.
IN	Index	Provides detailed access to the contents of this document.

Conventions used

The following typographical conventions are used throughout this user guide:

- **Bold** type is used for emphasis and to identify WaveStar CIT graphical user interface (GUI) menu and button selections.
- `Constant-Width` type is used to identify user-entered information or commands.

The term port unit is used to mean the optical cross-connect interface circuit packs, the OXI, OXI-10GC, and OXI-2GC.

The term network element is used to mean the WaveStar LambdaRouter 128/256 unless otherwise specified.

Related documentation

The *WaveStar LambdaRouter 128/256 Release 2.0 User Operations Guide* is part of a set of documents that support the WaveStar LambdaRouter 128/256. This set comprises the following documents:

Select Code	Document Title
365-375-004	*WaveStar LambdaRouter 128/256 Release 2.0 Installation Guide* Available to Lucent installers only.
365-375-000	*WaveStar LambdaRouter 128/256 Release 2.0 Applications and Planning Guide* Available on customer documentation CD-ROM and paper.
365-375-001	*WaveStar LambdaRouter 128/256 Release 2.0 User Operations Guide* Available on customer documentation CD-ROM and paper.
365-375-002	*WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide* Available on customer documentation CD-ROM and paper.
365-375-003	*WaveStar LambdaRouter 256 Release 2.0 Operations Systems Engineering Guide* Available on customer documentation CD-ROM and paper.
365-375-006	*WaveStar LambdaRouter 128 Release 2.0 Operations Systems Engineering Guide* Available on customer documentation CD-ROM and paper.
N/A	*WaveStar LambdaRouter 128/256 Software Release Description* Available on paper only.

Other documents

Customers may need information from the vendor of the personal computer used for the WaveStar CIT for LambdaRouter or other managing system, for example, WaveStar SNMS (SubNetwork Management System). Contact your account executive.

Related training

Lucent Technologies offers courses in various aspects of the WaveStar LambdaRouter 128/256, including an Operations and Maintenance course based in part on this User Operations Guide.

Instructor-led courses are offered at Lucent facilities in Altamonte Springs, Florida, or they may be given at customer locations.

The available WaveStar LambdaRouter 128/256 courses are listed in the table below.

Course Number	Course
LW2259	WaveStar LambdaRouter 128/256 Release 2.0 Applications and Planning—instructor-led This course covers multiple WaveStar LambdaRouter products.
LW2459	WaveStar LambdaRouter Installation and Testing—instructor-led, hands-on This course covers multiple WaveStar LambdaRouter products.
LW2659	WaveStar LambdaRouter Release 1.0 Operations and Maintenance—instructor-led, hands-on This course covers multiple WaveStar LambdaRouter products.

Course registration

You can access the Lucent training catalog online; use one of the following web sites:

Type	Description
Internal Lucent	*http://product-training.web.lucent.com*
External to Lucent	*http://www.lucent-product-training.com*

To arrange for courses to be taught at your facility (customized and dedicated scheduling), call the Lucent Learning Organization (LLO). Refer to one of the websites listed above for the phone number for your country. In the U.S., call 1-888-LUCENT8 (1-888-582-3688).

How to comment

Customer comments on WaveStar LambdaRouter 128/256 documents are welcome. A comment form can be found at the beginning of this document. The comment form can be faxed to

1-407-767-2760.

How to order

WaveStar LambdaRouter 128/256 customer documents can be ordered as individual paper copies or as a set on CD-ROM (*WaveStar LambdaRouter 128/256 Release 2.0 Documentation Library, 365-375-005*) from the Customer Information Center (CIC).

To order documents, specify the document or CD-ROM you need by select code. Order by contacting your account executive or by using a contact listed below.

Standard Mail Address:

Lucent Technologies Inc.
Customer Information Center
Attn: Order Entry Section
2855 N. Franklin Road
P. O. Box 19901
Indianapolis, IN 46219

Internet Address:

www.lucentdocs.com

Telephone/Fax Numbers:

USA

Telephone: 1-888-LUCENT8 (1-888-582-3688)
Fax: 1-800-566-9568

North American Region

Telephone: +317-322-6615
Fax: +317-322-6359

Asia/Pacific Region and Caribbean and Latin America Region

Telephone: +317-322-6411
Fax: +317-322-6699

Europe, Middle East, and Africa

Telephone: +441666832900
Fax: +441666832213

1 Safety

Overview

Purpose

This chapter provides important laser, electrostatic discharge (ESD), and other safety information that must be read and understood to ensure the safety of the operator as well as the equipment.

Contents

Laser Safety Information

Overview

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

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

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

Lasers and eye damage

The optical energy emitted by laser and high-radiance LEDs in the 400-1400 nm range may cause eye damage if absorbed by the retina. When a beam of light enters the eye, the eye magnifies and focuses the energy on the retina, magnifying the irradiance. The irradiance of the energy that reaches the retina is approximately 10^5 or 100,000 times more than at the cornea and, if sufficiently intense, may cause a retinal burn.

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

Classification of lasers

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

The International Electro-technical Commission (IEC) is an international standards body that writes laser safety standards. Classification schemes are similar with Classes divided into Classes 1, 2, 3A, 3B, and 4.

Lasers are classified according to the accessible emission limits and their potential for causing injury. Lightwave systems are generally classified as Class I/1, because, under normal operating conditions, all energized laser transmitting circuit packs are terminated on optical fibers which enclose the laser energy with the fiber sheath forming a protective housing. Also, covers are in place over the circuit pack shelves. The circuit packs themselves, however, may be FDA/CDRH Class I or IIIb or IEC Class 1, 3A, or 3B.

Lightwave safety precautions

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

The lightguide cables that interconnect various components of a lightwave system can disconnect or break, and may expose people to lightwave emission. Also, certain measures and maintenance procedures may expose the technician to emission from the semiconductor laser during installation and servicing.

Unlike more familiar laser devices, such as solid-state and gas lasers, the emission pattern of a semiconductor laser results in a highly divergent beam. In a divergent beam, the irradiance (power density) decreases rapidly with distance. The greater the distance, the less energy will enter the eye and the less potential risk for eye injury. Inadvertently viewing an unterminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches normally will not cause eye injury provided the power in the fiber is less than a few milliwatts at the shorter wavelengths and a few tens of milliwatts at the longer wavelengths. However, damage may occur if an optical instrument such as a microscope, magnifying glass, or eye loupe is used to stare at the energized fiber end.

CAUTION

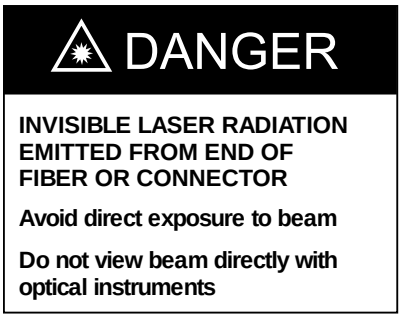
Use of controls, adjustments and procedures other than those specified herein may result in hazardous laser radiation exposure.

Safety precautions for enclosed systems

Under normal operating conditions, lightwave transmission systems are completely enclosed; nonetheless, the following precautions should be observed:

- Because of the potential for eye damage, technicians should not stare into optical connectors or broken fibers.
- Under no circumstance should lightwave/lightguide operations be performed by a technician before satisfactorily completing an approved training course.
- Since viewing lightwave emission directly in excess of Class I/1 limits with an optical instrument such as an eye loupe greatly increases the risk of eye damage, an appropriate label(s) must appear in plain view, in close proximity to the optical port, on the terminal equipment.

The figure below shows the FDA Class IIIb noninterlocked protective housing label.



NC-USM-111

Safety precautions for unenclosed systems

During service, maintenance, or restoration, a lightwave transmission system is considered unenclosed. Under these conditions, follow these practices:

- Only authorized, trained personnel shall be permitted to do service, maintenance, and restoration. Avoid exposing the eye to emissions from unterminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters and automatic power reduction (APR) are engineering controls that are also used to limit the emissions. However, technicians removing or replacing laser circuit packs should not stare or look directly into the optical port with optical instruments or magnifying lenses. (Normal eye wear or indirect viewing instruments, such as a FIND-R-SCOPE^{TM}, are not considered magnifying lenses or optical instruments.)

- Only authorized, trained personnel should use the lightwave test equipment during installation or servicing since this equipment contains semiconductor lasers. [Some examples of lightguide test equipment are Optical Time Domain Reflectometers (OTDRs), Hand-Held Loss Test Sets, and Feature Finders.]
- Under no circumstances shall any personnel scan a fiber with an optical microscope without verifying that all lightwave sources on the fiber are turned off.
- All unauthorized personnel shall be excluded from the immediate area of lightwave transmission systems during installation and service.

Consult *ANSI Z136.1, American National Standard for Safe Use of Lasers in the United States or outside the United States, IEC-60825, Part 2* for guidance on the safe use of optical fiber optic communication systems in the workplace.

The following table provides the optical specifications of the WaveStar LambdaRouter 128/256 internal laser circuit packs.

Laser Circuit Pack Code	Wavelength (nm)	Output Power (mW)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
LUU3AE	1300	1.0	SM (8.8)	LC	I/1
	1550	1.6	SM (8.8)	LC	I/1
LUU1AE	1300	0.5	SM (8.8)	LC	I/1

Lucent Technologies WaveStar LambdaRouter 128/256 complies with FDA/CDRH 21 CFR 1040.10 and 1040.11 as a Class I and as an IEC-60825-1 Class 1 laser product.

□

Electrostatic Discharge (ESD) Considerations

Overview

This section describes electrostatic discharge concerns.

Circuit pack/port unit handling precautions

CAUTION

Industry experience has shown that all integrated circuit packs can be damaged by static electricity that builds up on work surfaces and personnel. The static charges are produced by various charging effects of movement and contact with other objects. Dry air allows greater static charges to accumulate. Higher potentials are measured in areas with low relative humidity, but potentials high enough to cause damage can occur anywhere.

Observe the following precautions when handling circuit packs/units to prevent damage by electrostatic discharge:

- When handling circuit packs/units (storing, installing, removing, etc.) or when working on the backplane, always wear a grounded wrist strap or wear a heel strap and stand on a grounded, static-dissipating floor mat.
- Handle all circuit packs/units by the faceplate or latch and by the top and bottom outermost edges. Never touch the components, conductors, or connector pins.
- Observe all warning labels on bags and cartons. Whenever possible, do not remove circuit packs/units from antistatic packaging until ready to insert them into slots.
- If possible, open all circuit packs/units at a static-safe work position, using properly grounded wrist straps and static-dissipating table mats.
- Always store and transport circuit packs/units in static-safe packaging. Shielding is not required unless specified.

- Keep all static-generating materials such as food wrappers, plastics, and Styrofoam containers away from all circuit packs/units. When removing circuit packs/units from a cabinet, immediately place the circuit packs/units in static-safe packages.
- Whenever possible, maintain relative humidity above 20 percent.
- Always keep the electromagnetic interference (EMI)/ESD protective front covers on the shelves except during an upgrade or maintenance procedure. Once a circuit pack/unit is replaced in the shelf, immediately close the front cover.

Any connectors on the shelf interconnection panel that are not cabled should be fitted with a plastic dust cap to provide ESD protection.

Static control wrist straps

To reduce the possibility of ESD damage, shelves are equipped with grounding jacks to enable personnel to ground themselves using wrist straps, while handling circuit packs/units or working on a shelf. The wrist straps should be checked periodically with a wrist strap tester to ensure that they are working properly. The grounding jacks for connection of wrist straps are located on each user panel and the rear of the equipment bay. These jacks are labeled.

□

Important Safety Instructions

Overview

This section provides important safety instructions that must be followed in order to ensure the safety of the operator and the equipment.

Safety instructions

READ AND UNDERSTAND ALL INSTRUCTIONS.

When using this telecommunication equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

1. Follow all warnings and instructions marked on the product.
2. Slots and openings in this product are provided for ventilation. To protect it from overheating, these openings must not be blocked or covered.
3. Opening or removing rear covers or sheet-metal parts may present exposure to high current or electrical energy levels, or to other risks.
4. Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquid of any kind on the product.
5. Refer servicing to qualified service personnel.
6. Use caution when installing and modifying telecommunications lines.
7. Never install telecommunication wiring during a lightning storm.
8. Never install telecommunication jacks in wet locations unless the jack is specifically designed for wet locations.
9. Never touch uninsulated telecommunication wires or terminals unless the telecommunication line has been disconnected at the network interface.
10. Installation must include an independent frame ground conductor to building ground. Grounding/bonding circuit continuity is vital for safe operation of this equipment. Never operate with grounding/bonding conductor disconnected.

11. This product has two -48/-60 Vdc input power feeders. Disconnecting one power feeder will not de-energize the product. To reduce the risk of injury, disconnect both power supply cables when removing power from the system.
12. Metallic telecommunication interfaces should not leave the building premises unless connected to telecommunication devices providing primary and secondary protection, as applicable.
13. For continued protection against risk of fire, replace only with same type and rating of fuse.
14. Use only Lucent Technologies manufactured, recognized circuit packs/units/modules.
15. This equipment is intended for installation in Restricted Access Locations where access is controlled or where access can only be gained by service personnel with a key or tool. Access to this equipment is restricted to qualified service personnel only.
16. Power the unit only from -48/-60 Vdc sources providing Safety Extra Low Voltage (SELV) outputs.
17. This equipment must be provided with a readily accessible input power disconnect device as part of the building installation (such as a main power disconnect switch or external circuit breaker).

SAVE THESE INSTRUCTIONS.

□

2 Security Management

Overview

Purpose

This chapter provides detailed information on the WaveStar LambdaRouter 128/256 security management functions. This includes system security information for the WaveStar LambdaRouter 128/256 and user login administration on the WaveStar LambdaRouter 128/256 and the WaveStar CIT (Craft Interface Terminal) for LambdaRouter.

Contents

Introduction to Security Management

Overview

Security management is the process of administering user accounts (login IDs, passwords, and privilege levels) and monitoring system security to ensure that only valid users can perform allowed actions and receive authorized information from the system.

Each user must have a login ID and password on the WaveStar CIT or other managing system used to access a network element. Each user must also have a separate login ID and password on the network element being accessed.

Session management

In order to perform maintenance and administration tasks, users must log into the WaveStar CIT (or other managing system) and establish a logical connection, or session, with a network element. This establishes peer-to-peer communications with the selected system via the TCP/IP stack.

Each session is a unique entity that exists for the duration of the user's activity. The system uses a user ID to determine the authority of the user owning the session and monitors the activity of the session.

For the WaveStar LambdaRouter 128/256, up to a maximum of 13 simultaneous user sessions can be maintained per DCC circuit pack (12 regular users and one Superuser). The network element internally checks to ensure that no more than two Superuser sessions are active at any time for both of the DCC circuit packs.

The WaveStar CIT supports up to five simultaneous sessions (connections to network elements).

User Login Administration

Introduction

User login administration consists of creating, modifying and deleting user records for authorized users of the WaveStar CIT (or other managing system) and the WaveStar LambdaRouter 128/256.

A user record consists of

- a login ID
- a password
- a user type (WaveStar CIT or other managing system only)
- the user privilege levels
- the User Notification Registration List (network element only)

Each user has a user record that is stored and maintained in the security database on the WaveStar CIT (or other managing system) and a separate user record that is stored and maintained in the security database on the WaveStar LambdaRouter 128/256 being accessed.

Security administrator

Administration of the user security database on the WaveStar CIT and the network element requires a login with a security privilege level of S4 or S5. A user with a security privilege level of S4 can set the security parameters that are set on a system-wide basis (apply to all users on the network element). A user with a security privilege level of S5 can set the system-wide security parameters and can set security parameters that are specific to individual users.

WaveStar CIT

A Security Administrator on the WaveStar CIT can perform the following user provisioning tasks:

- view existing user logins
- add new users and assign user privileges
- delete users
- change passwords for any user
- modify user privileges

Individual users are also permitted to change their own passwords.

WaveStar LambdaRouter 128/256

A Security Administrator on the WaveStar LambdaRouter 128/256 can perform the following user provisioning tasks:

- view existing user logins
- view a list of users currently logged into the network element
- add new users and assign user privileges
- delete users
- change passwords for any user
- modify user privileges

Individual users are also permitted to change their own passwords.

WaveStar CIT user logins and passwords

Up to five user IDs on the WaveStar CIT are supported, each with password, privilege level, and preference information.

For more information, see “Login ID requirements” (2-5) and “Password requirements” (2-6).

When establishing a session with a network element, the user is prompted to enter a valid login ID and password for the network element.

> **Important!** It is possible to provision the same login ID and password on both the WaveStar CIT or other managing system and the network element. However, this is a security risk and it is not recommended.

WaveStar CIT Superuser logins and passwords

Up to two Superuser logins and passwords may be created on the WaveStar CIT. Superusers are allowed to change the password and preferences of any WaveStar CIT user.

For more information, see “Login ID requirements” (2-5) and “Password requirements” (2-6).

> **Important!** The WaveStar CIT Superusers are Superusers on the CIT only, not on the WaveStar LambdaRouter 128/256.

WaveStar LambdaRouter 128/256 user logins and passwords

On the WaveStar LambdaRouter 128/256, up to 500 users are supported, each with a unique login ID and password combination that is validated on each login attempt, and a privilege code which identifies the specific tasks the user is allowed to perform.

Passwords are stored in encrypted form in the network element non-volatile memory and in log files to prevent direct reading of the user passwords.

For more information, see “Login ID requirements” (2-5) and “Password requirements” (2-6).

WaveStar LambdaRouter 128/256 Superuser logins and passwords

Two Superuser logins and passwords with full privileges in all functional categories are pre-installed on the system. No other user can be assigned full privileges in all categories.

The Superuser passwords may be changed by any user with a security privilege level of S5. Superuser logins can not be deleted or added. However, Superusers are allowed to change their own login ID.

For more information, see “Login ID requirements” (2-5) and “Password requirements” (2-6).

> **Important!** It is recommended that Superuser logins not be used for normal operations.

Login ID requirements

Login IDs on both the WaveStar CIT and WaveStar LambdaRouter 128/256 are case-sensitive and may be between one and ten alphanumeric characters in length. Any sequence of characters is allowed with the following exception: the keyword ALL, by itself, in any combination of upper and lower case letters is not permitted. However, a login ID containing ALL as a substring (such as `tallman`), in any combination of upper and lower case letters is allowed.

Password requirements

Passwords on both the WaveStar CIT and WaveStar LambdaRouter 128/256 are case-sensitive, consist of between six and ten characters, and must

- contain at least two non-alphabetic characters (numbers or special characters), at least one of which must be a special character
- begin with a letter

The following table lists the characters that are allowed in a password. No other characters are allowed in a password.

Character	Description	Character	Description
A ... Z	Upper case letters	[	Left square bracket
a ... z	Lower case letters	]	Right square bracket
0 ... 9	Digits	^	Caret
’	Apostrophe	‘	Grave accent
-	Hyphen	{	Left curly brace
(	Left parenthesis	|	Vertical bar
)	Right parenthesis	}	Right curly brace
.	Period	<	Less than
/	Slash	>	Greater than
+	Plus sign	~	Tilde
!	Exclamation mark	%	Percent
*	Asterisk	#	Number sign

User privilege codes

The user privilege code is an alphanumeric code that consists of one or two letters that identify the functional category of commands the user may access, and a single digit that identifies the user authorization level within each functional category. A user can execute commands in a functional category that requires an authorization level equal or less than the authorization level assigned to the user.

A user privilege code is assigned to each user when a login is created or modified on either the WaveStar LambdaRouter 128/256 or the WaveStar CIT. User privilege codes assigned to login IDs on the WaveStar CIT do not apply to the WaveStar LambdaRouter 128/256.

Functional categories

All commands are grouped into the following functional categories:

- Maintenance (M)
- Provisioning (P)
- System and Security Administration (S)
- Test (T)

Authorization levels

The authorization level ranges from 0 (lowest) to 5 (highest) for all functional categories except security, which ranges from 1 to 5. Assigning an authorization level of 0 disables that functional category for that user.

WaveStar CIT user types

Predefined user types in the WaveStar CIT are used to set default values when establishing and modifying WaveStar CIT user logins. These user types apply only to the WaveStar CIT and not to the WaveStar LambdaRouter 128/256.

Each user type is defined and identified by a specific combination of User Privilege Codes (UPCs). The five predefined user types are as follows:

- Superuser—S5, T5, M5, P5
- Privileged User—S3, T5, M5, P5
- General User—S1, T4, M4, P3
- Maintenance User—S1, T4, M4, P3
- Reports Only User—S1, T1, M1, P1

Users may be assigned to combinations of privilege codes that are not one of the predefined sets for a specific user type. Users with privilege codes that do not match one of the predefined types are considered to have a user type of **Other**.

Superuser

A Superuser has access to all security and system provisioning capabilities including:

- adding and deleting users
- modifying user passwords and user priority levels
- assigning user privilege codes and user priority levels
- assigning the User Notification Registration List for other users
- modifying network element security variables
- retrieving logs
- performing backup and restore operations on the network element database
- system provisioning (configuration management, cross-connect management, software management, fault management)

Important! It is recommended that Superuser IDs not be used for normal operations. The Privileged User classification provides access to all typical operational features with the exception of user administration.

Privileged user

A Privileged User has access to all user capabilities (including those that are service-affecting) with the exception of security related capabilities.

General user

A General User has access to all user capabilities except the following:

- network element security administration (capable of changing own password only)
- software installation and system initialization capabilities
- network element access capabilities

Maintenance user

A Maintenance User has access to the following capabilities:

- testing functions
- retrieving network element information
- limited service-affecting commands
- changing own password

Reports Only user

A Reports Only User has access only to those capabilities that retrieve information but do not modify the system, with the following exceptions:

- may change own password
- does not have read access to user login information for other users

WaveStar LambdaRouter 128/256 User Notification Registration List

The Security Administrator on the WaveStar LambdaRouter 128/256 assigns a User Notification Registration List for each user, which determines what messages (other than responses to their own commands) a user is allowed to receive. Users will receive only those notifications for which they are registered.

Some message types are part of groups that are not separable. For example, if a user is registered for DBCHG (database change) messages, all such messages will be received, including modify notifications and establish/remove notifications.

The following notification and response types may be registered to each user:

- establish, modify, and remove database change notifications (DBCHG)
- state change notifications (STCHG)
- alarm notifications (ALARMS)
- protection switch notifications (PSCHG)
- all notifications and responses (ALL)
- responses to own commands (OWN)

□

WaveStar LambdaRouter 128/256 System Security Administration

Introduction

The following features provide security management functions for the WaveStar LambdaRouter 128/256:

- user identification and authentication
- user access control
- user notification control
- user command execution control
- user logout
- security activity audit trail
- security variable backup

User identification and authentication

In order to gain access to the WaveStar LambdaRouter 128/256, a user must enter a valid login ID and password combination that has been previously provisioned by a Security Administrator (privilege code S5).

Each user, including Superusers, will be prompted to change the originally assigned password on the first login attempt after being added to the system.

In addition to the login ID and password, the WaveStar LambdaRouter 128/256 supports the following provisionable user identification and authentication security features:

- User ID Aging Period
- Password Aging Period
- User ID Lockout Threshold
- User ID Lockout Interval
- User ID Lockout Aging Period

User ID aging period

The User ID Aging Period specifies the maximum number of days a user ID may go unused before being disabled. After a user ID is disabled, a Security Administrator with an S5 privilege level can either re-enable or delete the user ID.

The User ID Aging Period is defined on a system-wide basis by a Security Administrator with an S4 privilege level or higher. Valid settings for this parameter range from 0 to 999 days (default is 10). Setting the User ID Aging Period to 0 disables user ID aging.

The user ID aging period does not apply to Superuser logins.

Password aging period

The Password Aging Period specifies the maximum number of days a user's password remains valid before the system requires the password to be changed. After a password has expired, on the next login attempt, the user will be required to either change the password or cancel the login process.

Any time the password is changed, even if the Password Aging Period has not expired, the aging period counter is reset so that the new password is valid for the specified number of days.

The Password Aging Period is defined on a per-user basis by a Security Administrator with an S5 privilege level. Valid settings for this parameter are 0 or 7 to 999 days (default is 90). Setting the Password Aging Period to 0 disables password aging.

User ID lockout threshold

The User ID Lockout Threshold specifies the number of sequential invalid login attempts permitted by the same user ID before the user ID is locked out. The user ID is locked out for the amount of time specified by the User ID Lockout Interval. When a user ID is locked out, an Intruder Alert alarm is generated and logged.

The User ID Lockout Threshold is defined on a system-wide basis by a Security Administrator with an S4 privilege level or higher. Valid settings for this parameter range from 2 to 99 attempts (default is 5).

User ID lockout interval

The User ID Lockout Interval specifies the number of minutes the user ID will be locked out once the User ID Lockout Threshold is exceeded. After the lockout interval expires, the user will be allowed to attempt to log in again with the same user ID.

The User ID Lockout Interval is defined on a system-wide basis by a Security Administrator with an S4 privilege level or higher. Valid settings for this parameter range from 0 to 99 minutes (default is 10). Setting the User ID Lockout Interval to 0 disables user ID lockout.

User ID lockout aging period

The User ID Lockout Aging Period specifies the number of minutes before the invalid login attempt count is reset.

The User ID Lockout Aging timer starts upon the first invalid login attempt. If the number of sequential invalid login attempts by the same user ID reaches the User ID Lockout Threshold within this time period, the user ID is locked out.

If the number of sequential invalid login attempts by the same user ID does not reach the User ID Lockout Threshold (the user gives up without a successful login), the User ID Lockout Aging Period is applied. If the aging period expires with no further invalid login attempts by the same user ID, the invalid login attempt count is reset to zero and the user ID is not locked out.

The User ID Lockout Aging Period is defined on a system-wide basis by a Security Administrator with an S4 privilege level or higher. Valid settings for this parameter range from 1 to 999 minutes (default is 60).

User access control

User access control features determine what specific tasks each user is allowed to perform. This is accomplished by assigning each user ID privilege codes, which are made up of a Functional Category and an Authorization Level within each Functional Category (for example, S5, P3, M2, and so on).

Assigning combinations of privilege codes to a user determines which commands and functions the user may access.

For more information, see “User privilege codes” (2-6).

User notification control

User notification control determines which messages, besides responses to the user's own commands, each user is allowed to receive. This control is accomplished by registering the types of messages a user may receive in a User Notification Registration List.

A Security Administrator with an S5 privilege level assigns a User Notification Registration List for each user.

For more information, see "WaveStar LambdaRouter 128/256 User Notification Registration List" (2-9).

User logout

The current session is terminated when a user is logged out. A user logout occurs when the user

- manually logs out of the system
- is forcibly logged out of the system
- has exceeded the inactivity time-out period

Logout by user

Each user may manually log out of the system to terminate the current session.

Forced logout

A Security Administrator with an S5 privilege level may force the logout of individual users, or may simultaneously log out all user sessions.

Forced logout of all users will not log out the S5 user issuing the force logout command or another Superuser. However, a Superuser can force the logout of another Superuser individually.

Inactivity time-out period

The network element will automatically log out any session (including Superusers) that remains inactive for a defined number of consecutive minutes. This is the Inactivity Time-Out Period.

Any user actions that cause communications between the WaveStar CIT or managing system and the network element will reset the inactivity timer to zero. The inactivity timer does not run while the network element is processing commands associated with the session. A user will not be logged out due to inactivity during output from a long command, such as a transmission test.

When a user is logged out for exceeding the Inactivity Time-Out Period, the logout is recorded in the Security Activity Log.

The Inactivity Time-Out Period is defined on a per-user basis by a Security Administrator with an S5 privilege level. Valid settings for this parameter range from 0 to 999 minutes (default is 30). Setting the Inactivity Time-Out Period to 0 disables this feature.

Security activity audit trail

All commands submitted by the user are recorded in the User Session Activity Log. All security related events are recorded in the Security Activity Log. The events in each log are time-stamped.

For more information, see “Security Logs” (2-15).

Security variable backup and restore

The following data relating to security administration can be backed up and restored by a Security Administrator:

- configurable variables (including variables for the two Superusers)
  - thresholds and timeouts
  - user IDs and passwords
  - privileges
- password creation date and time

Security data is backed up to any allowable backup destination (such as non-volatile memory, WaveStar CIT, or a managing system). All security data backup and restore operations are recorded in the Security Activity Log and the User Session Activity Log.

□

Security Logs

Introduction

The WaveStar LambdaRouter 128/256 provides autonomous logging of events that affect system security. The following security log files are available:

- Security Activity Log
- User Session Activity Log

Each security log is a separate file that may be retrieved, saved, and printed. The logs are stored in the non-volatile memory (NVM) of the network element so that the logged data is retained across power failures and system resets.

The log files are circular files of a fixed size. Once the log has been filled to the specified capacity, the next new entry will overwrite the oldest existing entry. Therefore, the data that is available at any given time is limited to the capacity of the file. The time span covered by the log file is designed to provide approximately 72 hours of storage. However, the coverage time span may be reduced during periods of intense activity.

The Security Activity Log and the User Session Activity Log are not used for resynchronization with a management system.

Security Activity Log

The Security Activity Log is a time- and date-stamped history of the following security related events:

- successful login history
- network element security variable modification history
- user security data modification history
- software management command history
- system reset history
- logout history

User Session Activity Log

The User Session Activity Log provides a time- and date-stamped list of user-initiated commands and parameters, command completion codes, the AID on which the command was executed, and the login ID of the user that executed the command.

All user-initiated commands from login through logout are stored in the User Session Activity Log. Command replies and commands that are denied because of bad syntax are not logged in the file. Only the Success/Denial code is stored.

The following information is logged for security audit purposes:

- denied login attempt history
- successful login history
- network element security variable modification history
- user security data modification history
- logout history

□

3 Equipment Configuration Management

Overview

Purpose

This chapter provides detailed information on the WaveStar LambdaRouter 128/256 equipment configuration management functions.

Contents

Introduction to Equipment Configuration Management

Overview

Equipment provisioning includes configuration of the following data:

- common equipment provisioning data
  - identification data
  - functional parameters
  - configuration data
  - state information
  - signaling options
- slot provisioning data
  - state information
- port provisioning data
  - transport parameters
  - state information
  - signaling options

See “Equipment Provisioning” (3-5) for additional information.

□

AID Overview

Introduction

This section provides an overview of the external user AIDs for the WaveStar LambdaRouter 128/256. Information is provided for AID syntax and grammar rules used to define the AIDs, as well as terminology and names used to identify physical and logical entities.

For more information on AIDs, refer to the *WaveStar LambdaRouter 256 Release 2.0 Operations Systems Engineering Guide, 365-375-003* or *WaveStar LambdaRouter 128 Release 2.0 Operations Systems Engineering Guide, 365-375-006*.

AID hierarchy

The AID hierarchy is defined to represent the network element structure. AIDs are defined using a physical hierarchy (imposed by the physical architecture of the system), or a logical hierarchy (imposed by the logical grouping of entities).

AID structure

The following AID structure is used by the WaveStar LambdaRouter 128/256:

{*Entity Type*} [[-{*Shelf Number*} [[-{*Slot Number*}] or [-{*I/O Identifier*}-{*Block Identifier*}]]] -{*Entity Identifier*}]

Fields are separated by hyphens (-). Entries enclosed in { } are variables and fields enclosed in [ ] are optional.

The following table shows the AID structure and hierarchy.

Entity	Hierarchy
System	{*Entity Type*}
Shelf	{*Entity Type*} -{*Entity Identifier*}
Slot/Circuit Pack	{*Entity Type*} -{*Shelf Number*} -{*Entity Identifier*}
Port	{*Entity Type*} -{*Shelf Number*} -{*Slot Number*} -{*Entity Identifier*}
SWIP	{*Entity Type*} -{*Shelf Number*} -{*I/O Identifier*} -{*Block Identifier*} -{*Entity Identifier*}
Protection/ Maintenance Group	{*Entity Type*} -{*Entity Identifier*}
Fan	{*Entity Type*} -{*Entity Identifier*}

Entering “all” in an AID field

An AID field value of “all” can be used to specify a set of entities (such as slots or ports) as input parameter values for various TL1 commands.

If “all” is used at a higher level in the AID, lower-level AID components are not allowed. For example, if “all” is used in the Slot Number field, it is not used in the Entity Identifier field.

The following examples illustrate the use of the field value “all”:

- `hvdac-0-all` selects all HVDAC slots of High-Voltage Shelf 0
- `swip-0-in-all` selects all input SWIPs on Switch Shelf 0
- `och-1-3-all` selects all ports on the third port unit on the first optical interface shelf
- `och-1-all` selects all ports on the first optical interface shelf

□

Equipment Provisioning

Introduction

Equipment provisioning is the process of assigning values to a set of parameters of the system (or any of its subsystems) in order to enable or facilitate the expected use of the entity. Provisionable entities include

- system
- shelves
- slots/circuit packs
- SWIPs
- ports
- cross-connections
- maintenance groups

The provisioning of system components involves the creation of a software representation of the component and/or a record of its parameter values, as well as actual modification of the component parameters.

Working controllers are required to allow user provisioning of controlled equipment. No user provisioning is allowed until the controllers and control links have passed all diagnostics.

The provisionable parameters and values (current and original) are maintained in the non-volatile memory of the PRI MEM circuit packs in the System Controller Shelf.

Provisioning hierarchy

The provisioning of equipment is subject to the following hierarchy:

- system
- shelf
- slot/circuit pack (or SWIPs)
- port
- cross-connection

An entity may not be provisioned if the corresponding entities preceding it are not provisioned. For example, a slot may not be provisioned if the shelf in which it is located is not already provisioned.

De-provisioning hierarchy

The de-provisioning of equipment is subject to the following hierarchy:

- cross-connection
- slot/circuit pack
- shelf
- system

As with provisioning, in order to de-provision an entity, all preceding entities must have been de-provisioned. Deprovisioning an OXI, OXI-10GC, or OXI-2GC slot automatically deprovisions the ports associated with the slot.

Types of provisioning

The following types of provisioning are supported:

- manual provisioning
- pre-provisioning
- auto-provisioning

Manual provisioning

WaveStar LambdaRouter 128/256 software allows manual provisioning of all user-provisionable parameters using any available operations interface. This includes the WaveStar CIT for LambdaRouter or other managing system.

Pre-provisioning

Pre-provisioning refers to the creation of a component image by assigning parameter values to an entity prior to physically installing the component into the system.

With pre-provisioning, a mismatch is possible between the parameter settings in the component and in its image. In this case, parameter modifications may then be initiated either locally or remotely.

In the WaveStar LambdaRouter 128/256 system, only optical interface shelves and port unit slots may be pre-provisioned. This is done by identifying the optical interface shelf type, slot, and the circuit pack functional name and functional qualifier. Ports will be autonomously created upon pre-provisioning of the associated slot/circuit pack.

Auto-provisioning

Auto-provisioning refers to the automatic generation of a component image (with its current parameter settings) upon addition of the component to the system.

Auto-provisioning allows the system to discover its hardware configuration and to create the associated entities autonomously using the original (default) or user-defined, pre-provisioned parameters.

If equipment related parameters have been pre-provisioned and the inserted equipment does not match, the inserted equipment will not be enabled. Pre-provisioned parameters take precedence over auto-provisioning.

Initial system startup

For an initial system startup, some manual provisioning of the system configuration must be performed, including

- installation of system software and mirror mapping/calibration files
- setting the system configuration (identifying as a 128 or 256 system)
- setting network parameters (IP address, subnet mask, and default router address for each DCC circuit pack), Target Identifier (TID), and system date and time
- provisioning optical interface shelves (OIS-T, OIS-10G, OIS-2G, and OIS-MX)

Subsequent system startup

After the system has been configured for the initial startup, auto-provisioning is performed upon subsequent system startups and upon circuit pack insertion. Auto-provisioned entities receive default provisioning values.

The following entities are auto-provisioned upon system startup:

- system
- all provisioned shelves (except optical interface shelves)
- all slots on provisioned shelves
- equipped ports

The provisioning of the system configuration triggers the autonomous creation of the applicable shelf objects. The creation of a shelf object triggers the autonomous creation of the associated slot/circuit pack (or SWIPs) objects for all shelves except optical interface shelves. For optical interface shelves, only equipped slots are created autonomously. The creation of a slot/circuit pack triggers the autonomous creation of the associated ports.

Equipment removal

The system detects and reports the removal of any equipment (except shelves). The removal of equipment updates the state-related information but does not cause the system to delete any entities. The user must execute a specific "delete-entity" command to cause the system to remove the entity from the database.

The removal of equipment may result in alarms and insertion of maintenance signals.

Inventory and equipage checks

The network element provides an inventory of all electronic equipment that is provisioned in the system. The inventory information (type, version, serial number, and so on) is available to the user via an inventory request. The provisioned data information, including cross-connection information, can be reported on demand.

An equipage check at the slot level is provided to verify the compatibility between the slot provisioning and the circuit pack type and provisioning. An alarm is generated if an invalid configuration is detected.

The WaveStar LambdaRouter 128/256 has self-knowledge of equipage and status needed for operation, and supports a set of provisioned data that provides for addressing, communications, and operations. This is accomplished through the use of

- target identifiers (TIDs)
- access identifiers (AIDs)
- circuit pack identifiers

Target identifiers

A Target Identifier (TID) identifies a specific network element within an optical network and is used for remote login requests, and all commands and report requests from users.

The TID is stored in non-volatile memory, and can be provisioned by a user providing the system is in an out-of-service/management state (OOS-MA). Each network element in a network must have a unique TID, which is a case-insensitive string of up to 20 alphanumeric characters (A-Z, a-z, and 0-9), hyphens (-), and forward slashes (/).

Important! The TID must not begin or end with a hyphen.

Access identifiers

An Access Identifier (AID) identifies a specific physical or logical entity within a network element.

Each entity has a unique AID, which is a string of up to 20 alphanumeric characters and hyphens (-). Lowercase letters are translated into uppercase before they are stored in the network element.

Circuit pack identifiers

Each circuit pack provides an identifier that provides the following information for the circuit pack:

- apparatus code (circuit pack type)
- serial number
- series number (version)
- Common Language™ Equipment Identifier (CLEI™) code
- Equipment Catalog Item (ECI) code

The circuit pack identifier is readable by the system upon insertion of the circuit pack in any allowable slot. The circuit pack identifier is not provisionable by the user.

□

Equipment Configuration Logs and Reports

Introduction

The WaveStar LambdaRouter 128/256 provides an inventory of all of the electronic equipment that is available to the user, and can report provisioned data information, including cross-connection information, on demand. The following equipment configuration logs and reports are available:

- Equipment List
- Notification Log

Equipment List

The Equipment List provides a listing of equipment for a selected shelf, circuit pack, or port in the network element.

The report includes the AID for the selected entity, as well as additional information that describes the equipment that makes up the selected entity (such as CLEI code and serial number.)

Notification Log

The Notification Log provides a list of the most recent activity that has caused changes to the database.

The database change notifications are defined by changes in user-provisionable attributes and any non-user-provisionable attributes specified as being automatically reported via notification.

For additional information on notification registration, see “WaveStar LambdaRouter 128/256 User Notification Registration List” (2-9).

□

4 Alarm Monitoring and Fault Management

Overview

Purpose

This chapter provides an introduction to the WaveStar LambdaRouter 128/256 alarm monitoring and fault management functions. For detailed information on alarm monitoring and fault management, refer to the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002*.

Contents

Introduction to Alarm Monitoring and Fault Management

Fault management

Fault management is used to process failures and their contribution to the generation of alarms for transmission and system control equipment.

The fault management process involves

- system declaration of a failure (for example, loss of signal)
- system initiation of an internal correlation process over an integration period to generate alarm and status conditions after a failure is declared
- user response to alarm messages and alarm indicators
- user performance of routine maintenance

All transmission and system control faults are isolated to one or more field-replaceable units.

Alarm monitoring

Alarm monitoring allows the WaveStar LambdaRouter 128/256 to detect faults and degraded conditions, and to report the failure condition.

Failure conditions are reported by

- facility/equipment alarm messages
- user/alarm panels
- circuit pack LEDs
- office alarms

Maintenance

Maintenance is the system response to faults (defects and failures) to provide fast transmission and system control recovery.

The maintenance process involves

- recovery of failures
- recovery processing actions that are taken when a failure recovers

Related information

For related information and procedures for craft intervention in fault management and maintenance, refer to the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002*.

□

Alarm Monitoring

Introduction

The WaveStar LambdaRouter 128/256 supports the detection of common, optical channel, and equipment faults, and the autonomous generation and reporting of associated alarms.

Alarm indications include

- messages through the communications interface to the WaveStar CIT, WaveStar SNMS, or other managing system
- user panel LEDs
- circuit pack LEDs
- office alarms

User panels

User panels located on each shelf in the WaveStar LambdaRouter 128/256 provide alarm/status information for the shelf. If more than one alarm exists at the shelf, only the highest alarm level LED is illuminated.

An alarm cutoff (ACO) function is also provided.

Circuit pack LEDs

LEDs located on the faceplate of each circuit pack provide an indication of the current status of the individual circuit pack.

Office alarm interface

The WaveStar LambdaRouter 128/256 provides an interface to the Office Alarm System for each alarm level that leads to office audible or visual alarms. An audible alarm cutoff is provided locally on the system and remotely via user command.

Alarm logs

Alarm logs are maintained to provide a list of currently active alarms, as well as a history of alarms.

See “Alarm Monitoring and Fault Management Reports and Logs” (4-9) for additional information.

Alarm notification categories

Alarm reporting is grouped into the following categories:

- optical channel alarms
- equipment alarms
- common alarms

Optical channel alarms

Optical channel alarms cover input signal failures and are issued against an input port. Optical channel alarms include the following fault conditions:

- loss of monitored input optical power
- SONET/SDH failures
  - Loss of Signal optical (LOS)
  - Loss of Signal electrical (LOS)
  - Loss of Frame (LOF)
  - Signal Fail B2 Excessive Bit Error Rate (EBER)
  - Signal Degrade B2 Bit Error Rate (BER)
  - Alarm Indication Signal - Line/Multiplex Section (AIS-L/ AIS-MS)

Equipment alarms

Equipment alarms cover transmission and control equipment failures and are issued with respect to a port, circuit pack/slot, shelf, or the system. Equipment alarms include the following fault conditions:

- failures of equipment
- service interruption due to failures in a power supply, fuse, or fan assembly
- any equipment configuration problem
- improper removal
- output port detected transmission failures
  - Loss of Signal optical (LOS)
  - Loss of Signal electrical (LOS)
  - Loss of Frame (LOF)
  - Signal Fail B2 Excessive Bit Error Rate (EBER)
  - Signal Degrade B2 Bit Error Rate (BER)
  - Alarm Indication Signal - Line/Multiplex Section (AIS-L/ AIS-MS)

Common alarms

Common alarms are issued with respect to a circuit pack, controller complex, shelf, or the system, and include the following fault conditions:

- controller software fault
- controller autonomous reset
- data storage problems
- security-related issues (such as unsuccessful login attempts)

Alarm declaration types and states

Alarm notification declaration types consist of the following:

- persistent conditions
- transient conditions

The alarm declaration state for persistent alarms will be one of the following:

- Set (to report the occurrence of the fault)
- Clear (to report recovery/clearing of the fault)

Transient conditions do not require a clear.

Alarm correlation

The WaveStar LambdaRouter 128/256 has the ability to correlate alarms in order to minimize the number of alarm messages generated for a single fault condition. If multiple alarmable events are generated by a single fault, only the alarm causing the fault will be reported.

Alarm provisioning

Provisioning of alarm declaration and clearing times is supported.

Alarm severity levels

The reported alarm level is based on the type and state of the alarm declaration type. The following levels are used:

Declaration Type	Declaration State	Reported Alarm Level	Description
Persistent	Set	Critical	Service-affecting conditions (displayed as a red LED on the WaveStar CIT GUI)
		Major	Any condition inhibiting the ability to detect and/or report fault conditions (displayed as a yellow LED on the WaveStar CIT GUI)
		Minor	Non-service-affecting conditions that could affect service if a repeated failure occurs (displayed as a blue LED on the WaveStar CIT GUI)
		Not-alarmed	Non-service-affecting events (displayed as a green LED on the WaveStar CIT GUI)
	Clear	Clear	Alarm condition clears
Transient	Set	Not-alarmed	Non-persistent condition

Alarm declaration time

The alarm declaration time is a user-provisionable delay from the time a fault condition occurs to the time an alarm is generated. The fault condition must persist for the entire alarm declaration time delay for an alarm to be generated.

Alarm clearing time

The alarm clearing time is a user-provisionable delay from the time a fault condition clears to the time an alarm clear notification is generated. The fault condition must not recur for the entire alarm clear time delay for a clear notification to be generated.

□

Protection Switching

Introduction

Protection switching allows the system to automatically switch over to the standby or protection circuitry in the event of a failure. In addition, a manual or forced protection switch may be initiated as part of craft fault isolation procedures.

The following control system entities support protection switching:

- the System Controller Protection Group (SCCPG)
- the High-Voltage Shelf Controller Protection Group (HVCPG)
- the Optical Interface Shelf Controller Protection Group (OICPG)

The current state of the protection groups, both active and standby, can be retrieved. The information returned includes both the overall state of the protection group as well as the individual circuit packs that make up the protection group.

In addition, the output port 2:1 selector provides transmission protection switching between fabric 0 and 1.

Autonomous protection switching

Autonomous protection switching is an automatic, non-revertive response to a system-detected fault condition. Controller protection groups and output port 2:1 selectors both support autonomous protection switching in response to fault detection.

Autonomous protection switching takes priority over manual protection switching.

Manual protection switching

Manual protection switching may be initiated by craft personnel as part of fault isolation procedures or routine maintenance.

When performing a manual protection switch of the system controller complex, any active transactions that cannot be aborted will be completed prior to switching the controller complexes.

When performing a manual protection switch of a shelf controller, any active transactions within the shelf domain will be aborted prior to switching the shelf controller.

Manual protection switching may be overridden by an autonomous protection switch.

Forced protection switching

Forced protection switching may be initiated by craft personnel as part of fault isolation procedures or routing maintenance. Forced protection switching applies only to output port 2:1 selectors (not to shelf or system controllers).

A forced protection switch overrides an autonomous or manual protection switch, and remains active until released.

Releasing a protection switch

After operating a manual or forced protection switch on an output port 2:1 selector, craft personnel may release the protection switch. The release command may return the selector to an autonomous fault detection status.

A manual protection switch on a controller entity does not require a release in order to perform another protection switch on the controller entity.

□

Alarm Monitoring and Fault Management Reports and Logs

Overview

The WaveStar LambdaRouter 128/256 provides autonomous logging of system alarms and protection switching activity. The following reports and logs are available:

- Alarm List
- Alarm Log
- Protection Switch Log

Each log is a separate read-only file that is stored in the non-volatile memory (NVM) of the network element. The log files are circular files of a fixed size. Once the log has been filled to the specified capacity, the next entry will overwrite the oldest existing entry. Therefore, the data that is available at any given time is limited to the capacity of the file. The time span covered by the log file may be reduced during periods of intense activity. All entries within a log file are time- and date-stamped.

Each of the logs may be retrieved, saved, and printed.

Alarm List

The Alarm List provides a list of the currently active alarms on the network element.

The report includes the alarm level and type, identification of affected equipment, effect on service, condition type, and additional details of the failure (if available).

Alarm Log

The Alarm Log provides a history and time sequence of the setting and clearing of system alarms.

The log includes the type of trouble, time of occurrence, identification of affected equipment, effect on service, alarm level, alarm condition state, and additional details of the failure (if available).

Protection Switch Activity Log

The Protection Switch Activity Log provides a time-stamped list of protection switching activity that has occurred within the network element. This includes controller and output port 2:1 selector related switching activity.

For controller groups, the log includes the active group ID. For output port 2:1 selectors, the log includes the active unit ID, the type of protection switch (manual, forced, autonomous, or no request), and the active side.

□

5 Cross-Connection Management

Overview

Purpose

This chapter provides detailed information on the WaveStar LambdaRouter 128/256 cross-connection management functions and includes a brief description of the transmission interfaces that allow the WaveStar LambdaRouter 128/256 to interface with external Optical Line Systems (OLSs) and other network elements (NEs).

Contents

Introduction to Cross-Connection Management

Introduction

A cross-connection is a configurable optical, or optical-electrical-optical (OEO), transmission path interconnection between input and output ports within a network element. The input and output ports are the only entities from which, and to which, the user can provision cross-connections.

In the WaveStar LambdaRouter 128/256, all cross-connections are strictly non-blocking for all (one-way or two-way) point-to-point cross-connections. This means that no cross-connection request will be denied for lack of a path through the switch fabric. Both bit-rate-independent (transparent) and rate-specific interfaces are supported.

Cross-connection management functions

Cross-connection management functions include all activities necessary to

- provision transmission interfaces
- establish, modify, and remove cross-connections
- operate and release loopback cross-connections
- retrieve cross-connection parameters

□

Transmission Interfaces

Introduction

The Optical Cross-Connect Interface (OXI), Optical Cross-Connect Interface 10G Client (OXI-10GC), and Optical Cross-Connect Interface 2.5G Client (OXI-2GC) circuit packs are the transmission interfaces for the WaveStar LambdaRouter 128/256. They provide connectivity between external Optical Line Systems (OLSs) or client network elements (NEs) and the WaveStar LambdaRouter 128/256.

Types of transmission interfaces

The WaveStar LambdaRouter 128/256 supports both bit-rate-independent (transparent) and rate-specific transmission interface circuit packs.

Bit-rate-independent (transparent) interface

The OXI circuit packs are bit-rate-independent optical interfaces. When a bit-rate-independent, or transparent, optical interface is provisioned, no distinction is made in either the format (SONET/SDH, ATM, or IP) or rate (2.5 Gbps or 10 Gbps) of the signal as long as the input and output ports are consistently provisioned.

When provisioning the input ports on an OXI circuit pack, the following parameters are configurable:

- input primary state (IS [in-service] or OOS [out-of-service])
- input port usage (Client or NNI)
- input SWIP assignments on each fabric side
- input interface format (OC48/STM16, OC192/STM64, LSBB [low-speed broad band], HSBB [high-speed broad band], or Other)
- input interface optics (SR [short reach], IR [intermediate reach], LR [long reach], GBELX [gigabit ethernet], VSR12 [very short reach with 12 dB budget], or Other)
- minimum input power for detection of signal (–10 to +2 dB)

When provisioning the output ports on an OXI circuit pack, the following parameters are configurable:

- output primary state (IS or OOS)
- output port usage (Client or NNI)
- output SWIP assignments on each fabric side
- output interface format (OC48/STM16, OC192/STM64, LSBB [low-speed broad band], HSBB [high-speed broad band], or Other)

While neither format nor rate information is required in port provisioning, a distinction in format may be specified when a port is provisioned because the optical parameters for those signals may differ in wavelength and/or power. If a port is provisioned with an interface format, that information will be checked when a cross-connection request is made and the request will be denied if input port attributes do not match those of the output port.

After a cross-connection is established, the interface format cannot be changed.

Rate-specific interfaces

The OXI-10GC and OXI-2GC circuit packs are rate-specific optical interfaces. When a rate-specific optical interface with OEO functionality is provisioned, the interface standard and signal type information must be specified for both the input and output ports.

When provisioning the input ports on an OXI-10GC or OXI-2GC circuit pack, the following parameters are configurable:

- interface standard (SONET or SDH)
- input primary state (IS [in-service] or OOS [out-of-service])
- input port usage (Client or NNI)
- input signal type (1 or 4)
- auto laser shutoff (Enable or Disable)
- input section trace format (1 or 16)
- input signal degrade threshold (–5 to –9 dB)
- input signal failure threshold (–3, –4, or –6)
- input SWIP assignments on each fabric side

When provisioning the output ports on an OXI-10GC or OXI-2GC circuit pack, the following parameters are configurable:

- interface standard (SONET or SDH)
- output primary state (IS [in-service] or OOS [out-of-service])
- output port usage (Client or NNI)
- output signal type (1 or 4)
- output section trace format (1 or 16)
- output port selector autolock (Enable or Disable)
- output AIS-L protection switch (Enable or Disable)
- output BER protection switch (Enable or Disable)
- output signal degrade threshold (–5 to –9 dB)
- output excessive BER protection switch (Enable or Disable)
- output signal failure threshold (–3, –4, or –6)
- output SWIP assignments on each fabric side

After a cross-connection is established, the interface standard cannot be changed for a port on an OXI-2GC circuit pack. For a port on an OXI-10GC circuit pack, the interface standard and signal type cannot be changed after a cross-connection is established.

Signal maintenance

Signal maintenance involves detecting the presence or absence of optical power at the input and output ports of the interface circuit packs, generating appropriate alarms, and performing fabric path protection switching.

Power monitors are used to detect the presence or absence of optical power at the input and output ports on a transparent optical interface circuit pack, and on the output ports on rate-specific interface circuit packs.

Each port must be provisioned with the proper threshold levels to allow the associated power monitors to detect the loss and return of the optical signal.

Transparent ingress port provisioning

The signal detection and signal loss thresholds for the transparent ingress power monitors are configured by specifying the interface format and optics that are, or will be, connected to each port.

These values are initially set based on user provisioned system-wide default values. These values are sufficient to enable detection of the presence or loss of any allowable client signal.

Before a port is enabled for use in a cross-connection, the individual port may be provisioned to more accurately represent the connected client interface format and optics.

The system uses the provisioned interface format and interface optics type to compute the detection of signal (DOS) and loss of signal (LOS) thresholds for the input power monitors.

If the interface format and/or the interface optics type is set to **Other**, the minimum input power for DOS is selectable by the user. If neither the interface format nor the interface optics type are set to **Other**, the minimum input power for DOS is computed by the system and cannot be changed by the user.

The following table shows the nominal minimum ingress power levels for detection of signal for each allowable combination of the interface format and interface optics parameters. These values take into account small port-to-port variations in power monitor sensitivity.

Interface Format	Interface Optics	Minimum Input Power for DOS (dBm)
OC-48/STM-16	SR (ITU I-16)	-10
	IR (ITU S-16)	-5
	LR (ITU L-16)	-2
	Other	User provisioned value
OC-192/STM-64	VSR12	-1
	SR (ITU I-64.1)	-6
	IR (ITU S-64.2,3b)	-1
	LR (ITU L-64.2ac)	-2
	Other	User provisioned value
LSBB	LR	-3
	Other	User provisioned value
HSBB	LR	-1
	GBELX	-11
	Other	User provisioned value
Other	Any allowed value	User provisioned value

The associated thresholds for LOS are nominally set 10 dB below the DOS values shown in the table, after accounting for power monitor sensitivity variations.

OEO ingress port provisioning

Ingress ports on OEO interface circuit packs provide optical-electrical-optical conversion of the incoming signal, and circuitry to monitor the electrical signal and provide signal fail and signal degrade detection.

User provisioning of the OEO ingress ports is not permitted.

Egress port provisioning

The signal detection and signal loss thresholds for the egress power monitors are computed and set by the system. The egress power monitor thresholds are determined based on the thresholds set for the input power monitors and the expected loss values through the switch fabric.

User provisioning of the egress power monitor thresholds is not permitted.

□

Cross-Connection Configurations

Introduction

A cross-connection provides internal transmission capability between a set of input and output ports within a single network element. All cross-connections can be classified as either a one-way or two-way configuration.

A set of associated cross-connections can be established to provide the configuration needed for a particular communications application. The following cross-connection configurations are supported:

- one-way and two-way point-to-point
- one-way and two-way bridged and/or merged
- cross-connect loopback

A one-way transmission path that has been established from an input port to an output port within a single network element is called a cross-connection leg. Each leg is identified as an entity by

- its pair of input and output ports
- its configuration
- its cross-connection rate (when identified)
- the number of switch fabrics through which it passes

A leg with a transmission path through one switch fabric (either side 0 or side 1) is called a simplex leg. A leg that has a transmission path through both switch fabrics is called a duplex leg. All one-way and two-way point-to-point cross-connections are considered duplex.

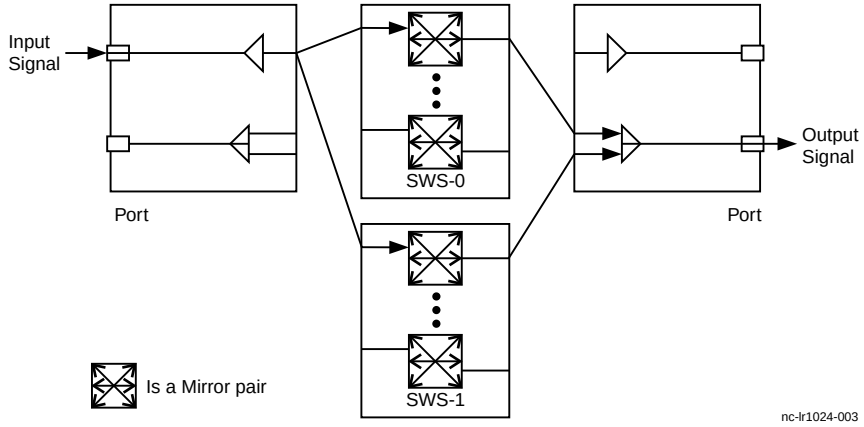
An existing cross-connection can be converted to a different cross-connection configuration by adding or deleting a leg. For example, a one-way duplex point-to-point configuration can be converted to a one-way bridge or merge. A two-way point-to-point configuration can become a bridge and merge configuration.

One-way point-to-point configuration

A one-way point-to-point configuration is a single-leg, duplex transmission path that carries traffic in one direction from an input port, through the duplicated switch fabric, to an output port.

The figure below illustrates an example of a one-way point-to-point configuration on a WaveStar LambdaRouter 256 system. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) divided into Side A and Side B.

In this example, an optical signal at the input port of an Optical Cross-connect Interface (OXI) circuit pack is split by a 1:2 splitter and routed to both switch fabrics. One of the two optical signals from the switch fabrics is selected by the output port 2:1 selector and passed through the output port.



Two-way point-to-point configuration

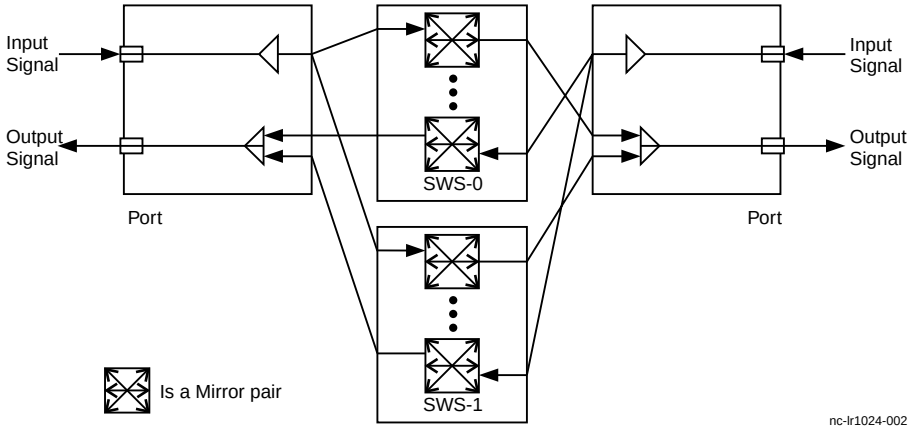
A two-way point-to-point configuration is a two-leg, duplex transmission path with each leg carrying traffic in one direction from an input port, through the duplicated switch fabric, to an output port. The input and output ports do not have to be on the same port unit, and two, three, or four ports can be used.

Each leg of the two-way point-to-point configuration is a one-way point-to-point cross-connection, and each must be at the same cross-connection rate (if identified).

A two-way point-to-point cross-connection may be established or removed by a single command to the network element.

The figure below illustrates an example of a two-way point-to-point configuration on a WaveStar LambdaRouter 256 system. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) divided into Side A and Side B.

In this example, each leg of the cross-connection is between the same input and output port.



Bridged and merged configuration

Bridging allows a one-way 1:2 multicast from an input port where a 1:2 splitter routes the two one-way signals through the duplicated switch fabric to two different output ports. Each one-way leg is a simplex transmission path.

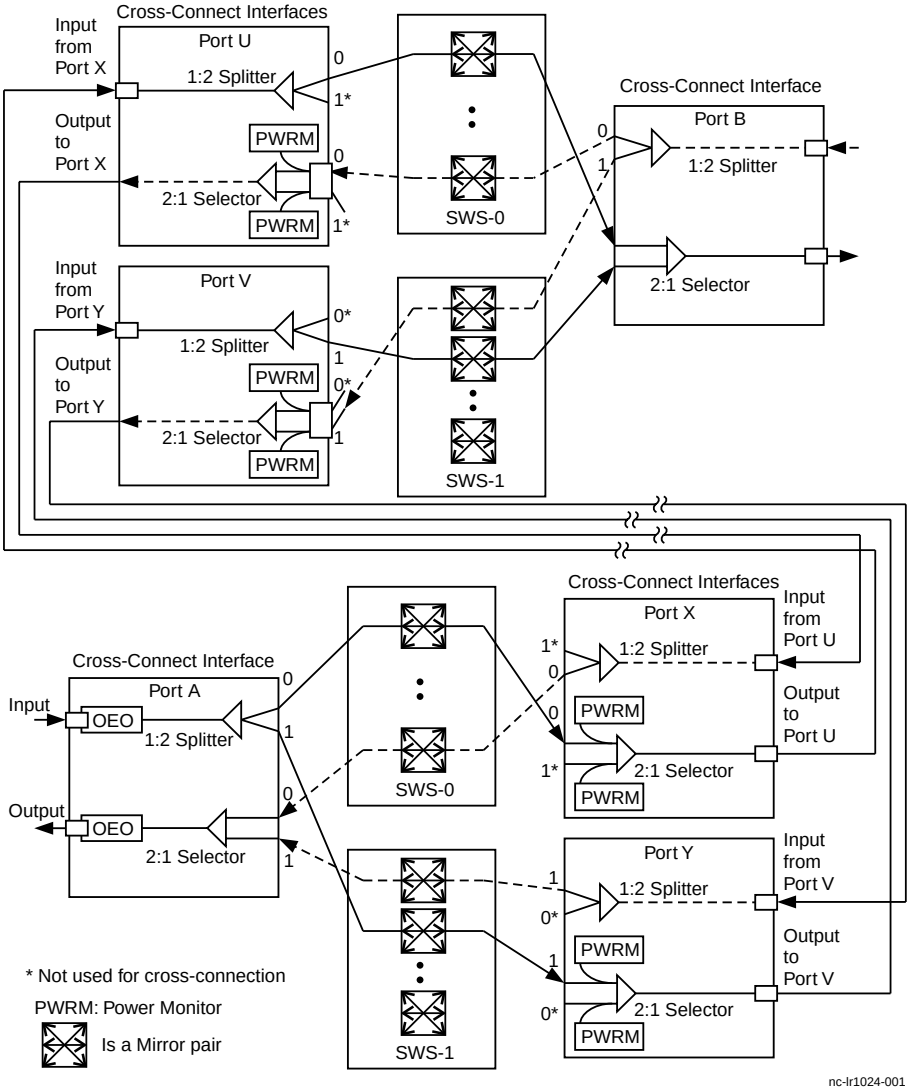
Merging is the cross-connecting of two different input ports to the output of a third port where a 2:1 selector chooses one of the incoming one-way simplex signals.

The use of both bridging and merging at a network element provides “1+1” path protection for two-way traffic or for two independent one-way paths that are carrying traffic in opposite directions.

For most cases, more than one cross-connection command must be used to establish or remove complex bridge and/or merge configurations.

The figure below illustrates an example of a bridged/merged configuration using two WaveStar LambdaRouter 256 systems. One node consists of cross-connect interface ports B, U, and V. The second node consists of cross-connect interface ports A, X, and Y. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) per node, each divided into Side A and Side B.

In this example, an optical signal at the input port B of an OXI circuit pack is split by a 1:2 splitter and routed to both switch fabrics. The two optical signals from the switch fabrics are routed to two different output ports (U and V). The optical signals from the output ports X and Y are received at two input ports (X and Y) on an OXI circuit pack and routed through both switch fabrics. One of the two optical signals from the switch fabrics is selected by the output port 2:1 selector and passed through the output port A of an OXI-10GC or OXI-2GC circuit pack.



Cross-connect loopback configuration

Cross-connect loopback configurations are used for maintenance purposes and involve cross-connecting an optical signal from an input port through the switch fabric and back to either the default loopback output port or to another compatible output port selected by the user.

The following types of cross-connect loopback topologies are supported:

- normal
- forced

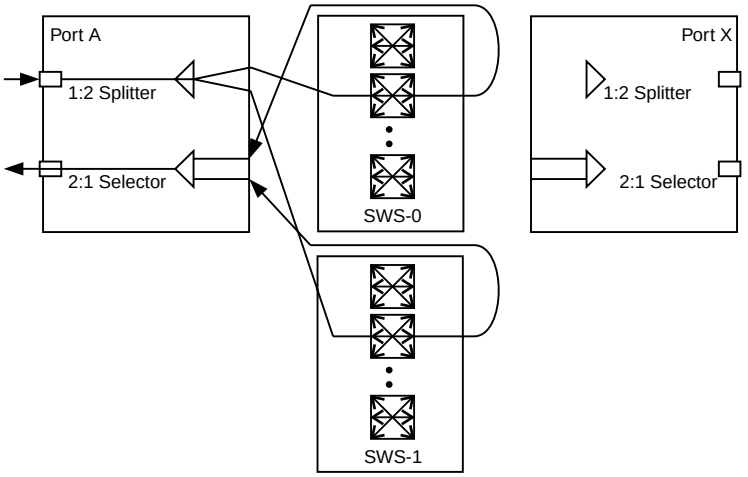
Normal cross-connect loopback

A normal cross-connect loopback is a non-service-affecting configuration that can be established on any type of input port, and applies only when the port is idle. The loopback is duplex if both fabrics are selected. If one fabric is selected, the loopback is simplex. Fabric selection is an optional parameter.

The default output port is the output port with the same AID as the input port on which the loopback is established. Any idle output port that is compatible with the input port may also be selected.

The figure below illustrates an example of a duplex normal cross-connect configuration on a WaveStar LambdaRouter 256 system. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) divided into Side A and Side B.

In this example, an optical signal at the input port of an OXI circuit pack is split by a 1:2 splitter and routed to both switch fabrics. One of the two optical signals from the switch fabrics is selected by the output port 2:1 selector and passed through the output port.



Forced cross-connect loopback

A forced cross-connect loopback configuration can be established on any type of input port that already has an existing cross-connection. The loopback is duplex if both fabrics are selected. If one fabric is selected, the loopback is simplex. Fabric selection is not an optional parameter as with normal cross-connect loopbacks.

A forced duplex cross-connect loopback is a service-affecting configuration. Because both switch fabrics are used for the loopback, no transmission path is available to reach the original output port.

A forced simplex cross-connect loopback is normally a non-service-affecting configuration. Because only one switch fabric is used for the loopback, the other fabric continues to provide a simplex transmission path for the original cross-connection. However, a forced simplex cross-connect loopback may cause the output selector to switch, depending upon the switch fabric that is specified, which could briefly interrupt the original cross-connection.

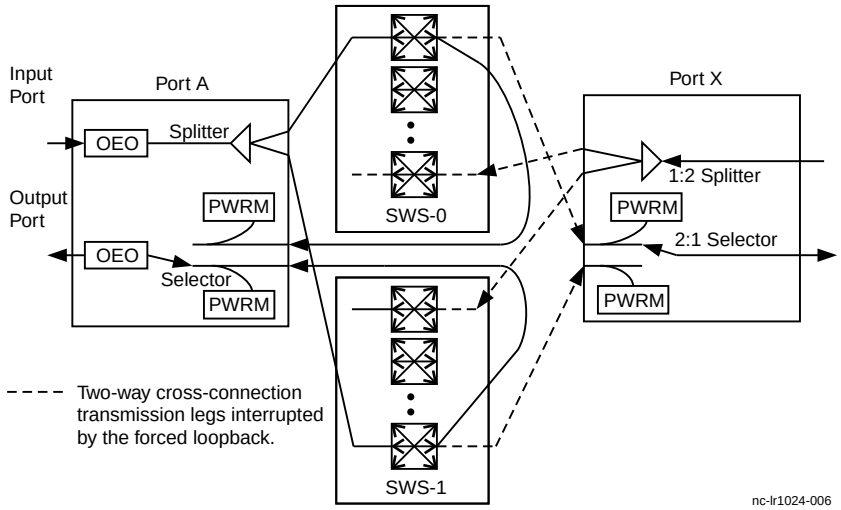
Any forced loopback request will be denied if the specified output port has a protection switch in effect or if the specified input port already has a loopback established.

The default output port for a forced loopback on a one-way configuration is the output port with the same AID as the input port on which the loopback is established. The default output port for a forced loopback on a two-way configuration is the output port being used for the opposite direction. Any idle output port that is compatible with the input port may also be selected.

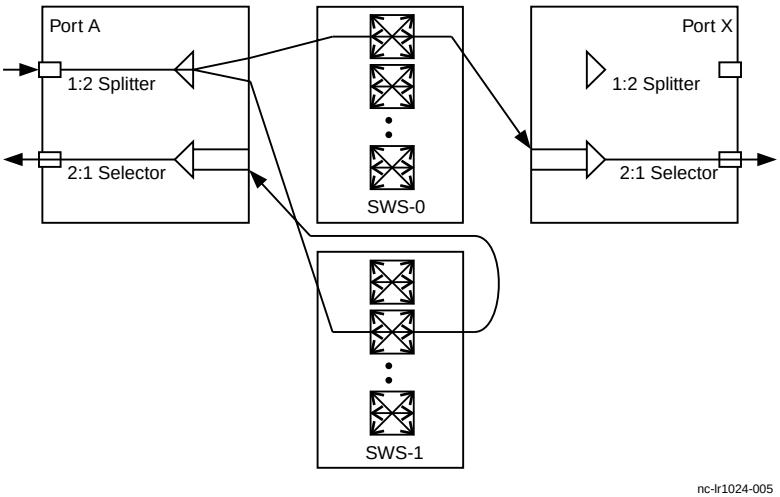
For a two-way forced simplex loopback using the default output port, the transmission path in the opposite direction will be interrupted.

When the forced loopback cross-connection is removed, the original cross-connection is automatically restored by the system.

The figure below illustrates a forced duplex cross-connect loopback for a two-way configuration on a WaveStar LambdaRouter 256 system. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) divided into Side A and Side B.



The figure below illustrates a forced simplex cross-connect loopback for a one-way configuration on a WaveStar LambdaRouter 256 system. Note that the configuration on a WaveStar LambdaRouter 128 system is similar, with a single Switch Shelf (SWS) divided into Side A and Side B.



Cross-Connection Commands

Introduction

The WaveStar CIT for LambdaRouter user interface provides a cross-connection wizard that allows a user to

- create new cross-connections
- add cross-connection legs to an existing cross-connection
- delete existing cross-connections or legs of an existing cross-connection

Additional user interface functions allow a user to

- retrieve cross-connection data
- operate (establish) loopback cross-connections
- release (remove) loopback cross-connections

Creating a new cross-connection

The cross-connection wizard automates the process of creating new cross-connections on the WaveStar LambdaRouter 128/256 by prompting for the selection of a cross-connection type and the input and output ports used by the cross-connection. The number of ports that must be selected is dependent upon the type of cross-connection being created.

After confirming the cross-connection information, the WaveStar CIT issues the required commands to the network element to create the new cross-connection. It may be necessary for multiple commands to be issued to establish the desired cross-connection configuration.

Command validation for creating a new cross-connection

Cross-connection command processing will validate the following in order to create a new cross-connection:

- input and output AIDs must be valid
- input and output port and at least one switch fabric must be equipped and in-service
- input and output ports must be idle (not currently in use as a destination for an existing cross-connection or loopback cross-connection)
- the number of cross-connection legs (including a loopback leg) originating from the same client-side input port is restricted to two
- input port attributes must match output port attributes

Adding cross-connection legs to an existing cross-connection

Cross-connection legs may be added to an existing cross-connection to create a new cross-connection configuration.

The cross-connection wizard prompts for the selection of an input or output port and displays all cross-connection legs associated with the selected port. A cross-connection associated with the port, type of cross-connection to be added is then selected, and the input and output ports to be used by the new cross-connection leg(s) are then selected. The number of ports that must be selected is dependent upon the type of cross-connection being added.

After reviewing and confirming the cross-connection information, the WaveStar CIT issues the required commands to the network element to add the cross-connection legs to the existing cross-connection. It may be necessary for multiple commands to be issued to establish the desired cross-connection configuration.

Command validation for adding cross-connection legs

Cross-connection command processing will validate the following in order to add legs to an existing cross-connection. Only valid ports will be displayed by the cross-connection wizard:

- if the existing cross-connection is a simplex configuration, all ports must be idle or one-side busy
- if the existing cross-connection is a duplex configuration, all ports must be idle

Additional validation is performed when adding

- a leg to form a one-way bridge
- a leg to form a one-way merge
- two-way legs to form a two-way bridge/merge
- a bridge to an existing bridge
- a merge to an existing merge
- a two-way bridge/merge to an existing two-way bridge/merge

Deleting cross-connections

One or more cross-connection legs may be removed from an existing cross-connection to either delete the cross-connection entirely or to create a new cross-connection configuration.

The cross-connection wizard prompts for the selection of an input or output port and displays all cross-connection legs associated with the selected port. A cross-connection associated with the port is then selected for deletion. A diagram of the selected cross-connection configuration can also be displayed.

If a cross-connection that involves more than one choice for deletion is selected (for example, deleting one or both legs of a merge), a single or group of cross-connections associated with the configuration must be selected. This allows individual legs or all legs of a cross-connection to be deleted. This selection window is not displayed if a one-way or two-way point-to-point cross-connection is selected.

After reviewing and confirming the cross-connection information, the WaveStar CIT issues the required commands to the network element to delete the selected cross-connection legs. It may be necessary for multiple commands to be issued to delete the selected cross-connection.

Command validation for deleting cross-connection legs

Cross-connection command processing will validate the following in order to delete a cross-connection:

- input and output port AIDs must be valid
- cross-connection configuration is valid
- input port is not currently used for an existing loopback cross-connection
- cross-connection must exist between the specified input port AID and output port AID
- a High-Voltage Shelf must be in-service

Retrieving cross-connection data

Cross-connection data may be retrieved to report the input AID, output AID, and configuration information for each leg or leg-pair of a specified cross-connection (including loopback cross-connections), or all existing cross-connections associated with the specified AID.

Cross-connection data associated with a port may be retrieved and displayed in either a text or graphic format. Cross-connection data associated with the system, shelf, or circuit pack may be displayed in text format only.

Command validation for retrieving cross-connection data

Cross-connection command processing will validate the following in order to retrieve information for a cross-connection:

- input and output AIDs must be valid
- scope parameter must be valid if specified

Operating a loopback cross-connection

Operating a loopback cross-connection establishes a loopback between an input port and an optionally specified output port. If no output port is specified, the default loopback output port is used as determined by the type of loopback cross-connection being established.

For normal and forced loopback cross-connections, the switch fabric to be used to establish the loopback (switch fabric 0, switch fabric 1, or both fabrics) must be specified. The WaveStar CIT for LambdaRouter GUI will display the currently active fabric.

Once a loopback cross-connection is established, it remains in effect until manually released. When a loopback cross-connection is released, the original cross-connection is automatically restored by the system.

Operate loopback cross-connection command validation

Cross-connection command processing will validate the following in order to establish a loopback cross-connection:

- input and output port AIDs must be valid
- a loopback cross-connection does not already exist on the specified port AID
- switch fabric must be valid

Releasing a loopback cross-connection

Releasing a loopback cross-connection removes a normal or forced loopback between the specified input port and the output port being used by the loopback.

Release loopback cross-connection command validation

Cross-connection command processing will validate the following in order to release a loopback cross-connection:

- input AID must be valid
- a loopback cross-connection must already exist on the specified port AID

□

Cross-Connection Reports

Overview

The WaveStar LambdaRouter 128/256 allows the generation of system and equipment status reports, including a list of cross-connections for a selected AID.

Cross-Connection List

The Cross-Connection List provides a list of the currently established cross-connections for a specific port, all ports on a specific circuit pack, all ports on a specific shelf, or all ports in the network element.

The report includes the input and output AID, cross-connection or loopback type, and switch fabric used in the cross-connection.

After the report is generated, the data may be saved and/or printed.

□

6 Software Management

Overview

Purpose

This chapter provides detailed information on the WaveStar LambdaRouter 128/256 software management functions. This includes information on software installation and upgrade, and database backup and restore.

Contents

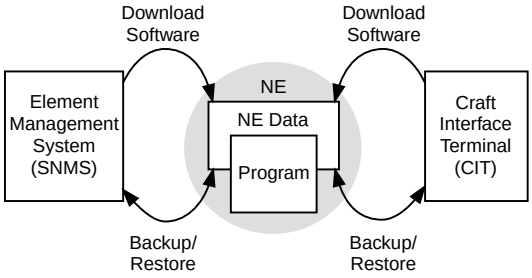
Introduction to Software Management

Introduction

Software management functions include all activities necessary to

- download, install, and upgrade the software generic on a network element
- perform remote backup and restore operations of the network element provisionable data
- perform local backup and restore operations of the network element provisionable data

The following figure illustrates the software management functions.



Software management functions may be accessed via all available operations interfaces, including the WaveStar CIT (Craft Interface Terminal) for LambdaRouter or other managing system.

Definitions

The following terms are used in this chapter:

Term	Definition
Generic	A collection of programs and the associated static data that fully support and perform all of the designed functions of the WaveStar LambdaRouter 128/256, the WaveStar CIT, or the Element Management System (EMS). Software systems that configure, control, maintain, and operate the transport network are referred to as generics.
Program	The executable code (software) that controls the network element or WaveStar CIT.
Provisionable Data	System configuration data provisioned by a user using a WaveStar CIT or managing system. This includes such data as port configuration parameters and cross-connection data.
Download	The process of transferring files from a managing system (such as the WaveStar CIT or SNMS) to a network element. Both software and data can be downloaded.
Upload	The process of transferring files from a network element to a managing system. The WaveStar LambdaRouter 128/256 can only upload data.
Activation	The process of starting the software or using the data in execution the first time after installation.
Installation	The process of delivering, expanding, and locating all of the files within a generic into the proper locations within the target system in such a manner that the generic will be activated properly.

Software and database states

A generic or database can assume the following states:

State	Description
PREVIOUS	A previous generic or database. This version of generic or database is available for installation in case of backout from the current installation.
RUNNING	The currently executing generic or current database.
DOWNLOADED	Applies to the previous bin of generic. Indicates that the generic just downloaded is ready for installation.
INPROGRESS	In the previous bin, this indicates that a download is in progress. In the current bin, this indicates that an installation is in progress. This is interpreted in conjunction with the current pointer.
CORRUPT	The generic or data in this bin is unavailable for invocation or execution. For example, a corrupted checksum has been detected.
FAILED	The non-volatile memory (NVM) has failed. This may be the last message written into the NVM prior to its being disabled (based on the life-cycle count of the NVM card.)
INITIAL	The bin on the NVM is empty, such as in a newly inserted blank NVM or an empty previous bin.

Infrastructure

System and shelf controllers

The WaveStar LambdaRouter 128/256 software executes in the network element system controllers and shelf controllers.

Non-volatile storage

The WaveStar LambdaRouter 128/256 provides primary and secondary non-volatile memory (NVM) for storage of software and all provisionable data.

Primary

Each of the duplicated primary NVMs has two partitions. Each partition stores one network element generic (one partition containing the current generic, the other partition containing a previous generic) and their related databases.

The duplicated primary NVM provides a backup to the active NVM. Maintaining two partitions allows for back out to a previous generic.

Secondary

A removable secondary NVM is provided for local software upgrade and data backups.

Labeling

The WaveStar LambdaRouter 128/256 provides for labeling of databases and software generics, as described in the sections that follow.

Database

Database labeling is provided for use in subsequent download operations. The labeling includes system target identifier (TID), date of the last modification, date backed up from the network element, and the software generic ID.

Generic

Labeling of the software generic is provided in order to uniquely identify the generic. The generic ID includes the supplier name and type, the version number of the generic, the date built or build number, and the date installed.

The generic label information can be retrieved via the managing system or WaveStar CIT.

Software and Database Installation and Upgrade

Introduction

Installation and upgrade operations may be performed on the WaveStar LambdaRouter 128/256 to install and/or update the generic or database on a single network element.

Installation process

Installation is the process of interpreting and unpacking the binary program or data that was downloaded to a network element NVM, and copying the constituent data items to their designated locations within the network element.

Initial installation

When a network element is first deployed, the generic can only be installed from an NVM card inserted into the Primary Memory (PRI MEM) circuit pack. The network element generic is delivered on a CD-ROM that also contains

- factory data
- WaveStar CIT software
- utilities to copy the software generic to a hard drive and to install the WaveStar CIT

The software is then copied from the CD-ROM on the WaveStar CIT to a blank NVM card, which is now ready for use in the network element. Refer to the *WaveStar LambdaRouter 128/256 Software Release Description* for information on downloading and installing software and data on the WaveStar LambdaRouter 128/256.

After the initial installation of the software, the network element is ready to be provisioned.

Software upgrade process

A software upgrade can only be installed by downloading remotely from an external system, or by delivering the generic on an NVM card that will be inserted into the Secondary Memory (SEC MEM) circuit pack.

The download method involves downloading the generic from an external system onto the PRI MEM circuit pack, after which the generic can be activated.

Delivering the generic on an NVM card involves

- creating an NVM card on the WaveStar CIT (which includes copying the software from CD-ROM to the NVM card)
- inserting the NVM card into the SEC MEM circuit pack NVM slot
- copying the software from SEC MEM to PRI MEM
- activating the generic

When an upgrade requires a conversion of the database from the existing format to a new format, a conversion utility will be provided to automatically convert the database to the new format prior to installing the new generic.

Commit to or back out from a new generic installation

During the installation of a new generic, a system reboot will occur. The initialization process will keep track of whether or not the new generic software functions as expected.

As each shelf controller completes its start-up of the generic, it will report the success or failure of the start-up to the next controller in the hierarchy. The active SYS50D determines the success, partial success, or complete failure of the system startup of the current generic, and reports this information to the user.

If the controller startup is not successful, the user must manually back out and reestablish the previous software.

Installing new Switch Shelf calibration data

When a new Switch Shelf is installed, the matching calibration data must be installed and activated with the shelf. The calibration data is delivered on an NVM card and is installed by inserting the card into the SEC MEM circuit pack and copying the calibration data from SEC MEM to PRI MEM. Once installed, the calibration data is activated and becomes part of the database.

□

Database Backup and Restore

Introduction

Database backup and restore operations may be performed on the WaveStar LambdaRouter 128/256 in order to provide protection and recovery from a failure of the primary NVM.

Restore operations are limited to a single network element and can be performed by a remote managing system or by a WaveStar CIT which may be remote or connected locally to the network element.

Backup process

The backup process is the saving of an image of the current data of a network element to a non-volatile storage area either within the network element itself (SEC MEM), or to remote file storage (managing system or WaveStar CIT).

Restore process

The restore process involves retrieving a previous backup for the same network element from a non-volatile storage area either within the network element (SEC MEM) or remote file storage (managing system or WaveStar CIT), verifying that the database is compatible with the current generic, and copying the image back into the network element.

7 Security Management Tasks

Overview

Purpose This chapter provides detailed procedures for performing user administration and system security tasks on the WaveStar LambdaRouter 128/256 and the WaveStar CIT (Craft Interface Terminal).

Contents

Task 100: Adding, Modifying, or Deleting User Login Parameters

Purpose

This procedure is used to perform the following security administration tasks on either the WaveStar CIT or WaveStar LambdaRouter 128/256:

- add a new user
- modify login parameters for an existing user (such as password and/or authorization levels)
- delete an existing user

Important! Preinstalled Superuser logins cannot be deleted, and additional Superuser logins cannot be created. With the exception of changing the login ID and password, Superuser logins cannot be modified.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and identify the user's login and any security parameters that must be provisioned.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S5.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 101: Changing the Password for the Currently Logged in User" (7-10)
- "Task 102: Viewing Session Information for the Currently Logged in User" (7-12)
- "Task 103: Changing a Superuser Login ID" (7-13)
- "Task 104: Viewing a List of User Logins" (7-15)

- "Task 107: Setting Security Parameters for a Network Element" (7-20)
- "Task 108: Viewing Security Logs" (7-22)

Task Complete the following steps to add, modify, or delete a user login on the WaveStar CIT or WaveStar LambdaRouter 128/256.

1

IF...	THEN...
adding, modifying, or deleting a user login on the WaveStar CIT	log into the WaveStar CIT with a security level of S5 and select **Administration> Security>CIT User Provisioning** from the Network View Main Menu bar. **Result:** The CIT User Provisioning Screen appears.
adding, modifying, or deleting a user login on a network element	connect the WaveStar CIT to the local network element, log in with a security level of S5, and select **Administration> Security>User Provisioning** from the System View Main Menu bar. **Result:** The NE User Provisioning Screen appears.

2

IF...	THEN...
adding a new user	go to "SE 100-1: Adding a new user" (7-5).
modifying login parameters for an existing user	go to "SE 100-2: Modifying login parameters for an existing user" (7-7).
deleting an existing user	go to "SE 100-3: Deleting an existing user" (7-9).

N D O F S T E P S

SE 100-1: Adding a new user

Complete the following steps to add a new user on the WaveStar CIT or network element.

1 Click **New User** and enter a login ID for the new user.

2 Enter the user's password in the Enter Password field, then enter the same password again in the Confirm Password field.

For security reasons, asterisks are displayed in place of the password.

3 Select a User Type from the drop-down list.

Result: The Authorization Levels will be pre-populated based on the selected User Type.

4 Make any required changes to the Authorization Levels.

5

IF adding a new user to...	THEN...
a network element	continue to Step 6.
the WaveStar CIT	continue to Step 9.

6 Set the Password Aging Interval for the new user:

IF password aging...	THEN...
will not be enabled (the password never expires)	click **Disable**.
will be enabled	click the radio button beside the Days entry field and enter the number of days (7–999) that the user's password will remain valid.

7 Set the Inactivity Timeout period for the new user:

IF inactivity timeout...	THEN...
will not be enabled (the user will never be logged out due to inactivity)	set the Inactivity Timeout period to **0** (zero).
will be enabled	set the number of minutes (1–999) a user is allowed to be inactive before the network element will automatically terminate the session.

8 Select the user's Notification Registration List.

9 Click **Add**.

Result: A Confirmation Screen appears.

10 Click **Yes**.

IF adding a new user to...	THEN...
a network element	the Confirmation Screen closes and the System View appears. *Stop! End of Supporting Element*.
the WaveStar CIT	the Confirmation Screen closes and a message appears indicating the new user has been successfully added.

11 Click **OK**.

Result: The User Provisioning Screen appears.

12 Click **Close** on the User Provisioning Screen.

Result: The User Provisioning Screen closes.

N D O F S T E P S

SE 100-2: Modifying login parameters for an existing user

Complete the following steps to modify the login parameters for an existing user on the WaveStar CIT or network element.

1 Click **Existing User** and select a user login ID from the drop-down list.

Result: The login parameters for the selected user are displayed. For security purposes, the user's password is not displayed.

2 Modify the login parameters for the selected user.

IF modifying a user login on...	THEN...
the WaveStar CIT	modify any of the following: • user type • authorization levels • password (in both the Enter Password and Confirm Password fields)
a network element	optionally disable the user's login ID by clicking **Disable** in the User ID Can Be Enabled? field. OR enable the user's login ID by clicking **Enable** in the User ID Can Be Enabled? field and modify any of the following: • user type • privilege levels • registration list • password (in both the Enter Password and Confirm Password fields) • password aging interval • inactivity timeout period

3 Click **Modify**.

Result: A Confirmation Screen appears.

4 Click **Yes**.

IF modifying a user login on...	THEN...
a network element	the Confirmation Screen closes and the System View appears. *Stop! End of Supporting Element*.
the WaveStar CIT	the Confirmation Screen closes and a message appears indicating the modified user data has been saved.

5 Click **OK**.

Result: The User Provisioning Screen appears.

6 Click **Close** on the User Provisioning Screen.

Result: The User Provisioning Screen closes.

END OF STEPS

SE 100-3: Deleting an existing user

Complete the following steps to delete an existing user from the WaveStar CIT or network element.

1 Click **Existing User** and select a user login ID from the drop-down list.

Result: The login parameters for the selected user are displayed. For security purposes, the user's password is not displayed.

2 Click **Delete**.

Result: A Confirmation Screen appears.

3 Click **Yes**.

IF modifying a user login on...	THEN...
a network element	the Confirmation Screen closes and the System View appears. *Stop! End of Supporting Element*.
the WaveStar CIT	the Confirmation Screen closes and a message appears indicating the user data has been successfully deleted.

4 Click **OK**.

Result: The User Provisioning Screen appears.

5 Click **Close** on the User Provisioning Screen.

Result: The User Provisioning Screen closes.

END OF STEPS

Task 101: Changing the Password for the Currently Logged in User

Purpose

This procedure is used to change the password for the currently logged in user on either the WaveStar CIT or WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 100: Adding, Modifying, or Deleting User Login Parameters" (7-3)

Task Complete the following steps to change the password for the currently logged in user on either the WaveStar CIT or WaveStar LambdaRouter 128/256.

1

IF changing the password on...	THEN...
the WaveStar CIT	log into the WaveStar CIT and select **Administration>Change Password** from the Network View Main Menu bar. **Result:** The Change CIT Login Password Screen appears.
a network element	connect the WaveStar CIT to the local network element, log in, and select **Administration>Change Password** from the System View Main Menu bar. **Result:** The Change NE Login Password Screen appears.

2 Enter the password information in the Old Password, New Password, and Confirm Password fields.

Important! The password entered in the New Password and Confirm Password fields must match. Asterisks will be displayed as the passwords are entered.

3 Click **OK**.

Result: A Confirmation Screen appears.

4 Click **Yes**.

Result: The Confirmation Screen closes.

END OF STEPS

Task 102: Viewing Session Information for the Currently Logged in User

Purpose

This procedure is used to view session information for the currently logged in user on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)

Task

Complete the following steps to view the session information for the currently logged in user on the WaveStar LambdaRouter 128/256.

1 Connect the WaveStar CIT to the local network element, log in to the network element, and select **Administration>Current Session Info** from the System View Main Menu bar.

Result: The Current Session Information Screen appears for the currently logged in user.

2 View the user ID (UID), user privilege code (UPC), and the date and time the current user logged into the network element. Click **OK** when you have finished viewing the information.

Result: The Current Session Information Screen closes.

END OF STEPS

□

Task 103: Changing a Superuser Login ID

Purpose

This procedure is used by Superusers to change their own login ID on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and identify the user's login and any security parameters that must be provisioned.
- Connect the WaveStar CIT to the local network element and log in as the Superuser for which the login ID will be changed.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 100: Adding, Modifying, or Deleting User Login Parameters" (7-3)
- "Task 101: Changing the Password for the Currently Logged in User" (7-10)

Task Complete the following steps to change the login ID for the currently logged in Superuser on the WaveStar LambdaRouter 128/256.

1 Connect the WaveStar CIT to the local network element, log in as a Superuser, and select **Administration>Security>User Provisioning** from the System View Main Menu bar.

Result: The User Provisioning Screen appears.

2 Click **Existing User** and select the login ID for the currently logged in Superuser from the drop-down list.

Result: The login parameters for the selected user are displayed and the New Login ID for SuperUsers field is enabled. For security purposes, the user's password is not displayed.

3 Enter the new login ID for the currently logged in Superuser in the New Login ID for SuperUsers field and click **Modify**.

Result: A Confirmation Screen appears.

4 Click **Yes**.

Result: A message appears asking if the changes should be saved to the WaveStar CIT security database.

5 Click **No**.

Important! Saving changes to network element login IDs and passwords in the WaveStar CIT security database is a potential security risk and it is not recommended.

Result: The message closes. The new Superuser login ID will not take effect until the next user session.

N D O F S T E P S

□

Task 104: Viewing a List of User Logins

Purpose

This procedure is used to view a list of user logins currently provisioned on either the WaveStar CIT or WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 100: Adding, Modifying, or Deleting User Login Parameters" (7-3)
- "Task 106: Forcing a User Logout" (7-18)

Task Complete the following steps to view a list of user logins on either the WaveStar CIT or WaveStar LambdaRouter 128/256.

1

IF viewing a list of user logins on...	THEN...
the WaveStar CIT	log into the WaveStar CIT and select **Administration>Security> View User Logins** from the Network View Main Menu bar. **Result:** The View User Logins Screen appears.
a network element	connect the WaveStar CIT to the local network element, log in, and select **Administration>Security> View User Logins** from the System View Main Menu bar. **Result:** The View User Logins Screen appears.

2 View the displayed login parameters for each user. Click on any heading to sort the list in ascending order by the selected heading. Clicking on the same heading a second time will sort the displayed data in descending order.

3 Click **Close**.

Result: The View User Logins Screen closes.

END OF STEPS

Task 105: Viewing a List of Logged-In Users

Purpose

This procedure is used to view a list of users currently logged into the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 106: Forcing a User Logout" (7-18)

Task

Complete the following steps to view a list of currently logged-in users.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Administration>Security>View Logged-In Users**.

Result: The View Logged In User Screen appears.

2 View the list of users currently logged into the network element, click **Close** when finished.

Result: The View Logged in User Screen closes.

END OF STEPS

Task 106: Forcing a User Logout

Purpose

This procedure is used to forcibly log out a user that is currently logged into the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S5.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 105: Viewing a List of Logged-In Users" (7-17)

Task

Complete the following steps to forcibly log out one or more currently logged-in users.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Administration>Security>Logout NE User**.

Result: The Log Out User Screen appears.

2 View the list of users currently logged into the network element.

Important! The login ID of the current WaveStar CIT user is not displayed.

3

IF forcibly logging out...	THEN...
individual users	select the user login ID that will be forcibly logged out, then click **Logout User**. **Result:** A Confirmation Screen appears.
all users	click **Logout All**. **Result:** A Confirmation Screen appears.

4 Click **Yes**.

IF forcibly logging out...	THEN...
individual users	the selected user is forcibly logged out and the Confirmation Screen closes.
all users	all currently logged in users are forcibly logged out except the S5 user executing the command and any other Superuser that is currently logged in.

END OF STEPS

Task 107: Setting Security Parameters for a Network Element

Purpose

This procedure is used to set security parameters for the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or higher.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 100: Adding, Modifying, or Deleting User Login Parameters" (7-3)
- "Task 104: Viewing a List of User Logins" (7-15)
- "Task 108: Viewing Security Logs" (7-22)

Task

Complete the following steps to set security parameters for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Administration>Security>Security Provisioning**.

Result: The Provision NE Security Screen appears.

2 Enter the required information in the following fields:

Field	Value
User ID Lockout Threshold	2 to 99 attempts
User ID Lockout Aging Period	1 to 999 minutes
User ID Lockout Period	1 to 99 minutes (clicking on **Disable** will disable the User ID Lockout)
User ID Aging Period	1 to 999 days (clicking on **Disable** will disable User ID Aging)

3 Click **OK**.

Result: A Confirmation Screen appears.

4 Click **Yes**.

Result: The Confirmation Screen closes.

END OF STEPS

Task 108: Viewing Security Logs

Purpose

This procedure is used to view the following security logs on the WaveStar LambdaRouter 128/256:

- Security Activity Log
- User Session Activity Log

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 100: Adding, Modifying, or Deleting User Login Parameters" (7-3)
- "Task 101: Changing the Password for the Currently Logged in User" (7-10)
- "Task 102: Viewing Session Information for the Currently Logged in User" (7-12)
- "Task 103: Changing a Superuser Login ID" (7-13)
- "Task 104: Viewing a List of User Logins" (7-15)
- "Task 105: Viewing a List of Logged-In Users" (7-17)
- "Task 106: Forcing a User Logout" (7-18)
- "Task 107: Setting Security Parameters for a Network Element" (7-20)

Task Complete the following steps to view the WaveStar LambdaRouter 128/256 security logs.

1

IF retrieving the...	THEN...
Security Activity Log	at the WaveStar CIT, from the System View Main Menu bar, select **Reports> NE Security Log**. **Result:** The Start Date/Time Selection Screen appears.
User Session Activity Log	at the WaveStar CIT, from the System View Main Menu bar, select **Reports> NE User Log**. **Result:** The Start Date/Time Selection Screen appears.

2

IF...	THEN...
retrieving all log entries	select **Retrieve ALL**.
retrieving log entries starting with a specific date and time	select the starting date and time.

3 Click **OK**.

Result: The selected security log appears.

4

IF...	THEN...
saving log data to a file	go to “SE 108-1: Saving log data to a file” (7-24).
printing log data	go to “SE 108-2: Printing log data” (7-25).
retrieving updated log data	click **Refresh**. **Result:** The displayed log data is updated.
viewing log data is completed	click **Close**. **Result:** The log screen closes.

N D O F S T E P S

SE 108-1: Saving log data to a file

Complete the following steps to save the displayed log data to a file.

1 Click **Save As**.

Result: The Save As dialog box appears.

2 Select the desired destination path, enter a file name, then click **Save**.

Result: The log data is saved to the specified file and the Save As dialog box closes.

N D O F S T E P S

SE 108-2: Printing log data

Complete the following steps to print the displayed log data.

1. Click **Print**.

   Result: The Print dialog box appears.

2. Select the desired printer, configure the necessary print options, then click **OK**.

   Result: The log data is printed to the selected printer.

END OF STEPS

8 Management Communication Setup Tasks

Overview

Purpose

This chapter provides detailed procedures for configuring the WaveStar CIT and WaveStar LambdaRouter 128/256 communication parameters, and for connecting the WaveStar CIT to a WaveStar LambdaRouter 128/256 and logging in. Procedures are also provided for connecting a terminal to the WaveStar LambdaRouter 128/256 RS-232 port and logging in.

Contents

Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element

Purpose

This procedure is used to physically connect the WaveStar CIT to, or disconnect the WaveStar CIT from, a local network element.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain a WaveStar CIT 10BaseT Ethernet interface cable (CAT 3 or higher) with RJ45 connectors.

Related information

For related information, see the following sections in this document:

- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 202: Viewing the WaveStar CIT Network Element IP Address List" (8-8)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 207: Logging Out and Disconnecting from a Network Element" (8-22)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 209: Logging Out of a Cut-Through Session" (8-31)

Task

Complete the following steps to connect the WaveStar CIT to, or disconnect the WaveStar CIT from, a local network element.

1

IF...	THEN...
connecting the WaveStar CIT to a network element	go to "SE 200-1: Connecting the WaveStar CIT to a network element" (8-4).
disconnecting the WaveStar CIT from a network element	go to "SE 200-2: Disconnecting the WaveStar CIT from a network element" (8-5).

ND OF STEPS

SE 200-1: Connecting the WaveStar CIT to a network element

Complete the following steps to connect the WaveStar CIT to a network element.

1 Plug one end of the interface cable into the WaveStar CIT and the other end into the CIT port on the network element System Controller Shelf User Panel.

2 Log into the WaveStar CIT and the network element.

Reference: "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

ND OF STEPS

SE 200-2: Disconnecting the WaveStar CIT from a network element

Complete the following steps to disconnect the WaveStar CIT from a network element.

1 Log out of all network elements and the WaveStar CIT.

Reference: "Task 207: Logging Out and Disconnecting from a Network Element" (8-22).

2 Disconnect the interface cable from the CIT port on the network element System Controller Shelf User Panel and from the WaveStar CIT.

ND OF STEPS

□

Task 201: Logging in to the WaveStar CIT

Purpose

This procedure is used to log in to the WaveStar CIT.

Before you begin

Before beginning this task, have a valid user ID and password on the WaveStar CIT.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 207: Logging Out and Disconnecting from a Network Element" (8-22)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 209: Logging Out of a Cut-Through Session" (8-31)

Task

Complete the following steps to log in to the WaveStar CIT.

1 Double-click on the WaveStar CIT icon on the *Microsoft Windows*® desktop.

Result: The WaveStar CIT Login Screen appears.

2 Enter a valid User ID and Password, then click **OK**.

IF...	THEN...
the login is completed successfully	the Legal Notice Screen appears.
the login fails	verify that the user ID and password are correct and attempt to log in again. If the login has failed a second time, contact the System Administrator. *Stop! End of Task.*

3 Click **OK**.

Result: The Legal Notice Screen closes and the WaveStar CIT for LambdaRouter Network View Screen appears.

ND OF STEPS

Task 202: Viewing the WaveStar CIT Network Element IP Address List

Purpose

This procedure is used to view the current list of network element IP addresses stored on the WaveStar CIT.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Log into the WaveStar CIT with a Privilege Code of S1. It is not necessary to connect to a network element.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 205: Setting the Network Element Name" (8-16)
- "Task 206: Setting Network Element IP Addresses" (8-19)

Task

Complete the following steps to view the current list of network element IP addresses stored on the WaveStar CIT.

1 At the WaveStar CIT, from the Network View Main Menu bar, select **Administration**>**NE IP Address List**.

Result: The NE IP Address List Screen appears.

2 Select a network element TID from the drop-down list.

Result: The IP addresses associated with the selected TID are displayed.

3

IF...	THEN...
viewing IP addresses for additional network elements	select each network element TID from the drop-down list. When the last TID has been selected, continue to the next step.
additional TIDs will not be selected	continue to the next step.

4 Click **OK**.

Result: The NE IP Address List Screen closes.

END OF STEPS

□

Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses

Purpose

This procedure is used to add, modify, or delete network element Target Identifiers (TIDs) and IP addresses on the WaveStar CIT.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Log into the WaveStar CIT with a Privilege Code of S3. It is not necessary to connect to a network element.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 202: Viewing the WaveStar CIT Network Element IP Address List" (8-8)
- "Task 205: Setting the Network Element Name" (8-16)
- "Task 206: Setting Network Element IP Addresses" (8-19)

Task

Complete the following steps to provision the WaveStar CIT with network element TIDs and IP addresses.

1 At the WaveStar CIT, from the Network View Main Menu bar, select **Administration**>**NE Name/Address Administration**.

Result: The NE Name/Address Administration Screen appears.

2

IF...	THEN...
entering a new network element name and IP address	click **Add**. **Result:** The Add IP Address Screen appears.
modifying an existing network element name and IP address	click the down arrow beside the TID field and select the TID to be modified from the list that is displayed. Click **Modify**. **Result:** The Modify IP Address Screen appears with the **TID** and **IP Address** fields populated with the current values for the selected network element.
deleting an existing network element name and IP address	click the down arrow beside the TID field and select the TID to be deleted from the list that is displayed. Click **Delete**. **Result:** A Confirmation Screen appears.

3

IF...	THEN...
adding or modifying a network element name and IP address	enter the required information in the TID field and both IP Address fields (in dotted decimal format) then click **Apply**. **Result:** A Successful Completion Message appears. The TID and IP Address for the network element are saved locally on the WaveStar CIT. The WaveStar CIT can now access the network element.
deleting a network element name and IP address	click **Yes**. **Result:** A Successful Completion Message appears.

4 Click **OK**.

Result: The Successful Completion Message closes and the Network View appears.

END OF STEPS

Task 204: Logging into a Network Element from the WaveStar CIT

Purpose

This procedure is used to log into a network element from the WaveStar CIT.

Before you begin

Before beginning this task:

- Have a valid user ID and password on both the WaveStar CIT and the network element.
- Ensure the WaveStar CIT has been provisioned with the network element Target Identifier (TID) and IP address.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 207: Logging Out and Disconnecting from a Network Element" (8-22)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 209: Logging Out of a Cut-Through Session" (8-31)

Task

Complete the following steps to log into a network element from the WaveStar CIT.

1 Connect the WaveStar CIT to the local network element.

Reference: "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3).

2 Log into the WaveStar CIT.

Result: The Network View Screen appears.

Reference: "Task 201: Logging in to the WaveStar CIT" (8-6).

3

IF...	THEN...
an icon exists in the Network View for the desired network element	double click on the network element icon.
an icon does not exist in the Network View for the desired network element	enter the network element TID in the Network View TID field, select the **System** button, then click **Connect**.

4

IF the network element...	THEN...
has been provisioned with two IP addresses	the IP Address Selection Screen appears. Continue to the next step.
has been provisioned with one IP address	the Network Element Login Screen appears. Continue to Step 6.

5 Select the IP address to use for the connection and click **OK**.

Result: The Network Element Login Screen appears.

6 Enter a valid User ID and Password then click **OK**.

IF...	THEN...
this is the first login for a new user	a message is displayed prompting for a password change. Enter a new password and click **OK**. **Result:** A Legal Notice Screen appears.
this is not the first login for a new user	a Legal Notice Screen appears.

7 Click **OK**.

IF the privilege level for the user login is...	THEN...
M0 or P0	a message is displayed stating that certain screens will be inaccessible due to the privilege level. Click **OK**. **Result:** The System View Screen for the selected network element appears.
anything other than M0 or P0	the WaveStar CIT System View Screen for the selected network element appears.

END OF STEPS

Task 205: Setting the Network Element Name

Purpose

This procedure is used to set the network element name, or Target Identifier (TID).

> **Important!** Because database backups are keyed to the network element TID, changing the network element TID will make all previous database backups invalid.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S3, P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 202: Viewing the WaveStar CIT Network Element IP Address List" (8-8)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 206: Setting Network Element IP Addresses" (8-19)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)

Task

Complete the following steps to provision the TID on the network element.

1 Ensure that the network element is in Maintenance Mode.

> **Reference:** "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

2 At the WaveStar CIT, from the System View Main Menu bar, select **Administration**>**Set TID**.

Result: The Provision TID/NE Name Screen appears.

3 Enter the TID for the network element in both the New TID/NE Name field and the Confirm TID/NE Name field.

4 Click **Apply**.

Result: A Confirmation Screen appears.

5 Click **OK**.

Result: A Disconnect Warning Message appears.

6 Click **OK**.

Result: The WaveStar CIT login session is terminated and a Communication Failure Message appears.

7 Click **OK**.

Result: The WaveStar CIT System View closes and the Network View appears.

8 Log back into the network element.

Reference: "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

9 Set the system date and time.

Reference: "Task 303: Setting the System Date and Time" (9-19).

10 Perform a database backup.

Reference: “Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory” (12-9).

“Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT” (12-14).

ND OF STEPS

□

Task 206: Setting Network Element IP Addresses

Purpose

This procedure is used to set network element IP addresses.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 202: Viewing the WaveStar CIT Network Element IP Address List" (8-8)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 205: Setting the Network Element Name" (8-16)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)

Task

Complete the following steps to provision the network element IP addresses.

1 Ensure that the network element is in Maintenance Mode.

Reference: "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

2 At the WaveStar CIT, from the System View Main Menu bar, select **Administration**>**NE IP Address**.

Result: The Equipment Selection Screen appears.

3 From the Equipment Selection Screen, enter an AID for the desired DCC circuit pack, or use the NE Explorer to select the equipment by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The NE IP Address Screen appears.

5 Enter the IP Address, Subnet Mask, and Default Router Address (in dotted decimal notation) for the DCC circuit pack.

6 Click **Apply**.

Result: A Disconnect Warning Message appears.

7 Click **Yes**.

Result: The WaveStar CIT login session is terminated and a Communication Failure Message appears.

8 Click **OK**.

Result: The WaveStar CIT System View closes and the Network View appears.

9 If necessary, log back into the network element and repeat this procedure for the second DCC circuit pack.

Reference: “Task 204: Logging into a Network Element from the WaveStar CIT” (8-13).

10 Provision the WaveStar CIT with the new network element IP addresses.

Reference: "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10).

N D O F S T E P S

□

Task 207: Logging Out and Disconnecting from a Network Element

Purpose

This procedure is used to log out and disconnect the WaveStar CIT from a network element.

Before you begin

Before beginning this task, be currently connected to a network element from a WaveStar CIT.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)
- "Task 209: Logging Out of a Cut-Through Session" (8-31)

Task

Complete the following steps to log out and disconnect from a network element.

1

IF...	THEN...
one or more network elements are still connected and all tasks are not complete	continue to the next task. *Stop! End of Task.*
only one network element is still connected and all tasks are complete	log out and disconnect from the network element. **Reference:** "SE 207-1: Disconnecting from one network element" (8-23).
several network elements are connected and all tasks are completed on all of them	log out from all currently connected network elements. **Reference:** "SE 207-2: Disconnecting from all network elements" (8-24).
all network elements are disconnected and all tasks are complete	log out of the WaveStar CIT. **Reference:** "SE 207-3: Logging out from the WaveStar CIT" (8-25).

2 Disconnect the WaveStar CIT from the network element.

Reference: "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3).

ND OF STEPS

SE 207-1: Disconnecting from one network element

Complete the following steps to log out and disconnect from one network element.

1

IF...	THEN...
the WaveStar CIT Network View is displayed	from the Main Menu bar, select **Network Element>Disconnect from NE**. **Result:** The NE Disconnect List appears.
the WaveStar CIT System View is displayed	from the Main Menu bar, select **File>NE Disconnect**. **Result:** A Confirmation Screen appears. Continue to Step 3.

2 Select the network element to be disconnected then click **Disconnect**.

Result: A Confirmation Screen appears.

3 Click **Yes**.

Result: The WaveStar CIT is disconnected from the selected network element and the WaveStar CIT Network View appears.

ND OF STEPS

SE 207-2: Disconnecting from all network elements

Complete the following steps to log out and disconnect from all network elements.

1 At the WaveStar CIT, from the Network View Main Menu bar, select **Network Element>Disconnect from All NEs**.

Result: A Confirmation Screen displaying a list of all currently connected network elements appears.

2 Click **Yes**.

Result: The WaveStar CIT is disconnected from all network elements and the WaveStar CIT Network View appears.

N D O F S T E P S

SE 207-3: Logging out from the WaveStar CIT

Complete the following steps to log out from the WaveStar CIT.

1 At the WaveStar CIT, from the Network View Main Menu bar, select **File>Exit**.

Result: A Confirmation Screen appears.

2 Click **Yes**.

Result: The WaveStar CIT application closes and the Windows desktop appears.

END OF STEPS

□

Task 208: Logging in to a Network Element by Cut-Through

Purpose

This procedure is used to log in to a network element by cut-through.

Before you begin

Before beginning this task:

- Have a valid user ID and password on both the WaveStar CIT and the network element.
- Ensure that the WaveStar CIT has been provisioned with the network element Target Identifier (TID) and IP address.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 207: Logging Out and Disconnecting from a Network Element" (8-22)
- "Task 209: Logging Out of a Cut-Through Session" (8-31)

Task

Complete the following steps to log in to the network element by cut-through.

1 Log in to the WaveStar CIT.

Result: The Network View Screen appears.

Reference: "Task 201: Logging in to the WaveStar CIT" (8-6).

2

IF...	THEN...
an icon exists in the Network View for the desired network element	right-click on the network element icon and select **Cut Through** from the pop up menu.
an icon does not exist in the Network View for the desired network element	enter the network element TID in the Network View TID field, select the **Cut-Through** button, then click **Connect**.

3

IF the network element...	THEN...
has been provisioned with two IP addresses	the IP Address Selection Screen appears. Continue to the next step.
has been provisioned with one IP address	continue to Step 5.

4 Select the IP address to use for the connection and click **OK**.

5

IF...	THEN...
the No Listbox File Exist error message appears	click **OK** to clear the message. The error message is just a warning. Cut-Through can work without the Listbox File. Continue to Step 8.
the Cut-Through window appears	the connection is established. Continue to Step 8.
no Cut-Through window appears, the icon in the Established NE Associations Panel disappears, and the TID field gets cleared	the session is not established. The TID and IP address may be incorrect or there may be a problem communicating with the network element. Verify that the TID and IP address are correct. Make corrections as necessary. Go to "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10). Return to Step 2 only once. If the connection fails a second time, continue to Step 6.

6 Click the Microsoft Windows **Start** button, then select **Programs> Command Prompt**.

Result: The Command Prompt Window appears.

7 In the command prompt window, enter `ping <IP address>` to determine if there are communications with the network element. Replace *<IP address>* with the IP address of the network element to which a connection is being attempted.

IF the ping command…	THEN...
indicates there are no communications (a Request Timed Out error is displayed)	contact the local network administrator to clear the problem. When the problem is cleared, return to Step 2.
indicates there are communications (ping reply times are displayed)	the problem may be in the WaveStar CIT. Call Lucent Technical Support. *Stop! End of Task*

8 Enter `ACT-USER:<tid>:<loginid>:<ctag>::<password>;` in the TL1 Command Entry Field, or select the ACT-USER command from the Cut-Through Window List Box and edit the command line to include the network element TID and a valid User ID and Password, and click **Send**.

IF the ACT-USER command...	THEN...
is successful	continue to the next step.
is not successful	the problem may be in the network element. Call Lucent Technical Support. *Stop! End of Task*

9

IF...	THEN...
this is the first login for a new user	a message is displayed prompting for a password change. Enter a new password and click **OK**. **Result:** The login session is established.
this is not the first login for a new user	The login session is established.

ND OF STEPS

□

Task 209: Logging Out of a Cut-Through Session

Purpose

This procedure is used to log out of a cut-through session.

Before you begin

Before beginning this task:

- Have a valid user ID and password on both the WaveStar CIT and the network element.
- Ensure that a cut-through session is in effect.

Related information

For related information, see the following sections in this document:

- Chapter 2, "Security Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 203: Provisioning the WaveStar CIT with Network Element TIDs and IP Addresses" (8-10)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 207: Logging Out and Disconnecting from a Network Element" (8-22)
- "Task 208: Logging in to a Network Element by Cut-Through" (8-26)

Task

Complete the following steps to log out of a cut-through session.

1 Enter `CANC-USER:<tid>::logoff;` in the TL1 Command Entry Field, or select the CANC-USER command from the Cut-Through Window List Box and edit the command line to include the network element TID as appropriate, and click **Send**.

Result: The login session is terminated.

2 At the WaveStar CIT Cut-Through Main Menu, select **File>Exit**.

Result: A Confirmation Screen appears.

3 Click **Yes**.

Result: The Cut-Through Screen closes and the Network View appears.

ND OF STEPS

□

Task 210: Connecting or Disconnecting a Terminal to or from a Network Element RS-232 Port

Purpose

This procedure is used to physically connect a terminal to, or disconnect a terminal from, a local network element RS-232 port.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain an RS-232 Adapter Cable assembly (COMCODE 848822995).
- Obtain either an RS-232 "null modem" serial cable (for direct connection) or two standard RS-232 serial cables and two modems (for connection via modem).

Related information

For related information, see the following sections in this document:

- Appendix B, Operations Interfaces
- “Task 211: Logging in to an RS-232 Terminal Session” (8-37)
- “Task 212: Logging out of an RS-232 Terminal Session” (8-40)

Task

Complete the following steps to connect a terminal to, or disconnect a terminal from, a local network element RS-232 port.

1

IF...	THEN...
connecting a terminal directly to a network element	go to “SE 210-1: Connecting a terminal directly to a network element” (8-34).
connecting a terminal to a network element via modem	go to “SE 210-2: Connecting a terminal to a network element via modem” (8-35).
disconnecting a terminal from a network element	go to “SE 210-3: Disconnecting a terminal from a network element” (8-36).

END OF STEPS

SE 210-1: Connecting a terminal directly to a network element

Complete the following steps to connect a terminal directly to a network element RS-232 port.

1 Plug the 25-pin end of the RS-232 adapter cable into the J189 DEBUG PORT connector on the network element System Controller Shelf backplane.

2 Plug one end of the RS-232 “null modem” serial cable into the terminal serial port and the other end into one of the 9-pin connectors on the RS-232 adapter cable.

3 Log into the network element from the terminal.

Reference: “Task 211: Logging in to an RS-232 Terminal Session” (8-37).

ND OF STEPS

SE 210-2: Connecting a terminal to a network element via modem

Complete the following steps to connect a terminal to a network element RS-232 port via modem.

1 Plug the 25-pin end of the RS-232 adapter cable into the J189 DEBUG PORT connector on the network element System Controller Shelf backplane.

2 Plug one end of a standard RS-232 serial cable into the terminal serial port and the other end into a modem.

3 Plug one end of one standard RS-232 serial cable into one of the 9-pin connectors on the RS-232 adapter cable on the network element and the other end into a modem.

4 Connect each modem to a telephone jack and power-on the modems.

It is recommended that the modems be configured as follows:

- autoanswer enabled
- flow control off (or disabled)
- only connect at the baud rate for which the network element is provisioned

Reference: See the modem and Microsoft Windows documentation for information on how to configure the modems.

5 Log into the network element from the terminal.

Reference: “Task 211: Logging in to an RS-232 Terminal Session” (8-37).

ND OF STEPS

SE 210-3: Disconnecting a terminal from a network element

Complete the following steps to disconnect a terminal from a network element RS-232 port.

1

IF...	THEN...
currently logged into an RS-232 terminal session	log out of the RS-232 terminal session. **Reference:** "Task 212: Logging out of an RS-232 Terminal Session" (8-40).
not currently logged into an RS-232 terminal session	continue to the next step.

2

IF the terminal is...	THEN...
connected directly to the network element	power-off the terminal and disconnect the RS-232 serial cable from the serial port on the terminal and from the RS-232 adapter cable connected to the network element System Controller Shelf backplane.
connected to the network element via modem	power-off the terminal and the modems. Disconnect the modems from the telephone jacks and disconnect the RS-232 cables from the modems and the terminal and the RS-232 adapter cable.

N D O F S T E P S

□

Task 211: Logging in to an RS-232 Terminal Session

Purpose

This procedure is used to log in to an RS-232 terminal session.

Before you begin

Before beginning this task:

- Have a valid user ID and password on the network element.

Related information

For related information, see the following sections in this document:

- Appendix B, Operations Interfaces
- "Task 210: Connecting or Disconnecting a Terminal to or from a Network Element RS-232 Port" (8-33)
- "Task 212: Logging out of an RS-232 Terminal Session" (8-40)

Task

Complete the following steps to log in to an RS-232 terminal session.

1 Connect the terminal to the network element RS-232 port.

Reference: "Task 210: Connecting or Disconnecting a Terminal to or from a Network Element RS-232 Port" (8-33).

2 Power-on the terminal.

IF...	THEN...
this is the first connection of a terminal to the network element	configure the terminal serial port to 19200 bits per second, 8 data bits, no parity, and 1 stop bit. **Reference:** See the terminal documentation for information on how to configure the terminal serial port.
this is not the first connection of a terminal to the network element	continue to the next step.

3 Press `Enter` on the keyboard.

Result: The RS-232 menu appears.

4

IF...	THEN...
logging in and entering TL1 commands	continue to the next step.
changing the RS-232 port baud rate	go to “SE 211-1: Changing the RS-232 port baud rate” (8-39).

5 Enter `1` at the RS-232 menu prompt.

Result: The TL1 Command menu appears.

6 Enter `T` at the TL1 Command menu prompt.

Result: Instructions for how to log in are displayed.

7 Enter `ACT-USER:<tid>:<loginid>:<ctag>::<password>;` at the TL1 Command prompt.

Result: A message is displayed indicating the login is successful.

8 Enter additional TL1 commands as required.

END OF STEPS

SE 211-1: Changing the RS-232 port baud rate

Complete the following steps to change the baud rate of the RS-232 port.

1 Enter `2` at the RS-232 menu prompt.

Result: The Baud Rate menu appears.

2 Select the desired baud rate from the menu.

Result: A string of random characters appears on the screen.

3 Set the terminal baud rate to match the baud rate selected for the RS-232 port.

Reference: See the terminal documentation for information on how to configure the terminal serial port.

4 Press `Enter` on the keyboard.

Result: The Baud Rate menu appears.

5 Enter `Q` at the Baud Rate menu.

Result: The RS-232 Menu appears.

N D O F S T E P S

□

Task 212: Logging out of an RS-232 Terminal Session

Purpose

This procedure is used to log out of an RS-232 terminal session.

Before you begin

Before beginning this task, an RS-232 terminal session must already be established.

Related information

For related information, see the following sections in this document:

- Appendix B, Operations Interfaces
- "Task 210: Connecting or Disconnecting a Terminal to or from a Network Element RS-232 Port" (8-33)
- "Task 211: Logging in to an RS-232 Terminal Session" (8-37)

Task

Complete the following steps to log out of an RS-232 terminal session.

1 Enter `CANC-USER:<tid>::logoff;` at the TL1 Command prompt.

Result: A message is displayed indicating the logout is successful.

2 Enter `Q` two times to return to the RS-232 menu.

Result: The RS-232 Menu appears.

3 Power-off the terminal and optionally disconnect the terminal from the network element.

Reference: "Task 210: Connecting or Disconnecting a Terminal to or from a Network Element RS-232 Port" (8-33).

END OF STEPS

□

9 Equipment Configuration Management Tasks

Overview

Purpose This chapter provides detailed procedures for performing equipment configuration tasks on the WaveStar LambdaRouter 128/256.

Contents

Task 300: Viewing the WaveStar LambdaRouter 128/256 Configuration Information

Purpose

This procedure is used to view the WaveStar LambdaRouter 128/256 configuration information. The information includes

- equipment details (such as: TID, system configuration, date and time, optics interface defaults, and state and alarm information)
- controller complex information (circuit pack members, alarm level, and state information)
- network configuration parameters (such as: IP address, Subnet Mask, and Default Router information)
- SWIP details (state and port association)
- SWIP Block and SWIP status

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S1 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, “Equipment Configuration Management”
- “Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element” (8-3)
- “Task 201: Logging in to the WaveStar CIT” (8-6)
- “Task 204: Logging into a Network Element from the WaveStar CIT” (8-13)
- “Task 205: Setting the Network Element Name” (8-16)
- “Task 206: Setting Network Element IP Addresses” (8-19)
- “Task 303: Setting the System Date and Time” (9-19)

Task Complete the following steps to view the WaveStar LambdaRouter 128/256 configuration information.

1

IF retrieving the...	THEN...
equipment details	go to “SE 300-1: Viewing equipment details” (9-4).
controller complex information	go to “SE 300-2: Viewing controller complex information” (9-6).
network configuration parameters	go to “SE 300-3: Viewing network configuration parameters” (9-7).
SWIP details	go to “SE 300-4: Viewing SWIP details” (9-8).
SWIP Block and SWIP status	go to “SE 300-5: Viewing the status of SWIP Blocks and SWIPs” (9-9).

N D O F S T E P S

SE 300-1: Viewing equipment details Complete the following steps to view equipment details for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu Bar, select **View>View Equipment Details**.

Result: The Equipment Selection Screen appears.

2 From the Equipment Selection Screen, enter an AID for the desired system, shelf, circuit pack, OCH port, or SWIP block, or use the NE Explorer to select the equipment by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: The View Details Screen for the selected equipment appears.

4 View the displayed equipment details.

IF...	THEN...
the View OCH Port Details Screen is displayed for ports on an OXI or OXI-2GC circuit pack	click **Previous Port** or **Next Port** to view the previous or next port on the same port unit as desired. **Result:** The equipment details for the previous or next OCH port are displayed as appropriate.
any View Details Screen other than the View OCH Port Details Screen is displayed OR the View OCH Port Details Screen is displayed for a port on an OXI-10GC circuit pack	continue to the next step.

5 Click **Close**.

Result: The View Details Screen closes.

END OF STEPS

SE 300-2: Viewing controller complex information

Complete the following steps to view controller complex information for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu Bar, select **View>Controller Complex**.

Result: The View Controller Complex Details Screen appears.

2 View the displayed controller complex details. Click **View scc-1-x** to view the details for the other controller complex if desired.

3 Click **Close**.

Result: The View Controller Complex Details Screen closes.

END OF STEPS

SE 300-3: Viewing network configuration parameters

Complete the following steps to view the network configuration parameters for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu Bar, select **Administration>View NE Administration**.

Result: The Equipment Selection Screen appears.

2 From the Equipment Selection Screen, enter an AID for the desired DCC circuit pack, or use the NE Explorer to select the DCC circuit pack by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: The View Details Screen for the selected DCC circuit pack appears.

4 View the displayed network configuration parameters.

5 Click **Close**.

Result: The View Details Screen closes.

END OF STEPS

SE 300-4: Viewing SWIP details

Complete the following steps to view SWIP details for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View, right-click on the relevant Switch Shelf.

Result: The Switch Shelf right-click pop-up menu appears.

2

IF retrieving a list of...	THEN...
available SWIPs	select **List Shelf Available SWIPs** from the pop-up menu. **Result:** A Confirmation Screen appears.
suspect SWIPs	select **List Shelf Suspect SWIPs** from the pop-up menu. **Result:** A Confirmation Screen appears.
faulty SWIPs	select **List Shelf Faulty SWIPs** from the pop-up menu. **Result:** A Confirmation Screen appears.

3 Click **Yes**.

Result: The SWIP Detail List Screen for the Switch Shelf appears with the selected information (available, suspect, or faulty SWIPs).

4 View the displayed SWIP information.

5 Click **Close**.

Result: The SWIP Detail List Screen closes.

END OF STEPS

SE 300-5: Viewing the status of SWIP Blocks and SWIPs

Complete the following steps to view SWIP Block and SWIP status information for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View, double-click on the relevant Switch Shelf.

Result: The Switch Shelf View appears. Each SWIP Block in the selected Switch Shelf is displayed in a color that indicates the status of the SWIP Block.

2 View the SWIP Block status.

IF the SWIP Block color is...	THEN...
white	the SWIP Block status is Unassigned.
light grey	the SWIP Block status is Reserved.
dark grey	the SWIP Block status is Assigned.

3 At the WaveStar CIT, from the Switch Shelf View, right-click on the relevant SWIP Block and select **Block Refresh** from the pop-up menu.

Result: The selected SWIP Block is updated to show the current status.

4 At the WaveStar CIT, from the Switch Shelf View, double-click on the SWIP Block that was refreshed in the previous step.

Result: The SWIP Block Display Screen appears with the individual SWIPs that make up the selected SWIP Block. Each SWIP in the selected SWIP Block is displayed in a color that indicates the status of the SWIP.

5 View the status of the SWIPs.

IF the SWIP color is...	THEN...
green	the SWIP status is In-Service (PST: IS-NR).
grey	the SWIP status is Available (PST: OOS-MA, SST: UEQ or UEQ&BUSY).
white	the SWIP status is Suspect (PST: OOS-MA, SST: MT or MT&BUSY).
a black cross	the SWIP status is Defective (PST: OOS-MA, SST: UAS, UAS&MEA, FLT, or FLT&MEA).

6 Click **Close**.

Result: The SWIP Block Display Screen closes.

7

IF the status of additional SWIPs...	THEN...
will be retrieved	go to Step 3.
will not be retrieved	at the WaveStar CIT, from the Shelf View menu, select **View>System View Display**. **Result:** The network element System View appears.

N D O F S T E P S

□

Task 301: Resetting a System, Shelf, or DCC Circuit Pack

Purpose

This procedure is used to reset a WaveStar LambdaRouter 128/256 system, optical interface shelf or High-Voltage Shelf, or DCC circuit pack.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of M4 and S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 303: Setting the System Date and Time" (9-19)

Task Complete the following steps to reset a WaveStar LambdaRouter 128/256 system, optical interface shelf or High-Voltage Shelf, or DCC circuit pack.

1

IF resetting a...	THEN...
DCC circuit pack	at the WaveStar CIT, from the System View Main Menu Bar, select **Fault>Reset>Circuit Pack**. **Result:** The Reset Circuit Pack Screen appears. Continue to the next step.
optical interface shelf or High-Voltage Shelf	at the WaveStar CIT, from the System View Main Menu Bar, select **Fault>Reset>Shelf**. **Result:** The Reset Shelf Screen appears. Continue to the next step.
system	at the WaveStar CIT, from the System View Main Menu Bar, select **Fault>Reset>System**. **Result:** A Service Affecting Warning appears. Continue to Step 4.

2 From the Equipment Selection Screen, enter an AID for the desired DCC circuit pack, optical interface shelf, or High-Voltage Shelf, or use the NE Explorer to select the equipment by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: A Service Affecting Warning appears.

4 Click **Yes**.

IF resetting a...	THEN...
system or the DCC circuit pack carrying the active login session	the reset terminates the WaveStar CIT login session and a Communication Failure Message appears. Continue to the next step.
shelf or the DCC circuit pack that is not carrying the active login session	this procedure is complete. *Stop! End of Task.*

5 Click **OK**.

Result: The WaveStar CIT System View closes and the Network View appears.

6 Log back into the network element when the reset has completed.

Reference: "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

7

IF resetting a...	THEN...
DCC circuit pack	this procedure is complete.
system	set the system date and time. **Reference:** "Task 303: Setting the System Date and Time" (9-19).

N D O F S T E P S

Task 302: Removing Equipment from and Returning Equipment to Service

Purpose

This procedure is used to change the primary state of the following WaveStar LambdaRouter 128/256 equipment:

- system
- port units (OXI, OXI-10GC, and OXI-2GC)
- port
- SWIP maintenance group (SWMG)

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of M4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)

Task

Complete the following steps to change the primary state of the WaveStar LambdaRouter 128/256 equipment.

1

IF changing the primary state of...	THEN...
the system	go to "SE 302-1: Changing the primary state of the system" (9-15).
a port unit, port, or SWMG	go to "SE 302-2: Changing the primary state of a port unit, port, or SWMG" (9-17).

ND OF STEPS

SE 302-1: Changing the primary state of the system

Complete the following steps to change the primary state of the system.

1 At the WaveStar CIT, from the System View Main Menu Bar, select **Fault>Return to/Remove from Service**.

Result: The Remove from/Return to Service Screen appears.

2 From the Equipment Selection tree on the left side of the screen, select the System, or enter the AID for the System, and click **Select Target**.

Result: The current primary state for the System appears.

3

IF...	THEN...
removing the System from service	select **Remove From Service** from the Action drop-down list and click **Apply**. **Result:** A Service Affecting Warning appears.
returning the System to service	select **Return To Service** from the Action drop-down list and click **Apply**. **Result:** A Service Affecting Warning appears.

4 Click **Yes**.

Result: The Service Affecting Warning closes.

5

IF the System was...	THEN...
removed from service	continue to the next step.
returned to service	the system restarts and a Communication Failure Message appears. Click **OK** and when the system restart has completed, log into the network element and reset the system date and time. *Stop! End of Task.* **Reference:** "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13), and "Task 303: Setting the System Date and Time" (9-19).

6 Click **Close**.

Result: The Remove from/Return to Service Screen closes.

END OF STEPS

SE 302-2: Changing the primary state of a port unit, port, or SWMG

Complete the following steps to change the primary state of a port unit, port, or SWMG.

1 At the WaveStar CIT, from the System View Main Menu Bar, select **Configuration>Provision**.

Result: The Provision Parameters for Equipment Screen appears.

2 From the Equipment Selection tree on the left side of the screen, enter the AID for the port unit, port, or SWMG, or use the NE Explorer to select the equipment by clicking on the plus (+) sign next to each entity.

3 Click **Provision**.

Result: The parameters for the selected equipment are displayed.

4

IF...	THEN...
removing the port unit, port, or SWMG from service	select **OOS** from the Primary State drop-down list and click **Apply**. **Result:** A Service Affecting Warning appears.
returning the port unit, port, or SWMG to service	select **IS** from the Primary State drop-down list and click **Apply**. **Result:** A Service Affecting Warning appears.

5 Click **Yes**.

Result: The Service Affecting Warning closes.

6

IF the primary state of additional equipment...	THEN...
will be changed	go to Step 2.
will not be changed	click **Close**. **Result:** The Provision Parameters for Equipment Screen closes.

N D O F S T E P S

□

Task 303: Setting the System Date and Time

Purpose

This procedure is used to set the system date and time on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3, M3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 301: Resetting a System, Shelf, or DCC Circuit Pack" (9-11)
- "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14)

Task

Complete the following steps to set the system date and time on the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Administration>NE System Provisioning**.

Result: The Provision NE System Screen appears.

2 Click the **System Time** tab and set the system year, month, day, and time.

3 Click **Apply**.

Result: A Service Affecting Warning appears.

4 Click **Yes**.

Result: The Provision NE System Screen closes.

END OF STEPS

□

Task 304: Provisioning Default Interface Format and Optics Parameters

Purpose

This procedure is used to provision default interface format and optics parameters on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3, M3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 305: Provisioning an Existing Slot" (9-23)
- "Task 306: Provisioning Optical Channel (OCH) Ports" (9-25)

Task

Complete the following steps to provision default interface format and optics parameters on the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Administration>NE System Provisioning**.

Result: The Provision NE System Screen appears.

2 Click the **System Parameters** tab and set the following parameters as required:

- Interface Standard
- Port Usage
- Interface Format
- Interface Optics
- System Primary State (requires a system reset)

3 Click **Apply**.

Result: A Service Affecting Warning appears.

4 Click **Yes**.

IF...	THEN...
setting the system primary state	the system restarts and a Communication Failure Message appears. Click **OK** and when the system restart has completed, log into the network element and reset the system date and time. **Reference:** "Task 303: Setting the System Date and Time" (9-19).
setting default interface parameters but not the system primary state	The default interface parameters are saved and the Provision NE System Screen closes.

END OF STEPS

Task 305: Provisioning an Existing Slot

Purpose

This procedure is used to provision the primary state for existing shelf slots.

> **Important!** Each slot is dedicated to a single circuit pack type. Therefore, slots and circuit packs are considered the same object and share the same AID. Only OXI, OXI-10GC, and OXI-2GC slots may be provisioned.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 304: Provisioning Default Interface Format and Optics Parameters" (9-21)
- "Task 306: Provisioning Optical Channel (OCH) Ports" (9-25)

Task

Complete the following steps to provision an existing slot.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration**>**Provision**.

Result: The Provision Parameters for Equipment Screen appears.

2 Enter an AID for the desired OXI, OXI-10GC, or OXI-2GC slot or use the NE Explorer to select the slot by clicking on the plus (+) sign next to each entity, then click **Provision**.

Result: The Provisioning Screen for the selected slot appears. The existing provisioning parameters are displayed.

3 Set the Primary State to one of the following options as appropriate then click **Apply**.

- **IS** (In-Service)
- **OOS** (Out-of-Service)

Result: A Service Affecting Warning appears.

4 Click **Yes**.

Result: The Service Affecting Warning closes and the selected slot is provisioned with the entered parameters.

5

IF...	THEN...
additional slots are being provisioned	repeat this task.
no other slots are being provisioned	click **Close** to exit the Provisioning Screen.

ND OF STEPS

□

Task 306: Provisioning Optical Channel (OCH) Ports

Purpose

This procedure is used to provision existing optical channel (OCH) ports.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 303: Setting the System Date and Time" (9-19)
- "Task 305: Provisioning an Existing Slot" (9-23)

Task

Complete the following steps to provision optical channel (OCH) ports.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration**>**Provision**.

Result: The Provision Parameters for Equipment Screen appears.

2 On the left side of the screen, enter an AID for the port, or use the NE Explorer to select the port by clicking on the plus (+) sign next to each entity, then click **Provision**.

Result: The parameters for the selected OCH port appear on the right side of the Provision Parameters for Equipment Screen.

3

IF provisioning an...	THEN...
input port	click the **Input** tab.
output port	click the **Output** tab.

4 Configure all port parameters as required, then click **Apply**.

Result: A Service Affecting Warning appears.

5 Click **Yes**.

Result: The Service Affecting Warning closes.

6

IF...	THEN...
additional ports are being or provisioned	repeat this task.
no other ports are being provisioned	click **Close** to exit the Provisioning Screen.

END OF STEPS

□

Task 307: Extracting and Inserting an NVM Card

Purpose

This procedure is used to extract and insert an NVM card.

Before you begin

Before beginning this task:

- Turn off the audible alarm, if necessary.
- Read and follow all safety precautions in this manual.
- Use an electrostatic discharge (ESD) strap.
- Connect the WaveStar CIT to the local network element and log in with a Privilege Code of P3 and M3 or higher.

Safety precautions

Read and understand the following safety precautions before beginning this task.

CAUTION

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar LambdaRouter 128/256 system to prevent electrostatic discharge damage to sensitive components.

CAUTION

Never try to eject the NVM card when the MEM pack LED is green.

Related information

For related information, see the following sections in this document:

- Chapter 6, "Software Management"
- "Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory" (12-9)
- "Task 602: Manually Restoring Data from Secondary Memory to Primary Memory" (12-11)

Task Complete the following steps to extract and insert an NVM card.

1 Remove the System Controller Shelf cover.

Reference: "Task 308: Removing or Replacing a Shelf Cover" (9-30).

2

IF...	THEN...
extracting an NVM card	continue to Step 3.
inserting an NVM card	continue to Step 6.

3

IF extracting a...	THEN...
PRI MEM NVM card	continue to Step 4.
SEC MEM NVM card	momentarily press the push button located on top of the SEC MEM pack. **Result:** The NVM card ejects from the SEC MEM pack. Continue to Step 7.

4 Remove the system from service.

Reference: "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

5 When the PRI MEM pack LED turns from green to red, momentarily press the push button located on top of the PRI MEM pack.

Result: The NVM card ejects from the PRI MEM pack.

6 Gently slide the NVM card into the appropriate MEM circuit pack.

IF inserting a...	THEN...
PRI MEM NVM card	return the system to an in-service (IS) state. **Reference:** "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).
SEC MEM NVM card	continue to the next step.

7 Replace the System Controller Shelf cover.

Reference: "Task 308: Removing or Replacing a Shelf Cover" (9-30).

END OF STEPS

□

Task 308: Removing or Replacing a Shelf Cover

Purpose

This procedure is used to remove or replace a shelf cover.

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain a screwdriver and electrostatic discharge (ESD) strap.

CAUTION

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar LambdaRouter 128/256 to prevent electrostatic discharge damage to sensitive components.

Related information

For related information, see the following sections in this document:

- "Task 307: Extracting and Inserting an NVM Card" (9-27)

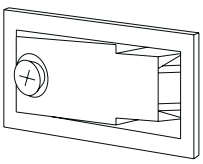
Task

Complete the following steps to remove or replace the shelf cover.

1

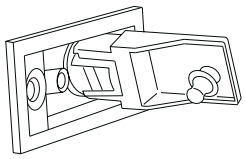
IF the cover is being...	THEN...
removed	continue to Step 2.
replaced	continue to Step 7.

2 Locate the two ¼-turn fasteners at the bottom of the shelf cover.



3 Use the appropriate size screwdriver to rotate the retaining screws counterclockwise approximately ¼-turn until the shelf cover fasteners are released.

4 Pull the shelf cover fasteners out and rotate the fasteners ¼-turn counterclockwise.



5 Grasp the bottom of the cover and pull it forward until it is horizontal (rotated 90 degrees from the closed position).

6 Lift the pivot pins located at the top of the cover, push back, and lift up on the pins again to remove the cover from the shelf, then lift the cover up until it is free from the shelf framing.

Stop! End of Task.

7 Position the pivot pins located at the top of the cover under the flange on the shelf framing.

8 Close the cover and rotate the two shelf cover fasteners ¼-turn clockwise and push back into the locked position.

9 Use the appropriate size screwdriver to rotate the retaining screws clockwise approximately ¼-turn until the shelf cover fasteners are secured.

END OF STEPS

Task 309: Adding a Port Unit Circuit Pack

Purpose

This procedure is used to add a port unit circuit pack to an existing optical interface shelf in order to add cross-connection capacity.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Use an electrostatic discharge (ESD) strap.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Safety precautions

Read and understand the following safety precautions before beginning this task.

CAUTION

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar LambdaRouter 128/256 system to prevent electrostatic discharge damage to sensitive components.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* "Task 411: Removing, Inserting, and Replacing a Circuit Pack", and the following sections in this document:

- Chapter 3, "Equipment Configuration Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 201: Logging in to the WaveStar CIT" (8-6)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 304: Provisioning Default Interface Format and Optics Parameters" (9-21)
- "Task 305: Provisioning an Existing Slot" (9-23)
- "Task 306: Provisioning Optical Channel (OCH) Ports" (9-25)

Task Complete the following steps to add a port unit circuit pack to an existing optical interface shelf in order to add cross-connection capacity.

1 At the WaveStar CIT, from the System View display, double-click on the optical interface shelf to which the port unit circuit pack will be added.

IF adding an...	THEN double-click on an...
OXI circuit pack	OIS-T shelf
OXI-10GC circuit pack	OIS-10G or OIS-MX shelf
OXI-2GC circuit pack	OIS-2G or OIS-MX shelf

Result: The Shelf View for the selected shelf appears.

2 Note all empty slots (no port unit label for the slot) in the Shelf View.

IF...	THEN...
at least one empty slot exists	continue to the next step.
no empty slots exist	continue to Step 7.

3 Right-click on the Shelf View and select **View Details** from the pop-up menu that appears.

Result: The View Shelf Details Screen appears.

4 Refer to the following table to determine which SWIP Block assignment parameters apply to the empty slot. For example, if slot 6 on an OIS-T shelf is empty, **SIDE0BLK2** and **SIDE1BLK2** apply.

OIS-T Shelf	**SWIP Block Assignment Parameters**
Slots 1 through 4	SIDE0BLK1, SIDE1BLK1
Slots 5 through 8	SIDE0BLK2, SIDE1BLK2
Slots 9 through 12	SIDE0BLK3, SIDE1BLK3
Slots 13 through 16	SIDE0BLK4, SIDE1BLK4
Slots 17 through 20	SIDE0BLK5, SIDE1BLK5
Slots 21 through 24	SIDE0BLK6, SIDE1BLK6
Slots 25 through 28	SIDE0BLK7, SIDE1BLK7
Slots 29 through 32	SIDE0BLK8, SIDE1BLK8
OIS-10G Shelf	**SWIP Block Assignment Parameters**
Slots 1 through 16	SIDE0BLK1, SIDE1BLK1
Slots 17 through 32	SIDE0BLK2, SIDE1BLK2
OIS-2G Shelf	**SWIP Block Assignment Parameters**
Slots 1 through 8	SIDE0BLK1, SIDE1BLK1
Slots 9 through 16	SIDE0BLK2, SIDE1BLK2
Slots 17 through 24	SIDE0BLK3, SIDE1BLK3
Slots 25 through 32	SIDE0BLK4, SIDE1BLK4
OIS-MX Shelf	**SWIP Block Assignment Parameters**
Slots 1 through 8 (for OXI-2GC packs only)	SIDE0BLK1, SIDE1BLK1
Slots 9 through 16 (for OXI-2GC packs only)	SIDE0BLK2, SIDE1BLK2
Slots 17 through 24 (for OXI-10GC packs only)	SIDE0BLK3, SIDE1BLK3

5 In the View Shelf Details Screen, verify that the SWIP Block Assignments for the empty slots show a valid SWIP Block and assignments (the SWIP Blocks are not unassigned [UAS]). For example, **SIDE0BLK2** is associated with SWIP Block **B2** and **SIDE0BLK2** is associated with SWIP Block **A8**.

6

IF...	THEN...
all SWIP Block assignments for the empty slots are unassigned (**UAS**)	click **Close** in the View Shelf Details Screen and continue to the next step.
at least one SWIP Block assignment for an empty slot is assigned	click **Close** in the View Shelf Details Screen and continue to Step 9.

7

IF...	THEN...
this is the last shelf	either additional fiber or additional shelves must be installed before port units can be added to the system. Contact Lucent Support. *Stop! End of Task.*
this is not the last shelf	at the WaveStar CIT, from the Shelf View Main menu, select **View>System View Display**. **Result:** The WaveStar CIT System View appears.

8 Go to Step 1 and repeat this task for the next applicable shelf.

9 Insert the port unit into the empty slot that was verified as having a valid SWIP Block assignment.

Reference: *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* "Task 411: Removing, Inserting, and Replacing a Circuit Pack".

10 Provision the port unit slot and ports as required.

Reference: “Task 305: Provisioning an Existing Slot” (9-23).

Reference: “Task 306: Provisioning Optical Channel (OCH) Ports” (9-25).

ND OF STEPS

□

10 Alarm Monitoring and Fault Management Tasks

Overview

Purpose

This chapter provides detailed procedures for configuring alarm monitoring and fault management features on the WaveStar LambdaRouter 128/256.

For additional information on alarm monitoring and fault management, refer to the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002*.

Contents

Task 400: Viewing Alarm and Fault Management Logs

Purpose

This procedure is used to view the following alarm and fault management reports and logs:

- NE Alarm List
- NE Alarm Log
- NE Protection Switch Activity Log

Before you begin

Before beginning this task, read and follow all safety precautions in this manual.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002*, and Chapter 4, "Alarm Monitoring and Fault Management" in this document.

Task

Complete the following steps to view alarm and fault management reports and logs.

1 Connect the WaveStar CIT to the WaveStar LambdaRouter 128/256 and log in with the appropriate Privilege code as listed below:

- NE Alarm List (S1, M1 or higher)
- NE Alarm Log (S2, M3 or higher)
- NE Protection Switch Activity Log (S2 or higher)

Reference: "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3).

"Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

2

IF viewing the...	THEN...
NE Alarm List	go to “SE 400-1: Viewing the NE Alarm List” (10-4).
NE Alarm Log	go to “SE 400-2: Viewing the NE Alarm Log” (10-4).
NE Protection Switch Activity Log	go to “SE 400-3: Viewing the NE Protection Switch Activity Log” (10-5).

3

IF the report data...	THEN...
will be saved as a text file	click **Save As**. From the Save As Screen, select a path, enter a filename, then click **Save**. **Result:** The report data is saved in the specified file and may be viewed using a text editor.
will be printed	click **Print**. From the Print Screen, select the desired printer and print options, then click **OK**. **Result:** The report data is printed on the selected printer.
will be updated	click **Refresh**. **Result:** The Report Screen updates.

4 Click **Close**.

Result: The Report Screen closes.

END OF STEPS

SE 400-1: Viewing the NE Alarm List

Complete the following steps to view the alarm list for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Fault>NE Alarm List**.

Result: The NE Alarm List Screen appears.

END OF STEPS

SE 400-2: Viewing the NE Alarm Log

Complete the following steps to view the alarm log for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Fault>NE Alarm Log**.

Result: The Start Date/Time Selection Screen appears.

2

IF...	THEN...
retrieving all log entries	select **Retrieve ALL**.
retrieving log entries starting with a specific date and time	select the starting date and time.

3 Click **OK**.

Result: The NE Alarm Log Screen appears.

END OF STEPS

SE 400-3: Viewing the NE Protection Switch Activity Log

Complete the following steps to view the protection switch activity log for the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Reports>NE Protection Switch Activity Log**.

Result: The Start Date/Time Selection Screen appears.

2

IF...	THEN...
retrieving all log entries	select **Retrieve ALL**.
retrieving log entries starting with a specific date and time	select the starting date and time.

3 Click **OK**.

Result: The NE Protection Switch Activity Log Screen appears.

END OF STEPS

Task 401: Setting Alarm Delay Intervals

Purpose

This procedure is used to set the following alarm delay intervals on a WaveStar LambdaRouter 128/256:

- Facility Alarm Clear Delay
- Facility Alarm Generate Delay
- Equipment Alarm Clear Delay
- Equipment Alarm Generate Delay

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3, M3 or greater.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* and the following sections in this document:

- Chapter 4, "Alarm Monitoring and Fault Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 400: Viewing Alarm and Fault Management Logs" (10-2)

Task

Complete the following steps to set the WaveStar LambdaRouter 128/256 alarm clear and generate delay intervals.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Alarms>Alarm Configuration**.

Result: The Alarm Configuration Provisioning Screen appears.

2

IF configuring the...	THEN...
Facility Alarm Clear Delay interval	enter the number of seconds (0, 10-60) a facility event must be continuously absent before an alarm is cleared.
Facility Alarm Generate Delay interval	enter the number of seconds (0, 10-60) a facility event must be continuously present before an alarm is set.
Equipment Alarm Clear Delay interval	enter the number of seconds (0, 10-60) an equipment event must be continuously absent before an alarm is cleared.
Equipment Alarm Generate Delay interval	enter the number of seconds (0, 10-60) an equipment event must be continuously present before an alarm is set.

3 Click **OK**.

Result: A Service Affecting Warning appears.

4 Click **Yes**.

Result: The Alarm Configuration Provisioning Screen closes.

END OF STEPS

Task 402: Testing LEDs and Office Alarms

Purpose

This procedure is used to test all LEDs on a shelf (except the Power On LED) and all visual and audible office alarm outputs and corresponding User Panel LEDs on a shelf.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of T4 or greater.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* and the following sections in this document:

- Chapter 4, "Alarm Monitoring and Fault Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 400: Viewing Alarm and Fault Management Logs" (10-2)

Task

Complete the following steps to test all LEDs on a shelf (except the Power On LED) and all visual and audible office alarm outputs and corresponding User Panel LEDs on a shelf.

1

IF testing the...	THEN...
shelf LEDs	at the WaveStar CIT, from the System View Main Menu bar, select **Fault>Test>LED**. **Result:** The Equipment Selection Screen appears.
office alarm visible and audible outputs	at the WaveStar CIT, from the System View Main Menu bar, select **Fault>Test>Office Alarm**. **Result:** The Equipment Selection Screen appears.

2 Enter an AID for the shelf, or use the NE Explorer to select the shelf by clicking on the plus (+) sign next to each entity, then click **Select**.

IF testing the...	THEN...
shelf LEDs	the Test LED Screen appears.
office alarm visible and audible outputs	the Test Office Alarm Screen appears.

3 Select the number of iterations and click **Start**.

IF testing the...	THEN...
shelf LEDs	a Confirmation Screen appears. Continue to the next step.
office alarm visible and audible outputs	all visual and audible office alarm outputs and the corresponding LED on the User Panel for the selected shelf are tested. When all tests are complete, a Test Complete message is displayed in the Test Office Alarm Screen. Continue to Step 5.

4 Click **Yes**.

Result: All LEDs (except the Power On LED) on the shelf, including the User Panel and circuit pack LEDs, are tested. During one iteration of the test, each LED is turned on for two seconds, then off for two seconds, three times. The test cycle is repeated for the number of iterations specified in Step 3.

When all iterations are complete, a Test Complete message is displayed in the Test LED Screen.

5

IF...	THEN...
testing is complete	click **Close**. **Result:** The Test LED/Test Office Alarm Screen closes.
the shelf LEDs or Office Alarms will be tested again	go to Step 3.

N D O F S T E P S

Task 403: Viewing the Current Status of the Protection Groups

Purpose

This procedure is used to view the current status of a protection group on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S1 or greater.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* and the following sections in this document:

- Chapter 4, "Alarm Monitoring and Fault Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 400: Viewing Alarm and Fault Management Logs" (10-2)
- "Task 404: Executing or Releasing a Forced or Manual Protection Switch" (10-13)

Task Complete the following steps to view the current status of a protection group on the WaveStar LambdaRouter 128/256.

1 At the WaveStar CIT, from the System View Main Menu bar, select **View>Protection**.

Result: The View Protection Screen appears.

2 In the equipment selection portion of the screen, enter an AID for the desired shelf in the AID field or use the NE Explorer to select the shelf by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: The protection information for the selected entity is displayed in the View Protection Screen.

4 View the current status of the selected protection group.

5 Click **Close** in the View Protection Screen.

Result: The View Protection Screen closes.

END OF STEPS

□

Task 404: Executing or Releasing a Forced or Manual Protection Switch

Purpose

This procedure is used to execute or release a forced or manual protection switch.

A manual protection switch may be initiated on the

- System Controller Complex Protection Group (SCCPG)
- High-Voltage Shelf Controller Protection Group (HVCPG)
- Optical Interface Shelf Controller Protection Group (OICPG)
- Output port 2:1 selector

A forced protection switch may be initiated on an output port 2:1 selector.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of M4 or greater.

Related information

For related information, see the *WaveStar LambdaRouter 128/256 Release 2.0 Alarm Messages and Trouble-Clearing Guide, 365-375-002* and the following sections in this document:

- Chapter 4, "Alarm Monitoring and Fault Management"
- "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3)
- "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13)
- "Task 400: Viewing Alarm and Fault Management Logs" (10-2)
- "Task 403: Viewing the Current Status of the Protection Groups" (10-11)

Task Complete the following steps to execute or release a forced or manual protection switch.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Fault>Protection Switch**.

Result: The Switch Protection Screen appears.

2 In the equipment selection portion of the screen, enter an AID for the desired shelf or Optical Channel (OCH) port in the AID field or use the NE Explorer to select the shelf or OCH port by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: The current protection information for the selected entity is displayed in the Switch Protection Screen.

4 View the current status of the selected OCH port or protection group.

Important! When a manual protection switch is operated on an OIS or HVS controller, the newly active OIS or HVS controller should not be addressed by any operations message until three system messages resulting from the controller protection switch have been received. They are as follows:

- **Complete** response to the operate protection switch command
- Report Event **initialization complete** message indicating the newly active OIS or HVS controller
- Report Database Change message indicating the formerly standby OIS or HVS controller has transitioned to active mode

Addressing the OIS or HVS controller before reception of these messages may result in unstable system operations.

5

IF...	THEN...
releasing a forced or manual protection switch	select **Clear** from the Switch Type dropdown list.
executing a forced or manual protection switch	select the protection switch type from the available options in the Switch Type dropdown list.

6 Click **Apply**.

Result: A Service Affecting Warning appears.

7 Click **Yes**.

Result: The protection switch is executed or cleared as appropriate.

8 Click **Close** in the Switch Protection Screen.

Result: The Switch Protection Screen closes and the System View appears.

END OF STEPS

□

11 Cross-Connection Management Tasks

Overview

Purpose

This chapter provides detailed procedures for performing cross-connection tasks on the WaveStar LambdaRouter 128/256.

Contents

Task 500: Establishing a New Cross-Connection

Purpose

This procedure is used to create a new cross-connection of one of the following types on the WaveStar LambdaRouter 128/256:

- one-way or two-way point-to-point
- one-way bridge
- one-way merge
- two-way bridge/merge

All ports involved in creating a new cross-connection must be idle.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note
  - the assigned AIDs for the input and output ports
  - the cross-connection type to be made
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 501: Adding Cross-Connection Legs to an Existing Cross-Connection" (11-19)
- "Task 502: Viewing and Reporting Cross-Connections" (11-22)
- "Task 503: Deleting a Cross-Connection" (11-27)

Task

Complete the following steps to create a new cross-connection.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Cross-Connection**.

Result: The Cross-Connection Wizard is invoked and the Cross-Connection Action Selection Screen appears.

2 Select **Create a new cross-connection** and click **Next**.

Result: The Cross-Connection Type Selection Screen appears.

3

IF establishing a...	THEN...
one-way point-to-point cross-connection	go to “SE 500-1: Establishing a new one-way point-to-point cross-connection” (11-4).
two-way point-to-point cross-connection	go to “SE 500-2: Establishing a new two-way point-to-point cross-connection” (11-6).
one-way bridge cross-connection	go to “SE 500-3: Establishing a new one-way bridge cross-connection” (11-9).
one-way merge cross-connection	go to “SE 500-4: Establishing a new one-way merge cross-connection” (11-12).
two-way bridge/merge cross-connection	go to “SE 500-5: Establishing a new two-way bridge/merge cross-connection” (11-14).

N D O F S T E P S

SE 500-1: Establishing a new one-way point-to-point cross-connection

Complete the following steps to establish a new one-way point-to-point cross-connection.

1 On the Cross-Connection Type Selection Screen, select **1-Way Point to Point** and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

2 Click **Select** under the source port field.

Result: The Source Port Selection Screen appears.

3 Enter an AID for the source port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

5 Click **Select** under the destination port field.

Result: The Destination Port Selection Screen appears.

6 Enter an AID for the destination port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

7 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

8 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

9 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Reselect the ports as necessary and return to Step 8.

10 Click **Yes**.

Result: A message appears indicating the cross-connection has been added.

11 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

12

IF...	THEN...
additional cross-connections are being established	return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
additional cross-connections are not being established	click **Close** to exit the Cross-Connection Wizard.

N D O F S T E P S

SE 500-2: Establishing a new two-way point-to-point cross-connection

Complete the following steps to establish a new two-way point-to-point cross-connection.

1 On the Cross-Connection Type Selection Screen, select **2-Way Point to Point** and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

2 Click **Select** under the first source port field (A).

Result: The Source Port Selection Screen appears.

3 Enter an AID for the first source port (A), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

5 Click **Select** under the first destination port field (B).

Result: The Destination Port Selection Screen appears.

6 Enter an AID for the first destination port (B), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

7 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

8

IF the source port for the second leg...	THEN...
is the same as the destination port for the first leg	the Cross-Connection Wizard defaults to using the destination port for the first leg (B) as the source port for the second leg (C). No port selection is required. Continue to Step 11.
is not the same as the destination port for the first leg	click **Select** under the second source port field (C). **Result:** The Source Port Selection Screen appears.

9 Enter an AID for the second source port (C), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

10 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

11

IF the destination port for the second leg...	THEN...
is the same as the source port for the first leg	the Cross-Connection Wizard defaults to using the source port for the first leg (A) as the destination port for the second leg (D). No port selection is required. Continue to Step 14.
is not the same as the source port for the first leg	click **Select** under the second destination port field (D). **Result:** The Source Port Selection Screen appears.

12 Enter an AID for the second destination port (D), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

13 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

14 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

15 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Reselect the ports as necessary and return to Step 14.

16 Click **Yes**.

Result: A message appears indicating the cross-connection has been added.

17 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

18

IF...	THEN...
additional cross-connections are being established	return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
additional cross-connections are not being established	click **Close** to exit the Cross-Connection Wizard.

ND OF STEPS

SE 500-3: Establishing a new one-way bridge cross-connection

Complete the following steps to establish a new one-way bridge cross-connection.

1 On the Cross-Connection Type Selection Screen, select **1-Way Bridge** and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

2 Click **Select** under the first source port field (A).

Result: The Source Port Selection Screen appears.

3 Enter an AID for the first source port (A), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

5 Click **Select** under the first destination port field (B).

Result: The Destination Port Selection Screen appears.

6 Enter an AID for the first destination port (B), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

7 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

8 Click **Select** under the second destination port field (C).

Result: The Destination Port Selection Screen appears.

9 Enter an AID for the second destination port (C), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

10 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

11 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

12 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Reselect the ports as necessary and return to Step 11.

13 Click **Yes**.

Result: A message appears indicating the cross-connection has been added.

14 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

15

IF...	THEN...
additional cross-connections are being established	return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
additional cross-connections are not being established	click **Close** to exit the Cross-Connection Wizard.

END OF STEPS

SE 500-4: Establishing a new one-way merge cross-connection

Complete the following steps to establish a new one-way merge cross-connection.

1 On the Cross-Connection Type Selection Screen, select **1-Way Merge** and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

2 Click **Select** under the first source port field (A).

Result: The Source Port Selection Screen appears.

3 Enter an AID for the first source port (A), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

5 Click **Select** under the destination port field (B).

Result: The Destination Port Selection Screen appears.

6 Enter an AID for the destination port (B), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

7 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

8 Click **Select** under the second source port field (C).

Result: The Source Port Selection Screen appears.

9 Enter an AID for the first source port (C), or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

10 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

11 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

12 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of “Task 500: Establishing a New Cross-Connection” (11-2).
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Reselect the ports as necessary and return to Step 11.

13 Click **Yes**.

Result: A message appears indicating the cross-connection has been added.

14 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

15

IF...	THEN...
additional cross-connections are being established	return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
additional cross-connections are not being established	click **Close** to exit the Cross-Connection Wizard.

END OF STEPS

SE 500-5: Establishing a new two-way bridge/merge cross-connection

Complete the following steps to establish a new two-way bridge/merge cross-connection.

1 On the Cross-Connection Type Selection Screen, select **2-Way Bridge/ Merge** and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

2 Click **Select** under the source port field (A) for the bridge cross-connection.

Result: The Source Port Selection Screen appears.

3 Enter an AID for the source port (A) for the bridge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

4 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

5 Click **Select** under the first destination port field (B) for the bridge cross-connection.

Result: The Destination Port Selection Screen appears.

6 Enter an AID for the first destination port (B) for the bridge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

7 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

8

IF the first source port for the merge cross-connection...	THEN...
is the same as the first destination port for the bridge cross-connection	the Cross-Connection Wizard defaults to using the first destination port for the bridge cross-connection (B) as the first source port for the merge cross-connection (C). No port selection is required. Continue to Step 11.
is not the same as the first destination port for the bridge cross-connection	click **Select** under the first source port field for the merge cross-connection (C). **Result:** The Source Port Selection Screen appears.

9 Enter an AID for the first source port (C) for the merge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

10 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

11

IF the destination port for the merge cross-connection...	THEN...
is the same as the source port for the bridge cross-connection	the Cross-Connection Wizard defaults to using the source port for the bridge cross-connection (A) as the destination port for the merge cross-connection (D). No port selection is required. Continue to Step 14.
is not the same as the source port for the bridge cross-connection	click **Select** under the destination port field for the merge cross-connection (D). **Result:** The Source Port Selection Screen appears.

12 Enter an AID for the destination port (D) for the merge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

13 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

14 Click **Select** under the second destination port field (E) for the bridge cross-connection.

Result: The Destination Port Selection Screen appears.

15 Enter an AID for the second destination port (E) for the bridge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

16 Click **Select**.

Result: The Destination Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

17

IF the second source port for the merge cross-connection...	THEN...
is the same as the second destination port for the bridge cross-connection	the Cross-Connection Wizard defaults to using the second destination port for the bridge cross-connection (E) as the second source port for the merge cross-connection (F). No port selection is required. Continue to Step 20.
is not the same as the second destination port for the bridge cross-connection	click **Select** under the second source port field for the merge cross-connection (F). **Result:** The Source Port Selection Screen appears.

18 Enter an AID for the second source port (F) for the merge cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

19 Click **Select**.

Result: The Source Port Selection Screen closes. The selected port is displayed on the Cross-Connection Port Selection Screen.

20 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

21 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Reselect the ports as necessary and return to Step 20.

22 Click **Yes**.

Result: A message appears indicating the cross-connection has been added.

23 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

24

IF...	THEN...
additional cross-connections are being established	return to Step 2 of "Task 500: Establishing a New Cross-Connection" (11-2).
additional cross-connections are not being established	click **Close** to exit the Cross-Connection Wizard.

ND OF STEPS

Task 501: Adding Cross-Connection Legs to an Existing Cross-Connection

Purpose

This procedure is used to add cross-connection legs to an existing cross-connection on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note
  - the assigned AIDs for the input and output ports
  - the cross-connection type to be made
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 500: Establishing a New Cross-Connection" (11-2)
- "Task 502: Viewing and Reporting Cross-Connections" (11-22)
- "Task 503: Deleting a Cross-Connection" (11-27)

Task

Complete the following steps to add cross-connection legs to an existing cross-connection.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Cross-Connection**.

Result: The Cross-Connection Wizard is invoked and the Cross-Connection Action Selection Screen appears.

2 Select **Add leg(s) to an existing cross-connection** and click **Next**.

Result: The Cross-Connection Type Selection Screen appears.

3 Select the type of cross-connection leg(s) to add and click **Next**.

Result: The Existing Cross-Connection Selection Screen appears.

4 Enter an AID for the port that has an existing cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

Result: All cross-connections associated with the selected port are shown on the right side of the Existing Cross-Connection Selection Screen.

5 Select the cross-connection from the list to which the cross-connection legs will be added and click **Next**.

Result: The Cross-Connection Port Selection Screen appears.

6 Click **Select** under a port field for a leg being added.

Result: The Port Selection Screen appears.

7 Enter an AID for the selected port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

8 Click **Select**.

Result: The Port Selection Screen closes and the selected port is displayed on the Cross-Connection Port Selection Screen.

9 Repeat Step 6 through Step 8 for each new port on the Cross-Connection Port Selection Screen.

Result: When all ports have been selected, the **Next** button is enabled.

10 Click **Next**.

Result: The Cross-Connection Summary Screen appears.

11 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection type is incorrect	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2 of this task to select a different cross-connection type.
the cross-connection type is correct but one or more ports are incorrect	click **Back**. **Result:** The Cross-Connection Port Selection Screen appears. Return to Step 6 of this task to reselect the ports.

12 Click **Yes**.

Result: The cross-connection leg(s) are added to the existing cross-connection. A message appears indicating the cross-connection was created successfully.

13 Click **OK**.

Result: The Cross-Connection Action Selection Screen appears.

14

IF...	THEN...
additional cross-connection leg(s) are being added	return to Step 2 of this task.
additional cross-connection leg(s) are not being added	click **Close** to exit the Cross-Connection Wizard.

END OF STEPS

Task 502: Viewing and Reporting Cross-Connections

Purpose

This procedure is used to view a list of cross-connections on the WaveStar LambdaRouter 128/256.

Cross-connection configurations associated with a port may be viewed either in text format or graphically. A text-only report may also be generated for cross-connection configurations associated with the system, shelf, or circuit pack.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P1 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, “Cross-Connection Management”
- “Task 500: Establishing a New Cross-Connection” (11-2)
- “Task 501: Adding Cross-Connection Legs to an Existing Cross-Connection” (11-19)
- “Task 503: Deleting a Cross-Connection” (11-27)

Task Complete the following steps to view cross-connections in either text or graphic format.

1

IF retrieving cross-connection configurations...	THEN...
associated with a port to view in graphic format	go to "SE 502-1: Viewing cross-connection configurations in a graphic format" (11-23).
associated with the system, shelf, circuit pack, or port to view in text format	go to "SE 502-2: Creating cross-connection text reports" (11-25).

END OF STEPS

SE 502-1: Viewing cross-connection configurations in a graphic format

Complete the following steps to view cross-connection configurations associated with a port in a graphic format.

1 At the WaveStar CIT, from the System View Main menu bar, select **View>Cross-Connections**.

Result: The View Cross-Connections Port Selection Screen appears.

2 Enter an AID for the desired port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

Result: The View Cross-Connections Selection Screen appears. All cross-connections associated with the selected port are shown in text format.

3 Select a cross-connection from the list in the View Cross-Connections Screen and click **View Graphic**.

Result: The selected cross-connection configuration is displayed in graphic format.

4

IF...	THEN...
additional cross-connections will be viewed in graphic format	click **Back**. **Result:** The View Cross-Connections Selection Screen appears. Continue to the next step.
no additional cross-connections will be viewed in graphic format	click **Close**. **Result:** The View Cross-Connections Screen closes and the System View appears. *Stop! End of Task.*

5

IF...	THEN...
a cross-connection associated with the currently selected port will be viewed in graphic format	return to Step 3 of this task.
a different port will be selected	click **Browse**. **Result:** The View Cross-Connections Port Selection Screen appears. Return to Step 2 of this procedure.

END OF STEPS

SE 502-2: Creating cross-connection text reports

Complete the following steps to create text reports of cross-connection configurations associated with the system, shelf, circuit pack, or port.

1 At the WaveStar CIT, from the System View Main menu bar, select **Reports>Cross-Connection List**.

Result: The Equipment Selection Screen appears.

2 Enter an AID for the system, shelf, circuit pack, or port for which cross-connection information will be displayed, or use the NE Explorer to select the system, shelf, circuit pack, or port by clicking on the plus (+) sign next to each entity.

3 Select the Retrieval Scope for the report (**ALL**, **1WAY**, **2WAY**, **LPBK**). Selecting **ALL** will retrieve all cross-connections associated with the selected entity. Selecting **1WAY**, **2WAY**, or **LPBK** will retrieve only cross-connections of the selected type that are associated with the entity.

4 Click **Select**.

Result: The Cross-Connection List Screen appears. The cross-connections are displayed in the order in which they are returned from the system. The information can be sorted by clicking on the desired column in the report.

5

IF the report data...	THEN...
will be saved as a text file	click **Save As**. From the Save As Screen, select a path, enter a filename, then click **Save**. **Result:** The report data is saved in the specified file and may be viewed using a text editor.
will be printed	click **Print**. From the Print Screen, select the desired printer and print options, then click **OK**. **Result:** The report data is printed on the selected printer.
will be updated	click **Refresh**. **Result:** The Cross-Connection List Screen updates.

6 Click **Close**.

Result: The Cross-Connection List Screen closes.

END OF STEPS

Task 503: Deleting a Cross-Connection

Purpose

This procedure is used to delete legs of an existing cross-connection on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note
  - the assigned AIDs for the input and output ports
  - the cross-connection type to be deleted
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of P3 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 500: Establishing a New Cross-Connection" (11-2)
- "Task 501: Adding Cross-Connection Legs to an Existing Cross-Connection" (11-19)
- "Task 502: Viewing and Reporting Cross-Connections" (11-22)

Task

Complete the following steps to delete a cross-connection.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Cross-Connection**.

Result: The Cross-Connection Wizard is invoked and the Cross-Connection Action Selection Screen appears.

2 Select **Delete leg(s) of an existing cross-connection** and click **Next**.

Result: The Existing Cross-Connection Selection Screen appears.

3 Enter an AID for the port that has an existing cross-connection, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

Result: All cross-connections associated with the selected port are shown on the right side of the Existing Cross-Connection Selection Screen.

4 From the table on the right side of the screen, select the cross-connection to be deleted and click **Next**.

IF the cross-connection type is...	THEN...
one-way merge, one-way bridge, or is part of a configuration	the Cross-Connection Leg Selection Screen appears. Continue to the next step.
one-way or two-way point-to-point	the Delete Cross-Connection Summary Screen appears. Continue to Step 6.

5

IF...	THEN...
one leg of the selected cross-connection configuration is being deleted	select the appropriate leg of the cross-connection and click **Next**.
both legs of a selected bridge or merge cross-connection are being deleted	select either both legs merged on the output port AID or both legs bridged on the input port AID and click **Next**.
all legs of a selected configuration are being deleted	select **All Legs** and click **Next**.

Result: The Delete Cross-Connection Summary Screen appears.

6 Verify the selected cross-connection parameters.

IF...	THEN...
all cross-connection parameters are correct	click **Finish**. **Result:** A Confirmation Screen appears. Continue to the next step.
the cross-connection information is incorrect	click **Back**. **Result:** The Existing Cross-Connection Selection Screen appears. Return to Step 3 to reselect the port, or Step 4 to select a different cross-connection as necessary.
starting the procedure over again	click **Start Over**. **Result:** A Confirmation Screen appears. Click **Yes** and return to Step 2.

7 Click **Yes**.

Result: A Service Affecting Warning appears.

8 Click **Yes**.

Result: The Cross-Connection Action Selection Screen appears.

9

IF...	THEN...
additional cross-connection leg(s) are being deleted	return to Step 2 of this task.
additional cross-connection leg(s) are not being deleted	click **Close** to exit the Cross-Connection Wizard.

END OF STEPS

Task 504: Establishing (Operating) a Cross-Connect Loopback

Purpose

This procedure is used to establish a cross-connect loopback of an optical signal from an input port, through an optionally specified switch fabric, to a selected output port on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of T4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 505: Viewing Cross-Connect Loopbacks" (11-33)
- "Task 506: Releasing a Cross-Connect Loopback" (11-35)

Task

Complete the following steps to establish a cross-connect loopback.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Fault>Loopbacks**.

Result: The Cross-Connect Loopback Screen appears.

2 On the left side of the Cross-Connect Loopback Screen, enter an AID for the desired input port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: Information for the selected port and loopback options are displayed on the right side of the Cross-Connect Loopback Screen.

4

IF...	THEN...
the default output port is acceptable	continue to Step 7.
the default output port is not acceptable	click **Select** under the Output AID field. **Result:** The Select Output Port Screen appears.

5 Enter an AID for the selected output port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

6 Click **Select**.

Result: The Select Output Port Screen closes and the selected port is displayed on the Cross-Connect Loopback Screen.

7 Select the switch fabric to be used for the cross-connect loopback (0, 1, or both). For a forced cross-connect loopback, the CIT displays the active fabric. The inactive fabric is the default choice.

8

IF the selected port...	THEN...
is not already associated with an existing cross-connection (Cross-Connect Status is No)	select **Operate Cross Connect Loopback**.
is already associated with an existing cross-connection (Cross-Connect Status is Yes)	select **Operate Forced Cross Connect Loopback**.

9 Click **Apply**.

Result: A Confirmation Screen appears.

10 Click **Yes**.

Result: The cross-connect loopback is established.

11

IF...	THEN...
additional cross-connect loopbacks are being established	return to Step 2 of this task.
additional cross-connect loopbacks are not being established	click **Close** to exit the Cross-Connect Loopback Screen.

N D O F S T E P S

□

Task 505: Viewing Cross-Connect Loopbacks

Purpose

This procedure is used to view existing cross-connect loopback connections on a system, optical interface shelf, port unit, or a port on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of M1 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 504: Establishing (Operating) a Cross-Connect Loopback" (11-30)
- "Task 506: Releasing a Cross-Connect Loopback" (11-35)

Task

Complete the following steps to view existing cross-connect loopback connections.

1 At the WaveStar CIT, from the System View Main Menu bar, select **View>Loopback**.

Result: The View Loopback Selection Screen appears.

2 Enter an AID for the system, shelf, circuit pack, or port for which loopback information will be displayed, or use the NE Explorer to select the system, shelf, circuit pack, or port by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: The View Loopback Screen appears.

4 Review the loopback information. Click **Close** when done.

Result: The View Loopback Screen closes.

END OF STEPS

□

Task 506: Releasing a Cross-Connect Loopback

Purpose

This procedure is used to release a cross-connect loopback of an optical signal on the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task and note the assigned AIDs.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of T4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 5, "Cross-Connection Management"
- "Task 504: Establishing (Operating) a Cross-Connect Loopback" (11-30)
- "Task 505: Viewing Cross-Connect Loopbacks" (11-33)

Task

Complete the following steps to release a cross-connect loopback.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Fault>Loopbacks**.

Result: The Cross-Connect Loopback Screen appears.

2 On the left side of the Cross-Connect Loopback Screen, enter an AID for the desired input port, or use the NE Explorer to select the shelf, circuit pack, and port by clicking on the plus (+) sign next to each entity.

3 Click **Select**.

Result: Information for the selected port and loopback options are displayed on the right side of the Cross-Connect Loopback Screen.

4

IF there is...	Then...
no cross-connect loopback associated with the selected port (Cross-Connect Loopback Status is No)	there is no loopback connection to release. *Stop! End of Task.*
a normal cross-connect loopback associated with the selected port (Cross-Connect Status is No, Cross-Connect Loopback Status is Yes)	select **Release Normal Cross Connect Loopback**.
a forced cross-connect loopback associated with the selected port (Cross-Connect Status is Yes, Cross-Connect Loopback Status is Yes)	select **Release Forced Cross Connect Loopback**.

5 Click **Apply**.

IF...	THEN...
the active fabric was selected	a Service Affecting Warning appears.
the inactive fabric was selected	a Confirmation Screen appears.

6 Click **Yes**.

Result: The cross-connect loopback is released.

7

IF...	THEN...
additional cross-connect loopbacks are being released	return to Step 2 of this task.
additional cross-connect loopbacks are not being released	click **Close** to exit the Cross-Connect Loopback Screen.

END OF STEPS

□

12 Software Management Tasks

Overview

Purpose

This chapter provides detailed procedures for performing software installation and database backup and restore tasks on the WaveStar LambdaRouter 128/256.

Contents

Task 600: Viewing Software and Data Properties

Purpose

This procedure is used to view

- the release of software currently active on the WaveStar CIT
- an overview of the release and status of the software in the secondary NVM, or in the Active and Previous partitions of the primary NVM on the network element
- detailed information for the software and data on the network element

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the NVM card containing the network element software, if required.

CAUTION

Use a static ground wrist strap whenever handling circuit packs or working on a WaveStar LambdaRouter 128/256, to prevent electrostatic discharge damage to sensitive components.

Related information

For related information, see the following sections in this document:

- Chapter 6, "Software Management"
- "Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory" (12-9)
- "Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT" (12-14)

Task Complete the following steps to view the properties of the WaveStar CIT or network element software and data.

1

IF retrieving...	THEN...
software release information on the WaveStar CIT	go to “SE 600-1: Viewing the WaveStar CIT software release number information” (12-4).
an overview of software and data properties on the network element	go to “SE 600-2: Viewing an overview of software and data properties on the network element” (12-5).
detailed software and data on the network element	go to “SE 600-3: Viewing detailed information for the software and data on the network element” (12-6).
detailed software and data on the WaveStar CIT	go to “SE 600-4: Viewing detailed information for the software and data on the WaveStar CIT” (12-7).

N D O F S T E P S

SE 600-1: Viewing the WaveStar CIT software release number information

Complete the following steps to view the release number of the software currently installed on the WaveStar CIT.

1 Log into the WaveStar CIT.

Reference: “Task 201: Logging in to the WaveStar CIT” (8-6).

2 At the WaveStar CIT, from the Network View Main Menu bar, select **Help>About WaveStar CIT**.

Result: The CIT About Screen appears with the current software release and build information.

3 Click **OK**.

Result: The CIT About Screen closes.

END OF STEPS

SE 600-2: Viewing an overview of software and data properties on the network element

Complete the following steps to retrieve an overview of the software and data properties on the network element.

1 Connect the WaveStar CIT to the network element and log in.

Reference: "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3).

"Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

2 At the WaveStar CIT, from the System View Main Menu bar, select **View>Software/Data in NE**.

Result: The Software and Data Info Screen appears.

3 View the software and data information. The information can be sorted by clicking on the desired column in the report.

4 When finished viewing the software and data properties, click **Close**.

Result: The Software and Data Info Screen closes.

N D O F S T E P S

SE 600-3: Viewing detailed information for the software and data on the network element

Complete the following steps to view detailed information on the software and data on the network element.

1 Connect the WaveStar CIT to the network element and log in.

> **Reference:** "Task 200: Connecting or Disconnecting the WaveStar CIT to or from a Network Element" (8-3).
>
> "Task 204: Logging into a Network Element from the WaveStar CIT" (8-13).

2

IF viewing properties for the...	THEN...
software generic	at the WaveStar CIT, from the System View Main Menu bar, select **View>Software Generic**. **Result:** The Select Generic Screen appears.
database	at the WaveStar CIT, from the System View Main Menu bar, select **View>NE Data**. **Result:** The Select Database Screen appears.

3 Select the desired entry, then click **OK**.

IF...	THEN...
a software generic was selected	the Generic Info Screen appears.
a database was selected	the Database Info Screen appears.

4 View the displayed information for the selected database or software generic. The information can be sorted by clicking on the desired column in the report.

5 When finished viewing the information for the selected database or software, click **Close**.

Result: The Generic Info or Database Info Screen closes.

END OF STEPS

SE 600-4: Viewing detailed information for the software and data on the WaveStar CIT

Complete the following steps to view detailed information on the software and data on the WaveStar CIT.

1 Log into the WaveStar CIT.

Reference: "Task 201: Logging in to the WaveStar CIT" (8-6).

2

IF viewing properties for the...	THEN...
software generic	at the WaveStar CIT, from the System View Main Menu bar, select **View>Software Generic**. **Result:** The Select Generic Screen appears.
database	at the WaveStar CIT, from the System View Main Menu bar, select **View>NE Data**. **Result:** The Select Database Screen appears.

3 Select **CIT** from the Look In drop-down list.

Result: The network element software generic or database information stored on the WaveStar CIT is displayed.

4 Select the desired entry, then click **OK**.

IF...	THEN...
a software generic was selected	the Generic Info Screen appears.
a database was selected	the Database Info Screen appears.

5 View the displayed information for the selected database or software generic. The information can be sorted by clicking on the desired column in the report.

6 When finished viewing the information for the selected database or software, click **Close**.

Result: The Generic Info or Database Info Screen closes.

END OF STEPS

□

Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory

Purpose

This procedure is used to manually back up network element data or a software release from the active primary NVM to the secondary (backup) NVM.

Backing up the network element data and/or software should be done

- before and after major provisioning data changes
- periodically according to local policy
- if the network element TID has been changed

Changes to the network element software generic and database are covered in the applicable *Software Release Description* document for the current software generic. This document should be reviewed prior to performing this task for any detailed procedures or cautions that may apply to software management of the generic running on the system.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 6, “Software Management”
- “Task 602: Manually Restoring Data from Secondary Memory to Primary Memory” (12-11)
- “Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT” (12-14)
- “Task 604: Manually Restoring Data from the WaveStar CIT to Primary Memory” (12-16)

Task Complete the following steps to manually back up network element data or a software release from the active primary NVM to the secondary (backup) NVM.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Software>Copy NVM**.

Result: The Copy NVM Screen appears.

2 Select **Active Primary to Secondary** for the type of copy.

3 Select the information to be copied from the Data Type drop-down list (Data, Generic Software, or Data and Generic Software).

4 Click **OK**.

Result: A Confirmation Screen appears.

5 Click **Yes**.

Result: The selected data is copied from the primary NVM to the secondary NVM.

END OF STEPS

Task 602: Manually Restoring Data from Secondary Memory to Primary Memory

Purpose

This procedure is used to manually restore network element data from the secondary NVM to the active primary NVM.

Restoring the network element data from the secondary NVM may need to be done after a known or suspected database corruption.

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

> **Important!** The data being restored must be data that was originally backed up from the same network element with the same TID. If the TID for the network element has been changed since the last backup, the data cannot be restored.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 6, “Software Management”
- “Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory” (12-9)
- “Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT” (12-14)
- “Task 604: Manually Restoring Data from the WaveStar CIT to Primary Memory” (12-16)

Task Complete the following steps to manually restore network element data from the secondary NVM to the active primary NVM.

1 Remove the system from service.

Reference: "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

2 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Software>Copy NVM**.

Result: The Copy NVM Screen appears.

3 Select **Data** as the data type to be copied.

Important! The SWIP calibration files are included in the database and are part of **Data**.

4 Select **Secondary to Active Primary** for the type of copy.

5

IF copying the data...	THEN...
should include a database restore	check the box beside Include Restore.
should not include a database restore	ensure the box beside Include Restore is not checked.

6 Click **OK**.

Result: A Confirmation Screen appears.

7 Click **Yes**.

IF the Data Type being copied is...	THEN...
Data and the Include Restore option was selected	the database is copied into the previous folder of the primary NVM and the system performs a reset. During the reset the database is copied into the current folder of primary NVM and becomes active. During the reset the system automatically disconnects the WaveStar CIT. When the system reset has completed, the system is in service. *Stop! End of Task.*
Data and the Include Restore option was not selected	the selected data is copied from the secondary NVM to the previous primary NVM. Continue to the next step.

8 Return the system to an in-service (IS) state.

Reference: "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

END OF STEPS

□

Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT

Purpose

This procedure is used to manually back up data from the WaveStar LambdaRouter 128/256 to remote WaveStar CIT storage.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 6, "Software Management"
- "Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory" (12-9)
- "Task 602: Manually Restoring Data from Secondary Memory to Primary Memory" (12-11)
- "Task 604: Manually Restoring Data from the WaveStar CIT to Primary Memory" (12-16)
- "Task 605: Creating an FTP Profile" (12-19)

Task

Complete the following steps to manually back up data from the WaveStar LambdaRouter 128/256 to remote WaveStar CIT storage.

1 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Software>Remote Backup**.

Result: The Backup Database Screen appears.

2 Select **CIT** from the Backup To drop-down list.

Result: The Destination Directory Path updates to display the directory, TID, software release running on the WaveStar LambdaRouter 128/256, and the date and time of the backup.

3 Select the **FTP** tab.

IF...	THEN...
the FTP profile has been previously created	select the appropriate FTP profile from the Profile drop-down list. **Result:** The FTP profile entry fields are populated with the information for the selected profile.
the FTP profile does not exist	create a new FTP profile. **Reference:** "Task 605: Creating an FTP Profile" (12-19).

4 Click **Backup**.

Result: A Confirmation Screen appears.

5 Click **Yes**.

Result: A Progress Indicator Screen appears and the database is backed up to the WaveStar CIT.

END OF STEPS

Task 604: Manually Restoring Data from the WaveStar CIT to Primary Memory

Purpose

This procedure is used to manually restore data from remote WaveStar CIT storage to the WaveStar LambdaRouter 128/256.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the work instructions for this task.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 6, "Software Management"
- "Task 601: Manually Backing Up Software or Data from Primary Memory to Secondary Memory" (12-9)
- "Task 602: Manually Restoring Data from Secondary Memory to Primary Memory" (12-11)
- "Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT" (12-14)
- "Task 605: Creating an FTP Profile" (12-19)

Task

Complete the following steps to manually restore data from remote WaveStar CIT storage to the WaveStar LambdaRouter 128/256.

1 Remove the system from service.

Reference: "Task 302: Removing Equipment from and Returning Equipment to Service" (9-14).

2 At the WaveStar CIT, from the System View Main Menu bar, select **Configuration>Software>Remote Restore**.

Result: The Restore Database Screen appears.

3 Select **CIT** from the Restore From drop-down list.

Result: The Destination Directory Path updates to display the directory, TID, software release running on the WaveStar LambdaRouter 128/256, and the date and time of the backup.

4 Select the **FTP** tab.

IF...	THEN...
the FTP profile has been previously created	select the appropriate FTP profile from the Profile drop-down list. **Result:** The FTP profile entry fields are populated with the information for the selected profile.
the FTP profile does not exist	create a new FTP profile. **Reference:** "Task 605: Creating an FTP Profile" (12-19).

5 Select the **CIT** tab and select the data file to be restored.

6 Click **Restore**.

Result: A Confirmation Screen appears.

7 Click **Yes**.

Important! The database restore operation may change previously provisioned parameters.

Result: A Service Affecting Warning appears.

8 Click **Yes**.

Result: The database is restored from the WaveStar CIT and the system resets.

9 Set the system date and time.

Reference: "Task 303: Setting the System Date and Time" (9-19).

N D O F S T E P S

□

Task 605: Creating an FTP Profile

Purpose

This procedure is used to create an FTP profile for the WaveStar CIT that is used when manually backing up data from a network element to the WaveStar CIT, or when manually restoring data from the WaveStar CIT to a network element.

Before you begin

Before beginning this task:

- Read and follow all safety precautions in this manual.
- Obtain the IP address for the WaveStar CIT and ensure that a Microsoft Windows user name and password have been set up to be used in the FTP profile. Refer to the Microsoft Windows user documentation for information.
- Connect the WaveStar CIT to the local network element and log in with a Privilege code of S4 or greater.

Related information

For related information, see the following sections in this document:

- Chapter 6, “Software Management”
- “Task 603: Manually Backing Up Data from Primary Memory to the WaveStar CIT” (12-14)
- “Task 604: Manually Restoring Data from the WaveStar CIT to Primary Memory” (12-16)

Task

Complete the following steps to create an FTP profile for the WaveStar CIT.

1 At the WaveStar CIT, from the System View Main Menu bar, select either **Configuration>Software>Remote Backup**.

Result: The Backup Database Screen appears.

2 Select the **FTP** tab.

Result: The Backup Database Screen updates to display the FTP profile entry fields.

3 Enter the following information:

Field	Description
Profile	A unique name for the FTP profile.
User Name and Password	A valid Microsoft Windows user name and password that have already been created on the WaveStar CIT.
Server	The IP address of the WaveStar CIT.

4 Click **Add**.

Result: The profile is added to the FTP profile list.

5 Click **Save**.

Result: The FTP profile list is saved.

6 Click **Close**.

Result: The Backup Database Screen closes.

END OF STEPS

Appendix A: WaveStar CIT Tutorial

Overview

Purpose

This tutorial provides an overview of the WaveStar CIT (Craft Interface Terminal) features and capabilities, and information on how to navigate and use the graphical user interface (GUI).

> **Important!** Multiple versions of the WaveStar CIT application can be installed on the WaveStar CIT at the same time. Screens, menus, and messages shown in this tutorial may differ slightly from those that appear on your system.

Related information

This tutorial is intended to provide generic information relating to the WaveStar CIT GUI operation only. For detailed information on how to use the WaveStar CIT to perform specific tasks on a WaveStar LambdaRouter or WaveStar LambdaRouter 128/256, refer to the following manuals that are appropriate for your system:

- User Operations Guide
- Alarm Messages and Trouble-Clearing Guide
- Operations Systems Engineering Guide

Unless otherwise specified, the term network element refers to any WaveStar LambdaRouter or WaveStar LambdaRouter 128/256 system.

Contents

Hardware Overview

Description

The WaveStar CIT is a customer-furnished laptop or desktop computer that is the primary tool used by Craft personnel to interface with, and provision, a network element.

The WaveStar CIT provides

- a Windows-based GUI
- a Transaction Level 1 (TL1) cut-through command interface
- direct and remote access to network elements
- security features to prevent unauthorized access

Minimum system requirements

It is recommended that the computer used to run the WaveStar CIT application meet or exceed the following specifications:

- Microsoft Windows 2000 Professional or Microsoft Windows NT Workstation 4.0 with Service Pack 6
- Intel *Pentium*® III 500 MHz processor with 256 MB of RAM
- standard floppy drive for 1.44 MB 3.5-inch disks
- a 6.5 GB hard disk with 500 MB free space
- 4x speed CD-ROM drive
- Personal Computer Memory Card International Association (PCMCIA) Type II slot with driver software that supports read/write of PCMCIA flash disk cards
- SVGA color display capable of 1024 x 768 resolution
- 10/100BaseT network interface card

In addition, Microsoft Peer Web Services (FTP server) must be installed on the computer used to run the WaveStar CIT application.

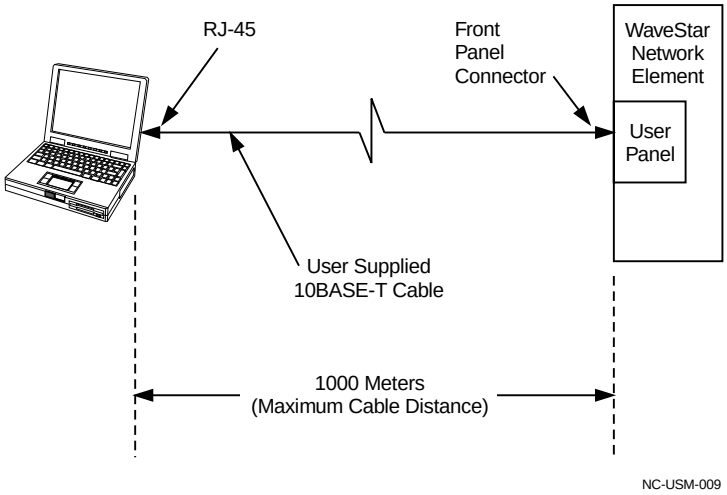
The WaveStar CIT application requires a minimum of 50 MB of hard disk space. An additional 30 MB is required during installation of the WaveStar CIT software.

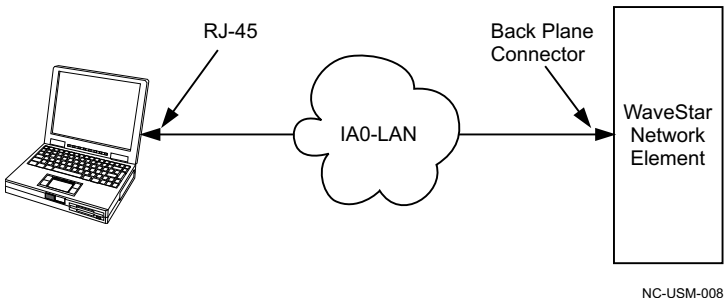
Communication

The WaveStar CIT communicates with the network of WaveStar network elements via a 10/100BaseT Local Area Network (LAN) connection.

The physical connection of the WaveStar CIT to the LAN may be either by direct connection to the CIT Port on the network element System Controller Shelf User Panel, or by a network connection using the intraoffice local area network (IAO LAN).

The interface between the WaveStar CIT and the network element supports TL1 commands and File Transfer Protocol (FTP) for software downloads and provisionable data backup and restore.





Software Overview

Features and uses

The WaveStar CIT application is a graphical user interface (GUI) that provides full access to the administrative, maintenance, and provisioning capabilities of the network element.

The services provided by the WaveStar CIT include

- protection from unauthorized access to CIT and network element functions through the use of logins, passwords, and multiple authorization levels
- easy access to each network element in the local network
- visual display of the bays, shelves, and equipped circuit pack types and states for a network element
- provisioning of cross-connections, equipment, software management, and fault management for a network element
- software upgrade and database backup and restore to and from a network element
- report generation for network element equipage, cross-connections, alarms, and states

Multi-User capability

A maximum of seven user IDs, each with an assigned password, privilege level, and preference information, may be provisioned on the WaveStar CIT.

Two of the seven user IDs are Superuser IDs that are automatically configured when the WaveStar CIT application is installed. The Superusers cannot be deleted, and with the exception of changing the Superuser password, may not be modified.

The remaining five user IDs can be added, modified, or deleted as necessary, and are provisioned by a Security Administrator (Superuser or any other user with an S5 security privilege).

Only one user may be logged into the WaveStar CIT at a time. However, the one user logged into the WaveStar CIT can be logged into up to five network elements at a time. Each network element can accommodate up to 26 simultaneous WaveStar CIT sessions (24 users plus two Superusers).

Window components

The WaveStar CIT application uses standard Microsoft Windows-based GUI components, which include:

- title bar
- menus (available from a menu bar and, in some cases, right-click pop-up menus)
- toolbar
- status bar
- display areas/views

Important! Not all window components are available in every view.

Window types

The WaveStar CIT application uses the window types described in the following table:

Window Type	Description
Display Screen or View	A primary window that displays a graphical depiction of an object and allows the user to view configuration information or parameters (but not set them), or to select an object for further interaction.
Modal Window	A secondary window which requires the user to complete interaction within that window, including closing the window, before continuing with any further interaction outside the window.
Non-Modal Window	A secondary window which allows the user to interact with any other window.
Dialog Box	A secondary window designed to allow the user to enter additional information.

Navigation

The WaveStar CIT application uses standard Windows functionality for using the keyboard or a pointing device (such as a mouse, touchpad, trackball, or other integrated pointing device) to navigate screens and select objects. This functionality includes:

- single-clicking the left pointing device button to highlight (or select) a menu item, window button, or other object
- double-clicking the left pointing device button to select or open an object
- pressing the Tab key to advance the cursor to the next window field or button

Pop-up menus

The WaveStar CIT application provides context-sensitive pop-up menus that duplicate some of the functionality of the Main menus.

Right-click with the screen pointer positioned over an element on the screen, or over an area of the screen, to display a pop-up menu with options that are valid for that selection.

Menu shortcuts (hotkeys)

Menu shortcuts, or hotkeys, are a keyboard key or combination of keys that invoke a particular command. WaveStar CIT menus with an underlined letter in the menu name may be accessed using keyboard shortcuts.

Press and hold the **Alt** key, then press the underlined letter in the menu to select that option.

Tooltips

Tooltips provide a small pop-up window that contains a brief description of the item currently under the screen pointer.

Position the pointer over the desired object and remain stationary for one to two seconds to display the object tooltip.

Drop-down list boxes

Drop-down list boxes are standard Windows control items that display a current setting or option, but can be opened to display a valid list of choices by clicking on the list box or a “down-arrow” button beside the list box.

User interface views

The following main views make up the WaveStar CIT application:

- WaveStar CIT login
- Network View
- System View
- Cut-Through View

All tasks performed on the WaveStar CIT or a network element use one or more of these views. Each view contains additional screens, menus, and dialogs used to perform the required task.

□

WaveStar CIT Login Screen

Overview

The WaveStar CIT Login Screen allows a user to log into and access the WaveStar CIT application functions.

It should be noted that after successfully logging in, the user is only logged into the WaveStar CIT and is not automatically logged into a network element.

Once logged in, the user may

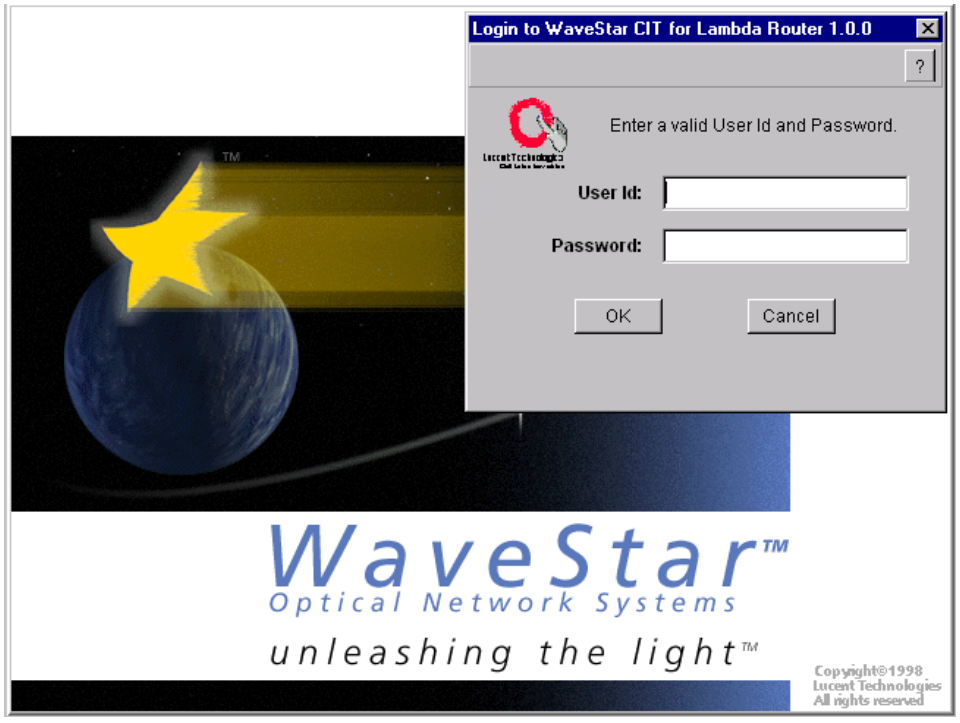
- perform provisioning tasks on the WaveStar CIT
- connect and log into one or more network elements

Login Screen components

The WaveStar CIT Login Screen is made up of the

- copyright screen
- login dialog box

The following figure shows an example of the Login Screen.



Accessing the WaveStar CIT Login Screen

Before you begin If provisioning tasks will be performed on a network element, connect the WaveStar CIT to the network element before starting this procedure. If provisioning tasks will be performed only on the WaveStar CIT, no connection to a network element is required.

Task Complete the following steps to access the WaveStar CIT Login Screen.

1 Power on the WaveStar CIT and boot the Microsoft Windows operating system.

2 On the Windows desktop, double-click on the WaveStar CIT icon.

Result: The WaveStar CIT Login Screen appears.

N D O F S T E P S

□

WaveStar CIT Network View

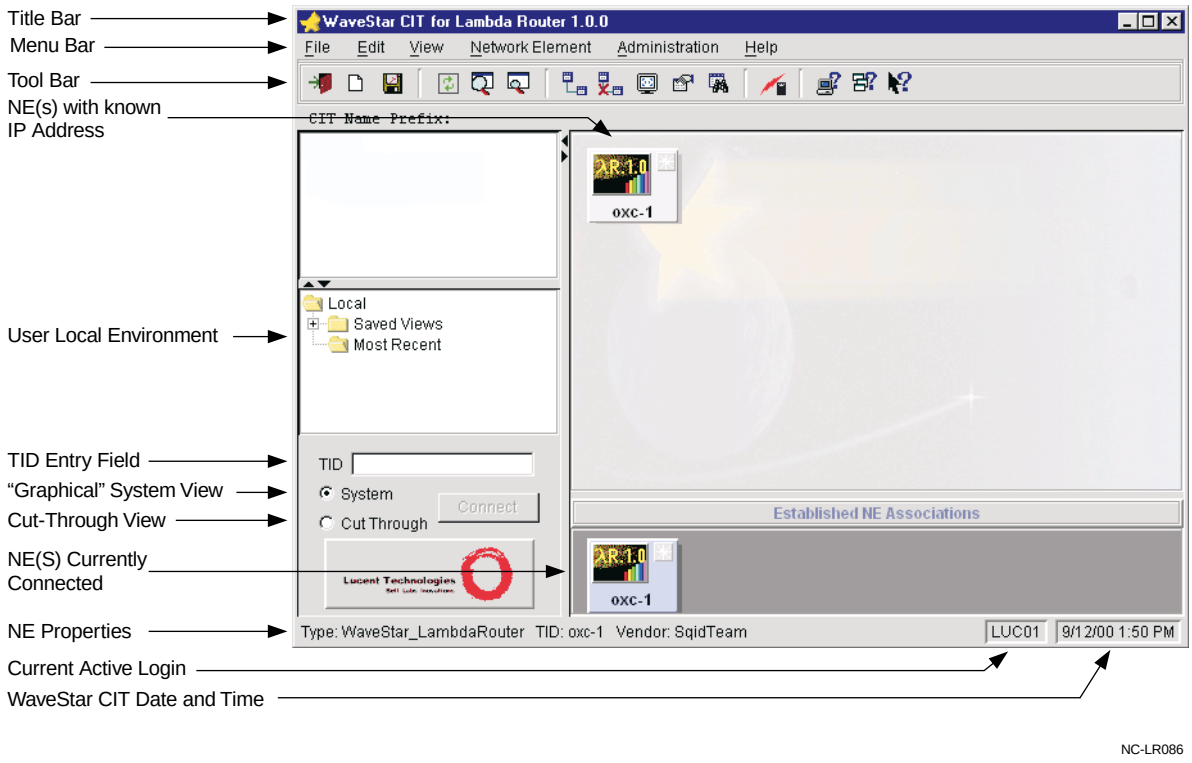
Overview

The WaveStar CIT Network View allows a user to

- perform provisioning tasks on the WaveStar CIT
- view all network elements accessed or previously provisioned with a known TID and IP address
- connect and log into one or more network elements

Network View components

The following figure shows the WaveStar CIT Network View with major components identified.



NC-LR086

The following table provides a brief description of each WaveStar CIT Network View component.

Component	Description
Title Bar	Displays the name and software release number of the WaveStar CIT user interface.
Menu Bar	Provides the drop-down menus used to provision the WaveStar CIT and access network elements.
Tool Bar	Provides one-click access to certain menu commands.
NE(s) with Known IP Addresses	Shows an icon view of each of the network elements with a known TID and IP address that are available for connection.
User Local Environment	Provides an Explorer-like tree view of the local environment. Allows for easy access to saved views and network elements that have been recently connected.
TID Entry Field	Allows for entry of a system Target Identifier (TID) for connection to a network element in either the graphical system view, or the cut-through view.
System View Selection	When selected, manually entering a system TID displays the WaveStar CIT graphical System View for the network element.
Cut-Through View Selection	When selected, manually entering a system TID displays the WaveStar CIT Cut-Through View for the network element.
NE(s) Connected	Displays an icon for each network element to which the WaveStar CIT is currently connected.
NE Properties	Displays network element type, TID, and vendor information for a selected network element.
Current Active Login	Displays the user ID for the currently logged in user.
Date and Time	Displays the current date and time set locally on the WaveStar CIT.

WaveStar CIT Network View Menus

Main menu

The WaveStar CIT Network View Main menu bar has the following menu selections:

- File
- Edit
- View
- Network Element
- Administration
- Help

Each Main menu selection allows the user to perform specific tasks as described in the sections that follow. The currently logged in user must have the appropriate security privilege code to access the Network View menus.

File menu

The File menu allows the user to

- create, delete, and save views in the Saved Views portion of the Network View
- save settings to a specified file
- login as a new user
- exit the WaveStar CIT application

The user must have a security privilege code of S1 or higher to access the File menu selections.

Edit menu

The Edit menu allows the user to

- cut, copy, paste, and delete a selected object from the Network View
- undo the last delete operation
- create a new icon to represent a network element

The user must have a security privilege code of S1 or higher to access the Edit menu selections.

View menu

The View menu allows the user to

- display network elements as large or small icons
- arrange the network element icons by TID, Type, Vendor, or Generic
- refresh the Network View
- configure the WaveStar CIT application default display preferences for the Network View, System View, and the toolbar

The user must have a security privilege code of S1 or higher to access the View menu selections.

Network Element menu

The Network Element menu allows the user to

- connect and disconnect from a selected network element
- disconnect from all connected network elements
- invoke the Cut-Through View for a selected network element
- find a specified network element
- display a properties window for a selected network element

The user must have a security privilege code of S1 or higher to access the Network Element menu selections.

Administration menu

The Administration menu allows the user to

- change the password for the currently logged in user
- perform security administration tasks on the CIT including
  - view all user logins currently administered on the WaveStar CIT
  - add, modify, or delete user login IDs, passwords, and authorization levels (requires a security privilege code of S3 or higher)
- prepare PCMCIA disks (requires a security privilege code of M4 or higher)
- manually enter or change a network element TID and IP address association on the WaveStar CIT (requires a security privilege code of S3 or higher)
- display the current network element TID and IP address list stored on the WaveStar CIT

The user must have a security privilege code of S1 or higher to access the Administration menu selections except as noted above.

Help menu

The Help menu allows the user to

- display the WaveStar CIT application revision and build information
- invoke the Help browser screen, which provides a help index and search capabilities (available in a future release)
- view a list of network element types and releases supported by the WaveStar CIT application
- view online documentation (available in a future release)

The user must have a security privilege code of S1 or higher to access the Help menu selections.

□

Accessing the WaveStar CIT Network View

Before you begin

If provisioning tasks will be performed on a network element, connect the WaveStar CIT to the network element before starting this procedure. If provisioning tasks will be performed only on the WaveStar CIT, no connection to a network element is required.

Task

Complete the following steps to access the WaveStar CIT Network View.

1 With the WaveStar CIT Login Screen displayed (see Accessing the WaveStar CIT Login Screen (A-10)), enter a valid user ID and password and click **OK**.

Result: A Legal Notice Screen appears.

2 Click **OK.**

Result: The Legal Notice Screen closes and the WaveStar CIT Network View appears.

END OF STEPS

Configuring Display Preferences

Before you begin A connection to a network element is not required to perform this task.

Task Complete the following steps to configure the WaveStar CIT display preferences.

1 From the WaveStar CIT Network View Main menu (see Accessing the WaveStar CIT Network View (A-16)), select **View>Preferences**.

Result: The CIT Preferences dialog box appears.

2 Click the **Network View** tab and configure the icon size, screen dividers, and miscellaneous preference settings as required.

3 Click the **System View** tab and configure the alarm format settings as required.

4 Click the **Toolbar** tab and select the toolbar location and the buttons that will be available on the toolbar as required.

5 Click **OK**.

Result: The CIT Preferences dialog box closes and the WaveStar CIT Network View appears. The new settings take effect immediately.

END OF STEPS

□

Refreshing the Network View

Before you begin A connection to a network element is not required to perform this task.

Task Complete the following steps to refresh the Network View.

1 From the WaveStar CIT Network View Main menu (see Accessing the WaveStar CIT Network View (A-16)), select **View>Refresh View**.

Result: The Network View is refreshed (updated).

END OF STEPS

Saving or Creating Network Views

Before you begin A connection to a network element is not required to perform this task.

Task Complete the following steps to save the information being displayed in the Network View.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), save or create a network view.

IF...	THEN...
the information currently displayed in the Network View is being saved to a specified view name	from the Network View Main menu, select **File>Save View As**. **Result:** The Save View As dialog box appears. Continue to Step 2.
a new blank view is being created	from the Network View Main menu, select **File>New View.** **Result:** The New View dialog box appears. Continue to Step 2.

2 Enter the desired name for the view and click **OK**.

Result: The view is saved, and the specified view name appears in the Saved Views directory.

END OF STEPS

Creating Network Element Icons in a Saved Network View

Before you begin

The user must be logged into the WaveStar CIT to display previously saved views. No network connection is required.

Task

Complete the following steps to create network element icons in a saved Network View.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), select **Administration>NE Name/ Address Administration**.

Result: The NE Name/Address Administration dialog box appears.

2 Click **Add**.

Result: The Add IP Address dialog box appears.

3 Enter the TID and IP Address information for the network element and click **APPLY**.

Result: A successful completion message appears.

4 Click **OK**.

Result: The WaveStar CIT Network View appears.

5 With the WaveStar CIT Network View displayed, in the User Local Environment, expand the **Saved Views** path until the desired view name is displayed.

6 Click on the desired view name in the **Saved Views** path.

Result: The selected view is displayed.

7 From the Network View Main menu, select **Edit>New NE**.

Result: The New Icon dialog box appears.

8 Enter the TID for the network element, select the network element type, and click **OK**.

Result: A network element icon is displayed in the Network View for the entered TID.

9 From the Network View Main menu, select **File>Save Settings**.

Result: The current view information is saved.

END OF STEPS

□

Displaying Previously Saved Network Views

Before you begin

The user must be logged into the WaveStar CIT to display previously saved views. No network connection is required.

Task

Complete the following steps to display previously saved Network Views.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), in the User Local Environment, expand the **Saved Views** path until the desired view name is displayed.

2 Click on the desired view name in the **Saved Views** path.

Result: The selected view is displayed.

ND OF STEPS

Deleting Saved Network Views

Before you begin The user must be logged into the WaveStar CIT to display previously saved views. No network connection is required.

Task Complete the following steps to delete saved Network Views.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), in the User Local Environment, expand the **Saved Views** path until the desired view name is displayed.

2 Click on the desired name in the **Saved Views** path.

Result: The selected view is displayed.

3 From the Network View Main menu, select **File>Delete View**.

Result: The selected view is deleted from the **Saved Views** path.

END OF STEPS

Viewing the Most Recent Network Element Connections

Before you begin

The user must be logged into the WaveStar CIT to display the most recent network element connections. No network connection is required.

Task

Complete the following steps to display the most recent network element connections.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), in the User Local Environment, click **Most Recent**.

Result: Icons for the most recent network element connections appear in the Network View.

END OF STEPS

□

Displaying Network Element Properties

Before you begin

The user must be logged into the WaveStar CIT to display the network element properties. No network connection is required.

Task

Complete the following steps to display the properties for a selected network element.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), click on a network element icon.

Result: The network element icon is highlighted.

2 From the WaveStar CIT Network View Main menu, select **Network Element>Properties**.

Result: The NE Properties Screen appears and displays the network element type, TID, and vendor.

3 Click **OK**.

Result: The NE Properties Screen closes and the WaveStar CIT Network View appears.

END OF STEPS

□

Displaying the List of Supported Network Element Types and Releases

Before you begin

The user must be logged into the WaveStar CIT to display the list of supported network elements. No network connection is required.

Task

Complete the following steps to display the list of network element types and releases supported by the WaveStar CIT.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), select **Help>Supported NEs**.

Result: The Supported NEs list box appears.

2 View the list of supported network element types and releases. Click **OK** when complete.

END OF STEPS

Accessing the System View

Before you begin The WaveStar CIT must be connected to the network and the user must be logged into the WaveStar CIT to access the System View.

Task Complete the following steps to access the System View.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), select a network element to display in the System View.

IF the network element icon...	THEN...
is currently displayed in the Network View	double-click on the network element icon. **Result:** If the network element has been provisioned with two IP addresses, the IP Address Selection Screen appears. Continue to Step 2. **Result:** If the network element has been provisioned with one IP address, the Network Element Login Screen appears. Continue to Step 3.
is not currently displayed in the Network View	enter the TID for the network element in the **TID** field, select the **System** radio button, then click **Connect**. **Result:** If the network element has been provisioned with two IP addresses, the IP Address Selection Screen appears. Continue to Step 2. **Result:** If the network element has been provisioned with one IP address, the Network Element Login Screen appears. Continue to Step 3.

2 Select the IP address to use for the connection and click **OK**.

Result: The Network Element Login Screen appears.

3 Enter a valid network element user ID and password and click **OK**.

Result: A Legal Notice appears.

4 Click **OK**.

Result: The Legal Notice closes and the System View for the selected network element appears. All bays in the network element are displayed.

END OF STEPS

□

Accessing the Cut-Through View

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into the WaveStar CIT to access the Cut-Through View.

Task

Complete the following steps to access the Cut-Through View.

1 With the WaveStar CIT Network View displayed (see Accessing the WaveStar CIT Network View (A-16)), select a network element.

IF the network element TID...	THEN...
is currently displayed as an icon in the Network View	right-click on the network element icon and select **Cut-Through** from the pop-up menu. Continue to Step 3.
is not currently displayed in the Network View and will be manually entered	enter the TID for the network element in the **TID** field, select the **Cut-Through** radio button, then click **Connect**. Continue to Step 3.
is not currently displayed in the Network View and will be selected from a list of TIDs	from the Network View Main menu, select **Network Element>Cut-Through**. **Result:** The NE Cut-Through List dialog box appears. Continue to the next step.

2 Select either the **directory** or **Local data store** radio button to display a list of known TIDs. Select a TID from the Found box, then click **Cut-Through**.

3

IF the network element...	THEN...
has been provisioned with two IP addresses	the IP Address Selection Screen appears. Continue to the next step.
has been provisioned with one IP address	continue to Step 5.

4 Select the IP address to use for the connection and click **OK**.

5

IF...	THEN...
the No Listbox File Exist error message appears	click **OK** to clear the message. The error message is just a warning. Cut-Through can work without the Listbox File.
the Cut-Through window appears	the connection is established.

6 Enter `ACT-USER:<tid>:<loginid>:<ctag>::<password>;` in the TL1 Command Entry Field, or select the ACT-USER command from the Cut-Through Window List Box and edit the command line to include the network element TID and a valid User ID and Password, and click **Send**.

Result: The cut-through login session is established.

END OF STEPS

□

WaveStar CIT System View

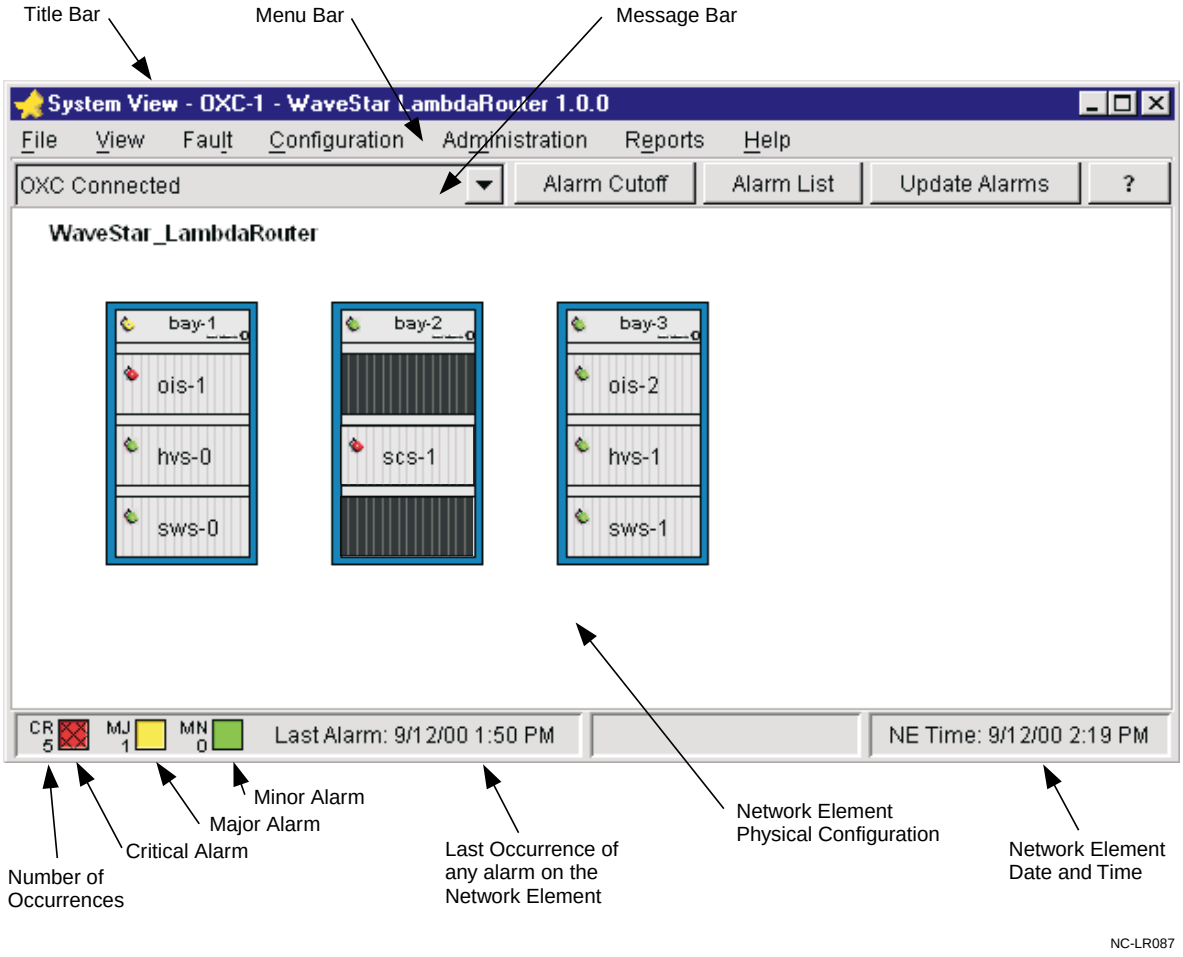
Overview

The WaveStar CIT System View allows a user to

- display a graphical view of the physical configuration of a network element
- perform system and user provisioning tasks on a network element
- display shelf and circuit pack details for a network element
- perform cross-connection operations
- backup and restore software and the database
- execute and release protection switching
- change the network element primary state
- view reports and logs for a network element
- restart a network element

System View components

The following figure shows the WaveStar CIT System View with major components identified.



The following table provides a brief description of each WaveStar CIT System View component.

Component	Description
Title Bar	Displays the type and TID of the network element, and the software release number of the network element.
Menu Bar	Provides the drop-down menus used to provision the network element.
Message Bar	Provides a history of messages received in response to commands. Buttons are also provided for Alarm Cutoff, Alarm List, and Update Alarms.
Network Element Configuration	Shows an icon view of each of the physical configuration of a network element. Each shelf is shown with an alarm LED to indicate the highest level alarm for that shelf.
Alarm Indicators	Provides visual indications of Critical, Major, and Minor alarms anywhere within the network element. The number of occurrences for each alarm type is also displayed.
Last Alarm	Displays the date and time of the last occurrence of any alarm on the network element.
Date and Time	Displays the current date and time set on the network element.

WaveStar CIT System View Menus

Main menu

The WaveStar CIT System View Main menu bar has the following menu selections:

- File
- View
- Fault
- Configuration
- Administration
- Reports
- Help

Each Main menu selection allows the user to perform specific tasks as described in the sections that follow. The currently logged in user must have the appropriate security privilege code on the network element to access the System View menus.

File menu

The File menu allows the user to

- enable and disable TL1 logging
- set or change the TL1 logging file (requires a security privilege code of S3 or higher)
- disconnect from the network element

The user must have a security privilege code of S1 or higher to access the File menu selections except as noted above.

View menu

The View menu allows the user to

- display the network element system view consisting of all bays and shelves
- display a shelf view of the network element
- display equipment details
- display protection group information
- display cross-connections
- display a loopback connection list
- display controller complex details
- display a list of stored software generics
- display a list of network element data files

- display an overview of the software and data stored on the network element
- refresh the System View to display current equipage information

The user must have a security privilege code of S1 or higher to access the View menu selections.

Fault menu

The Fault menu allows the user to

- retrieve and display current alarms from the network element (requires a security privilege code of M1 or higher)
- retrieve and display network element alarm information from a specified start date and time (requires a security privilege code of M1 or higher)
- manually invoke protection switching
- return equipment to, or remove equipment from service
- operate and release loopback connections
- test network element LEDs and office alarms (requires a security privilege code of T4 or higher)
- reset a network element DCC circuit pack, OIS or HVS shelf, or the entire network element
- cut-off audible alarms (requires a security privilege code of M3 or higher)

The user must have a security privilege code of M4 or higher to access the Fault menu selections except as noted above.

Configuration menu

The Configuration menu allows the user to

- provision a network element shelf or circuit pack
- create new shelves or circuit packs in a network element
- delete shelves or circuit packs from a network element
- create, modify, or delete cross-connections
- perform software related tasks including (requires a security privilege code of S3 or higher)
  - remote backup and restore
  - copy non-volatile memory (NVM) cards
  - download and install software generics

The user must have a security privilege code of P3 or higher to access the Configuration menu selections except as noted above.

Administration menu

The Administration menu allows the user to

- change the password for the currently logged in user
- view session information for the currently logged in user
- view user logins and logged-in users
- forcibly log out a user
- add, modify, and delete users (requires a security privilege code of S5)
- set system-wide security parameters for a network element
- view the network element TCP/IP configuration
- set or change the TID for a network element (requires a security privilege code of S3, P3 or higher)
- provision network element system parameters (requires a security privilege code of P3, M3 or higher)
- set the system configuration (requires a security privilege code of P3 or higher)
- set or change the IP addresses for a network element (requires a security privilege code of S4 or higher)

The user must have a security privilege code of S1 or higher to access the Administration menu selections except as noted above.

Reports menu

The Reports menu allows the user to

- view shelf, circuit pack, and port equipment lists (requires a security privilege code of S1, P1 or higher)
- view cross-connection lists for selected end points (requires a security privilege code of P3 or higher)
- view alarm lists (requires a security privilege code of S1, M1 or higher)
- view the alarm log (requires a security privilege code of S3, M3 or higher)
- view the protection switch activity log
- view the user login/logout activity log
- view the network element security log (requires a security privilege code of S5)
- view the notification log

The user must have a security privilege code of S3 or higher to access the Reports menu selections.

Help menu

The Help menu allows the user to

- display the network element TID, configuration, and release
- invoke the Help browser screen, which provides a help index and search capabilities (available in a future release)
- view online documentation (available in a future release)

The user must have a security privilege code of S1 or higher to access the Help menu selections.

Refreshing the System View

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into a network element to refresh the System View.

Task

Complete the following steps to refresh the System View.

1 From the WaveStar CIT System View Main menu (see Accessing the System View (A-27)), select **View**>**Refresh Equipment**.

Result: The Equipment Selection Screen appears.

2 Enter an AID for the desired equipment, or use the NE Explorer to select the equipment clicking on the plus (+) sign next to each entity.

3 Highlight the required equipment and click **Select**.

Result: The System View is refreshed (updated) to display current equipage information.

ND OF STEPS

□

Viewing the Command Response History

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into a network element to view the command response history.

Task

Complete the following steps to view the command response history.

1 With the WaveStar CIT System View displayed (see Accessing the System View (A-27)), click on the Message bar.

Result: The Message bar expands to display all command responses received during the current login session.

2 When viewing of the Command Response History is complete, click on the Message bar in the System View.

Result: The Message bar collapses and displays the most recent command response received.

END OF STEPS

Enabling and Disabling TL1 Logging

Before you begin The WaveStar CIT must be connected to the network and the user must be logged into a network element to enable or disable TL1 logging.

Task Complete the following steps to enable or disable TL1 logging.

1 Access the WaveStar CIT System View.

Reference: Accessing the System View (A-27).

2

IF TL1 logging...	THEN...
is not currently enabled and is being enabled	from the System View Main menu, select **File>Enable TL1 Logging**. **Result:** The Enable TL1 Logging Screen appears. Continue to Step 3.
is currently enabled and is being disabled	from the System View Main menu, select **File>Disable TL1 Logging**. **Result:** TL1 commands will no longer be saved to the log file. *Stop! End of Task*.
is currently enabled and the TL1 log file is being changed	from the System View Main menu, select **File>Set/Change TL1 Logging File**. **Result:** The Set/Change TL1 Logging File Screen appears. Continue to Step 3.

3 Select the path for the log file and enter the log file name in the File Name field, then click **Use as Log File**.

Result: All TL1 commands will now be saved to the specified file.

N D O F S T E P S

□

Accessing the Network Element Shelf View

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into the WaveStar CIT to access the Shelf View.

Task

Complete the following steps to access the Network Element Shelf View.

1 With the WaveStar CIT System View displayed (see Accessing the System View (A-27)), double-click on the shelf to display in the Network Element Shelf View.

Result: The Shelf View Screen appears and displays each circuit pack and slot in the selected shelf.

END OF STEPS

□

WaveStar CIT Network Element Shelf View

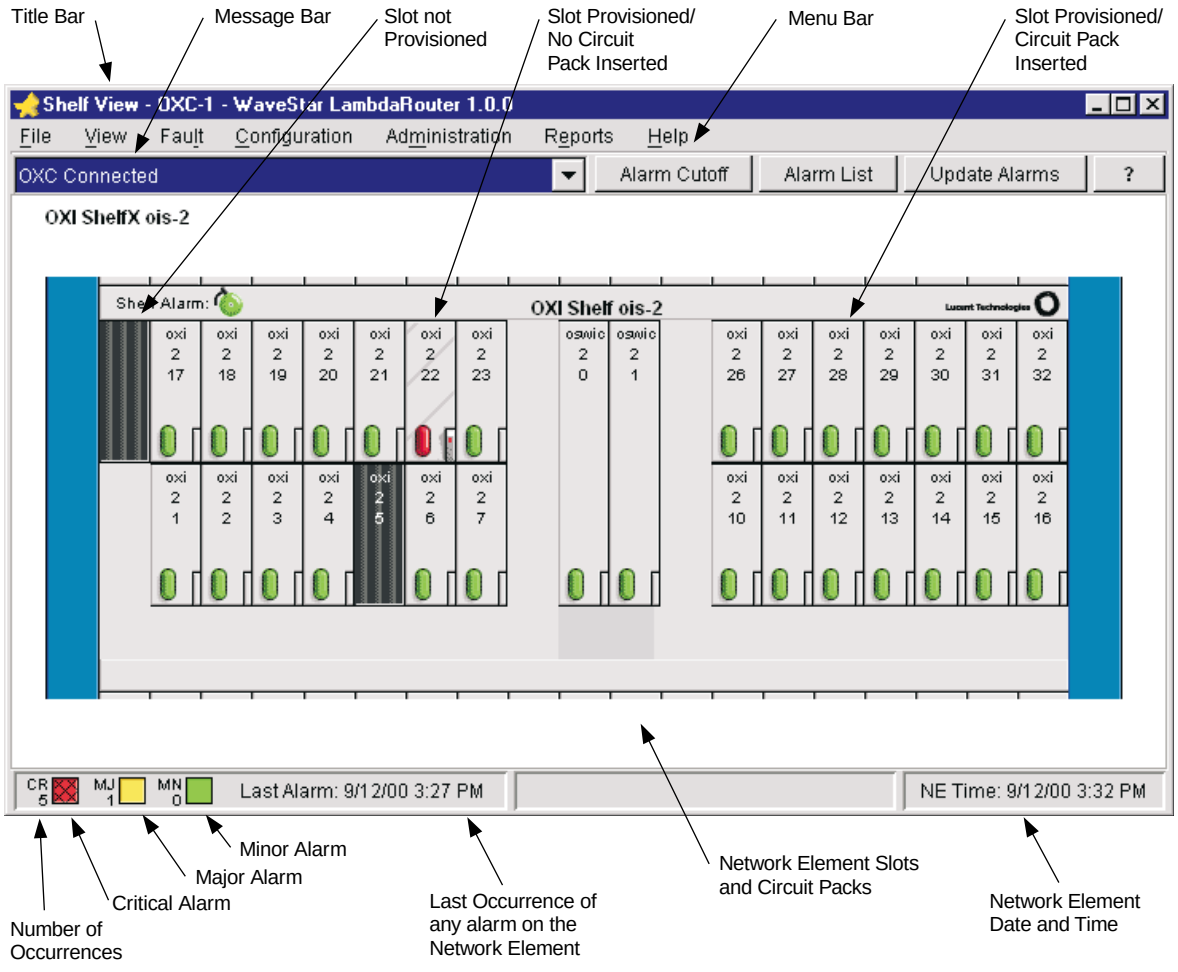
Overview

The WaveStar CIT Network Element Shelf View allows a user to

- view a graphical representation of a shelf, and the circuit packs in the shelf, within the network element
- access the shelf, individual circuit packs, or ports (when equipped) to view information for, or provision, the shelf, circuit packs, or ports
- view protection information for circuit packs in the shelf (when applicable)
- invoke a protection switch (when applicable)

Network Element Shelf View components

The following figure shows the WaveStar CIT Network Element Shelf View with major components identified.



The following table provides a brief description of each WaveStar CIT Network Element Shelf View component.

<table>
<tr><th>Component</th><th colspan="2">Description</th></tr>
<tr><td>Title Bar</td><td colspan="2">Displays the type and TID of the network element, and the software release number of the network element.</td></tr>
<tr><td>Menu Bar</td><td colspan="2">Provides the drop-down menus used to provision the network element.</td></tr>
<tr><td>Message Bar</td><td colspan="2">Provides a history of messages received in response to commands.</td></tr>
<tr><td rowspan="5">Slots and Circuit Packs</td><td colspan="2">Shows an alarm LED to indicate the highest level alarm for the shelf, and the name and a graphical representation of each slot and circuit pack in the shelf.
The appearance of the slot provides an indication of how the slot is equipped:</td></tr>
<tr><td>IF the slot appears...</td><td>THEN...</td></tr>
<tr><td>black (empty)</td><td>the slot is not provisioned.</td></tr>
<tr><td>as a circuit pack with diagonal lines across the faceplate</td><td>the slot is provisioned but a circuit pack is not inserted.</td></tr>
<tr><td>as a circuit pack faceplate</td><td>the slot is provisioned and a circuit pack is inserted.</td></tr>
<tr><td>Ports</td><td colspan="2">Provide visual indications of the ports available on optical cross-connect interface circuit packs (WaveStar LambdaRouter 128/256 Release 2.0 only).</td></tr>
<tr><td>Alarm Indicators</td><td colspan="2">Provide visual indications of Critical, Major, and Minor alarms anywhere within the network element. The number of occurrences for each alarm type is also displayed.</td></tr>
<tr><td>Last Alarm</td><td colspan="2">Displays the date and time of the last occurrence of any alarm on the network element.</td></tr>
<tr><td>Date and Time</td><td colspan="2">Displays the current date and time set on the network element.</td></tr>
</table>

□

WaveStar CIT Network Element Shelf View Menus

Main menu

The WaveStar CIT Network Element Shelf View Main menu bar has the following menu selections:

- File
- View
- Fault
- Configuration
- Administration
- Reports
- Help

The Main menu selections are functionally the same as those available from the Network Element Shelf View Main menu. For information, see WaveStar CIT System View Menus (A-34).

Displaying Shelf and Circuit Pack Details

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into a network element to display shelf, circuit pack, and port information.

Task

Complete the following steps to display shelf, circuit pack, and port information.

1 With the WaveStar CIT Network Element Shelf View displayed (see Accessing the Network Element Shelf View (A-41)), display detail information for the shelf or for a slot/circuit pack.

IF displaying information for a...	THEN
shelf	right-click with the screen pointer positioned anywhere within the shelf EXCEPT over a slot. **Result:** A pop-up menu appears.
slot/circuit pack	right-click with the screen pointer positioned over the desired slot/circuit pack. **Result:** A pop-up menu appears.
port (WaveStar LambdaRouter 128/256 Release 2.0 only)	right-click with the screen pointer positioned over the desired port. **Result:** A pop-up menu appears.

2 Select **View Details** from the pop-up menu.

Result: The View Details Screen for the selected object appears.

3 Click **Close**.

Result: The View Details Screen closes and the Network Element Shelf View appears.

END OF STEPS

Refreshing the Network Element Shelf View

Before you begin

The WaveStar CIT must be connected to the network and the user must be logged into a network element to refresh the Network Element Shelf View.

Task

Complete the following steps to refresh the Network Element Shelf View any time the network element configuration or status may have changed since the last time the WaveStar CIT retrieved the network element information.

1 With the WaveStar CIT Network Element Shelf View displayed (see Accessing the Network Element Shelf View (A-41)), refresh the shelf view or an individual slot in the shelf.

IF refreshing a...	THEN...
shelf	right-click with the screen pointer positioned anywhere within the shelf EXCEPT over a slot. **Result:** A pop-up menu appears.
slot/circuit pack	right-click with the screen pointer positioned over the slot/circuit pack to be refreshed. **Result:** A pop-up menu appears.

2 Select the appropriate refresh option from the pop-up menu.

IF refreshing a...	THEN...
shelf	select **Refresh Shelf**. **Result:** A Confirmation dialog box appears.
slot/circuit pack	select **Refresh Circuit Pack**. **Result:** The circuit pack is refreshed (updated) to display current equipage information. *Stop! End of Task.*

3 Click **Yes.**

Result: The Network Element Shelf View is refreshed (updated) to display current equipage information.

ND OF STEPS

□

Returning to the Network Element System View

Before you begin

The WaveStar CIT must be connected to the network, the user must be logged into a network element, and a Shelf View must be currently displayed.

Task

Complete the following steps to return to the Network Element System View from the Network Element Shelf View.

1 From the WaveStar CIT Network Element Shelf View Main menu (see Accessing the Network Element Shelf View (A-41)), select **View> System View Display.**

Result: The Network Element Shelf View closes and the Network Element System View appears.

END OF STEPS

WaveStar CIT Cut-Through View

Overview

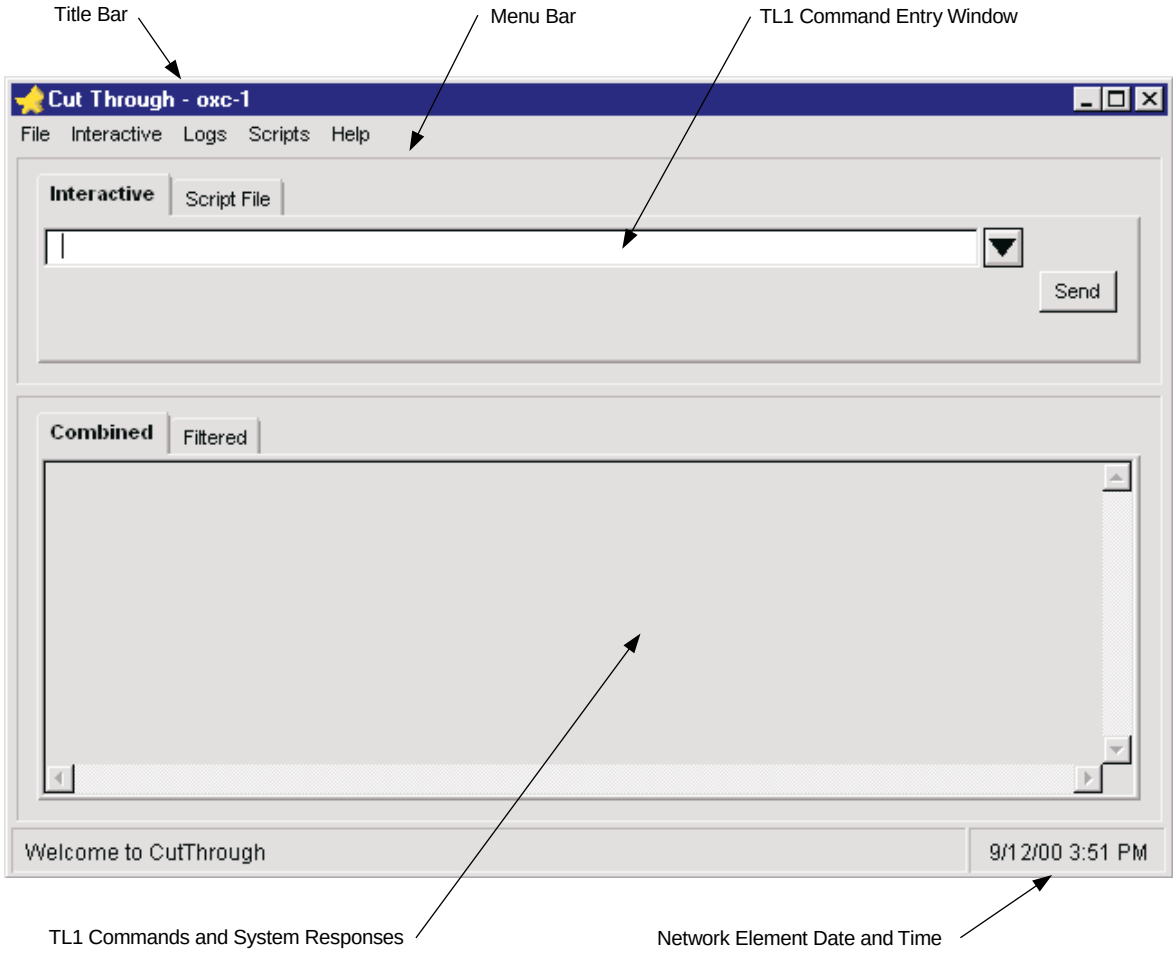
The WaveStar CIT Network Cut-Through View allows a user to bypass the graphical user interface and manually execute TL1 commands on a network element.

The TL1 commands may be executed either one at a time (interactive mode) or as part of a script.

Cut-Through View components

Important! When performing provisioning tasks with the graphical user interface, warnings are generated to inform the user if an action may have service affecting results. No service affecting warnings are generated when using the Cut-Through View.

The following figure shows the WaveStar CIT Cut-Through View with major components identified.



The following table provides a brief description of each WaveStar CIT Cut-Through View component.

Component	Description	
Title Bar	Displays the TID of the selected network element.	
Menu Bar	Provides the drop-down menus used to execute TL1 commands and scripts.	
TL1 Command Entry	Allows the user to manually enter TL1 commands, select TL1 commands from a list, or select a TL1 command script.	
TL1 Commands and System Responses	Displays the TL1 commands and the system responses to the commands. There are two display modes: combined and filtered.	
	Mode	**Description**
	Combined	Displays commands in the order in which they are sent along with system responses as they are received. In this mode, the commands and their associated responses may be separated by other commands and responses.
	Filtered	Displays sent commands only after a system response to the command is received. Autonomous messages are displayed in a separate window.
Date and Time	Displays the current date and time set on the network element.	

□

WaveStar CIT Cut-Through View Menus

Main menu

The WaveStar CIT Cut-Through View Main menu bar has the following menu selections:

- File
- Interactive
- Logs
- Scripts
- Help

Each Main menu selection allows the user to perform specific tasks as described in the sections that follow. The currently logged in user must have the appropriate security privilege code on the network element to access the Cut-Through View menus.

File menu

The File menu allows the user to exit the Cut-Through View.

The user must have a security privilege code of S1 or higher to access the File menu selections.

Interactive menu

The Interactive menu allows the user to

- select and edit TL1 listbox files
- add the last command to a listbox file

The user must have a security privilege code of S1 or higher to access the Interactive menu selections.

Logs menu

The Logs menu allows the user to

- start and stop TL1 logging
- view the TL1 log
- enter a time and date stamp in the TL1 log

The user must have a security privilege code of S1 or higher to access the Logs menu selections.

Scripts menu

The Scripts menu allows the user to

- create a new TL1 command script
- run a TL1 command script
- stop a currently running TL1 command script

The user must have a security privilege code of S1 or higher to access the Scripts menu selections.

Help menu

The Help menu allows the user to display the current software release and build information for the WaveStar CIT application.

The user must have a security privilege code of S1 or higher to access the Help menu selections.

Entering TL1 Commands in Interactive Mode

Task Complete the following steps to enter TL1 commands in interactive mode.

1 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)), enter or select a TL1 command in the **TL1 Command Entry** field.

IF...	THEN...
manually entering a TL1 command	type the TL1 command in the **TL1 Command Entry** field. Continue to Step 2.
selecting a TL1 command from a list	click the down-arrow located beside the **TL1 Command Entry** field to display a drop-down list of TL1 commands, then select the desired TL1 command from the list. **Result:** The selected command appears in the **TL1 Command Entry** field.

2 Click **Send**.

Result: The result of the TL1 command execution is dependant upon the command response mode. See Changing TL1 Command Response Mode (A-55).

3

IF...	THEN...
the command response mode is Combined	the TL1 command appears in the TL1 Command/Response window. The system response is displayed when it is received.
the command response mode is Filtered	the TL1 command is displayed in the TL1 Command/Response window when the system response to the command is received.

4 Repeat this task as necessary to enter additional TL1 commands in interactive mode.

N D O F S T E P S

□

Changing TL1 Command Response Mode

Task Complete the following steps to change the TL1 command response mode to either Combined or Filtered.

1 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)) select the desired TL1 command response mode.

IF setting the command response mode to...	THEN...
combined	click the **Combined** tab located above the TL1 Command/Response window.
filtered	click the **Filtered** tab located above the TL1 Command/Response window.

2 Execute TL1 commands as required.

IF...	THEN...
executing TL1 commands in Interactive mode	see Entering TL1 Commands in Interactive Mode (A-53).
executing a TL1 command script	see Running a TL1 Command Script (A-58).

END OF STEPS

Creating a TL1 Command Script

Task Complete the following steps to create a TL1 command script.

1 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)), select **Scripts>New** from the Main menu.

Result: A warning message is displayed indicating that ASCII text is the only file format supported.

2 Click **OK**.

Result: The *Microsoft Windows*® Notepad appears.

3 Enter the TL1 commands in the script file as required.

Note the following:

- one TL1 command is allowed per line
- the command script may contain any number of lines
- lines beginning with // are ignored

4 When the script is complete, from the Notepad Main menu, select **File>Exit**.

Result: A Confirmation message is displayed asking if the changes should be saved.

5 Click **Yes**.

Result: The SaveAs dialog box appears.

6 Enter a name for the command script, select the destination directory, and click **Save**.

Result: The command script is saved and the SaveAs dialog box closes.

ND OF STEPS

□

Running a TL1 Command Script

Task Complete the following steps to run a TL1 command script.

1 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)), select **Scripts>Run** from the Main menu.

Result: The Run TL1 Script File dialog box appears.

2 Enter the path and filename for the TL1 command script, or click **Browse** to select the script file.

3 Click **OK**.

Result: The Select TL1 Script Execution Mode dialog box appears.

4 Select the TL1 script execution mode.

IF...	THEN...
Pause and Prompt Each Command is selected	the script will pause after each command is sent.
Stop on Deny from NE is selected	the script will stop executing commands if a deny is received from the network element.
Send All Commands is selected	all script commands will be sent to the network element.

5 Click **OK**.

Result: The TL1 command script begins executing.

6

IF the execution mode is...	THEN...
Pause and Prompt Each Command	the script pauses after each command is sent and a dialog box appears asking if the next command should be sent. Continue to Step 7.
Stop on Deny from NE	all commands are sent to the network element. Continue to Step 8.
Send All Commands	all commands are sent to the network element. After the last command is sent, a Warning message appears. Continue to Step 9.

7

IF...	THEN...
the next command should be executed	click **Yes**. Repeat Step 7 for each command. **Result:** When the last command has been sent to the network element, a Warning message appears. Continue to Step 9.
the next command should not be executed	click **No**. **Result:** Execution of the command script is aborted and a Warning message appears. Continue to Step 9.

8

IF...	THEN...
no Deny is received from the network element.	all commands are sent to the network element. After the last command is sent, a Warning message appears.
a Deny is received from the network element.	execution of the command script is aborted and a Warning message appears.

9 Click **OK**.

Important! Continue to monitor the TL1 Command/Response window for responses received from the network element.

Result: The Warning message closes and the Cut-Through View appears.

END OF STEPS

Stopping a Running TL1 Command Script

Task Complete the following steps to stop a running TL1 command script.

1 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)) and a TL1 command script running, select **Scripts>Stop** from the Main menu.

Result: A Confirmation dialog box appears.

2 Click **Yes**.

Result: The command script aborts and a Warning message appears.

3 Click **OK**.

Result: The Warning message closes and the Cut-Through View appears.

END OF STEPS

Exiting the WaveStar CIT Cut-Through View

Task Complete the following steps to exit the WaveStar CIT Cut-Through View.

1 Enter `CANC-USER:<tid>::logoff;` in the TL1 Command Entry Field, or select the CANC-USER command from the Cut-Through Window List Box and edit the command line to include the network element TID as appropriate, and click **Send**.

Result: The login session is terminated.

2 With the WaveStar CIT Cut-Through View displayed (see Accessing the Cut-Through View (A-29)), select **File>Exit** from the Main menu.

Result: A Confirmation dialog box appears.

3 Click **Yes**.

Result: The Cut-Through View closes and the WaveStar CIT Network View appears.

END OF STEPS

□

Appendix B: Operations Interfaces

Overview

Purpose

This appendix describes the WaveStar LambdaRouter 128/256 operations interfaces.

Contents

General

Introduction

There are remote and local operations interfaces supported by the WaveStar LambdaRouter 128/256, which provide for provisioning, administration, and maintenance functions.

The local operations interfaces consist of the WaveStar (CIT) Craft Interface Terminal and RS-232 terminal access. The remote operations interfaces include the WaveStar Optical Service Manager (OSM) and WaveStar SubNetwork Management System (SNMS).

The operations interface employs standard Transaction Language 1 (TL1) messaging transported by means of the TCP/IP protocol stack via a 10BaseT physical LAN interface. The system also provides local alarm indications and an interface to the local office alarm grid.

The WaveStar LambdaRouter 128/256 supports File Transfer Protocol (FTP) for WaveStar LambdaRouter 128/256-to-Managing-System file transfers of generic and database files. The WaveStar implementation of FTP follows IETF STD 0009.

The WaveStar LambdaRouter 128/256 supports a single method of user interface accessible by the WaveStar SNMS and WaveStar CIT. These operations interfaces provide:

- a fully functional GUI through which most WaveStar LambdaRouter 128/256 tasks can be performed
- local/remote access control based on user privilege levels (password protected)
- network discovery and exploration for easy access to each network element in the local network
- displays of the WaveStar LambdaRouter 128/256 equipment and their states
- displays alarms
- support for user provisioning tasks
- support for software upgrades and backup and restore functions
- generation of equipage, cross-connection, and state reports.

Communication interface

The interface between the WaveStar LambdaRouter 128/256 and the operations environment—the WaveStar CIT, WaveStar SNMS, WaveStar OSM or other Managing System—is provided by the 802.3 compliant 10BaseT LAN.

One to three LAN connections can be used to interface to the customer's intraoffice (IAO) LAN. If an external hub is used on one of the LAN connectors, the number of possible LAN connections is increased. With external hubs, the number of possible LAN connections depends on the size and number of hubs used. For example, with a sixteen-port hub, the total number of available ports is the 15 ports in the hub plus the remaining three LAN connection ports.

If an external hub is used, it is connected to EI1 port 4 on the SCS.

□

WaveStar CIT

Description

The WaveStar CIT is a desktop or laptop computer loaded with the required WaveStar LambdaRouter 128/256 software. It provides the following:

- A GUI based on *Windows NT*® or *Windows*® 2000 Professional
- Transaction Language 1 (TL1) interface to the network element
- TL1 command entry cut-through
- Access connections
- Security features to prevent unauthorized access.

The WaveStar CIT GUI provides an easy and intuitive access to operations. When this GUI is used the TL1 interface is not visible to the user. Many customers develop standardized scripts for use in the field for standard operations.

The WaveStar CIT user has the means for local and remote access with the CIT. Remote access uses an external WAN connection to the WaveStar LambdaRouter 128/256's LAN port.

The WaveStar CIT is generally co-located with the WaveStar LambdaRouter 128/256. The WaveStar CIT PC can be connected directly to the front of the WaveStar LambdaRouter 128/256 frame. This connection can also be made over the IAO LAN.

The WaveStar CIT provides detailed information and control of the following:

- Provisioning
- Loopback operation and testing
- Reporting
- Alarms
- Equipment view and status
- Cross-connect assignments
- Protection switching.

PCMCIA card

The PC or laptop computer must be equipped with a 10BaseT interface network card to communicate with the network element, and a drive that supports a PCMCIA card to create a flash card that will be inserted into the WaveStar LambdaRouter 128/256.

Remote access

A WaveStar CIT or other managing system connected to a WaveStar LambdaRouter 128 or WaveStar LambdaRouter 256 may remotely access other WaveStar LambdaRouter 128s and WaveStar LambdaRouter 256s on the network. The support capabilities are the same for both local and remote WaveStar LambdaRouter 128/256 systems.

Remote access requires TCP/IP connectivity from the local WaveStar LambdaRouter 128 or WaveStar LambdaRouter 256 to the remote WaveStar LambdaRouter 128 or WaveStar LambdaRouter 256. File transfers are accomplished by means of FTP.

□

WaveStar Optical Service Manager (OSM)

Description

The WaveStar OSM communicates with all the WaveStar LambdaRouter 128/256 in a network to perform centralized end-to-end service provisioning and restoration across the network. The WaveStar OSM has a GUI and is used to set up network-wide optical paths and to calculate and assert restoration paths in response to network transmission failures.

The user logs on to the WaveStar LambdaRouter 128/256, in a fashion similar to that for the WaveStar SNMS, through the WaveStar OSM user interface. The WaveStar LambdaRouter 128/256 recognizes the user and logs session activities and performs other critical interactions.

Features

The following features are available in the WaveStar OSM:

- optical cross-connect management
- multiple Quality of Service (QoS) service provisioning
- end customer GUI and service provider GUI
- end customer optical VPN management
- point-and-click, web-based user interface
- centralized restoration.

WaveStar SNMS

Description

The WaveStar SNMS is an element management system (EMS) that supports the WaveStar LambdaRouter 128/256 through LAN connectivity and centralized element management functions. The WaveStar SNMS has a GUI and communicates with the WaveStar LambdaRouter 128/256 using TL1 messages. The WaveStar SNMS communicates with each WaveStar LambdaRouter 128 and WaveStar LambdaRouter 256 individually.

When used as an end-user system, WaveStar SNMS provides a Java®-based GUI for users to access and manage a WaveStar LambdaRouter 128/256 system with visibility down to the circuit pack and port levels. As an end-user system, WaveStar SNMS provides element management functions including fault, configuration, and security management.

After a successful login, the WaveStar SNMS then logs session activities and performs other critical interactions.

WaveStar NMS

Description

The WaveStar Network Management System (NMS) is a management tool that provides comprehensive and integrated management of an entire transport network. WaveStar NMS can provide provisioning and maintenance management for the WaveStar LambdaRouter 128/256s and other network elements in the WaveStar LambdaRouter 128/256 network.

The WaveStar NMS interfaces with other systems, such as WaveStar SNMS, to provide complete network management from a single point.

Refer to the documentation provided with WaveStar NMS for additional information.

□

RS-232 Terminal Access

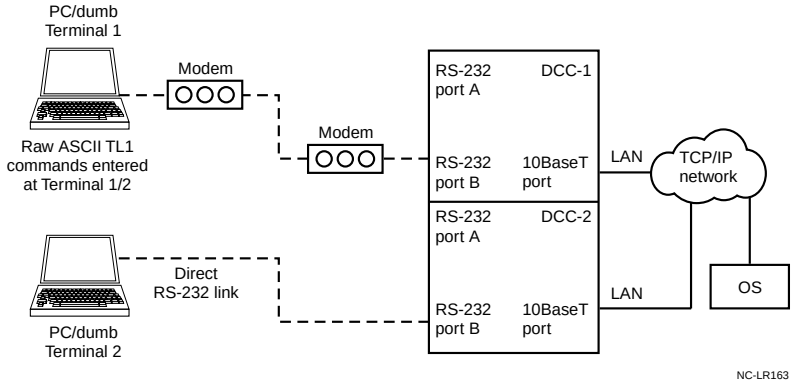
Description

The RS-232 terminal access feature allows a WaveStar LambdaRouter 128/256 system to be provisioned using TL1 commands issued from a dumb terminal or personal computer running terminal emulation software.

Connection

The terminal is connected, either directly using an RS-232 null modem cable or via modem, to one of the WaveStar LambdaRouter 128/256 dual independent RS-232 serial ports located on the System Controller Shelf (SCS). An RS-232 adapter cable is used to connect the terminal to the SCS. The adapter cable splits the DB25 connection on the SCS into two DB9 connectors.

The following figure illustrates the connection of a terminal to the WaveStar LambdaRouter 128/256 using both a direct null modem link and a modem link.



To access the RS-232 interface, the terminal must initially be configured as follows:

Parameter	Setting
Bits Per Second	19200
Data Bits	8
Parity	N (none)
Stop Bits	1

After the initial connection, the Bits Per Second parameter can be changed.

Access considerations

Security parameters, as provisioned on the WaveStar LambdaRouter 128/256, apply to the RS-232 connection. Users must log in prior to issuing TL1 commands, and may only issue TL1 commands for which they have adequate security privilege levels.

When using the RS-232 terminal access link, due to the relatively slow speed of the connection, it is recommended that autonomous messages be limited.

□

Appendix C: Abbreviations and Acronyms

Numerics

10BT 10 Base T

10G 10 Gigabits per second

100BT 100 Base T

2G/2.5G 2.5 Gigabits per second

A

ABN Abnormal

ACO Alarm Cut-Off

ACO/TST Alarm Cut-Off and Test

ACT Active

ACTY Activity

ADC Analog-to-Digital Converter

AID Access Identifier

AINS Automatic In-Service

AIS Alarm Indication Signal

AlS-L Alarm Indication Signal-Line

AIS-MS Alarm Indication Signal-Multiplex Section

ALM Alarm

ANR Abnormal

ANSI American National Standards Institute

APP Apparatus Code

APR Automatic Power Reduction

ARP Address Resolution Protocol

ARST Autonomous Reset

ASCII American Standard Code for Information Interchange

ASIC Application-Specific Integrated Circuit

ATM Asynchronous Transfer Mode

ATTR Attribute

B

BBE Background Block Error

BER Signal Degrade B2 Bit Error Rate

BIP Bit Interleaved Parity

BT Base-T

C

CARES Customer Assistance Request Entry System

CC Communication Client

CCD CTLI-D Controller Device

CIC Customer Information Center

CIT Craft Interface Terminal

CLEI Common Language™ Equipment Identifier

CO Central Office

COM Common

CONTR Controller

CP Circuit Pack

CP-ID Circuit Pack Identifier

CPF Circuit Pack Failure

CPLD Complex Programmable Logic Device

CPU Central Processing Unit

CR Critical

CSA Canadian Standards Association

CSIEX Control System Interface Expander

CSMA/CD Carrier Sense Multiple Access/Collision Detect

CSR Composite Service Request

CTL Controller

CTLI-D Control Interface to Devices

CV Coding Violation

D

DAC Digital-to-Analog Converter

DATAFLT Database Fault

DBCHG Database Change

DCC Data Communications Controller; Data Communications Channel

DCE Data Communications Equipment

DCN Data Communications Network

DHCP Dynamic Host Configuration Protocol

DLC Download Client

DLS Download Server

DNS Domain Name Server

DOS Detection of Signal

DTE Data Terminal Equipment

DTP Data Transfer Process

DVM Digital Voltage Meter

DWDM Dense Wavelength Division Multiplexing

E

EB Errored Block

EBER Signal Fail B2 Excessive Bit Error Rate

ECI Equipment Catalog Item

ECS Express Connection Service

EEPROM Electrically Erasable Programmable Read Only Memory

EI External Interface

EIS Engineering Information Standards

ELSR Edge Label Switched Router

EM Equipment Management

EMI Electromagnetic Interference

EMS Element Management System

EO Expansion Operations Network

EOF End of File

EOL End of Line

EOR End of Record

EPROM Electrically Programmable Read Only Memory

EQ Equipped; Equipment

EQPT Equipment

ESD Electrostatic Discharge

ETS European Telecommunications Standard

ETSI European Telecommunications Standards Institute

F

FCC Federal Communications Commission; Fast Communications Channel

FCIO Function Controller Input/Output Device

FDA/CDRH Federal Drug Administration, Center for Devices and Radiological Health

FDP Fiber Distribution Panel

FE Far End

FEND Far End

FI Facility Interface

FIFO First In First Out

FIT Failure In Time

FLT Fault

FM Fault Management

FTP File Transfer Protocol

G

GBELX Gigabit Ethernet

GMT Greenwich Mean Time

GPIO General Purpose Input/Output

GUI Graphical User Interface

H

HSBB High-Speed Broadband

HSWIC High-Voltage Shelf Switch Interface Controller

HV High Voltage

HVCPG High-Voltage Shelf Controller Protection Group

HVDAC High-Voltage Digital-to-Analog Converter

HVFAN High-Voltage Shelf Fan

HVS High-Voltage Shelf

I **IAO** Intraoffice

IAO LAN Intraoffice Local Area Network

ID Identifier

IDC Insulation Displacement Connector

IEC International Engineering Consortium

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IF In Frame

IFMT Interface Format

IIC Inter-Integrated Circuit

IMF Infant Mortality Factor

IMPROPRML Improper Removal

INTSFT Internal Software

I/O Input/Output

IOPT Interface Optics

IP Internet Protocol

IP-CPY-MEM In Progress–Copy Memory

IR Intermediate Reach

IS In Service

IS-NR In Service-Normal

ISO International Standards Organization

ITE Information Technology Equipment

ITU International Telecommunications Union

ITU-T International Telecommunications Union—Telecommunication Standardization Sector

J

J0 SONET/SDH Section Trace Byte

JTAG Joint Test Action Group

L

L<number> Layer <number>

L/MS Line/Multiplex Section

LAN Local Area Network

LBC Laser Bias Current

LC Lucent Connector

LED Light-Emitting Diode

LID LED Interface Device; Logical Identifier

LLC Logical Link Control

LLO Lucent Learning Organization

LM Loss Parameter

LMPTST Lamp Test

LOF Loss of Frame

LOS Loss of Signal

LPBKCRS Loopback Cross-Connect

LPBK-DX Loopback–Duplex

LPBK-SX Loopback–Simplex

LR Long Reach

LSAP LLC Service Access Point

LSBB Low Speed Broadband

LVDS Low Voltage Differential Signal

M **M** Maintenance

MA Management; Messaging Agent

MAC Media Access Control

MAN Metropolitan Area Network

MD Mediation Device

MEA Mismatch of Equipment and Attributes

MEM Memory

MEMS Micro-Electromechanical System

MIB Management Information Base

MJ Major

MMIS Memory Mismatch

MN Minor

MON Monitoring

MS Multiplex Section

MT Maintenance

MTBMA Mean Time Between Maintenance Activities

MTTF Mean Time To Failure

MTTR Mean Time To Repair

N **NBF** Non-blocking Fabric

NDF New Data Flag

NE Near End; Network Element

NEBS Network Equipment-Building System

NEDS Network Equipment Development Standards

NEND Near End

NIC Network Interface Card

NMON Non-Monitoring

NMS Network Management System

NNI Network to Network Interface

NP Network Path

NR Not Reported

NSA Non-Service-Affecting

NVM Non-Volatile Memory

NVMU Non-Volatile Memory Usage

NVMW Non-Volatile Memory Wearout

NVRAM Non-Volatile RAM

O

OC-n Optical Carrier <number>

OCH Optical Channel

OEO Optical to Electrical to Optical

OICPG Optical Interface Shelf Controller Protection Group

OIFAN Optical Interface Shelf Fan

OIM Optical Interface Module

OIS Optical Interface Shelf

OIS-10G Optical Interface Shelf-10Gbps

OIS-2G Optical Interface Shelf-2.5Gbps

OIS-MX Optical Interface Shelf-Mixed

OIS-S Optical Interface Shelf-SDH/SONET

OIS-T Optical Interface Shelf-Transparent

OLS Optical Line System

OMERR Out of Memory Error

ON Operations Network

ONI Operations Network Interface

OOF Out of Frame

OOS Out of Service

OOS-MA Out of Service Management

OPI Operations Peripheral Interface

OPR Operate

OS Operations System

OSWIC Optical Interface Shelf Switch Interface Controller

OTDR Optical Time Domain Reflectometer

OTU Optical Translator Unit

OXC Optical Cross-Connect

OXI Optical Cross-Connect Interface

OXI-10GC Optical Cross-Connect Interface-10 Gbps Client

OXI-2GC Optical Cross-Connect Interface-2.5 Gbps Client

P **P** Provisioning

PCMCIA Personal Computer Memory Card International Association

PFVP Power Filter Voltage Protection

PFVP-CB Power Filter Voltage Protection with Circuit Breaker

PIC Peripheral Interface Controller

PID Password Identifier

PLD Programmable Logic Device

PMD Polarization Mode Dispersion

POR Power On Reset

PRI Primary Nonvolatile Memory

PROGFLT Program Fault

PROV Provisioned

PSCHG Protection Switch Change

PST Primary State

PU Port Unit

PWR Power

PWRM Power Monitor

Q

QoS Quality of Service

R

RS Regenerator Section

RTAC Regional Technical Assistance Center

RU Resource Usage

S

S Security

SA Service-Affecting

SAP Service Access Point

SB Secondary Boot

SCC System Controller Complex

SCCPG System Controller Complex Protection Group

SCFAN System Controller Shelf Fan

SCMMA System Controller in Maintenance

SCS System Controller Shelf

SD Signal Degrade

SDH Synchronous Digital Hierarchy

SDRAM Synchronous Dynamic Random Access Memory

SEC MEM Secondary Non-Volatile Memory

SEEPROM Serial EEPROM

SELV Safety Extra Low Voltage

SF Signal Fail

SI Switch Interface

SID Source Identifier

SLN Serial Number

SMC Serial Management Controller

SMEM Secondary MEM

SMF Single Mode Fiber

SMI Serial Management Interface

SMS Service Management System

SN Serial Number

SNIP Serial Number Identification Port

SNMP Simple Network Management Protocol

SNMS SubNetwork Management System

SONET Synchronous Optical Network

SPLTR Splitter

SR Short Reach

SRC Subrack Controller

SSN Series Number

STBY Standby

STBYS Standby Switched

STCHG State Change

STM Synchronous Transfer Mode

STS Synchronous Transport Signal

SWIC Switch Interface Controller

SWIP Switch Interface Point

SWMG SWIP Maintenance Group

SWS Switch Shelf

SYSCTL System Controller

T

T Test

TCP/IP Transmission Control Protocol/Internet Protocol

TID Target Identifier

TL1 Transaction Language 1

TMN Transport Management Network

TSA Test Alarm

TSS Technical Support Services

U

UAS Unassigned; Unavailable Seconds

UEQ Unequipped

UI Unit Interface

UIA Unit Interface Appliance

UID User Identification

UL Underwriters Laboratories

UNEQ Unequipped

UPC User Privilege Code

V

V/V Voltage to Voltage

VPN Virtual Private Network

VSR Very Short Reach

W

WAN Wide Area Network

WDM Wavelength Division Multiplexing

WINS Windows Internet Network Service

Glossary

Numerics

0x1 Facility Interface
A transmission interface without line or equipment protection switching.

0x1 Line Operation
Operation between network elements, without protection in a single bidirectional line (no protection line is available).

1+1 Client Protection
A WaveStar LambdaRouter 128/256 Release 2.0 feature in which connections between WaveStar LambdaRouter 128/256 and client network elements can be configured as 1+1 at the optical level.

1+1 Protection Group
A protection architecture, in which one working function is protected by one protection function. In addition, the protection function is fully synchronized with the working function. The functions are permanently bridged upstream, and one is selected downstream.

1+1 Restoration
A type of network restoration supported in WaveStar LambdaRouter 128/256. The restoration path, including the end-points, is provisioned when initial path provisioning is done. The restoration path always carries the same signal as the service path, and the egress WaveStar LambdaRouter 128/256 automatically switches over to it when the service path fails.

1x1 Protection Group
A protection architecture, in which one working function is protected by one protection function. In contrast to the 1+1 Protection Group, the protection function is not fully synchronized with the working function.

A

Access Identifier (AID)
A technical specification for explicitly naming entities (both physical and logical) of a network element, following Telcordia TL1 syntax.

Activation
The process of starting software or using the data in execution the first time after installation.

Active (ACT)
Indication that a circuit pack or module is in service and is currently providing service functions. *See also* Standby.

Active Path
One of two signals entering a constituent path selector. The active path is the one currently being selected.

Add/Drop Multiplexer (ADM)
A synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

Air Baffle
A WaveStar LambdaRouter 128/256 bay component that facilitates air intake and exhaust.

Alarm
A visible or audible signal to the operations environment that a communication, equipment, or processing failure has occurred.

Alarm Correlation
A WaveStar LambdaRouter 128/256 feature that minimizes the number of alarm messages generated for a single fault condition.

Alarm Cut-Off (ACO)
A mechanism to silence local Central Office audible alarms. It is activated by a user panel button or a user command.

Alarm Indication Signal (AIS)
A code sent downstream in a network to indicate an upstream failure.

Alarm List
A WaveStar LambdaRouter 128/256 status report that lists active alarms on the network element. It includes alarm level and type, affected equipment, effect on service, probably cause, and additional details of the failure, if available.

Alarm Log
A history and time sequence of the setting and clearing of alarms on the WaveStar LambdaRouter 128/256. The alarm log contains as many as 512 alarm messages. It includes the type of trouble, time of occurrence, identification of affected equipment, effect on service, alarm level, alarm condition state, and additional details of the failure, if available.

Alarm Notification Category
One of three types of WaveStar LambdaRouter 128/256 alarm messages: Optical Channel, Equipment, or Common Alarm.

Alarm Severity
An attribute that defines the priority of an alarm message. The way alarms are processed depends on their severity.

American Standard Code for Information Interchange (ASCII)
A standard seven-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

Apparatus Code (APP)
A circuit pack identifier stored in EEPROM.

Asynchronous
The essential characteristic of time-scales or signals, such that their corresponding significant instants do not necessarily occur at the same average rate.

Asynchronous Transfer Mode (ATM)
A high-speed transmission technology characterized by high bandwidth and low delay. It uses a packet switching and multiplexing technique that allocates bandwidth on demand.

Authorization Level
A numeric code that determines what commands within a functional category a user may access on the WaveStar LambdaRouter 128/256. The authorization level ranges from 0 (lowest) to 5 (highest) for all functional categories except security, which ranges from 1 to 5. Assigning an authorization level of 0 disables that functional category for a particular user.

Auto-Provisioning
The capability of the WaveStar LambdaRouter 128/256 to discover its hardware configuration and to create associated database entries autonomously using the original (default) or user-defined, pre-provisioned parameters. These parameters are maintained in non-volatile memory (NVM) and/or hardware registers.

Automatic Protection Switch
A protection switch that occurs automatically in response to an automatically detected fault condition.

B

Backup and Restore
In WaveStar LambdaRouter 128/256, the capability to copy and restore databases between Primary Non-Volatile Memory (NVM) and Secondary NVM, Primary NVM and WaveStar SNMS, and Primary NVM and WaveStar CIT.

Bandwidth
Throughput capacity in a transmission channel.

Bandwidth Management
The capability that allows WaveStar LambdaRouter 128/256 users to provision either unidirectional or bidirectional optical, or optical-electrical-optical (OEO), cross-connections for transmission paths through the switch fabric.

Bay
A hardware frame in which shelves are mounted and housed.

Bidirectional Line
A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bit Error Rate (BER)
The ratio of error bits received to the total number of bits transmitted.

Blank (BLK)
The status of a circuit pack slot that contains a bus extender (blank) circuit pack; the pack itself.

Bridging
A one-way 1:2 multicast from an input port where a 1:2 splitter routes the two one-way signals through the duplicated switch fabric to two different output ports. Each one-way leg is a simplex transmission path. *See also* Merging.

Broadband Communications
Voice, data, and/or video communications at greater than 2 Mbps rates.

Busy State
Indication that a port is being used in a cross-connection.

C

Calibration Database
A database that indicates initial control voltages for each Switch Shelf mirror in an array. The calibration data is delivered on a non-volatile memory (NVM) card and is installed by inserting the card into the secondary NVM (SEC MEM) on the WaveStar LambdaRouter 128/256.

Card
A removable integrated circuit board/circuit pack.

Central Office (CO)
A building in which common carriers terminate customer circuits.

Channel
A (one-way) transmission pathway from an input port to an output port in the network element, at any supported transmission rate and/or format.

Circuit Pack (CP)
A single field-replaceable electronic or opto-electronic unit. It comprises mechanical piece-parts, electronic components, and their associated connections and performs a specific function.

Circuit Pack Extraction
The process of software acknowledgement of an event associated with the physical removal of a circuit pack from a shelf slot, or the opening of its latch.

Circuit Pack Identifier (CP-ID)
A code that is derived from the circuit pack type (apparatus code), serial number, series number (version), CLEI code, and ECI code of each circuit pack. The circuit pack identifier is readable by the system upon insertion of the pack in any allowable slot.

Circuit Pack Insertion
The process of acknowledging and subsequently provisioning a valid circuit pack that has been inserted into a shelf slot. Circuit pack insertion requires equipage and latch closure acknowledgments, and a response to the insertion cannot be completed prior to the detection of the latch closure.

Client
A client network interface.

Cold Standby
A standby function that does not function simultaneously with the active function. It requires a form of initialization (provisioning) before it can assume the role of the active function.

Command Echo
The ability of WaveStar LambdaRouter 128/256 to repeat the text of entered commands to a user provisioned for this feature.

Command Functional Categories
Logical groupings of WaveStar LambdaRouter 128/256 commands. These include maintenance (M), provisioning (P), security (S), and test (T).

Command Group
An administrator-defined group that defines commands to which a user has access.

Common Alarm
A WaveStar LambdaRouter 128/256 alarm message category that indicates a controller software fault, controller autonomous reset, data storage problem, software version mismatch, or security-related issue. Common alarm issue points are circuit pack, controller complex, shelf, or system.

Common Language Equipment Identifier (CLEI)
A Telcordia code that identifies telecommunications equipment to facilitate inventory, maintenance, investment tracking, and circuit maintenance processes. CLEI codes are stored in circuit pack EEPROM.

Compact Duplex (CD)
1. Generic term for the WaveStar LambdaRouter architecture of one logically segregated switch fabric. 2. Specific term for the WaveStar LambdaRouter Release 1.0 two-bay configuration. It comprises one Switch Shelf, one High-Voltage Shelf, one System Controller Shelf, and one Optical Interface Shelf.

Compact Duplex 2 (CD2)
Software term for the WaveStar LambdaRouter 128 Release 2.0 configuration.

Configuration Management (CM)
The activities necessary to create, modify, retrieve, and delete data that controls the configuration and operation of WaveStar LambdaRouter 128/256 hardware and software. These activities include equipment provisioning, alarm monitoring and fault management, cross-connection management, and software management.

Configuration Query
A user-initiated request for a report on provisioned data.

Control Bay
The WaveStar LambdaRouter 128/256 frame that contains one System Controller Shelf and up to two Optical Interface Shelves. There is one Control Bay per WaveStar LambdaRouter 128/256 system.

Control System Interface Expander (CSIEX)
The WaveStar LambdaRouter 128/256 circuit pack that expands the number of internal interfaces to and from the SYS50D circuit pack. It is located in the System Controller Shelf.

Controller Reset
The capability of rebooting shelf controllers locally (manually, on equipment) and through command. WaveStar CIT or WaveStar SNMS or other managing system can reset the WaveStar LambdaRouter 128/256 system or shelf controllers without affecting transmission.

Craft Interface Terminal (CIT)
See WaveStar CIT (Craft Interface Terminal).

Critical (CR) Alarm
An indication of a severe, service-affecting condition.

Cross-Connection
A configurable optical, or optical-electrical-optical (OEO), transmission path interconnection between input and output ports within a single network element.

Cross-Connection Capacity
The total number of cross-connections, as measured by the number of fabric input and fabric output points. A fabric with N input points and N output points provides a cross-connection capacity of N. *See also* Non-Blocking Cross-Connection Capacity; Switch Interface Capacity.

Cross-Connection Configuration
A set of one or more associated cross-connection legs. Examples of configurations that are supported in WaveStar LambdaRouter 128/256 are one-way point-to-point (one duplex leg); two-way point-to-point (two duplex legs); one-way bridge (two simplex legs); one-way merge (two simplex legs); one-way bridge and merge (three simplex legs); and two way bridge and merge (four simplex legs).

Cross-Connection Fabric
See Switch Shelf (SWS).

Cross-Connection Leg
A one-way connection provisioned from one input port to one output port within a single network element. A leg with a transmission path through one switch fabric is called a simplex leg. A leg that has a transmission path between both fabrics is called a duplex leg.

Cross-Connection List
A WaveStar CIT for LambdaRouter status report that lists current cross-connections for the following: a specific port, all ports on a specific circuit pack, all ports on a specific shelf, or all ports in the network element. The report includes the input and output AID, cross-connection typology or loopback type, and switch fabric used.

Cross-Connection Loopback
A cross-connection, for maintenance purposes, from an input port through the switch fabric to an output port. An output port may be selected with an access identifier (AID) that is the same or different from the input AID. WaveStar LambdaRouter 128/256 supports normal, forced simplex, and forced duplex loopbacks. A forced simplex loopback allows one of the transmission paths in the forward direction to remain operational.

Cross-Connection Management
The activities necessary to establish and remove cross-connections, operate and release loopback cross-connections, and retrieve cross-connection parameters.

Cross-Connection Rate
The transmission rate associated with the cross-connection, which is determined by the type of ports being used. Ports provided by transparent circuit packs allow cross-connections to be bit-rate-independent. Ports provided by optical-electrical-optical circuit packs limit cross-connections to a specific rate, such as 10 Gbps.

Cross-Connection Topology
The basic nature of a cross-connection configuration. All cross-connections can be classified into two topologies: one-way (unidirectional) and two-way (bidirectional).

Cross-Connection Type
See Cross-Connection Configuration.

Crosstalk
An unwanted signal introduced into one transmission path from another.

Cut-Through
An American Standard Code for Information Interchange (ASCII) interface to a network element (NE). It enables the user to send Transaction Language 1 (TL1) messages directly to the NE.

D

Data Communications Controller (DCC)
A WaveStar LambdaRouter 128/256 circuit pack that provides the interface between the system and the operations data communications network, which is physically accessed via the LAN connection on the External Interface packs. In WaveStar LambdaRouter 128/256 Release 2.0 there are two DCC packs on the System Controller Shelf, for active/active service.

Database Labeling
A WaveStar LambdaRouter 128/256 feature that records system target identifier (TID), date of last database modification, date backed up from the network element, and the software generic ID, for use in subsequent download operations.

Debug Support
Maintenance activity access for Lucent personnel.

Default Provisioning
The implementation of parameter values that are preprogrammed at 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. *See also* Failure.

Dense Wavelength Division Multiplexing (DWDM)
The transmitting of two or more signals of different wavelengths simultaneously over a single fiber.

Deprovisioning
The inverse order of provisioning, to manually remove or delete previously provisioned parameters.

Details Screen
A text-based display of parameter settings, states, and all other information related to the detailed item on the display.

Detection of Signal (DOS)
The detection of a signal that meets provisioned threshold values, applying to both input and output ports.

Diagnostics
In WaveStar LambdaRouter 128/256, the capability to test a range of equipment and software entities. Some diagnostics run autonomously (for example, during boot or circuit pack insertion). Others are on-demand, on either an in-service basis (for example, LED test) or out-of-service basis (for example, cable testing).

Dialog Box
A secondary WaveStar CIT window designed to allow the user to enter additional information.

Dimmed State
The condition of a graphical user interface (GUI) control whose normal functionality is not currently available to a user. This state is indicated on the WaveStar CIT screen by a greyed image.

Discovery
The process of detecting circuit pack presence during system initialization, prior to hardware interrupt enabling.

Dispersion
The phenomenon in which different wavelengths or different polarizations of light travel at different speeds through a fiber optic cable.

Dither
In WaveStar LambdaRouter 128/256, the capability to make small adjustments to the orientation of ingress and egress switch fabric mirrors in order to minimize cross-connection signal loss.

Diverse Duplex (DD)
1. Generic term for the WaveStar LambdaRouter architecture of two diverse switch fabrics separated by a bay. 2. Specific term for the WaveStar LambdaRouter [256] Release 1.0 three-bay configuration. It comprises two Switch Shelves, two High-Voltage Shelves, one System Controller Shelf, and two Optical Interface Shelves.

Diverse Duplex 2 (DD2)
Software term for the WaveStar LambdaRouter 256 Release 2.0 configuration.

Download
The process of transferring files from a managing system such as the WaveStar CIT or WaveStar SNMS to a network element, such as WaveStar LambdaRouter 128/256. Both software and data can be downloaded to the WaveStar LambdaRouter 128/256. *See also* Upload.

Downstream
At or toward the destination of the considered transmission stream.

Duplex Control
A control architecture that includes two controllers, one active, one standby, that protect each other; if the active one fails, the inactive takes over.

Duplex Cross-Connection
A cross-connection that has a transmission path through both switch fabrics.

Duplex Cross-Connection Fabric
A cross-connection fabric consisting of two identical subunits (Switch Shelves), which form a 1+1 protection group.

E

Egress
The direction away from the fabric.

Electromagnetic Compatibility (EMC)
The ability of equipment or systems to operate without causing or receiving degradation from electromagnetic interference (EMI).

Electromagnetic Interference (EMI)
High-energy, electrically induced magnetic fields that cause data corruption in cables passing through the fields.

Electronic Industries Association (EIA)
A trade association of the electronic industry that establishes electrical and functional standards.

Electrostatic Discharge (ESD)
A static electrical energy potentially harmful to circuit packs.

Enabled
The state in which an equipped subsystem or component is fully capable of operation.

End Guard
A panel that is installed at ends of a WaveStar LambdaRouter 128/256 bay lineup; it meets ETSI standards.

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.

Equipage Check
A system check of equipment that results in an alarm if there is a mismatch between a circuit pack and the provisioned slot in which it is installed.

Equipment Alarm
A WaveStar LambdaRouter 128/256 alarm message category that indicates transmission and control equipment failures and service interruption owing to failures in power supply, fuse, or fan assembly, or configuration problems. Equipment alarms are issued for port, circuit pack/slot, shelf, and system.

Equipment Catalog Item (ECI)
A circuit pack identifier stored in Erasable Electrical Programmable Read Only Memory (EEPROM).

Equipment Fail (EF) State
A state in which any of the protection group's circuit packs have failed, and no higher priority request (for example, Clear, Forced Switch) is present. The protection group leaves the EF state when all EF indications are cleared, or a higher priority request has been received.

Equipment List
A report, available through user request, that lists equipment for a selected shelf, circuit pack, or port in the WaveStar LambdaRouter 128/256. The report includes the AID for the selected entity and other information, such as CLEI code, serial number, and cabling information.

Equipment Protection
The protection switching for the redundant common transmission and control equipment in the network element.

Equipment Provisioning
The assigning of values to a set of parameters of the system, or any of its subsystems, to enable the expected use of the entity. Provisionable WaveStar LambdaRouter 128/256 entities include system, shelves, slots/circuit packs, ports, cross-connections, and protection groups.

Equipped (EQ) Status
Indication that a circuit pack or interface module is in the system database and physically in the frame.

Event

Significant change detected by the system. Events in controlled network elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs, the controlled network element will generate an alarm or status message and send it to the management system.

External Interface (EI)

The WaveStar LambdaRouter 128/256 circuit pack that provides interfaces to the Data Communications Controller (DCC) circuit pack, WaveStar CIT port, and Intraoffice (IAO) LAN. The EI provides local office alarm relay closures and miscellaneous discrete inputs and outputs. It also provides the interface to alarm closures on the System Controller Shelf (SCS) User Panel. Duplex EIs are located on the SCS.

Extraction

Physical removal of a circuit pack from a slot, causing a system-initiated removal of an entity from service.

F

Fabric

The physical hardware that provides the switching function within the network element; a mesh of interconnections between inputs and outputs. In WaveStar LambdaRouter 128/256, the fabric is a set of mirrors that allows connection between any one of a set of inputs to any one of a set of outputs.

Fabric Wavelength Window

The allowable range of wavelengths transmitted by a given fabric. For WaveStar LambdaRouter 128/256, that range is from 1260 nm to 1360 nm, and from 1500 nm to 1620 nm.

Facility

A one-way or two-way circuit that carries a transmission signal.

Facility Interface (FI)

See Transmission Interface.

Facility Loopback

A loopback of the incoming facility signal to the output of the same facility, without going through a switch fabric. A facility loopback is not supported on WaveStar LambdaRouter 128/256.

Failure

A persistent defect. *See also* Software Failure.

Failures in Time (FIT)
A unit of hazard rate used to measure the reliability of non-reparable equipment. A hazard rate of 1 FIT corresponds to a Mean Time to Failure (MTTF) of one billion hours.

Fan Filter
A field-replaceable part that keeps dust and debris out of the Fan Unit. There are two types of Fan Filters in the WaveStar LambdaRouter 128/256: OIS-S Fan Filters and SCS/HVS/OIS-T Fan Filters.

Fan Unit
A field-replaceable module that provides forced air cooling for the WaveStar LambdaRouter 128/256. There are two types of Fan Unit: SCS/HVS/OIS-T Fan Unit and OIS-S Fan Unit.

Far End (FE)
Any network element in a maintenance subnetwork other than the one at which the user is posted. Also called remote.

Fault
A generic term for anomaly, defect, and failure.

Fault Detection
The ability to identify communications, equipment, and processing failures. WaveStar LambdaRouter 128/256 provides continuous, autonomous, in-service fault detection and isolation on transmission and control equipment.

Fault Management
In WaveStar LambdaRouter 128/256, capabilities that provide fault detection, isolation, reporting and facility/equipment alarms, user/alarm displays, circuit pack LEDs, office alarms, and records provisioning.

Fiber Distribution Panel (FDP)
In WaveStar LambdaRouter [256] Release 1.0 and WaveStar LambdaRouter 128/256 Release 2.0, a Switch Shelf panel that contains connectors for 256 inputs and 256 outputs.

Fiber Management Unit
A WaveStar LambdaRouter 128/256 Release 2.0 duct used to control and store cables and protect them from physical damage. It is used in both overhead and underfloor installations.

Fiber Organizer
A frame between bays that is used for managing fiber cables.

File Transfer Protocol (FTP)
A protocol used by WaveStar LambdaRouter 128/256 for transfer of software and data between the network element and its management system and between network elements.

G

General User
A WaveStar CIT user type with access to all commands except network element (NE) security administration, software installation, system initialization, and NE access capabilities.

Generic
A collection of programs and associated static data that fully support and perform all of the designed functions of the WaveStar LambdaRouter 128/256, WaveStar CIT, or element management system (EMS).

Generic Labeling
The unique identification of a software generic release so that it is recognized by the system and is available to the user upon query. The label includes the supplier name and type, version number of the generic, the date built or build number, and the date installed. The generic label information can be retrieved via the managing system or WaveStar CIT.

H

Hard Failure
An unrecoverable nonsymptomatic (primary) failure that causes signal impairment or interferes with critical network functions.

High-Voltage Digital-to-Analog Converter (HVDAC)
The WaveStar LambdaRouter 128/256 Release 2.0 circuit pack that provides the digital-to-analog converters and high-voltage linear amplifiers used to control a subset of the Micro-electromechanical System (MEMS) mirrors in the Switch Shelf (SWS).

High-Voltage Shelf (HVS)
The WaveStar LambdaRouter 128/256 Release 2.0 shelf that houses High-Voltage Digital-to-Analog Converter (HVDAC) circuit packs.

High-Voltage Shelf/Optical Interface Shelf (HVS/OIS) User Panel
The WaveStar LambdaRouter 128/256 Release 2.0 module that receives alarm status information. It provides visual indications of shelf status through LEDs and a means for generating alarm cutoff and LED test interrupts to the shelf Switch Interface Controller (SWIC) circuit packs. *See also* System Controller Shelf (SCS) User Panel.

Hot Standby
A standby function that is fully operational and acts in synchronism with an active function. It is able to take over the role of the active function without the need for initialization. *See also* Active; Cold Standby.

I

Idle State
The state of a port that is not cross-connected.

Ingress
The direction toward the fabric.

Insert
The physical insertion of a circuit pack into a slot, causing a system-initiated restoral of an entity into service and/or creation of an entity and associated attributes.

Insertion Loss
The decrease in optical signal power incurred by a signal passing through the entire system.

In-Service (IS) State
An administrative state for equipment entities (ports, circuit packs). IS indicates that the entity is fully capable and allowed to perform its specified functions.

Interface Bay
The WaveStar LambdaRouter 128/256 Release 2.0 frame that contains optical interface shelves.

Intermediate Reach (IR)
A standard for optics, concerning transmitters and receivers in a system, that insures that transmission can be maintained for intermediate distances (50 km). This standard constrains the output power of the transmitter and the sensitivity of the receiver for moderate haul applications (up to 50 km; a compromise between long and short reaches) without the need for regeneration. *See also* Long Reach; Short Reach; Very Short Reach.

International Telecommunications Union–Telecommunications Standards Sector (ITU-T)
One of three sectors of the ITU. The ITU-T sets global telecommunications standards.

Inventory Query
A user-initiated request for a report on all electronic equipment in the system.

J Jitter

The short-term variation of the significant instants of a digital signal from their ideal positions in time. Jitter may cause crosstalk or distortion of the original analog signal, or both, and is potentially a source of bit errors at the input ports of digital equipment. *See also* Wander.

L Labeling

The WaveStar LambdaRouter 128/256 capability to label database and software generics. *See also* Database Labeling; Generic Labeling.

Lambda

The Greek letter used to signify the wavelength of a complete cycle of signal that propagates through space. Common examples of such signals are radio waves and light waves.

LambdaRouter

See WaveStar LambdaRouter; WaveStar LambdaRouter 128; WaveStar LambdaRouter 256.

Lamp Test (LMPTST)

A user panel button used to test LEDs.

LC Connector (LC)

A Lucent-designed small form-factor plastic optical fiber connector, designed for applications where space is limited. The LC, which is half the size of other common connectors, is ferrule-based and uses the familiar insertion/release mechanism similar to an ordinary telephone plug.

Line

See Port.

Line Protection

Backup for optical interfaces. Line protection protects against failures of line facilities, including the interfaces at both ends of a line, the optical fibers, switching failures, and any equipment between the two ends.

Location

A user-provisionable identifier of the physical positioning of a specific shelf.

Log

System-maintained data of user session activity, including changes, alarms and security activity, and protection switching.

Login ID
See User ID.

Long Reach (LR)
A standard for optics, concerning transmitters and receivers in a system, that insures that transmission can be maintained for long distances (tens of kilometers). This standard constrains the output power of the transmitter and the sensitivity of the receiver for long-haul applications (up to 80 km) without the need for regeneration. *See also* Intermediate Reach; Short Reach; Very Short Reach.

Loopback
A circuit configuration used to compare an original transmitted signal with the resulting received signal. WaveStar LambdaRouter 128/256 supports cross-connection loopback for maintenance purposes.

Loss of Frame (LOF)
An indication of consecutive errored framing patterns in an incoming signal.

Loss of Signal (LOS)
An indication that a signal is below the provisioned threshold values for either the input or output port.

Low-Voltage Shutdown
The capability of WaveStar LambdaRouter 128/256 to detect when power drops below a predefined input voltage level and to shut down gracefully. Cross-connection maps and other provisioned data are maintained through the power loss.

M

Maintenance Condition
An equipment state in which some normal service functions are suspended, either because of a problem or for special functions (copy memory) that cannot be performed while normal service is being provided.

Maintenance Cross-Connection
A diagnostic tool used to evaluate the functions of WaveStar LambdaRouter 128/256 mirrors without involving ports.

Maintenance User
A WaveStar CIT user login with access to testing, retrieval of network element information, and limited service-affecting commands.

Major (MJ)
An indication of a service-affecting failure.

Manual Provisioning and Deprovisioning

User-initiated provisioning or deprovisioning by the following commands or graphical user interface (GUI) equivalent actions: create, delete, modify, remove, restore.

Manual Switch State

The events that follow the issuing of the manual switch command. 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.

Mediation Device (MD)

A device that allows for exchange of management information between managing systems and network elements.

Memory (MEM)

The WaveStar LambdaRouter 128/256 circuit pack that provides the non-volatile memory (NVM) necessary to store executable code and data for the system. Two primary MEMs (PRI MEMs) are located in the System Controller Shelf and serve as duplicated NVM. They communicate with the SYS50D circuit packs. A secondary MEM (SEC MEM) provides backup to the primary MEMs and communicates with the CSIEX circuit packs. Program and configuration data are stored on a PCMCIA card, which can be accessed from the faceplate of the MEM and is removable.

Merging

The use of two simplex cross-connection legs between two different input ports and one output port where a 2:1 selector chooses one of the incoming one-way signals. The use of bridging and merging at a network element provides 1+1 path protection for two-way traffic. *See also* Bridging.

Micro-electromechanical System (MEMS)

The WaveStar LambdaRouter 128/256 fabric technology, which consists of a large number of electrically configurable mirrors, fabricated on a single substrate.

Minimum Configuration

A set of network element (NE) entities that are required to exist for the NE to be operational. These entities are created automatically by the system during initialization.

Minor (MN)
An indication of a non-service-affecting failure of equipment or facility.

Module
A self-contained entity that performs a well-defined function in the system.

N

Network Element (NE)
A telecommunications network node that supports network transport services and is directly manageable by a management system.

Network View
The WaveStar CIT screens and menu options used to set up an association with network elements or to administer the WaveStar CIT GUI itself.

Node
All equipment that is controlled by one system controller. A node is not always directly manageable by a management system.

Non-Blocking Cross-Connection Capacity
The service cross-connection capacity guaranteed to the user to be free from blocking.

Non-Blocking Fabric
The characteristic that no cross-connection request will be denied because of a lack of a path through the fabric, when the desired input and output ports are available.

Non-Revertive Protection Switching
A process in which an active and standby line exist. 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 standby line. This status remains in effect even when the fault clears (there is no automatic switch back to the original status). *See also* Revertive Protection Switching.

Non-Volatile Memory (NVM)
Memory that retains its stored data after power has been removed; for example, a hard disk.

No Request State
The state in which no protection switching activities are occurring.

Not Monitored (NMON)
A provisioning state for equipment that is not equipped with monitors or alarms.

O

Off-Board Devices

Transmission devices that are associated with a controller but are located on another circuit pack. *See also* On-Board devices.

Office Alarm Interface

An interface to the Office Alarm System for each alarm level that leads to audible or visible Central Office alarms. Audible alarm cutoff (ACO) is provided locally on the equipment and remotely through user command. Critical, Major, and Minor audible and visible alarms are supported.

On-Board Devices

Transmission devices associated with a controller and located on the same circuit pack. *See also* Off-Board devices.

One-Way Bridge and Merge Cross-Connection

A complex one-way cross-connection configuration that consists of two concatenated basic bridge and merge cross-connection configurations that share a common simplex leg.

One-Way Double Merge Cross-Connection

A complex one-way cross-connection configuration that consists of two merge cross-connections that share the same source (input) ports. It can also be considered as two bridge cross-connections that share the same destination (output) ports.

One-Way Point-to-Point Cross-Connection

A one-leg duplex interconnection between an input port and an output port. It can be set up and taken down by a single command to the network element.

One-Way Simplex Cross-Connection

A cross-connection leg with a transmission path through a single switch fabric. A simplex cross-connection leg can be added to or deleted from an existing cross-connection to form another type of cross-connection configuration. For example, a simplex leg can be deleted from an existing bridge or merge cross-connection to form a one-way point-to-point cross-connection.

Opacity

Bit-rate and format dependence. The WaveStar LambdaRouter 128/256 Release 2.0 opaque interfaces are the OXI-10GC and OXI-2GC.

Open Systems Interconnection (OSI)
A seven-layer reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Operations Interface
Any interface providing information on the system behavior or control. In WaveStar LambdaRouter 128/256, operations interfaces include equipment LEDs, user panels, WaveStar CIT, and office alarms.

Operations System (OS)
A central-computer-based system used to provide operations, administration, and maintenance functions. An example of an OS is the WaveStar SNMS (SubNetwork Management System).

Operator
User of the system with operator-level user privileges.

Optical Channel Alarms
A WaveStar LambdaRouter 128/256 alarm message category that reports input signal failures and are issued against an input port. Optical channel alarms include the following fault conditions: loss of monitored input power, detection of Alarm Indication Signal-Line, SONET/SDH failures (Loss of Signal [LOS], Loss of Frame [LOF], Signal Fail B2 Excessive Bit Error Rate [EBER], Signal Degrade B2 Bit Error Rate [BER], Alarm Indication Signal-Line/Multiplex Section (AIS-L/ AIS-MS]), Unequipped, and Trace Mismatch.

Optical Channel Management
A WaveStar LambdaRouter 128/256 application that enables adding, dropping or connecting of services traffic through the network, through optical line systems (OLSs).

Optical Cross-Connect Interface (OXI)
1. A generic term for any transmission interface used in WaveStar LambdaRouter 128/256, including, in Release 2.0, the OXI transparent packs and the OXI-10GC and OXI-2GC opaque packs. 2. The name of the transmission interface circuit pack that performs optical splitting, power monitoring, and rate- and format-independent switching for signals to and from the network element. OXIs are located in the Optical Interface Shelf (WaveStar LambdaRouter Release 1.0) and Optical Interface Shelf-Transparent (WaveStar LambdaRouter 128/256 Release 2.0). Each transparent OXI pack provides four input and four output ports.

Optical Cross-Connect Interface-2.5 Gbps Client (OXI-2GC)
A WaveStar LambdaRouter 128/256 Release 2.0 circuit pack that supports 2.5 Gbps SONET/SDH signals (OC-48/STM-16). OXI-2GCs are located in the Optical Interface Shelf-2Gbps (OIS-2G) and the Optical Interface Shelf-Mixed (OIS-MX). Each OXI-2GC provides two input and two output ports.

Optical Cross-Connect Interface-10 Gbps Client (OXI-10GC)
A WaveStar LambdaRouter 128/256 Release 2.0 circuit pack that supports 10 Gbps SONET/SDH signals (OC-192/STM-64). OXI-10GCs are located in the Optical Interface Shelf-10Gbps (OIS-10G) and the Optical Interface Shelf-Mixed (OIS-MX). Each OXI-10GC provides one input and one output port.

Optical Interface Shelf (OIS)
1. A generic term for any transmission interface shelf used in WaveStar LambdaRouter 128/256, including the OIS-T shelf for transparent circuit packs, the OIS-10G for OXI-10GC circuit packs, the OIS-2G for OXI-2GC circuit packs, and the OIS-MX for a combination of OXI-10GC and OXI-2GC circuit packs. 2. The name of the WaveStar LambdaRouter [256] Release 1.0 shelf that contains the Optical Cross-Connect Interface (OXI) circuit packs. The corresponding shelf in WaveStar LambdaRouter 128/256 Release 2.0 is the Optical Interface Shelf-Transparent (OIS-T).

Optical Interface Shelf-2.5 Gbps (OIS-2G)
The WaveStar LambdaRouter 128/256 Release 2.0 transmission interface shelf that contains 32 OXI-2GC optical-electrical-optical circuit packs and two Switch Interface Controllers (SWICs).

Optical Interface Shelf-10 Gbps (OIS-10G)
The WaveStar LambdaRouter 128/256 Release 2.0 transmission interface shelf that contains 32 OXI-10GC optical-electrical-optical circuit packs and two Switch Interface Controllers (SWICs).

Optical Interface Shelf/High-Voltage Shelf (OIS/HVS) User Panel
The WaveStar LambdaRouter 128/256 Release 2.0 module that receives alarm status information. It provides visual indications of shelf status through LEDs and a means for generating alarm cutoff and LED test interrupts to the shelf Switch Interface Controller (SWIC) circuit packs. *See also* System Controller Shelf (SCS) User Panel.

Optical Interface Shelf-Mixed (OIS-MX)
The WaveStar LambdaRouter 128/256 Release 2.0 transmission interface shelf that contains a combination of 16 OXI-2GC circuit packs, 16 OXI-10GC circuit packs and two Switch Interface Controllers (SWICs).

Optical Interface Shelf-SDH/SONET (OIS-S)
The WaveStar LambdaRouter 128/256 Release 2.0 general shelf type that contains OXI-10GC or OXI-2GC circuit packs, which provide the opaque OC-192/STM-64 and OC-48/STM-16 interfaces between the WaveStar LambdaRouter 128/256 and customer equipment. Each OIS-S contains opaque circuit packs and cannot contain transparent circuit packs.

Optical Interface Shelf-Transparent (OIS-T)
The WaveStar LambdaRouter 128/256 Release 2.0 shelf that contains the transparent OXI circuit packs. Each OIS-T contains as many as 32 OXI circuit packs and two Switch Interface Controllers (SWICs).

Optical Line System (OLS)
Any system using a fiber-optic or other optical technology for transmission.

Optical Loss Budget
The allocation of allowable or necessary signal loss in a transmission system, or signal loss to connection subsections of that system.

Optical Return Loss (ORL)
The power of a signal, reflected back to its source in an optical system.

Optical Translator Unit (OTU)
The Wavestar OLS 400G/800G/1.6T module that provides wavelength translation and signal regeneration from or to the line system.

Out of Service (OOS)
A state in which an equipment entity is not allowed or is incapable of providing its intended function.

P

Parameter
A variable that is given a value for a specified application, or a constant, variable, or expression that is used to pass values between components.

Personal Computer Memory Card International Association (PCMCIA) card
Non-volatile memory in a form similar to a floppy disk. WaveStar LambdaRouter 128/256 program and configuration data are stored on a PCMCIA card in the MEM circuit packs.

Point-to-Point Cross-Connection
A duplex cross-connection from a single input point to a single output point. It can be either one-way or two-way.

Polarization Mode Dispersion (PMD)
Output pulse broadening due to random coupling of the two polarization modes in an optical fiber.

Port
A physical transmission interface, comprising both an input and an output, which may be used to carry traffic between network elements. (Also called line. Port emphasizes the physical interface, and line emphasizes the interconnection. Either may be used to identify the signal being carried.)

Port Pack
See Port Unit.

Port State Provisioning
A feature that allows a user to set the port state to in-service or out-of-service.

Port Unit (PU)
A transmission circuit pack that receives and transmits optical signals. The OXI, OXI-10GC, and OXI-2GC are the WaveStar LambdaRouter 128/256 Release 2.0 port units.

Power Filter Voltage Protection (PFVP) Unit
A WaveStar LambdaRouter 128/256 unit that receives power supply current, suppresses high-frequency emissions, and passes current through the backplane to the circuit packs. This unit also disconnects current through the power source when input voltage falls below an acceptable level, or when a short circuit occurs. PFVPs are located on the Switch Shelf, Optical Interface Shelves, and System Controller Shelf. In the OIS-10G and OIS-2G, the PFVP has an internal circuit breaker.

Pre-provisioning
The process by which a user specifies parameter values for an entity before all of the equipment is present. These parameters are stored in non-volatile memory (NVM).

Primary Non-Volatile Memory (PRI MEM)
A non-volatile MEM circuit pack designated as the primary storage device for the WaveStar LambdaRouter 128/256. *See also* Memory.

Privilege Code
See User Privilege Code.

Privileged User
A WaveStar CIT user login with access to all user capabilities, including those that are service-affecting, with the exception of security-related capabilities.

Program
The executable software code that controls the WaveStar LambdaRouter 128/256 network element or WaveStar CIT.

Protection
Extra capacity (channels, circuit packs) in power or control equipment that is intended to be used not for service but rather as backup for equipment failures. In active and standby contexts, protection is used to describe a function that at power-up becomes standby.

Protection Group
Protection switching configuration. Within a protection architecture, one working function is protected by one protection function. WaveStar LambdaRouter 128/256 supports protection switching with a System Controller Protection Group, High-Voltage Shelf Controller Protection Group, and Optical Interface Shelf Protection Group. *See also* Revertive Protection Switching; Non-Revertive Protection Switching.

Protection Switch Activity Log
A time-stamped list of WaveStar LambdaRouter 128/256 protection switching activity that has occurred within the network element. Facility, equipment, and synchronization-related switching activity is covered. The log includes the protection group ID and the type of protection switch (manual, forced, clear, or automatic).

Protection Switching
WaveStar LambdaRouter 128/256 capability to automatically switch to standby or protection circuitry in the event of failure. A manual or forced protection switch may also be initiated as part of operator fault isolation procedures.

Provisioned (PROV)
Indication that a circuit pack is ready to perform its intended function. A provisioned circuit pack can be active (ACT), in-service (IS), standby (STBY), or out-of-service (OOS).

Provisioning
The process of assigning values to a set of variable parameters of the system (or any of its subsystems) to enable or facilitate the expected use of the system (or subsystem). Provisioning of system components includes the creation of a software representation of the component and/or a record of its parameter values, as well as actual modification of the component parameters. Provisioning can be automatic or initialized by manual command. *See also* Auto-Provisioning; Manual Provisioning and Deprovisioning; Pre-Provisioning.

Q Quality of Service (QoS)

The performance specification of a communications channel.

R Rapid Network Restoration

A WaveStar LambdaRouter 128/256 application that enables speedy restoration of services via alternate paths by removing the need for manual recabling operations. WaveStar LambdaRouter 128/256 offers 1+1 pre-planned and pre-provisioned network restoration.

Rapid Service Provisioning

A WaveStar LambdaRouter 128/256 application that enables speedy provisioning of optical-layer service, eliminating the need to dispatch craft personnel for manual facility interconnections.

Receive-Direction

The signal direction toward the network element.

Recovery

A predefined process, in response to communication, equipment, or processing failure, that results in a return to normal operation of the network element.

Recovery after Power Failure

The WaveStar LambdaRouter 128/256 capability to automatically reset the system after power failure without user intervention, when input voltage rises above a pre-set level. The system returns to its provisioned state prior to the failure.

Reliability

The ability of a software system to perform its required functions under stated conditions for a stated period of time, or the probability for equipment to fulfill its function.

Remote Network Element

Any network element (NE) that is connected to the NE under consideration. *Also called* Far End.

Remote Provisioning

A feature allowing the user to provision from a remote location through a managing system and LAN.

Reports Only User

A WaveStar CIT user type with permissions to access only those capabilities that retrieve information from the system but do not modify the system.

Revertive Protection Switching
The ability of a working and protection function to revert autonomously to active and standby, respectively, upon the repair of the failure that caused a protection switch. *See also* Non-Revertive Protection Switching.

S

SanDisk
A vendor Personal Computer Memory Card International Association (PCMCIA) card; a pre-formatted SanDisk is used in WaveStar LambdaRouter 128/256 Release 2.0 for software installation. *See also* Personal Computer Memory Card International Association (PCMCIA) card.

Scripting
The WaveStar CIT feature that supports the ability for the user to create and edit Transaction Language 1 (TL1) scripts and save them for later use.

Secondary Non-Volatile Memory (SEC MEM)
A MEM circuit pack designated as the secondary storage device for WaveStar LambdaRouter 128/256. *See also* Memory.

Section Trace (J0 Byte) Mismatch
An indication of a defect that occurs when an Accepted Section Trace Identifier does not match the provisioned Expected Section Trace Identifier on an incoming signal.

Security Administrator
1. A WaveStar CIT or managing system user who has been assigned a security privilege level of S5 and can view existing user logins, add new users and assign user privileges, delete users, change passwords for any user, and modify user privileges. 2. A WaveStar LambdaRouter 128/256 user with a privilege level of S5 who can view existing user logins, view a list of users currently logged into the network element, add new users and assign user privileges, delete users, and change passwords for any user.

Security Log
A WaveStar LambdaRouter 128/256 file of all security-related events. It is stored in non-volatile memory of the network element.

Security Management
In WaveStar LambdaRouter 128/256, the administration of user accounts (login IDs, passwords, and privilege levels) and the monitoring of system security to insure that only valid users can perform allowed actions and receive authorized information.

Serial Number (SLN)
A circuit pack identifier that is stored in Electrically Erasable Programmable Read-Only Memory (EEPROM).

Serial Number Identification Port (SNIP)
A Switch Shelf interface to the High-Voltage Shelf that provides the unique 16-bit serial number of the Switch Shelf.

Series Number (SSN)
A circuit pack identifier that is stored in Electrically Erasable Programmable Read-Only Memory (EEPROM).

Session
A logical connection from the WaveStar CIT or other managing system to a network element.

Shelf
A set of circuit packs sharing a common physical housing, power source, electronic or opto-electronic backplane, and shelf controller.

Shelf View
A WaveStar CIT graphical depiction of one shelf. Selectable objects in this view are the shelf, the slots/circuit packs, and the ports.

Short Reach
A standard for optics, concerning transmitters and receivers in a system, that ensures that transmission can be maintained for short distances (10 km). *See also* Long Reach; Intermediate Reach.

Signal Degrade (SD)
A condition that triggers automatic protection switching when the line bit error rate (B2) exceeds a user-provisionable threshold.

Signal Fail (SF)
Loss of signal (LOS), loss of frame (LOF), Alarm Indication Signal-Line (AIS-L), or line bit error rate (B2) greater than the user-provisionable threshold.

Signal Injection
In WaveStar LambdaRouter 128/256 Release 2.0, the capability of the system to inject a keep-alive or test signal on any output transmission interface where electrical to optical conversion is done, for the purposes that are served by Unequipped and AIS-L signals.

Signal Maintenance
In WaveStar LambdaRouter 128/256 Release 2.0, the capability of the system to detect the presence or absence of optical power at input and output ports, monitor and react to maintenance signals, generate appropriate alarms, and perform fabric-path protection switching.

Signal Rate
An attribute that defines the bit rate and format of a signal.

Single-Mode Fiber (SM)
An 8.3-µ diameter low-loss, long-span optical fiber typically operating at either 1310 nm, 1550 nm, or both.

Site Address
The unique address for a network element.

Slip
A repetition or deletion of a block of bits in a bit-stream, caused by a sufficiently large discrepancy in the read and write rates at a receiver buffer.

Slot
A physical position in a shelf designed to hold a circuit pack and connect it to the backplane.

Slot Provisioned State
A transition state for circuit pack insertion. A slot will transition from empty to equipped when the circuit pack insertion is detected and validated, and the hardware registers are loaded. The slot remains so provisioned until the object is deprovisioned.

Slot State Provisioning
Modification of a slot state through a user command.

Software Backup
The process of saving an image of the current network element (NE) databases, which are contained in NE primary non-volatile memory (NVM, PRI MEM), to SEC MEM or remote storage.

Software Delivery
In WaveStar LambdaRouter 128/256, the delivery to a customer of network element generic software, WaveStar CIT software, factory data, and utilities on a CD-ROM, with accompanying documentation in hard copy and on CD-ROM.

Software Failure
A data or results error detected by the software itself during execution.

Software ID
A number that provides the software version information for the system.

Software Installation
The process of interpreting and unpacking the binary data program that was downloaded to a network element non-volatile memory (NVM) and copying the constituent data items to their designated locations in the network element.

Software Management
The activities necessary to download, upgrade, install, back up, and restore the generic software and provisionable data on the WaveStar CIT and network element.

Software Upgrade
The process that installs a new release of software.

Standby (STBY)
A state in which a circuit pack is in service but is not providing service functions. The circuit pack is ready to be used to replace a similar circuit pack either by protection or by duplex switching, in hot standby or cold standby functions. *See also* Active; Cold Standby; Hot Standby.

Start-up Configuration
1. In WaveStar LambdaRouter 256 Release 2.0, an orderable three-bay configuration that includes one System Controller Shelf (SCS), two High-Voltage Shelves (HVS), two Switch Shelves (SWS), and either one Optical Interface Shelf-Transparent (OIS-T) and one Optical Interface Shelf-SDH/SONET (OIS-S), or two Optical Interface Shelf-Transparent (OIS-T). 2. In WaveStar LambdaRouter 128 Release 2.0, an orderable two-bay configuration that includes one System Controller Shelf (SCS), one High-Voltage Shelf (HVS), one Switch Shelf (SWS), and one Optical Interface Shelf-Transparent (OIS-T).

State
A software parameter indicating the current autonomous and user-defined limitations on the behavior of the entity in question.

Status
The indication of the instantaneous condition of an equipment entity.

Strictly Non-Blocking Fabric (NBF)
Architecture that ensures unhindered signal throughput. Strictly NBF is a fabric architecture such that any incoming signal can be directed to any idle output port, without the need to rearrange any of the existing cross-connections, and without blocking, degrading, or otherwise affecting any of the remaining signals through the system.

Subnetwork
A group of interconnected/interrelated network elements.

Superuser
1. A WaveStar CIT user type with highest level of permissions to access the system. Up to two superusers logins and passwords may be created on the WaveStar CIT.
2. A WaveStar LambdaRouter 128/256 user with full privileges in all functional categories. Two superuser logins and passwords are pre-installed on the system.

Suppression
A process by which alarms that have been identified as an “effect” are not displayed to a user. Alarms can be suppressed through user provisioning.

Switch Bay
In WaveStar LambdaRouter 128/256 Release 2.0, the frame that houses the Switch Shelf, High-Voltage Shelf, and optical interface shelf, either the OIS-T, OIS-10G, OIS-2G, or OIS-MX.

Switch Interface Cable (SI cable)
Cable that connects the Optical Interface Shelf backplane and the Fiber Distribution Panel.

Switch Interface Capacity
The capacity in number of optical interconnection links between any one of the transmission interface shelves and the cross-connection fabric. This term applies to bidirectional capacity (for example, switch interface capacity of 128 corresponds to 128 optical links in each direction).

Switch Interface Controller (SWIC, LGH1 and LGH1AE)
A WaveStar LambdaRouter 128/256 circuit pack that provides control functions for optical cross-connect interface (OXI) or High-Voltage Digital-to-Analog Converter (HVDAC) functions, and a control interface to the Control Bay. There are two types of SWICs. The SWIC for the Optical Interface Shelf-Transparent (OIS-T) and High-Voltage Shelf (HVS) is coded LGH1 and is referred to in software as oswic when in an OIS-T and hswic when in an HVS. The SWIC for the Optical Interface Shelf-SDH/SONET (OIS-S) is coded LGH1AE and is referred to in software as oswic.

Switch Interface Point (SWIP)
A Micro-electromechanical System (MEMS) mirror, the dedicated optical interface (connector and collimator) connected to it, and the dedicated electrical control interface (electrodes, cable connectors) for its operation. Users of WaveStar LambdaRouter 128/256 software will view it as a single object in the system.

Switch Interface Point (SWIP) Maintenance Group (SWMG)
A grouping of Switch Interface Points (SWIPs) that are treated as a unit for switch maintenance. This grouping is sometimes referred to as *switch side*.

Switch Request States
State that is defined for protection groups: Forced Switch, Manual Switch Failure, and No Request.

Switch Shelf (SWS)
The WaveStar LambdaRouter 128/256 component that contains the Micro-electromechanical System (MEMS) mirror arrays, optical lenses, fibers and connectors, also referred to as switch fabric.

Synchronization
The function that assures accuracy and stability of clocks used to transmit data in digital networks. In WaveStar LambdaRouter 128/256 Release 2.0, clocking is used for 10 Gbps and 2.5 Gbps signals that go through optical-electrical-optical conversion for performance monitoring. The clocking is extracted from the ingress signal and used to transmit egress signal (through timing). An internal clock is used to transmit signal defect (AIS) when the clock from the ingress signal is not available. Synchronization is done on the OXI-10GC and OXI-2GC packs.

Synchronous Digital Hierarchy (SDH)
A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

Synchronous Optical Network (SONET)
The North American standard for the rates and formats that define optical signals and their constituents.

SYS50D
The WaveStar LambdaRouter 128/256 circuit pack that provides the main system control functions. Duplex SYS50Ds are located in the System Controller Shelf and operate as an active/standby pair.

System Controller Bay
The WaveStar LambdaRouter [256] Release 1.0 bay that houses the system control circuit packs. The comparable WaveStar LambdaRouter 128/256 Release 2.0 bay is the Control Bay.

System Controller Complex
The grouping of a SYS50D circuit pack, Control System Interface Expander (CSIEX), and an External Interface (EI) circuit pack, treated as a unit for controller maintenance and protection switching.

System Controller Shelf (SCS)
The middle shelf of the WaveStar LambdaRouter 128/256 Control Bay. It contains the SYS50D and other control packs.

System Controller Shelf (SCS) User Panel
The WaveStar LambdaRouter 128/256 Release 2.0 module that monitors the temperature of the shelf, receives alarm status information, and provides visual indications of shelf status through LEDs. The SCS User Panel provides an ESD wrist strap ground connector and a port used to connect a WaveStar CIT to the system. An NE Acty LED indicates software download, loopback, or a forced or manual switch.

System Logs
Autonomous records of system events that can be retrieved by user commands. The system provides a User Session Activity Log, Database Change Log, Alarm Log, Security Activity Log, and Protection Switch Log. Each log has a capacity to store 72 hours of data.

System View
A WaveStar CIT graphical depiction of the entire network element. Selectable objects in this view are bays and shelves in the network element.

T

Target Identifier (TID)
A provisionable parameter used to identify a particular network element within a network. The parameter is a case-insensitive ASCII character string of up to 20 characters. The allowed characters are the letters *A* through *Z* and *a* through *z*, the numbers *0* through *9*, and the special characters hyphen (-) and forward slash (*/*). The string must not begin or end with a hyphen.

Template
A collection of parameters that define a specific network element configuration.

Through Timing
Timing derived by the network element from the ingress signal and used to transmit the egress signal.

Transaction Language 1 (TL1)
A machine-to-machine communications language that is a subset of ITU human-to-machine language. TL1 is the interface language between the WaveStar CIT and WaveStar LambdaRouter 128/256.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Networking protocols used by WaveStar LambdaRouter 128/256 to interface with a customer's Intraoffice Local Area Network (IAO LAN).

Transmission Interface
Also known as facility interface. The components that provide connectivity between external Optical Line Systems (OLSs) or client network elements (NEs) and the WaveStar LambdaRouter 128/256. The WaveStar LambdaRouter 128/256 Release 2.0 transmission interfaces are the Optical Cross-Connect Interface (OXI) transparent bidirectional ports, and the Optical Cross-Connect Interface-10 Gbps (OXI-10GC) and Optical Cross-Connect Interface-2.5 Gbps (OXI-2GC) opaque bidirectional ports. Transmission interface functions include receipt, splitting, selection, and output of signals.

Transmission Interface Shelf
See Optical Interface Shelf entries.

Transmit-Direction
The direction away from the network element.

Transparency
Bit-rate and format independence. The Optical Cross-Connect Interface (OXI) circuit packs are the WaveStar LambdaRouter 128/256 transparent interfaces.

Trouble-Clearing
Activity to correct an alarmed condition.

Two-Way Bridge/Merge Cross-Connection
A two-way cross-connection configuration that consists of a bridge cross-connection in one direction, and a merge cross-connection in the other direction.

Two-Way Double Merge Cross-Connection
A complex two-way cross-connection configuration that consists of two one-way double merge cross-connections, one in each direction of the two-way.

Two-Way Point-to-Point Cross-Connection
Two cross-connection duplex legs that interconnect two input ports and two output ports. A pair of input and output ports used for opposite directions may or may not have the same access identifier (AID). Each of the two cross-connection legs can be established by a single command to the network element and must have a compatible transmission rate.

Two-Way Simplex Cross-Connection
Two simplex cross-connection legs that interconnect two input ports and two output ports. A pair of input and output ports used for opposite directions may or may not have the same access identifier (AID). A pair of two-way simplex cross-connection legs can be added to or deleted from an existing cross-connection to form another type of cross-connection configuration. For example, a two-way simplex cross-connection can be added to an existing two-way point-to-point cross-connection to form a two-way bridge/merge cross connection.

U

Unequipped (UNEQ) Signal
An indication that an incoming signal has valid SDH/SONET Section/Regenerator Section overhead with a Synchronous Payload Envelope (SPE) comprising all zeroes.

Unit Interface Appliance (UIA)
The physical device used by the person who runs WaveStar CIT software and accesses network elements. The WaveStar LambdaRouter 128/256 UIA is a PC or laptop with Windows NT or Windows 2000.

Unit Interface (UI) Cable
The specified cable type used in the interface between the System Controller Shelf circuit packs and the Switch Interface Controller (SWIC) circuit packs.

Universal Coordinated Time (UTC)
Formerly called Greenwich Mean Time (GMT). A time-zone-independent indication of an event. The local time can be calculated from the Universal Coordinated Time.

Upgrade Kit
Orderable components that enable either a lower capacity WaveStar LambdaRouter system to be upgraded to a higher capacity WaveStar LambdaRouter system, or an earlier version/release WaveStar LambdaRouter system to be upgraded to a later version/release WaveStar LambdaRouter system.

Upload
The process of transferring files from a network element to a management system. WaveStar LambdaRouter 128/256 can only upload data. *See also* Download.

Upstream
At or toward the source of the considered transmission stream.

User ID (UID)
A WaveStar CIT or WaveStar LambdaRouter user code that comprises one to ten alphanumeric, case-sensitive characters. Any sequence of characters is allowed, except as follows: The keyword ALL by itself, in any combination of uppercase and lowercase (that is, ALL AlL, alL, and so on), is not allowed as a valid user ID. A user ID containing ALL as a substring, however, in any combination of uppercase and lowercase (such as tallman), is allowed as a valid user ID.

User Notification Registration List
A security feature that determines what messages a WaveStar LambdaRouter 128/256 user is allowed to receive.

User Panels
Components on each shelf of the WaveStar LambdaRouter 128/256 that monitor the temperature of shelves, receive alarm status information, and provide visual indications of shelf status through LEDs. These panels also provide a means for generating alarm cutoff and LED test interrupts to the shelf Switch Interface Controller (SWIC) circuit packs.

In addition to the status LEDs, the System Controller Shelf user panel provides an ESD wrist strap ground connector and a port used to connect a WaveStar CIT to the system.

Temperature monitoring, ESD wrist strap ground connectors, and WaveStar CIT ports are not included in the user panels for the Optical Interface Shelves and High-Voltage Shelves. They also do not support near end (NE) or far end (FE) alarms.

User Privilege Code (UPC)
Permissions assigned to each user when a login is created or modified on either the WaveStar CIT or WaveStar LambdaRouter 128/256. The UPC is an alphanumeric code of one or two letters that identify the functional category of commands the user may access, and a single digit that indicates the user authorization level for that functional category. UPCs assigned to login IDs on the WaveStar CIT do not apply to WaveStar LambdaRouter 128/256.

User Record
Data associated with each user on a WaveStar CIT or other managing system and on the WaveStar LambdaRouter 128/256 network element (NE). Each record (separate on the managing system and the NE) comprises a login ID, password, user type, user privilege level, user priority level (NE only), and User Notification Registration list (NE only).

User Session Activity Log
A WaveStar LambdaRouter 128/256 file of all user-initiated commands from login through logout.

User Type
Assigned privilege codes for WaveStar CIT users that determine which commands and capabilities the user may access. Predefined user types are Superuser, Privileged User, General User, Maintenance User, and Reports Only User. Users may also be assigned a type of "Other." The default user type is "Reports Only."

V

Very Short Reach (VSR)
A standard for optics, concerning transmitters and receivers in a system, that insures that transmission can be maintained for very short distances. *See also* Long Reach; Intermediate Reach; Short Reach.

Virtual Private Network (VPN)
A leased network that is part of a larger network but operated independently.

Volatile Memory
A type of memory that is lost if electrical power is interrupted.

W

Wander
The long-term variation of the significant instants of a digital signal from their ideal positions in time. Wander is mainly generated by the variation in transmission characteristics of the media and equipment, which includes disruption in synchronization reference distribution. Wander is a potential source of slips in synchronous networks. *See also* Jitter.

Wavelength Division Multiplexing (WDM)
A means of increasing the information-carrying capacity of an optical fiber by simultaneously transmitting signals at different wavelengths.

Wavelength Range of Operation
A range within the infrared wavelength spectrum in which the system is designed to operate.

Wavelength Window
A standard range of wavelengths in which the intrinsic transmission loss of an optical fiber is low enough to be usable for optical transmission systems. The standard wavelength windows are approximately 850 nm (not used in telecommunications), 1310 nm, and 1550 nm.

WaveStar® CIT (Craft Interface Terminal)
The user interface terminal used by craft personnel to communicate with the network element. The WaveStar CIT runs on a PC with Windows NT® or Windows 2000 and provides graphical user interface (GUI) functionality and Transaction Language 1 (TL1) command entry through cut-through.

WaveStar® LambdaRouter
The Lucent Technologies fully optical signal switching system that uses Micro-electromechanical System (MEMS), a fabric technology consisting of arrays of electrically configurable mirrors. It supports as many as 256x256 input and output ports.

WaveStar® LambdaRouter 128
The Lucent Technologies fully optical signal switching system that uses Micro-electromechanical System (MEMS), a fabric technology consisting of arrays of electrically configurable mirrors. It supports as many as 128x128 input and output ports.

WaveStar® LambdaRouter 256
The Lucent Technologies fully optical signal switching system that uses Micro-electromechanical System (MEMS), a fabric technology consisting of arrays of electrically configurable mirrors. It supports as many as 256x256 input and output ports.

WaveStar® OLS (Optical Line System)
A Lucent Technologies lightwave transmission system, for example, WaveStar® OLS 1.6T. Using Dense Wave Division Multiplexing technology, the system combines multiple signals of different wavelengths, transmits the resulting signal over a single fiber, and then demultiplexes the signal at the receiving end.

WaveStar® SNMS (SubNetwork Management System)
A Lucent product that provides element management functionality for a variety of networking products, including WaveStar LambdaRouter 128/256.

Wizard
Form of user assistance that automates a task through a dialog with the user.

Working
Descriptor for a physical entity. In revertive switching, the working entity carries service under normal operation. In non-revertive switching the descriptor has no particular meaning. In active and standby operations, *working* indicates the function, when present and healthy, that will become active at power-up. *See also* Protection; Revertive Protection Switching; Non-Revertive Protection Switching.

Index